Firmado digitalmente por:
GONZALES SEGOVIA WILFREDO FIR
40215020 hard
Motivo: En señal de conformidad
Fecha: 25/08/2026 16:56:39-0500

Firmado digitalmente por TOMY
BALTAZAR MARCO ANTONIO
Motivo: Soy el autor del documento
Fecha: 25.08.2026 18:12:46 -05:00

Anuncio Específico de Adquisiciones

Solicitud de Ofertas
Bienes
(Proceso de Licitación de sobre único)

País: Perú

Nombre del Proyecto: "Creación de un Sistema de Atención de Emergencias, Urgencias e Información mediante un Número Único 911 en Lima Metropolitana y el Callao".

Título del Contrato: "Adquisición de equipamiento ofimático y de redes LAN para la Central 911 en el marco del Proyecto Creación de un Sistema de Atención de Emergencias, Urgencias e Información mediante un Número Único en Lima Metropolitana y el Callao – Proyecto 911"**.**

N.° de préstamo: Contrato de Préstamo Nº 9039-PE

N.° de referencia de la SDO: PE-PRONATEL-569321-GO-RFB

1. La República del Perú ha recibido financiamiento del Banco Mundial para financiar el costo del Proyecto "Creación de un Sistema de Atención de Emergencias, Urgencias e Información mediante un Número Único en Lima Metropolitana y el Callao - Proyecto 911", y se propone utilizar parte de los fondos para efectuar pagos en virtud del contrato correspondiente a la "Adquisición de equipamiento ofimático y de redes LAN para la Central 911 en el marco del Proyecto Creación de un Sistema de Atención de Emergencias, Urgencias e Información mediante un Número Único en Lima Metropolitana y el Callao – Proyecto 911".
2. El Programa Nacional de Telecomunicaciones - PRONATEL, a través del Proyecto 911, invita a los Licitantes elegibles a presentar Ofertas en sobre cerrado para la **"Adquisición de equipamiento ofimático y de redes LAN para la Central 911 en el marco del Proyecto Creación de un Sistema de Atención de Emergencias, Urgencias e Información mediante un Número Único en Lima Metropolitana y el Callao – Proyecto 911"**, de conformidad con las especificaciones, cantidades, plazos y demás requisitos establecidos en el Documento de Licitación.
3. La adquisición comprende el suministro de **equipamiento ofimático, infraestructura de redes LAN, equipamiento de centro de datos, soluciones de seguridad, respaldo y ciberseguridad, así como los servicios conexos de implementación, instalación, configuración, integración, pruebas y puesta en operación**, de acuerdo con las características, cantidades, especificaciones técnicas, requisitos de garantía y soporte establecidos en los documentos de licitación, disponibles en el siguiente enlace: ***"https://drive.google.com/drive/u/1/folders/1_P2rdxC82HGQ8PCkr4gIqYOMqUGmQBYi".***
4. El PROVEEDOR tendrá un plazo máximo de hasta setenta y cinco (75) días calendario para la entrega de los bienes, contabilizados a partir del día siguiente de la

Firmado digitalmente por:
SOLORZANO LEON JACHELINE FIR
45366553 hard
Motivo: Soy el autor del documento
Fecha: 25/08/2026 19:57:04-0500

suscripción del Contrato. El plazo total para la implementación será de hasta noventa (90) días calendario, contabilizados a partir del día siguiente de la suscripción del Contrato, conforme al numeral 4.17 de las Especificaciones Técnicas aprobadas. La implementación integral comprende la instalación, configuración, integración, pruebas y puesta en operación de los equipos. La puesta en operación del servicio será posterior a la aceptación operativa, mediante el acta correspondiente, conforme a las Especificaciones Técnicas.

5. La licitación se llevará a cabo por medio de una adquisición competitiva con enfoque nacional en la que se utilice el método de Solicitud de Ofertas (SDO), conforme a lo previsto en las Regulaciones de Adquisiciones para Prestatarios de Financiamiento para Proyectos de Inversión del Banco Mundial, Regulaciones de Adquisiciones para Prestatarios de Financiamiento para Proyectos de Inversión del Banco Mundial", con fecha julio de 2016 y revisadas en noviembre de 2017 y agosto de 2018, y se encuentra abierta a todos los Licitantes elegibles, según se define en las Regulaciones de Adquisiciones.
6. Los Licitantes elegibles interesados podrán solicitar más información a la Unidad Ejecutora 1720: Programa Nacional de Telecomunicaciones y consultar el documento de licitación en el horario de 09:00 a 17:30 horas, en la dirección que figura más abajo crep911@pronatel.gob.pe.
7. Los Licitantes interesados podrán obtener el documento de licitación en español, previa presentación de una solicitud por escrito dirigida a la dirección que figura más abajo o al correo crep911@pronatel.gob.pe.
8. Las Ofertas deberán dirigirse a la dirección que se indica más **abajo** a más tardar el día **24 de septiembre 2026 a las 15:00 Horas**. No Está permitida la presentación electrónica de la Oferta. Las Ofertas recibidas fuera del plazo establecido serán rechazadas. La apertura pública de las Ofertas se llevará a cabo ante la presencia de Notario Público y de los representantes designados por los Licitantes y de cualquier otra persona que se encuentre presente en la dirección que figura más abajo el dia 24 de septiembre 2026 a las 15:30 Horas.
9. Todas las Ofertas deben ir acompañadas de una "Declaración de Mantenimiento de Oferta", conforme al formato incluido en el Documento de Licitación.
10. La dirección a la que se hace referencia más arriba es la siguiente:

Programa Nacional de Telecomunicaciones - PRONATEL
Atención: Proyecto 911
Dirección: Av. Paseo de la República Nº 1645 - La Victoria
Ciudad: Lima
Código postal: 15034
País: Perú
Correo electrónico: crep911@pronatel.gob.pe
Página Web: http://www.pronatel.gob.pe

DOCUMENTO ESTÁNDAR DE ADQUISICIONES

Solicitud de Ofertas
Bienes
(Proceso de Licitación de sobre único)

BANCO MUNDIAL
BIRF • AIF

Firmado digitalmente por:
SOLORZANO LEON JACHELINE FIR 45366553 hard
Motivo: Soy el autor del documento
Fecha: 25/08/2026 16:59:05-0500

Firmado digitalmente por TOMY BALTAZAR MARCO ANTONIO
Motivo: Soy el autor del documento
Fecha: 25.08.2026 17:02:50 -05:00

Firmado digitalmente por:
GONZALES SEGOVIA WILFREDO FIR 40215020 hard
Motivo: En señal de conformidad
Fecha: 25/08/2026 16:55:32-0500

Solicitud de Ofertas
Bienes
(Proceso de Licitación de sobre único)

“Adquisición de Equipamiento Ofimático y de Redes LAN para la Central 911 en el marco del Proyecto Creación de un Sistema de Atención de Emergencias, Urgencias e Información mediante un Número Único en Lima Metropolitana y el Callao - Proyecto 911”

SDO Nº: PE-PRONATEL-569321-GO-RFB

Proyecto: “Creación de un Sistema de atención de emergencias, urgencias e información mediante un número único 911 en Lima Metropolitana y el Callao” - Proyecto 911.

Comprador: Programa Nacional de Telecomunicaciones - PRONATEL

País: Perú

Emitido el día: **25 de agosto 2026**

Documento Estándar de Adquisiciones

Índice general

PARTE 1. Procedimientos de la Licitación 2

Sección I. Instrucciones a los Licitantes 3
Sección II. Datos de la Licitación (DDL) 37
Sección III. Criterios de Evaluación y Calificación.....48
Sección IV. Formularios de la Oferta ……..54
Sección V. Países Elegibles……...…….……109
Sección VI. Fraude y Corrupción……..111

PARTE 2. Requisitos de los Bienes y Servicios Conexos…….……114

Sección VII. Requisitos de los Bienes y Servicios Conexos…….……115

PARTE 3. Contrato……255

Sección VIII. Condiciones Generales del Contrato……...258
Sección IX. Condiciones Especiales del Contrato…….284
Sección X. Formularios del Contrato…….297

PARTE 1. Procedimientos de la Licitación

Sección I. Instrucciones a los Licitantes

Índice

A. Disposiciones Generales 5
1. Alcance de la Licitación 5
2. Fuente de Financiamiento 5
3. Fraude y Corrupción 6
4. Licitantes Elegibles 6
5. Elegibilidad de los Bienes y Servicios Conexos 10

B. Contenido del Documento de Solicitud de Ofertas 10
6. Secciones del Documento de Licitación 10
7. Aclaración del Documento de Licitación 11
8. Enmienda del Documento de Licitación 12

C. Preparación de las Ofertas 12
9. Costo de la Oferta 12
10. Idioma de la Oferta 12
11. Documentos que componen la Oferta 12
12. Carta de la Oferta y Lista de Precios 14
13. Ofertas Alternativas 14
14. Precios de la Oferta y Descuentos 14
15. Monedas de la Oferta y de Pago 17
16. Documentos que Establecen la Elegibilidad y Conformidad de los Bienes y Servicios Conexos 17
17. Documentos que Establecen la Elegibilidad y las Calificaciones del Licitante 18
18. Período de Validez de las Ofertas 19
19. Garantía de Mantenimiento de Oferta 19
20. Formato y Firma de la Oferta 22

D. Presentación y Apertura de las Ofertas 23
21. Presentación, Cierre e Identificación de las Ofertas 23
22. Plazo para Presentar las Ofertas 24
23. Ofertas Tardías 24
24. Retiro, Sustitución y Modificación de las Ofertas 24
25. Apertura de las Ofertas 25

E. Evaluación y Comparación de las Ofertas 27
26. Confidencialidad 27
27. Aclaración de las Ofertas 27
28. Desviaciones, Reservas y Omisiones 27
29. Determinación del Cumplimiento de las Ofertas 28
30. Falta de Conformidad, Errores y Omisiones 29

31. Corrección de Errores Aritméticos 29
32. Conversión a una Sola Moneda 30
33. Margen de Preferencia 30
34. Evaluación de las Ofertas.....30
35. Comparación de las Ofertas 32
36. Ofertas Excesivamente Bajas.....32
37. Calificación del Licitante 33
38. Derecho del Comprador a Aceptar Cualquier Oferta y a Rechazar Cualquiera o Todas las Ofertas 33

F. Adjudicación del Contrato 34

39. Criterios de Adjudicación 34
40. Derecho del Comprador a Variar las Cantidades en el Momento de la Adjudicación 34
41. Notificación de Adjudicación del Contrato 34
42. Firma del Contrato 35
43. Garantía de Cumplimiento.....36

Sección I. Instrucciones a los Licitantes

A. Disposiciones Generales

1. Alcance de la Licitación

1.1 En relación con el Anuncio Específico de Adquisiciones: Solicitud de Ofertas (SDO), especificado **en los Datos de la Licitación (DDL)**, el Comprador, que se indica **en los DDL**, emite este documento de licitación para la adquisición de los Bienes y, si corresponde, de cualesquiera Servicios Conexos que puedan ser necesarios, conforme a lo especificado en la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos". El nombre, la identificación y la cantidad de lotes (contratos) de esta SDO **se especifican en los DDL**.

1.2 Para todos los efectos de este documento de licitación:

(a) Por el término "por escrito" se entiende comunicación en forma escrita (por ejemplo, por correo postal, correo electrónico, fax, incluso, si así **se especifica en los DDL**, aquella enviada o recibida a través del sistema electrónico de adquisiciones utilizado por el Comprador) con prueba de recibo.

(b) Si el contexto así lo requiere, "singular" significa "plural" y viceversa.

(c) Por "día" se entiende día calendario, salvo que se especifique lo contrario mediante la expresión "días hábiles". Son días hábiles todos los días laborables del Prestatario. Se excluyen los feriados oficiales del Prestatario.

2. Fuente de Financiamiento

2.1 El Prestatario o Beneficiario (en adelante, el "Prestatario") **indicado en los DDL** ha solicitado o recibido financiamiento (en adelante, "fondos") del Banco Internacional de Reconstrucción y Fomento (BIRF) o de la Asociación Internacional de Fomento (IDA) (en adelante denominados el "Banco Mundial" o el "Banco") por el monto **mencionado en los DDL**, para el proyecto especificado **en los DDL**. El Prestatario destinará una porción de dichos fondos para efectuar pagos elegibles en virtud del contrato para el cual se emite este documento de licitación.

2.2 El Banco efectuará pagos solamente a pedido del Prestatario y una vez que los haya aprobado de conformidad con los términos y las condiciones establecidos en el Convenio de Préstamo (u otro tipo de financiamiento). El Convenio de Préstamo (u otro tipo de financiamiento) prohíbe el retiro de fondos de la cuenta de Préstamo para pagos de cualquier naturaleza a personas o entidades, o para cualquier importación de bienes, si dicho pago o importación ha sido prohibido por decisión del Consejo de Seguridad de las Naciones Unidas en virtud del capítulo VII de la Carta de las Naciones Unidas. Ninguna otra parte más que el Prestatario podrá derivar derecho alguno del Préstamo (u otro tipo de financiamiento) o reclamar los fondos.

3. Fraude y Corrupción

3.1 El Banco requiere el cumplimiento de sus Directrices Contra el Fraude y la Corrupción y de sus políticas y procedimientos de sanciones vigentes incluidos en el Marco de Sanciones del Grupo del Banco Mundial, conforme se describe en la Sección VI, “Fraude y Corrupción”.

3.2 En virtud de esta política, los Licitantes deberán permitir al Banco —y requerir que lo permitan sus agentes (hayan sido declarados o no), subcontratistas, subconsultores, prestadores de servicios, proveedores y personal— inspeccionar todas las cuentas, registros y otros documentos relativos a cualquier procesos de selección inicial o precalificación, las presentaciones de ofertas o propuestas y la ejecución de contratos (en el caso de adjudicación), y disponer que sean auditados por auditores designados por el Banco.

4. Licitantes Elegibles

4.1 Un Licitante puede ser una firma que sea una entidad privada, una empresa o ente estatal de acuerdo con la Instrucción a los Licitantes (IAL) 4.6, o una combinación de ellas, bajo la forma de una Asociación en Participación, Consorcio o Asociación (“APCA”), a través de un convenio existente o con la presentación de una carta de intención que manifieste su voluntad de celebrar el convenio que formalice la conformación de dicha APCA. En el caso de una APCA, todos sus miembros serán solidariamente responsables por la ejecución de la totalidad del Contrato, de acuerdo con sus términos. La APCA deberá designar un Representante, que deberá estar facultado para llevar a cabo todos los

procedimientos y gestiones en nombre de cualquiera y todos los miembros de la APCA durante el proceso de la licitación y, en el caso de que la APCA fuera adjudicataria, durante la ejecución del Contrato. Salvo que se especifique **en los DDP**, no existe límite en el número de miembros de una APCA.

4.2 Ningún Licitante podrá tener conflictos de interés. Cualquier Licitante que se determine que tiene conflictos de interés será descalificado. A los fines de este proceso de Licitación, se considerará que un Licitante tiene conflictos de interés si:

(a) Controla de manera directa o indirecta a otro Licitante, es controlado de manera directa o indirecta por otro Licitante o es controlado junto a otro Licitante por una entidad en común;

(b) recibe o ha recibido subsidios directos o indirectos de otro Licitante;

(c) tiene el mismo representante legal que otro Licitante;

(d) tiene una relación con otro Licitante, directamente o a través de terceros en común, que lo coloca en una posición de influir en la oferta de otro Licitante, o de influir en las decisiones del Comprador en relación con este proceso de Licitación;

(e) cualquiera de sus filiales ha participado como consultora en la preparación del diseño o especificaciones técnicas de los bienes y servicios conexos que constituyen el objeto de la Oferta;

(f) cualquiera de sus filiales ha sido contratada (o se propone para ser contratada) por el Comprador o por el Prestatario para la ejecución del Contrato;

(g) proveerá bienes, obras o servicios distintos de los de consultoría que resulten o estén directamente relacionados con servicios de consultoría para la preparación o implementación del proyecto especificado en la IAL 2.1 de los DDL que fue provisto o fuera provisto por cualquier filial que directa o indirectamente controle, sea controlada por esa firma o esté bajo su control común, o

(h) posee una estrecha relación comercial o familiar con un algún profesional del Prestatario (o de la agencia

de implementación del proyecto, o del receptor de una parte del préstamo) que (i) esté directa o indirectamente relacionado con la preparación del documento de licitación o las especificaciones del Contrato, o el proceso de evaluación de la Oferta de ese Contrato, o (ii) pudiera estar relacionado con la ejecución o supervisión de ese Contrato, a menos que el conflicto derivado de tal relación haya sido resuelto de manera aceptable para el Banco durante el proceso de Licitación y la ejecución del Contrato.

4.3 Una firma que sea Licitante (ya sea en forma individual o como miembro de una Asociación en Participación, Consorcio o Asociación ("APCA") no podrá participar en más de una oferta, salvo en el caso de las ofertas alternativas permitidas. Esto incluye su participación en calidad de subcontratista. Tal participación redundará en la descalificación de todas las ofertas en las que haya estado involucrada la firma en cuestión. Por su parte, una firma que no sea Licitante ni tampoco parte de una APCA podrá participar en calidad de subcontratista en más de una Oferta.

4.4 Un Licitante podrá tener la nacionalidad de cualquier país, sujeto a las restricciones establecidas en la IAL 4.8. Se considerará que un Licitante tiene la nacionalidad de un país cuando esté constituido o inscripto en ese país y opere de conformidad con sus leyes, de lo cual deberán dar cuenta sus estatutos (o documentos de constitución o asociación equivalentes) o sus documentos de registro, en caso de corresponder. Estos criterios también se aplicarán para determinar la nacionalidad de los subcontratistas o subconsultores propuestos por cualquiera de las partes del Contrato, incluyendo los servicios conexos.

4.5 Un Licitante que haya sido sancionado conforme a las Directrices del Banco Contra el Fraude y la Corrupción y a sus políticas y procedimientos de sanciones vigentes incluidos en el Marco de Sanciones del Grupo del Banco Mundial, tal como se describe en el párrafo 2.2 (d) de la Sección VI, no podrá ser precalificado para la adjudicación de contratos financiados por el Banco, presentar ofertas a tales efectos ni recibir la adjudicación de dichos contratos, así como tampoco recibir cualquier beneficio, financiero o de otra índole, de un contrato financiado por el Banco durante el período determinado

por este. La lista de firmas inhabilitadas se encuentra disponible en la dirección electrónica que se indica en los DDL.

4.6 Los Licitantes que sean empresas o entes estatales del País del Comprador solamente podrán ser elegibles para competir y recibir la adjudicación de uno o más Contratos si pueden establecer, de forma aceptable para el Banco, que (i) tienen autonomía legal y financiera; (ii) operan conforme a las leyes comerciales, y (iii) no se encuentran bajo la supervisión del Comprador.

4.7 Un Licitante no debe estar suspendido por el Comprador para presentar ofertas como resultado del incumplimiento con una Declaración de Mantenimiento de la Oferta o de la Propuesta.

4.8 Las empresas y las personas podrán ser declaradas inelegibles si así se indica en la Sección V. "Países Elegibles", y (a) si las leyes o reglamentaciones del país del Prestatario prohíben las relaciones comerciales con el país de dichas empresas y personas, siempre y cuando se demuestre, de manera satisfactoria para el Banco, que la exclusión no impedirá la competencia efectiva con respecto al suministro de bienes o la contratación de obras o servicios requeridos, o (b) si, en cumplimiento de una decisión del Consejo de Seguridad de las Naciones Unidas adoptada en virtud del capítulo VII de la Carta de esa institución, el país del Prestatario prohíbela importación de bienes o la contratación de obras o servicios de ese país, o el pago a personas o entidades en ese país.

4.9 Los Licitantes deberán proporcionar al Comprador evidencia documental satisfactoria de su elegibilidad, cuando el Comprador la solicite de manera razonable.

4.10 Una firma a la cual el Prestatario haya impuesto una sanción de inhabilitación que impida que se le adjudique un contrato será elegible para participar en esta adquisición, salvo que el Banco corrobore, a pedido del Prestatario, que la inhabilitación:

(a) está relacionada con un caso de fraude o corrupción; y

(b) se llevó a cabo en cumplimiento de un procedimiento judicial o administrativo en virtud del cual la firma estuvo sujeta al debido proceso.

5. Elegibilidad de los Bienes y Servicios Conexos

5.1 Todos los Bienes y Servicios Conexos que hayan de suministrarse de conformidad con el Contrato y que sean financiados por el Banco podrán tener su origen en cualquier país, de acuerdo con la Sección V, "Países Elegibles".

5.2 A los fines de estas IAL, el término "bienes" incluye mercaderías, materias primas, maquinarias, equipos y plantas industriales; el término "servicios conexos" incluye servicios tales como seguros, instalaciones, capacitación y mantenimiento inicial.

5.3 Por el término "origen" se entiende el país donde los bienes han sido extraídos, cosechados, cultivados, producidos, fabricados o procesados, o, tras su procesamiento, manufactura o ensamblaje, dan como resultado otro artículo reconocido en el ámbito comercial que difiere sustancialmente de las características básicas de sus componentes.

B. Contenido del Documento de Solicitud de Ofertas

6. Secciones del Documento de Licitación

6.1 El documento de licitación está compuesto por las partes 1, 2, y 3, que incluyen todas las secciones que a continuación se indican y deben leerse junto con cualquier enmienda emitida en virtud de la IAL 8.

PARTE 1. Procedimientos de Licitación

- Sección I. Instrucciones a los Licitantes
- Sección II. Datos de la Licitación
- Sección III. Criterios de Evaluación y Calificación
- Sección IV. Formularios de la Oferta
- Sección V. Países Elegibles
- Sección VI. Fraude y Corrupción

PARTE 2. Requisitos de los Bienes y Servicios Conexos

- Sección VII. Requisitos de los Bienes y Servicios Conexos

PARTE 3. Contrato

- Sección VIII. Condiciones Generales del Contrato
- Sección IX. Condiciones Especiales del Contrato
- Sección X. Formularios del Contrato

6.2 El Anuncio Específico de Adquisiciones: Solicitud de Ofertas (SDO) emitido por el Comprador no forma parte de este documento de licitación.

6.3 Salvo que se hubieran obtenido directamente del Comprador, este no se responsabiliza por la integridad del documento, las respuestas a las solicitudes de aclaración, las actas de las reuniones previas a la presentación de Ofertas, si las hubiere, o las enmiendas a los documentos de licitación de acuerdo con la IAL 8. En caso de contradicción, prevalecerán los documentos obtenidos directamente del Comprador.

6.4 Es responsabilidad del Licitante examinar todas las instrucciones, los formularios, los términos y las especificaciones del documento de licitación y presentar toda la información o documentación de la Oferta requerida en dicho documento.

7. Aclaración del Documento de Licitación

7.1 Todo Licitante que requiera alguna aclaración sobre el documento de licitación deberá comunicarse con el Comprador por escrito a la dirección del Comprador que se suministra **en los DDL**. El Comprador responderá por escrito a todas las solicitudes de aclaración, siempre que dichas solicitudes sean recibidas antes del vencimiento del plazo para la presentación de ofertas dentro del período especificado **en los DDL**. El Comprador enviará copia de las respuestas a todos los Licitantes que hubiesen adquirido el documento de licitación de acuerdo con la IAL 6.3, incluyendo una descripción de las consultas realizadas, sin identificar su fuente. Si así estuviera especificado **en los DDL**, el Comprador también deberá publicar prontamente su respuesta en la

página web identificada **en los DDL**. Si como resultado de las aclaraciones surgieran cambios a elementos esenciales del documento de licitación, el Comprador podrá enmendar dicho documento siguiendo el procedimiento indicado en las IAL 8 y 22.2.

8. Enmienda del Documento de Licitación

8.1 El Comprador podrá, en cualquier momento antes del vencimiento del plazo para la presentación de ofertas, enmendar el documento de licitación mediante la emisión de una enmienda.

8.2 Toda enmienda emitida formará parte integral del documento de licitación y deberá ser comunicada por escrito a todos los que hayan obtenido el documento de licitación del Comprador, de acuerdo con la IAL 6.3. El Comprador deberá también publicar prontamente la enmienda en su página web de acuerdo con la IAL 7.1.

8.3 El Comprador podrá, a su discreción, prorrogar el plazo de presentación de ofertas a fin de dar a los posibles Licitantes un plazo razonable para que puedan tomar en cuenta las enmiendas en la preparación de sus Ofertas, de conformidad con la IAL 22.2.

C. Preparación de las Ofertas

9. Costo de la Oferta

9.1 El Licitante financiará todos los costos relacionados con la preparación y presentación de su Oferta, y el Comprador no será responsable en ningún caso por dichos costos, independientemente del desarrollo o del resultado del proceso de Licitación.

10. Idioma de la Oferta

10.1 La oferta, así como toda la correspondencia y los documentos relativos a la Oferta que intercambien el Licitante y el Comprador, deberán ser escritos en el idioma especificado **en los DDL**. Los documentos de respaldo y el material impreso que formen parte de la Oferta podrán estar escritos en otro idioma siempre y cuando vayan acompañados de una traducción fidedigna de las secciones pertinentes al idioma que se especifica **en los DDL**, en cuyo caso la traducción prevalecerá en lo que respecta a la interpretación de la Oferta.

11. Documentos que componen la Oferta

11.1 La Oferta deberá contener los siguientes documentos:

(a) **Carta de la Oferta**, preparada de acuerdo con la IAL 12;

(b) **Listas de Precios** completas, de acuerdo con las IAL 12 y 14;

(c) **Garantía de Mantenimiento de Oferta** o **Declaración de Mantenimiento de Oferta**, de conformidad con la IAL 19.1;

(d) **Oferta Alternativa**, si estas fueran permitidas, de acuerdo con la IAL 13;

(e) **Autorización** escrita que autorice al firmante de la Oferta a comprometer al Licitante, de conformidad con la IAL 20.3;

(f) **Calificaciones:** Prueba documental, de conformidad con la IAL 17, que establezca que el Licitante está calificado para ejecutar el Contrato en caso de que su oferta sea aceptada;

(g) **Elegibilidad del Licitante:** Prueba documental, de conformidad con la IAL 17, que establezca que el Licitante es elegible para presentar una oferta;

(h) **Elegibilidad de los Bienes y Servicios Conexos:** Prueba documental, de conformidad con la IAL 16, que demuestre la elegibilidad de los Bienes y Servicios Conexos que proporcionará el Licitante;

(i) **Cumplimiento de las disposiciones:** Prueba documental, de conformidad con las IAL 16 y 30, que establezca que los Bienes y Servicios Conexos cumplen con las disposiciones del documento de licitación;

(j) Cualquier otro documento requerido **en los DDL**.

11.2 Además de los requisitos estipulados en la IAL 11.1, las ofertas presentadas por una APCA deberán incluir una copia del Convenio de APCA celebrado por todos sus miembros. Alternativamente, se deberá presentar conjuntamente con la Oferta una carta de intención de suscribir un Convenio de APCA, firmada por todos sus miembros, en el caso de que la Oferta sea adjudicada, acompañada de una copia del Convenio propuesto.

11.3 El Licitante deberá suministrar información en la Carta de la Oferta sobre comisiones y gratificaciones, si hubiera, pagadas o por pagarse a agentes u a otra parte relacionada con esta Oferta.

12. Carta de la Oferta y Lista de Precios

12.1. El Licitante presentará la Carta de la Oferta y las Listas de Precios utilizando los formularios suministrados en la Sección IV, Formularios de la Oferta. Estos formularios deberán ser debidamente llenados sin alterar su forma y no se aceptarán sustitutos, excepto según lo dispuesto en la IAL 20.3. Todos los espacios en blanco deberán ser llenados con la información solicitada.

13. Ofertas Alternativas

13.1. A menos que se indique lo contrario **en los DDL**, no se considerarán Ofertas Alternativas.

14. Precios de la Oferta y Descuentos

14.1 Los precios y descuentos cotizados por el Licitante en la Carta de la Oferta y en la Lista de Precios deberán ajustarse a los requerimientos que se indican a continuación.

14.2 Todos los lotes y artículos deberán enumerarse y cotizarse por separado en las Listas de Precios.

14.3 El precio cotizado en la Carta de la Oferta de acuerdo con la IAL 12.1deberá ser el precio total de la Oferta, excluyendo cualquier descuento que se ofrezca.

14.4 El Licitante cotizará cualquier descuento e indicará su método de aplicación en la Carta de la Oferta, de acuerdo con la IAL 12.1.

14.5 Los precios cotizados por el Licitante serán fijos durante la ejecución del Contrato y no estarán sujetos a ninguna variación por ningún motivo, salvo indicación contraria **en los DDL**. Una oferta presentada con precios ajustables no responde a lo solicitado y, en consecuencia, será rechazada de conformidad con la IAL 29. Sin embargo, si, de acuerdo con lo indicado **en los DDL**, los precios cotizados por el Licitante pueden estar sujetos a ajustes durante la ejecución del Contrato, las ofertas que coticen precios fijos no serán rechazadas, y el ajuste de los precios se tratará como si fuera cero.

14.6 Si así se indica en la IAL 1.1, el Llamado a Licitación se hará por Ofertas para lotes individuales (contratos) o para combinación de lotes (grupo de contratos). A menos que se indique lo contrario **en los DDL**, los precios cotizados deberán corresponder al 100 % de los artículos indicados en cada lote y al 100 % de las cantidades indicadas para cada artículo de un lote. Los Licitantes que deseen ofrecer descuentos por la adjudicación de más de un Contrato deberán indicar en su Oferta los descuentos aplicables para cada grupo de contratos o,

alternativamente, para Contratos individuales en el grupo. Los descuentos deberán presentarse de conformidad con la IAL 14.4, siempre y cuando las ofertas por todos los lotes sean presentadas y abiertas al mismo tiempo.

14.7 Las expresiones "EXW", "CIP" y otros términos afines se regirán por las normas prescritas en la edición vigente de Incoterms, publicada por la Cámara de Comercio Internacional, según lo especificado **en los DDL**.

14.8 Los precios deberán cotizarse como se indica en cada lista de precios incluida en la Sección IV, "Formularios de la Oferta". El desglose de los componentes de los precios se requiere con el único propósito de facilitar al Comprador la comparación de las Ofertas. Esto no limitará de ninguna manera el derecho del Comprador de contratar en cualquiera de los términos ofrecidos. Al cotizar los precios, el Licitante podrá incluir costos de transporte cotizados por empresas transportadoras registradas en cualquier país elegible, de conformidad con la Sección V, "Países Elegibles". Asimismo, el Licitante podrá adquirir servicios de seguros de cualquier país elegible de conformidad con la Sección V, "Países Elegibles". Los precios deberán registrarse de la siguiente manera:

(a) Para Bienes fabricados en el País del Comprador:

(i) el precio de los Bienes cotizados EXW (taller, fábrica, bodega, sala de exhibición o en existencia, según corresponda), incluyendo todos los derechos de aduana y los impuestos a la venta o de otro tipo ya pagados o por pagar sobre los componentes y materia prima utilizada en la fabricación o ensamblaje de los Bienes;

(ii) todo impuesto a las ventas u otro tipo de impuesto que obligue el País del Comprador a pagar sobre los Bienes en caso de ser adjudicado el Contrato al Licitante;

(iii) el precio de transporte interno, seguros y otros servicios necesarios para hacer llegar los Bienes al destino final (emplazamiento del Proyecto) especificado **en los DDL**.

(b) Para Bienes fabricados fuera del País del Comprador y que serán importados:

(i) el precio de los Bienes, cotizados CIP lugar de destino convenido, en el País del Comprador, según se indica **en los DDL**;

(ii) el precio de transporte interno, seguros y otros servicios locales necesarios para hacer llegar los Bienes del lugar de destino convenido a su destino final (emplazamiento del Proyecto) indicado **en los DDL**.

(c) Para Bienes fabricados fuera del País del Comprador, e importados previamente:

(i) el precio de los Bienes, incluyendo el valor original de importación más cualquier margen (o descuento), más cualquier otro costo relacionado, derechos de aduana y otros impuestos de importación pagados o por pagar sobre los Bienes previamente importados;

(ii) los derechos de aduana y otros impuestos de importación pagados (deberán ser respaldados con prueba documental) o pagaderos sobre los Bienes previamente importados;

(iii) el precio de los Bienes obtenido de la diferencia entre (i) y (ii);

(iv) cualquier impuesto sobre la venta u otro impuesto pagadero en el País del Comprador sobre los Bienes si el Contrato es adjudicado al Licitante;

(v) el precio de transporte interno, seguro y otros servicios locales necesarios para hacer llegar los Bienes al lugar de destino final (emplazamiento del Proyecto) indicado **en los DDL**.

(d) Para los Servicios Conexos distintos del transporte interno y otros servicios necesarios para hacer llegar los Bienes a su destino final, cuando dichos Servicios Conexos estén especificados en la Lista de Requisitos de los Bienes y Servicios Conexos, el precio de cada artículo que comprende los

Servicios Conexos (incluido cualquier impuesto aplicable).

15. Monedas de la Oferta y de Pago

15.1 La(s) moneda(s) de la Oferta y la(s) moneda(s) de pago serán las mismas. El Licitante deberá cotizar en la moneda del País del Comprador la parte del Precio de la Oferta correspondiente a los gastos incurridos en la moneda del País del Comprador, salvo que se estipule lo contrario **en los DDL**.

15.2 El Licitante podrá expresar el Precio de su Oferta en cualquier moneda. Si el Licitante desea recibir el pago en una combinación de montos en diferentes monedas, podrá cotizar su precio en las monedas que correspondan. Sin embargo, no podrá incluir más de tres monedas extranjeras además de la del País del Comprador.

16. Documentos que Establecen la Elegibilidad y Conformidad de los Bienes y Servicios Conexos

16.1 Para establecer la elegibilidad de los Bienes y Servicios Conexos de conformidad con la IAL 5, los Licitantes deberán completar las declaraciones del país de origen en los Formularios de Lista de Precios, incluidos en la Sección IV, "Formularios de la Oferta".

16.2 Con el fin de establecer la conformidad de los Bienes y Servicios Conexos con el documento de licitación, los Licitantes deberán proporcionar, como parte de su Oferta, prueba documental que acredite que los Bienes cumplen con las especificaciones técnicas y los estándares especificados en la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos".

16.3 La prueba documental podrá consistir en material bibliográfico, planos o datos, y deberá incluir una descripción detallada de las características esenciales técnicas y de funcionamiento de cada artículo que demuestre conformidad sustancial de los Bienes y Servicios Conexos con las especificaciones técnicas, y, de ser procedente, una declaración de desviaciones y excepciones a las disposiciones de la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos".

16.4 Los Licitantes también deberán proporcionar una lista detallada que incluya disponibilidad y precios actuales de repuestos, herramientas especiales, etc., necesarios para el funcionamiento adecuado y continuo de los Bienes durante el período **indicado en los DDL**, a partir

del momento en que el Comprador comience a utilizar dichos Bienes.

16.5 Las normas de fabricación, procesamiento, material y equipos, así como las referencias a marcas o a números de catálogos que haya incluido el Comprador en la Lista de Requisitos de los Bienes y Servicios Conexos, son de carácter meramente descriptivo, y no restrictivo. Los Licitantes podrán ofrecer otras normas de calidad, marcas y/o números de catálogo, siempre y cuando demuestren, a satisfacción del Comprador, que las sustituciones son sustancialmente equivalentes o superiores a las especificadas en la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos".

17. Documentos que Establecen la Elegibilidad y las Calificaciones del Licitante

17.1 Para establecer su elegibilidad de conformidad con la IAL 4, los Licitantes deberán completar la Carta de la Oferta, incluida en la Sección IV, "Formularios de la Oferta".

17.2 La prueba documental de las calificaciones del Licitante para ejecutar el Contrato, si su Oferta es aceptada, deberá establecer, a completa satisfacción del Comprador, que:

(a) si se requiere **en los DDL**, el Licitante que no fabrica ni produce los Bienes que propone proveer deberá presentar una autorización del fabricante utilizando el formulario incluido en la Sección IV, "Formularios de la Oferta", para demostrar que ha sido debidamente autorizado por el fabricante o productor de los Bienes para suministrarlos en el País del Comprador;

(b) si se requiere **en los DDL**, en el caso de un Licitante que no esté establecido comercialmente en el País del Comprador, el Licitante está o estará (si se le adjudica el Contrato) representado por un agente en el País del Comprador equipado y con capacidad para cumplir con las obligaciones de mantenimiento, reparaciones y almacenamiento de repuestos del Proveedor estipuladas en las condiciones del Contrato y/o las especificaciones técnicas;

(c) el Licitante cumple con cada uno de los criterios de calificación estipulados en la Sección III, "Criterios de Evaluación y Calificación".

18. Período de Validez de las Ofertas

18.1. Las ofertas deberán mantener su validez hasta la fecha especificada **en los DDL** o cualquier fecha extendida si el Comprador la modifica de conformidad con la IAL 8. Una Oferta que no sea válida hasta la fecha especificada en **los DDL**, o cualquier fecha extendida por el Comprador de conformidad con la IAL 8, será rechazada por el Comprador por incumplimiento.

18.2. En circunstancias excepcionales, antes de la fecha de expiración de la validez de la Oferta, el Comprador podrá solicitar a los Licitantes que extiendan el período de la validez de sus Ofertas. Las solicitudes y las respuestas deberán hacerse por escrito. Si se hubiese solicitado una Garantía de Mantenimiento de Oferta, de acuerdo con la IAL 19, también esta deberá prorrogarse por el período correspondiente. Un Licitante puede rechazar tal solicitud sin que ello implique la pérdida de su Garantía de Mantenimiento de Oferta. Al Licitante que acepte la solicitud de prórroga no se le pedirá ni permitirá modificar su Oferta, salvo en los casos previstos en la IAL 18.3.

18.3. Si la adjudicación se retrasase por un período mayor a 56 (cincuenta y seis) días a partir del vencimiento de la validez inicial de la Oferta, el precio del Contrato será determinado de la siguiente forma:

(a) en el caso de contratos con precio fijo, el precio del Contrato será el precio de la Oferta ajustado según el factor especificado **en los DDL**;

(b) en el caso de contratos con precio ajustable, no se harán ajustes;

(c) en todos los casos, la evaluación de la Oferta deberá basarse en el precio cotizado sin tomar en cuenta la corrección aplicable que corresponda según los casos indicados arriba.

19. Garantía de Mantenimiento de Oferta

19.1. El Licitante deberá presentar, como parte de su Oferta, una Garantía de Mantenimiento de Oferta o una Declaración de Mantenimiento de Oferta, según lo especificado **en los DDL**, en formulario original, y, en el caso de una Garantía de Mantenimiento de Oferta, por el monto y en la moneda especificados **en los DDL**.

19.2. Para la Declaración de Mantenimiento de Oferta se utilizará el formulario incluido en la Sección IV, "Formularios de la Oferta".

19.3. Si, según lo especificado en la IAL 19.1, se debe presentar una Garantía de Mantenimiento de Oferta, esta deberá ser una garantía a primer requerimiento emitida por una institución de prestigio de un país elegible y deberá tener cualquiera de las siguientes formas, a opción del Licitante:

(a) una garantía incondicional emitida por un banco o una institución financiera no bancaria (como una compañía de seguros, fianzas o avales);

(b) una carta de crédito irrevocable;

(c) un cheque de gerencia o cheque certificado;

(d) otra garantía especificada **en los DDL**,

emitida por una institución de prestigio de un país elegible. Si una garantía incondicional es emitida por una institución financiera no bancaria localizada fuera del país del Comprador, la institución financiera no bancaria deberá tener una institución financiera corresponsal ubicada en el país del Comprador para hacer efectiva la garantía, salvo que el Comprador haya acordado por escrito, antes de la presentación de la Oferta, que la existencia de dicha institución financiera corresponsal no es obligatoria. En el caso de una garantía bancaria, la Garantía de Mantenimiento de Oferta deberá presentarse utilizando el Formulario de Garantía de Mantenimiento de Oferta incluido en la Sección IV, "Formularios de la Oferta", o en otro formato sustancialmente similar aprobado por el Comprador antes de la presentación de la Oferta. La Garantía de Mantenimiento de Oferta tendrá una validez de veintiocho (28) días a partir de la fecha original de expiración de la validez de la Oferta o de cualquier fecha extendida, si ésta se hubiera solicitado de conformidad con lo establecido en la IAL 18.2.

19.4. Si se exige una Garantía de Mantenimiento de Oferta de conformidad con la IAL 19.1, todas las Ofertas que no estén acompañadas de una Garantía de Mantenimiento de Oferta que se ajuste sustancialmente a los requisitos pertinentes serán rechazadas por el Comprador por incumplimiento.

19.5. Si en la IAL 19.1 se establece la obligación de presentar una Garantía de Mantenimiento de Oferta, las Garantías de Mantenimiento de Oferta de los Licitantes cuyas ofertas no fueron seleccionadas serán devueltas tan pronto como sea posible una vez que el Licitante seleccionado firme el Contrato y provea la Garantía de Cumplimiento, de conformidad con la IAL 46.

19.6. La Garantía de Mantenimiento de Oferta del Licitante seleccionado será devuelta tan pronto como sea posible una vez que el Licitante seleccionado suscriba el Contrato y proporcione la Garantía de Cumplimiento.

19.7. La Garantía de Mantenimiento de Oferta podrá hacerse efectiva o la Declaración de Mantenimiento de Oferta podrá ejecutarse si:

(a) un Licitante retira su Oferta antes de la fecha de expiración de la validez de la Oferta especificada por el Licitante en la Carta de la Oferta, o cualquier fecha extendida otorgada por el Licitante; o

(b) el Licitante seleccionado:

(i) no suscribe el Contrato de conformidad con lo dispuesto en la IAL 45, o

(ii) no suministra una Garantía de Cumplimiento de conformidad con lo dispuesto en la IAL 46.

19.8. La Garantía de Mantenimiento de Oferta o la Declaración de Mantenimiento de Oferta de una APCA se emitirán en nombre de la Asociación que presenta la Oferta. Si la APCA no se hubiera constituido formalmente como entidad jurídica al momento de presentar la Oferta, la Garantía de Mantenimiento de Oferta o la Declaración de Mantenimiento de Oferta se emitirán en nombre de todos los futuros miembros que figuren en la carta de intención mencionada en las IAL 4.1 y 11.2.

19.9. Si **en los DDL** no se exige una Garantía de Mantenimiento de Oferta según se estipula en la IAL 19.1, y si

(a) un Licitante retira su Oferta antes de la fecha de expiración de la validez de la Oferta estipulada por

el Licitante en la Carta de la Oferta o cualquier fecha extendida otorgada por el Licitante; o

(b) el Licitante seleccionado:

(i) no suscribe el Contrato con arreglo a lo dispuesto en la IAL 45; o

(ii) no proporciona una Garantía de Cumplimiento de conformidad con la IAL 46,

el Prestatario podrá, si así se dispone **en los DDL**, declarar al Licitante inelegible para ser adjudicatario de un contrato otorgado por el Comprador por el período que se especifique **en los DDL**.

20. Formato y Firma de la Oferta

20.1 El Licitante preparará un original de los documentos que comprenden la Oferta según se describe en la IAL 11 y lo marcará claramente como "ORIGINAL". Las Ofertas Alternativas, si son admitidas de acuerdo con la IAL 13, deberán estar claramente marcadas como "ALTERNATIVA". Además, el Licitante deberá presentar el número de copias de la Oferta **que se indica en los DDL** y marcar claramente cada ejemplar como "COPIA". En caso de discrepancia, el texto del original prevalecerá sobre el de las copias.

20.2 Los Licitantes deberán marcar como "CONFIDENCIAL" la información incluida en sus Ofertas que revista carácter confidencial para sus empresas. Esto puede incluir información reservada, secretos comerciales o información delicada de índole comercial o financiera.

20.3 El original y todas las copias de la Oferta deberán mecanografiarse o escribirse con tinta indeleble, y deberán estar firmadas por la persona debidamente autorizada para firmar en nombre del Licitante. Esta autorización consistirá en una confirmación escrita de acuerdo con lo especificado **en los DDL** y se adjuntará a la Oferta. El nombre y el cargo de cada persona que firme la autorización deberán mecanografiarse o escribirse en letra de imprenta bajo la firma. Todas las páginas de la Oferta que contengan anotaciones o enmiendas deberán estar firmadas o inicialadas por la persona que suscriba la Oferta.

20.4 En el caso de que el Licitante sea una APCA, la Oferta deberá estar firmada por un representante autorizado de la APCA en nombre de esta y en representación

legalmente vinculante para actuar en nombre de todos los miembros, formalizado por un poder firmado por sus representantes legales.

20.5 Los textos entre líneas, borraduras o palabras superpuestas serán válidos solamente si llevan la firma o las iniciales de la persona que firma la Oferta.

D. Presentación y Apertura de las Ofertas

21. Presentación, Cierre e Identificación de las Ofertas

21.1. El Licitante deberá presentar la Oferta en un único sobre cerrado (proceso de Licitación con mecanismo de sobre único), en cuyo interior deberá colocar los siguientes sobres cerrados:

(a) un sobre identificado como "ORIGINAL", que contendrá todos los documentos que componen la Oferta, como se describe en la IAL 11;

(b) un sobre identificado como "COPIAS", que contendrá las copias de la Oferta que se hubieran solicitado;

(c) si se permiten Ofertas alternativas según lo dispuesto en la IAL 13 y, si corresponde:

i un sobre identificado como "ORIGINAL: OFERTA ALTERNATIVA", donde se colocará la Oferta alternativa,

ii un sobre identificado como "COPIAS: OFERTA ALTERNATIVA", donde se colocarán todas las copias de la Oferta alternativa que se hubieran solicitado.

21.2. Los sobres interiores y exteriores deberán:

(a) llevar el nombre y la dirección del Licitante;

(b) estar dirigidos al Comprador de acuerdo con lo indicado en la IAL 22.1;

(c) llevar la identificación específica de este proceso de Licitación indicada en la IAL 1.1; y

(d) llevar la advertencia de no abrir antes de la hora y fecha de apertura de Ofertas.

21.3. Si los sobres no están cerrados e identificados como se requiere, el Comprador no se responsabilizará en caso de que la Oferta se extravíe o sea abierta prematuramente.

22. Plazo para Presentar las Ofertas

22.1. El Comprador deberá recibir las Ofertas en la dirección y, a más tardar, en la fecha y hora que se especifican **en los DDL**. Cuando así se especifique **en los DDL**, los Licitantes tendrán la opción de enviar sus Ofertas de forma electrónica. Los Licitantes que opten por esta modalidad, deberán ajustarse a los procedimientos de presentación electrónica de Ofertas establecidos **en los DDL**.

22.2. El Comprador podrá, a su discreción, extender el plazo para la presentación de Ofertas mediante una enmienda al documento de licitación, de conformidad con la IAL 8. En este caso, todos los derechos y las obligaciones del Comprador y de los Licitantes previamente sujetos al plazo original para presentar las ofertas quedarán sujetos al plazo prorrogado.

23. Ofertas Tardías

23.1. El Comprador no considerará ninguna Oferta que llegue con posterioridad al término del plazo para la presentación de Ofertas, de conformidad con lo dispuesto en la IAL 22. Toda Oferta que reciba el Comprador después del plazo para la presentación de las Ofertas será declarada tardía, rechazada y devuelta al Licitante sin abrir.

24. Retiro, Sustitución y Modificación de las Ofertas

24.1. Un Licitante podrá retirar, sustituir o modificar su Oferta después de presentada mediante el envío de una comunicación por escrito, debidamente firmada por un representante autorizado; que deberá incluir una copia de la autorización (poder) de acuerdo con lo estipulado en la IAL 20.3 (con excepción de la comunicación de retiro, que no requiere copias). La Oferta sustitutiva o la modificación deberán adjuntarse a la respectiva comunicación por escrito. Todas las comunicaciones deberán ser:

(a) preparadas y presentadas de conformidad con las IAL 20 y 21 (con excepción de la comunicación de retiro, que no requiere copias) y, además, los respectivos sobres deberán llevar claramente indicado "RETIRO", "SUSTITUCIÓN" o "MODIFICACIÓN"; y

(b) recibidas por el Comprador antes de que venza el plazo establecido para la presentación de las Ofertas, de conformidad con la IAL 22.

24.2. Las ofertas cuyo retiro fue solicitado de conformidad con la IAL 24.1 se devolverán sin abrir a los Licitantes.

24.3. Ninguna Oferta podrá retirarse, sustituirse ni modificarse durante el intervalo comprendido entre la fecha límite para la presentación de Ofertas y el vencimiento del período de Validez de la Oferta indicado por el Licitante en la Carta de Oferta o cualquier prórroga de ese período.

25. Apertura de las Ofertas

25.1. Salvo en los casos especificados en las IAL 23 y 24.2, el Comprador, en el acto de apertura de las Ofertas, abrirá públicamente y leerá en voz alta todas las Ofertas recibidas antes del vencimiento del plazo indicado, en la fecha, a la hora y en el lugar especificados **en los DDL**, en presencia de los representantes designados por los Licitantes y de cualquier persona que desee asistir. Los procedimientos específicos para la apertura de Ofertas presentadas en forma electrónica, si estuvieran permitidas en virtud de la IAL 22.1, se realizarán conforme a lo dispuesto **en los DDL**.

25.2. Primero se abrirán y leerán en voz alta los sobres marcados "RETIRO"; el sobre con la Oferta correspondiente se devolverá sin abrir al Licitante. Si el sobre del retiro no contiene una copia del "poder" que confirme que el firmante es una persona autorizada por el Licitante para firmar en representación de él, se procederá a abrir la Oferta. No se permitirá el retiro de ninguna Oferta a menos que la respectiva comunicación de retiro contenga la autorización válida para solicitarlo y se lea en voz alta en el acto de apertura de las Ofertas.

25.3. Seguidamente se abrirán los sobres marcados como "SUSTITUCIÓN", los cuales se leerán en voz alta y se intercambiarán con la Oferta correspondiente que se está reemplazando; la Oferta sustituida se devolverá sin abrir al Licitante. No se permitirá ninguna sustitución, a menos que la respectiva comunicación de sustitución contenga una autorización válida para solicitar la sustitución y se lea en voz alta en el acto de apertura de las Ofertas

25.4. A continuación, se abrirán y se leerán en voz alta los sobres marcados con el rótulo "MODIFICACIÓN" con la

Oferta correspondiente. No se permitirá ninguna modificación de Ofertas, a menos que la comunicación de sustitución correspondiente contenga una autorización válida para solicitar la modificación y sea leída en voz alta en el acto de apertura de las Ofertas.

25.5. Luego se abrirán de a uno los demás sobres y se leerá en voz alta la siguiente información: el nombre del Licitante y si se ha presentado alguna modificación; el Precio total de la Oferta, por lote (contrato), si corresponde, incluidos los descuentos u Ofertas alternativas que hubiese; la existencia o inexistencia de Garantía de Mantenimiento de Oferta, si se hubiese solicitado, y cualquier otro detalle que el Comprador juzgue pertinente.

25.6. En la evaluación solo se considerarán las Ofertas, las Ofertas Alternativas y los descuentos abiertos y leídos en voz alta. La Carta de la Oferta y las Listas de Precios deberán ser inicialados por los representantes del Comprador que asistan al acto de apertura de Ofertas, tal como se especifica **en los DDL**.

25.7. El Comprador no discutirá los méritos de las Ofertas ni rechazará ninguna (excepto las Ofertas tardías, según lo dispuesto en la IAL 23.1).

25.8. El Comprador preparará un acta del acto de apertura de las Ofertas que incluirá como mínimo:

(a) el nombre del Licitante y si hubo retiro, sustitución o modificación;

(b) el precio de la Oferta, por lote (contrato) si corresponde, incluyendo cualquier descuento;

(c) cualquier Oferta Alternativa;

(d) la existencia o no de Garantía de Mantenimiento de Oferta o de la Declaración de Mantenimiento de Oferta, de haberse requerido.

25.9. Se solicitará a los representantes de los Licitantes presentes que firmen el acta. La omisión de la firma de uno de los Licitantes en el acta no invalidará el contenido ni los efectos de esta. Se entregará una copia del acta a todos los Licitantes.

E. Evaluación y Comparación de las Ofertas

26. Confidencialidad

26.1 No se divulgará a los Licitantes ni a ninguna persona que no participe oficialmente en el proceso de Licitación, información relacionada con la evaluación de las Ofertas o con la recomendación de adjudicación del contrato hasta que la información sobre la adjudicación del Contrato se haya publicado, con arreglo a la IAL 41.

26.2 Cualquier intento por parte de un Licitante de influenciar al Comprador en las decisiones relacionadas con la evaluación de las Ofertas o en la adjudicación del Contrato podrá resultar en el rechazo de su Oferta.

26.3 No obstante, lo dispuesto en la IAL 26.2, si durante el plazo transcurrido entre el acto de apertura y la fecha de adjudicación del Contrato, un Licitante desea comunicarse con el Comprador sobre cualquier asunto relacionado con el proceso de Licitación, deberá hacerlo por escrito.

27. Aclaración de las Ofertas

27.1 Para facilitar el examen, la evaluación, comparación de las Ofertas y la calificación de los Licitantes, el Comprador podrá, a su discreción, solicitar a cualquier Licitante aclaraciones sobre su Oferta. No se considerarán aclaraciones presentadas por un Licitante cuando nos sean en respuesta a una solicitud del Comprador. La solicitud de aclaración del Comprador y la respuesta deberán constar por escrito. No se solicitará, ofrecerá ni permitirá ninguna modificación, incluidos aumentos o reducciones voluntarios, de los precios o de la sustancia de la Oferta, salvo para confirmar la corrección de errores aritméticos que el Comprador hubiera descubierto durante la evaluación de las Ofertas, de conformidad con lo dispuesto en la IAL 31.

27.2 Si un Licitante no provee las aclaraciones a su Oferta antes de la fecha y hora indicada por el Comprador en su solicitud de aclaraciones de la Oferta, su Oferta puede ser rechazada.

28. Desviaciones, Reservas y Omisiones

28.1 Durante la evaluación de las Ofertas, se aplicarán las siguientes definiciones:

(a) “desviación” es cualquier variación respecto de los requisitos especificados en el documento de licitación;

(b) "reserva" es la imposición de condiciones limitativas o la negativa a aceptar plenamente los requisitos especificados en el documento de licitación;

(c) "omisión" es la falta de presentación de parte o de la totalidad de la información o de la documentación requeridas en el documento de licitación.

29. Determinación del Cumplimiento de las Ofertas

29.1 Para determinar si la Oferta se ajusta sustancialmente al documento de licitación, el Comprador se basará en el contenido de la propia Oferta, según se define en la IAL 11.

29.2 Una Oferta que se ajusta sustancialmente al documento de licitación es aquella que satisface todos los términos, condiciones y especificaciones estipuladas en dicho documento sin desviaciones, reservas u omisiones significativas. Una desviación, reserva u omisión significativa es aquella que:

(a) en caso de ser aceptada:

(i) afectaría de una manera sustancial el alcance, la calidad o el funcionamiento de los Bienes y Servicios Conexos especificados en el contrato;

(ii) limitaría de modo sustancial, incongruente con el documento de licitación, los derechos del Comprador o las obligaciones del Licitante en virtud del Contrato, o

(b) en caso de ser rectificada, afectaría injustamente la posición competitiva de otros Licitantes que presenten Ofertas que se ajusten sustancialmente a lo estipulado.

29.3 El Comprador examinará los aspectos técnicos de la Oferta presentada de acuerdo con las IAL 16 y 17, en particular, para confirmar que se hayan cumplido todos los requisitos de la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos", sin ninguna desviación, reserva ni omisión significativa.

29.4 Si una Oferta no se ajusta sustancialmente al documento de licitación, será rechazada por el Comprador y el Licitante no podrá ajustarla posteriormente mediante la corrección de las desviaciones, reservas u omisiones significativas.

30. Falta de Conformidad, Errores y Omisiones

30.1 Siempre y cuando una Oferta se ajuste sustancialmente al documento de licitación, el Comprador podrá dispensar cualquier falta de conformidad.

30.2 Siempre y cuando una Oferta se ajuste sustancialmente al documento de licitación, el Comprador podrá solicitar al Licitante que, dentro de un plazo razonable, presente la información o la documentación necesarias para corregir las discrepancias u omisiones no significativas relacionadas con requisitos de documentación. Dichas omisiones no podrán estar relacionadas con ningún aspecto del precio de la Oferta. Si el Licitante no cumple con la solicitud, podrá rechazarse su Oferta.

30.3 Siempre y cuando una Oferta se ajuste sustancialmente al documento de licitación, el Comprador corregirá las discrepancias no significativas cuantificables relativas al Precio de la Oferta. A tal efecto, se ajustará el Precio de la Oferta únicamente a los efectos de la comparación, para reflejar el precio de una partida o un componente que falte o en el que se observen discrepancias, un ítem o un componente que falte o en el que se observen discrepancias, agregando el precio promedio del ítem o componente cotizado por los Licitantes que cumplieron sustancialmente. Si el precio del ítem o componente no se puede derivar del precio de otras Ofertas que cumplen sustancialmente, el Comprador deberá utilizar su mejor estimación.

31. Corrección de Errores Aritméticos

31.1 Siempre y cuando la Oferta se ajuste sustancialmente al documento de licitación, el Comprador corregirá los errores aritméticos de la siguiente manera:

(a) Si hay una discrepancia entre un precio unitario y el precio total que se ha obtenido multiplicando el precio unitario por la cantidad correspondientes, prevalecerá el precio unitario y se corregirá el precio total, a menos que, a juicio del Comprador, hubiera un error evidente en la expresión del punto decimal en el precio unitario, en cuyo caso prevalecerá el total cotizado para ese rubro y se corregirá el precio unitario.

(b) Si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán sobre el total y este último deberá ajustarse.

(c) Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras, a menos que este último corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras, de conformidad con los párrafos (a) y (b) precedentes.

31.2 Se pedirá a los Licitantes que acepten la corrección de los errores aritméticos. Si no aceptan la corrección realizada con arreglo a lo dispuesto en la IAL 31.1, su Oferta será rechazada.

32. Conversión a una Sola Moneda

32.1 A los fines de evaluación y comparación, la moneda o las monedas de la Oferta serán convertidas a una sola moneda, tal como se especifica **en los DDL**.

33. Margen de Preferencia

33.1 Salvo que se indique lo contrario **en los DDL**, no se aplicará ningún margen de preferencia.

34. Evaluación de las Ofertas

34.1 El Comprador empleará los criterios y las metodologías enumerados en estas IAL y en la Sección III, "Criterios de Evaluación y Calificación". No se aceptará ningún otro criterio ni metodología de evaluación. Mediante la aplicación de dichos criterios y metodologías, el Comprador determinará cuál es la Oferta más Conveniente, que será la oferta presentada por un Licitante que reúna los criterios de calificación y respecto de la cual se haya determinado que:

(a) se ajusta sustancialmente al documento de licitación; y

(b) tiene el costo evaluado más bajo.

34.2 Al evaluar una Oferta, el Comprador considerará lo siguiente:

(a) la evaluación se hará por artículos o lotes (contratos) de la manera especificada **en los DDL**; el Precio de la Oferta se cotizará conforme a lo establecido en la IAL 14;

(b) el ajuste de precios por corrección de errores aritméticos, conforme a lo establecido en la IAL 31.1;

(c) el ajuste de precios por descuentos ofrecidos, conforme a lo establecido en la IAL 14.4;

(d) la conversión a una moneda única del monto resultante de la aplicación de los apartados (a) a (c) precedentes, si procede, de conformidad con la IAL 32;

(e) el ajuste de precios por falta de conformidad cuantificables, conforme a lo establecido en la IAL 30.3; y

(f) los factores de evaluación adicionales especificados en la Sección III, "Criterios de Evaluación y Calificación".

34.3 En la evaluación de las Ofertas no se tendrá en cuenta el efecto estimado de las disposiciones sobre ajuste de precios que se hayan establecido en las Condiciones Contractuales, aplicadas durante el período de ejecución de este Contrato.

34.4 Si este documento de licitación permite que los Licitantes coticen precios separados para diferentes lotes (contratos), la metodología para determinar el costo evaluado más bajo de las combinaciones de lotes (contratos), incluidos los descuentos ofrecidos en la Carta de la Oferta, se especificará en la Sección III, "Criterios de Evaluación y Calificación".

34.5 Al evaluar una Oferta, el Comprador excluirá y no tendrá en cuenta:

(a) en el caso de Bienes producidos en el País del Comprador, los impuestos sobre las ventas y otros impuestos similares pagaderos sobre los bienes si el Licitante resulta adjudicatario del Contrato;

(b) en el caso de Bienes no producidos en el País del Comprador, previamente importados o que se importarán, los derechos de aduana y otros impuestos a la importación, los impuestos sobre las ventas y otros impuestos similares pagaderos sobre los Bienes si el Licitante resulta adjudicatario del Contrato;

(c) cualquier disposición relativa al ajuste de precios durante el período de ejecución del Contrato, en el caso de que figure en la Oferta.

34.6 La evaluación de una Oferta puede requerir que el Comprador considere otros factores, además del precio

cotizado de conformidad con la IAL 14. Estos factores podrán estar relacionados con las características, el rendimiento, los términos y las condiciones de compra de los Bienes y Servicios Conexos. El efecto de los factores seleccionados, si los hubiere, se expresará en términos monetarios para facilitar la comparación de las Ofertas, a menos que se indique lo contrario en la Sección III, "Criterios de Evaluación y Calificación" **de los DDL**. Se aplicarán los criterios y las metodologías especificados en la IAL 34.2 (f).

35. Comparación de las Ofertas

35.1 El Comprador comparará, conforme a lo establecido en la IAL 34.2, los costos evaluados de todas las Ofertas que se ajusten sustancialmente al documento de licitación, para determinar cuál es la Oferta con el costo evaluado más bajo. La comparación se hará sobre la base de precios CIP (lugar de destino final) en el caso de los bienes importados y precios EXW más el costo de transporte interno y seguro hasta el lugar de destino en el caso de los bienes fabricados dentro del País del Comprador, junto con los precios de cualquier instalación, capacitación, comisiones y otros servicios requeridos. En la evaluación de precios no deberán tenerse en cuenta los impuestos de aduanas y otros impuestos recaudados sobre bienes importados cotizados CIP ni impuestos a las ventas o similares en relación con la venta o distribución de bienes.

36. Ofertas Excesivamente Bajas

36.1 Una Oferta excesivamente baja es aquella cuyo precio, en combinación con otros elementos constitutivos de la Oferta, parece ser tan bajo que despierta serias dudas en el Comprador sobre la capacidad del Licitante para ejecutar el Contrato al precio cotizado.

36.2 En caso de detectar lo que podría constituir una Oferta excesivamente baja, el Comprador pedirá al Licitante que brinde aclaraciones por escrito, y en especial, que presente análisis pormenorizados del Precio de la Oferta en relación con el objeto del contrato, el alcance, la metodología propuesta, el cronograma, la distribución de riesgos y responsabilidades y cualquier otro requisito establecido en el documento de licitación.

36.3 Tras evaluar los análisis de precios, si determina que el Licitante no demostrado su capacidad para ejecutar el Contrato al precio cotizado, el Comprador rechazará la Oferta.

37. Calificación del Licitante

37.1 El Comprador determinará, a su entera satisfacción, si el Licitante elegible seleccionado por haber presentado la Oferta que tiene el costo evaluado más bajo y que se ajusta sustancialmente al documento de licitación, reúne los requisitos de calificación especificados en la Sección III, "Criterios de Evaluación y Calificación".

37.2 La determinación se basará en el examen de las pruebas documentales presentadas por el Licitante para respaldar sus calificaciones, de conformidad con la IAL 17. No se tendrán en cuenta las calificaciones de otras empresas, como las subsidiarias, la casa matriz, las filiales y los subcontratistas (excepto los Subcontratistas Especializados permitidos por el documento de licitación) del Licitante, ni de ninguna otra empresa distinta de este.

37.3 Antes de la adjudicación del Contrato, el Comprador verificará que el Licitante seleccionado (incluyendo cada uno de los miembros de la APCA o JV) no esté descalificado por el Banco como consecuencia del incumplimiento de las obligaciones contractuales de EAS /ASx, El Comprador hará la misma verificación para cada uno de los subcontratistas propuestos por el Licitante seleccionado. Si alguno de los subcontratistas propuestos no cumple con el requisito, el Comprador exigirá que el Licitante proponga un subcontratista sustituto.

37.4 El Comprador determinará, a su entera satisfacción, si el Licitante elegible seleccionado por haber presentado la Oferta que tiene el costo evaluado más bajo y que se ajusta sustancialmente al documento de licitación, reúne los requisitos de calificación especificados en la Sección III, "Criterios de Evaluación y Calificación".

38. Derecho del Comprador a Aceptar Cualquier Oferta y a Rechazar Cualquiera o Todas las Ofertas

38.1 El Comprador se reserva el derecho de aceptar o rechazar cualquier Oferta, de anular el proceso de Licitación y de rechazar todas las Ofertas en cualquier momento antes de la adjudicación del Contrato, sin que por ello adquiera responsabilidad alguna frente a los Licitantes. En caso de anularse el proceso, el Comprador devolverá prontamente a los Licitantes todas las Ofertas y, específicamente, las Garantías de Mantenimiento de Oferta que hubiera recibido.

F. Adjudicación del Contrato

39. Criterios de Adjudicación

39.1 Con sujeción a lo dispuesto en la IAL 38, el Comprador adjudicará el Contrato al Licitante que ofrezca la Oferta más Conveniente, es decir, aquella que ha sido presentada por un Licitante que cumple con los criterios de calificación y que, además:

(a) se ajusta sustancialmente al documento de licitación; y

(b) tiene el costo evaluado más bajo.

40. Derecho del Comprador a Variar las Cantidades en el Momento de la Adjudicación

40.1 Al momento de adjudicar el Contrato, el Comprador se reserva el derecho de aumentar o disminuir la cantidad de los Bienes y Servicios Conexos especificados originalmente en la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos", siempre y cuando esta variación no exceda los porcentajes indicados **en los DDL**, ni altere los precios unitarios u otros términos y condiciones de la Oferta y del documento de licitación.

41. Notificación de Adjudicación del Contrato

41.1 Antes de la fecha de expiración de la Validez de la Oferta o de cualquier prórroga otorgada, si la hubiera, el Comprador notificará al Licitante seleccionado, por escrito, que su Oferta ha sido aceptada. En la notificación de adjudicación (denominada adelante y en los Formularios del Contrato, la "Carta de Aceptación") se especificará el monto que pagará al Proveedor por la ejecución del Contrato (denominado en lo sucesivo, así como en las Condiciones Contractuales y en los Formularios del Contrato, el "Precio del Contrato").

41.2 Dentro de los diez (10) días hábiles posteriores a la fecha de transmisión de la Carta de Aceptación, el Comprador publicará la Notificación de la Adjudicación del Contrato, que contendrá, como mínimo, la siguiente información:

(a) el nombre y la dirección del Comprador;

(b) el nombre y el número de referencia del contrato que se está adjudicando y método de selección utilizado;

(c) los nombres de todos los Licitantes que hubieran presentado Ofertas, con sus respectivos precios tal como se leyeron en voz alta y tal como se evaluaron;

(d) los nombres de los Licitantes cuyas Ofertas fueron rechazadas (ya sea por no responder a los requisitos o por no cumplir con los criterios de calificación) o no fueron evaluadas, con los motivos correspondientes;

(e) el nombre del Licitante ganador, el precio final total del Contrato, su duración y un resumen de su alcance; y

41.3 La Notificación de la Adjudicación del Contrato se publicará en el sitio web de acceso gratuito del Comprador, si se encontrara disponible, o en al menos un periódico de circulación nacional del País del Comprador o en el boletín oficial. El Comprador también deberá incluir dicha notificación en el sitio web de la publicación de las Naciones Unidas *Development Business*.

41.4 Hasta que se prepare y perfeccione el Contrato formal, la Carta de Aceptación constituirá un Contrato vinculante.

41.5 El Comprador responderá por escrito prontamente a cualquier Licitante no seleccionado que, luego de la notificación de la adjudicación de acuerdo con las Subcláusulas 41.1 y 41.2 de las IAL, solicite por escrito los motivos por los cuales su oferta no fue seleccionada.

42. Firma del Contrato

42.1 El Comprador enviará al Licitante seleccionado la Carta de Aceptación, incluido el Convenio

42.2 El Licitante seleccionado tendrá un plazo de veintiocho (28) días después de la fecha de recibo del formulario del Convenio de Contrato para firmarlo, fecharlo y devolverlo al Comprador.

42.3 No obstante, lo establecido en la IAL 42.2 precedente, en caso de que la firma del Convenio de Contrato se vea impedida por alguna restricción de importación atribuible al Comprador, al País del Comprador o al uso de los productos/bienes, sistemas o servicios que han de proveerse y que dichas restricciones de importación

provengan de regulaciones comerciales de un país proveedor de los productos/bienes, sistemas o servicios, el Licitante no será obligado por su Oferta. Lo anterior tendrá efecto siempre y cuando el Licitante pueda demostrar, a satisfacción del Banco y el Comprador, que la firma del Convenio de Contrato no se ha visto impedida por la falta de diligencia de parte del Licitante en el cumplimiento de las formalidades tales como las solicitudes para permisos, autorizaciones y licencias necesarias para la exportación de los productos/bienes, sistemas o servicios de acuerdo con los términos del Contrato.

43. Garantía de Cumplimiento

43.1 Dentro de los veintiocho (28) días posteriores a la fecha en que reciba la Carta de Aceptación enviada por el Comprador, el Licitante seleccionado deberá presentar la Garantía de Cumplimiento del Contrato, de conformidad con la Cláusula 18 de las CGC, utilizando para ello el formulario de Garantía de Cumplimiento incluido en la Sección X, "Formularios del Contrato", u otro formulario aceptable para el Comprador. Si el Licitante seleccionado presenta la Garantía de Cumplimiento del Contrato en forma de fianza, deberá cerciorarse de que esta haya sido emitida por una empresa de fianzas o seguros que resulte aceptable para el Comprador. Toda institución extranjera que proporcione una fianza deberá tener una institución financiera corresponsal domiciliada en el País del Comprador, salvo que este haya acordado por escrito que la existencia de dicha institución financiera corresponsal no es obligatoria.

43.2 El incumplimiento, por parte del Licitante seleccionado, de su obligación de presentar la Garantía de Cumplimiento antes mencionada o de firmar el Convenio constituirá causa suficiente para la anulación de la adjudicación y la pérdida de la Garantía de Mantenimiento de Oferta. En tal caso, el Comprador podrá adjudicar el Contrato al Licitante que haya presentado la segunda Oferta más Conveniente.

Sección II. Datos de la Licitación (DDL)

Los datos específicos que se presentan a continuación sobre los bienes que hayan de adquirirse complementarán, suplementarán o enmendarán las disposiciones de las Instrucciones a los Licitantes (IAL). En caso de conflicto, las disposiciones contenidas aquí prevalecerán sobre las disposiciones de las IAL.

<table>
<tr><th>Referencia en las IAL</th><th>A. Disposiciones generales</th></tr>
<tr><td>IAL 1.1</td><td>
El número de referencia de la Solicitud de Ofertas (SDO) es: PE-PRONATEL-569321-GO-RFB.

El Comprador es: Programa Nacional de Telecomunicaciones - PRONATEL.

El nombre de la SDO es:

“Adquisición de equipamiento ofimático y de redes LAN para la Central 911 en el marco del Proyecto Creación de un Sistema de Atención de Emergencias, Urgencias e Información mediante un Número Único en Lima Metropolitana y el Callao - Proyecto 911”.

La adquisición comprende un (01) <u>Único Lote</u> y comprende los siguientes ítems:
<table>
<tr><th>Item</th><th>Denominacion de Equipos</th><th>Cantidades expresadas en unidades</th></tr>
<tr><td>1</td><td>Computadora de Escritorio Tipo 1</td><td>210</td></tr>
<tr><td>2</td><td>Computadora de Escritorio Tipo 2</td><td>71</td></tr>
<tr><td>3</td><td>Monitor para Computadoras</td><td>696</td></tr>
<tr><td>4</td><td>Teclado y Mouse</td><td>281</td></tr>
<tr><td>5</td><td>Soporte para 03 Monitores Computadoras de Escritorio Tipo 1</td><td>210</td></tr>
<tr><td>6</td><td>Equipo Portátil</td><td>9</td></tr>
<tr><td>7</td><td>Auricular Monoaural</td><td>210</td></tr>
<tr><td>8</td><td>Micrófono</td><td>115</td></tr>
<tr><td>9</td><td>Altavoces</td><td>115</td></tr>
<tr><td>10</td><td>PPT de pie</td><td>210</td></tr>
<tr><td>11</td><td>Cámara Web</td><td>281</td></tr>
<tr><td>12</td><td>Teléfonos IP Tipo 1</td><td>201</td></tr>
<tr><td>13</td><td>Teléfonos IP Tipo 2</td><td>62</td></tr>
<tr><td>14</td><td>Teléfonos IP Tipo 3</td><td>16</td></tr>
<tr><td>15</td><td>Teléfonos IP Tipo 4</td><td>4</td></tr>
<tr><td>16</td><td>Botonera para teléfono IP 4</td><td>1</td></tr>
<tr><td>17</td><td>Pantalla para Monitoreo</td><td>2</td></tr>
<tr><td>18</td><td>Videoconferencia</td><td>4</td></tr>
<tr><td>19</td><td>Impresora tipo personal</td><td>13</td></tr>
<tr><td>20</td><td>Impresora tipo mediano volumen</td><td>5</td></tr>
<tr><td>21</td><td>Proyector Multimedia</td><td>4</td></tr>
<tr><td>22</td><td>Tabletas Rugerizadas</td><td>37</td></tr>
</table>
</td></tr>
</table>

	23	Switches Spine Data Center	2
	24	Switches Leaf Data Center	8
	25	Solución de Orquestador DC	1
	26	Switch Core LAN Campus	2
	27	Switch de acceso 48 puertos PoE	23
	28	Switch de acceso 24 puertos PoE	4
	29	Switch DMZ	2
	30	Switch de Gestión Fuera de Banda	2
	31	Controlador inalámbrico	2
	32	Access Point	47
	33	Solución de Administración y Gestión Campus	1
	34	Solución de Control de Acceso	1
	35	Hardware de Hiperconvergencia	4
	36	Software Hiperconvergencia	1
	37	Servidor para backup	1
	38	Servidor de inmutabilidad	1
	39	Almacenamiento para backup	1
	40	Librería de backup	1
	41	Software de backup	1
	42	Firewall NGFW (Perimetral)	2
	43	Firewall Interno	2
	44	Consola de analítica y reportes	1
	45	XDR (Extended Detection & Response)	1
	46	ZTNA (Zero Trust Network Access)	1
	47	Seguridad para correo electronico	1
	48	WAF - Seguridad para Aplicaciones Web	1
	49	SIEM	1
	50	Plataforma de detección y respuesta de amenazas externas e internas	1
	51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	1
	52	ADC (application Delivery Controller)	2
	53	Anti - DDos	2
	54	MFA - Administración de identidad y acceso	1
	55	PAM - Administración de acceso privilegiado	1
	56	NDR (Network Detection and Response)	1
	57	Sandboxing	1
	58	Solución de Análisis de Tráfico de Red	1
	59	Servicios conexos	1

Nota Importante:

Es requisito indispensable que la oferta debe incluir la totalidad de los ítems especificados, **no admitiéndose ofertas parciales**.

IAL 1.2 (a)	**Sistema electrónico de adquisiciones:** No Aplica.
IAL 2.1	El nombre del Prestatario es: **República del Perú**. Nombre del Proyecto: **Creación de un Sistema de Atención de Emergencias, Urgencias e Información mediante un Número Único en Lima Metropolitana y el Callao – Proyecto 911.** Número del Proyecto: **P170658**.

	Contrato de Préstamo: **N.° 9039-PE**. Monto del Convenio de Préstamo o Financiamiento: **USD 36'324,000 (Treinta y seis Millones Trescientos Veinticuatro Mil Dólares).** Organismo ejecutor/Comprador: **Programa Nacional de Telecomunicaciones - PRONATEL**.
IAL 4.1	El número máximo de miembros de la APCA será: Tres (03).
IAL 4.5	La lista de firmas y personas inhabilitadas para participar en proyectos del Banco Mundial se puede consultar en el sitio web externo del Banco: http://www.worldbank.org/debarr.
B. Contenido del Documento de Licitación	
IAL 7.1	Para **aclaraciones del proceso de Licitación** solamente, la dirección del Comprador es: Atención: Presidente de Comité de Evaluacion Dirección: Av. Paseo de la República Nº 1645 - La Victoria - Lima – Peru. Piso/oficina: Piso 17 Ciudad: Lima Código postal: 15034 País: Perú. Número de fax: N/A Dirección de correo electrónico: crep911@pronatel.gob.pe. **El Comprador no recibirá solicitudes de aclaraciones luego de catorce (14) días útiles, contabilizados a partir del día siguiente de publicado el Anuncio Específico de Adquisiciones.** Pagina Web: https://www.gob.pe/pronatel **Importante:** ▪ El Licitante puede hacer uso del correo electrónico para la presentación de aclaraciones y/o consultas referidas al proceso de selección. ▪ Los Licitantes podrán formular consultas relacionadas con el proceso de licitación, incluyendo aspectos técnicos, administrativos y condiciones de entrega bajo el Incoterm DDP (Delivered Duty Paid) conforme a Incoterms 2020. ▪ Para la presentación de solicitudes de aclaración y/o consultas, se adjunta el formato correspondiente en la **Sección IV - Formularios de la Oferta**.

	▪ Cuando las solicitudes de aclaración y/o consultas sean presentadas por medios electrónicos, se recomienda que el tamaño de cada correo electrónico no exceda de **25 MB**. Será responsabilidad del Licitante verificar la correcta remisión de sus comunicaciones. El Comprador realizará el correspondiente **acuse de recibo** al correo electrónico del Licitante que haya remitido la solicitud.
C. Preparación de las Ofertas	
IAL 10.1	El idioma en que se presentará la Oferta es el **español**. Todo intercambio de correspondencia se hará en el idioma **español.** El idioma para la traducción de la documentación de apoyo y material impreso es el **español**.
IAL 11.1 (i)	Se agrega: **(i) Documentación que acredita la conformidad técnica de los Bienes y Servicios Conexos:** El Licitante deberá presentar documentación técnica suficiente y verificable que permita acreditar la conformidad de los Bienes y Servicios Conexos ofertados con los requisitos establecidos en la Sección VII - Requisitos de los Bienes y Servicios Conexos. Para tal efecto, deberá identificar, según corresponda, el fabricante, marca, modelo, código, SKU o Part Number de los bienes ofertados, el cual se completará con el Anexo 1. Para la evaluación técnica, deberá evidenciar de manera fehaciente con documentación pública del fabricante los establecido en el Anexo 02 de la Sección IV, el no cumplimiento descalifica al Licitante. La documentación presentada deberá permitir al Comprador establecer de manera objetiva la conformidad de la Oferta con las especificaciones técnicas aprobadas, sin modificar, sustituir o complementar los requisitos establecidos en la Sección VII. Los requisitos específicos relativos a EOL/EOS, servicios posteriores a la venta y demás condiciones particulares se acreditarán exclusivamente conforme a los numerales correspondientes de los DDL y la Sección VII, según corresponda.

IAL 11.1 (j)	Los Licitantes deberán presentar los siguientes documentos adicionales con su Oferta: **<u>Documentos de presentación general:</u>** ✓ Índice del contenido de la Oferta. La Oferta deberá presentarse foliada. **<u>Documentos Legales y Financieros:</u>** ✓ Copia simple de constitución social de la empresa vigente e inscrita en los Registros Públicos o su equivalente en el país de origen del Licitante. La legalización de este requisito podrá ser exigible al(os) Licitante(s) que resulte(n) adjudicado(s). ✓ Poder del Representante Legal de la empresa Licitante, con atribuciones para presentar Ofertas y suscribir contratos. ✓ Declaración Jurada firmada por el Representante Legal de no estar impedido de contratar con el Estado Peruano; en el caso de APCA, cada integrante presentará esta declaración. ✓ De ser el caso, Convenio de APCA o carta de intención de suscribir un Convenio de APCA, de conformidad con la IAL 11.2. ✓ Estados financieros correspondientes a los tres (03) últimos ejercicios fiscales cerrados, anteriores a la fecha límite de presentación de Ofertas, preparados conforme a las NIIF o a las normas contables vigentes en el país del Licitante, auditados cuando corresponda conforme a la normativa aplicable, incluyendo como mínimo el Balance General, el Estado de Resultados y las notas a los estados financieros. Para los Licitantes constituidos en el Perú, podrá adjuntarse la constancia de presentación de declaraciones ante la SUNAT u otro documento equivalente que permita verificar la información financiera declarada. Para los Licitantes extranjeros, se aceptará documentación equivalente emitida por la autoridad competente de su país de origen. **<u>Documentos técnicos:</u>** ✓ **Anexo N.° 01 – Hoja de presentación de los bienes ofertados y sustento de cumplimiento de las características técnicas.** El Licitante deberá identificar claramente, según corresponda, el fabricante, marca, modelo, código de producto, SKU o número de parte (Part Number) de los bienes ofertados, así como la documentación técnica que permita verificar los requisitos establecidos en el Anexo 01.

	✓ **Anexo N.° 02 - Características Técnicas a Sustentar.** El Licitante deberá adjuntar las fichas técnicas, hojas de datos, catálogos, manuales, certificados, documentación oficial del fabricante que permita verificar el cumplimiento de las características técnicas establecidas en la Sección en el Anexo 02. La documentación presentada deberá permitir identificar de manera clara y trazable el requisito que se acredita y el documento, página, sección o referencia técnica donde se encuentra sustentado. ✓ **Anexo N.° 03 – Declaración Jurada de Compromiso de Garantía de los Equipos y sus Componentes**, conforme a las condiciones establecidas en la Sección VII – Requisitos de los Bienes y Servicios Conexos. **<u>Disposición general sobre la documentación técnica:</u>** o La documentación técnica presentada deberá corresponder a los Bienes efectivamente ofertados y deberá ser clara, consistente, verificable y trazable. o Cuando el Documento de Licitación requiera expresamente documentación emitida por el fabricante, dicha condición deberá acreditarse mediante el documento correspondiente, conforme al numeral específico que regule dicho requisito. o Los requisitos relativos a EOL/EOS, servicios posteriores a la venta y demás condiciones específicas se acreditarán conforme a las IAL y a la Sección VII que los regulan, sin que resulte necesario reproducir dichos requisitos en el presente numeral.
IAL 13.1	No se considerarán ofertas alternativas.
IAL 14.5	Los precios cotizados por el Licitante serán **fijos durante la ejecución del Contrato y no estarán sujetos a ajustes**.
IAL 14.6	Los precios cotizados para el Lote (Contrato) deberán cubrir el **100 % de los ítems especificados en el Lote Único**, incluyendo, cuando corresponda, los Servicios Conexos asociados. Asimismo, los precios cotizados para cada ítem deberán corresponder al **100 % de las cantidades especificadas** para dicho ítem. En consecuencia, **no se aceptarán Ofertas parciales** respecto de los ítems ni de las cantidades requeridas en el Lote Único.

IAL 14.7	La edición de Incoterms aplicable será **Incoterms® 2020**. Para efectos de la presente Licitación, los Bienes serán cotizados bajo el término **DDP (Delivered Duty Paid)**, conforme a Incoterms® 2020.
IAL 14.8 (b) (i) y (c) (v)	Lugar de destino: De acuerdo a lo señalado en el apartado "Plazo y Lugar de Entrega" de las Especificaciones Técnica de la Sección VII.
IAL 14.8 (a) (iii); (b) (ii) y (c) (v)	Destino final (emplazamiento del Proyecto): **Av. El Sol S/N, distrito de Chorrillos, provincia y departamento de Lima, Perú.**
IAL 15.1	El Licitante no está obligado a cotizar en la moneda del País del Comprador la porción del precio de la Oferta que corresponde a gastos en que se incurra en esa moneda.
IAL 16.4	El período para el cual el Licitante deberá proporcionar información sobre la disponibilidad de repuestos, herramientas especiales y demás elementos necesarios para el funcionamiento adecuado y continuo de los Bienes será de cinco (05) años, conforme a las condiciones establecidas en la Sección VII - Requisitos de los Bienes y Servicios Conexos. Los Bienes ofertados no deberán encontrarse ni ingresar en condición de End of Life (EOL) o End of Support (EOS) durante los cinco (05) años siguientes a la fecha límite de presentación de las Ofertas. Esta condición deberá acreditarse mediante documentación oficial emitida por el fabricante, conforme a lo requerido en la Sección VII. Este requisito no será aplicable a los accesorios y periféricos, cconforme a lo establecido en la Sección VII.
IAL 17.2 (a)	**No se requiere Autorización del Fabricante.** Para acreditar su capacidad para suministrar los bienes ofertados, el Licitante podrá acreditar su condición de distribuidor, representante comercial, integrador, revendedor autorizado o proveedor habitual, conforme a los requisitos establecidos en la Sección III.
IAL 17.2 (b)	Se requieren servicios posteriores a la venta, de conformidad con lo establecido en el **Anexo 3 - "Garantía y Soporte de los Bienes" de las Especificaciones Técnicas**, contenido en la **Sección VII – Requisitos de los Bienes y Servicios Conexos**.
IAL 18.1	La Oferta deberá ser válida hasta: **23 de diciembre de 2026**.

IAL 18.3 (a)	El precio del contrato no estará sujeto a reajuste durante la ejecución. Sin embargo, en caso de que la adjudicación se retrase más de 56 días después de la expiración de la validez inicial de la oferta, la porción en moneda nacional será ajustada mediante el Índice de Precios al Consumidor (IPC) publicado por [INEI], correspondiente al período de prórroga. La porción en moneda extranjera del precio del Contrato se ajustará mediante la aplicación de un factor que refleje la inflación internacional, utilizando el Índice de Precios al Consumidor (CPI) del país correspondiente a la moneda extranjera ofertada, durante el período de prórroga
IAL 19.1	La Oferta deberá incluir una "Declaración de Mantenimiento de Oferta", utilizando el formulario incluido en la Sección IV. Formularios de la Oferta.
IAL 19.3 (d)	Otro tipo de garantías aceptables: **No aplica**.
IAL 19.9	Si el Licitante incurre en alguna de las acciones previstas en las IAL 19.9(a) o 19.9(b), el Prestatario podrá declarar al Licitante inelegible para ser adjudicatario de un contrato por un período de **dos (02) años**, cconforme a lo establecido en la Declaración de Mantenimiento de Oferta.
IAL 20.1	Además de la oferta original, el número de copias es: ✓ **Una (01) copia en archivo digital**, copia fiel de la Oferta original, debidamente encriptada y presentada en un medio de almacenamiento digital (USB, CD u otro similar), que deberá entregarse conjuntamente con la Oferta original como parte del mismo acto de presentación. ✓ De presentarse diferencias entre el ejemplar original y la información del archivo digital, prevalece la información del ejemplar original de la Oferta.
IAL 20.3	La confirmación escrita de la autorización para firmar en nombre del Licitante comprenderá: i. Copia simple de la vigencia de poder o documento equivalente que acredite las facultades del representante autorizado para presentar y suscribir la Oferta y, cuando corresponda, suscribir el Contrato. ii. Para los Licitantes extranjeros se aceptará el documento equivalente emitido conforme a la legislación de su país de origen.

	iii. Copia del documento de identidad o documento equivalente del país de origen del representante autorizado.
D. Presentación y apertura de las Ofertas	
IAL 22.1	Para fines de **presentación de la Oferta**, la dirección del Comprador es: Atención: Comité de Evaluación Dirección: Av. Paseo de la República Nº 1645 - La Victoria - Lima - Peru. Piso/oficina: Piso 01 Ciudad: Lima. Código postal: 15034 País: Perú **La fecha límite para presentar las ofertas es:** Fecha: **24 de setiembre de 2026**. Hora: 15:00 horas (Hora local) Los Licitantes no tendrán la opción de presentar sus Ofertas electrónicamente.
IAL 25.1	La apertura de las Ofertas tendrá lugar en: Dirección: Av. Paseo de la República Nº 1645 - La Victoria - Lima - Peru. Piso/oficina: Piso 01 Ciudad: Lima País: Perú Fecha: **24 de setiembre de 2026**. Hora: 15:30 horas (Hora local) **Los Licitantes no tendrán la opción de presentar sus Ofertas electrónicamente.**
IAL 25.6	Durante el acto público de apertura de las Ofertas, el Notario Público que certifique el acto procederá a rubricar la **Carta de la Oferta y las Listas de Precios** presentadas por los Licitantes.

	Dichos documentos también serán rubricados por los **tres (03) representantes del Comprador** que participen en el acto de apertura de las Ofertas.
E. Evaluación y Comparación de las Ofertas	
IAL 32.1	La moneda que se utilizará a fin de evaluar y comparar las Ofertas para convertir en una sola moneda, al tipo de cambio vendedor, todoslos precios de las Ofertas expresados en diversas monedas es: Soles (S/). La fuente del tipo de cambio será la **tasa de cambio tipo venta publicada por la Superintendencia de Banca, Seguros y AFP del Perú (SBS)**. La fecha del tipo de cambio será: siete (07) días calendario antes a la fecha de presentación de las Ofertas.
IAL 33.1	No se aplicará un margen de preferencia nacional.
IAL 34.2 (a)	La evaluación se hará por: **Lote único.** Las Ofertas serán evaluadas considerando el precio total ofertado para todos los artículos que integran el lote, bajo la condición de entrega Delivered Duty Paid (DDP) en el lugar de destino final indicado por el Comprador, conforme a Incoterms 2020. La evaluación y comparación de las Ofertas se realizará aplicando exclusivamente los criterios y metodologías establecidos en las IAL y en la Sección III - Criterios de Evaluación y Calificación. <u>Importante:</u> Los licitantes deberán cotizar la totalidad de los artículos incluidos en el lote; de lo contrario, la Oferta podrá ser considerada **<u>no</u>** sustancialmente conforme.
IAL 34.6	Los ajustes se determinarán utilizando los siguientes criterios de entre los enumerados en la Sección III, "Criterios de Evaluación y Calificación": (a) Desviación en el Cronograma de Entregas: **No aplica.** (b) Desviación en el plan de pagos: **No aplica.** (c) Costo de reemplazo de componentes importantes, repuestos obligatorios y servicio **No aplica.** (d) Disponibilidad en el País del Comprador de repuestos y servicios posteriores a la venta para los equipos ofrecidos en la Oferta: **No Aplica.**

	(e) Costos durante la vida útil: Los costos en que se incurra durante la vida útil de los bienes o los equipos **No aplica.** (f) El rendimiento y la productividad de los equipos ofrecidos: **No aplica.**
F. Adjudicación del Contrato	
IAL 42	Las cantidades podrán aumentarse, como máximo, en un 15%. Las cantidades podrán reducirse, como máximo, en un 15%

Sección III. Criterios de Evaluación y Calificación

Esta Sección contiene los criterios que el Comprador utilizará para evaluar una Oferta y determinar si los Licitantes cumplen con las calificaciones requeridas. No se utilizará ningún otro factor, método ni criterio que no sean los que se especifican en este documento de licitación.

Índice

1. Margen de preferencia (IAL 33)..... 49

2. Evaluación (IAL 34)..... 49

3. Calificación (IAL 37) 49

1. Margen de preferencia (IAL 33)

"No Aplica"

2. Evaluación (IAL 34)

2.1. Criterios de evaluación (IAL 34.6)

"No Aplica"

2.2. Contratos múltiples (IAL 34.4)

"No Aplica"

2.3. Ofertas Alternativas (IAL 13.1)

"No Aplica"

3. Calificación (IAL 37)

3.1. Criterios de calificación (IAL 37.1)

Luego de determinar entre las Ofertas que cumplen sustancialmente con los requisitos la que presenta el costo evaluado más bajo de acuerdo con la IAL 34, y, si corresponde, de evaluar cualquier Oferta Excesivamente Baja de acuerdo con la IAL 36, el Comprador efectuará la calificación posterior del Licitante de acuerdo con la IAL 37, empleando únicamente los requisitos estipulados en la presente Sección.

Los requisitos que no estén incluidos en el siguiente texto no podrán utilizarse para evaluar las calificaciones del Licitante.

Todos los criterios establecidos en los numerales 3.1.1 a 3.1.7 son requisitos mínimos habilitantes y serán evaluados exclusivamente bajo la modalidad **CUMPLE / NO CUMPLE**, sin asignación de puntaje, bonificación, preferencia o ventaja comparativa por superar los mínimos establecidos.

3.1.1 CAPACIDAD FINANCIERA

El Licitante deberá demostrar que cuenta con capacidad financiera suficiente para financiar la ejecución del Contrato sin depender exclusivamente de los pagos del Comprador.

a) **Solidez financiera.** El Licitante deberá presentar estados financieros correspondientes a los tres (3) últimos ejercicios fiscales cerrados anteriores a la fecha límite de presentación de Ofertas, auditados cuando corresponda conforme a la legislación aplicable.

El patrimonio neto correspondiente al último ejercicio fiscal cerrado deberá ser positivo y el capital de trabajo, entendido como la diferencia entre activo corriente

y pasivo corriente, correspondiente al último ejercicio fiscal cerrado deberá ser positivo.

b) **Asociación en Participación, Consorcio o Asociación (APCA)**. En caso de APCA, todos sus integrantes deberán presentar la información financiera correspondiente a los tres (3) últimos ejercicios fiscales cerrados y acreditar patrimonio neto positivo en el último ejercicio.

3.1.2 EXPERIENCIA ESPECÍFICA DEL LICITANTE

El Licitante deberá acreditar la ejecución satisfactoria, durante los diez (10) años anteriores a la fecha límite de presentación de Ofertas, de al menos dos (2) contratos que hayan comprendido el suministro e implementación de soluciones de tecnologías de información, infraestructura de centro de datos, redes LAN/campus, equipamiento informático y/o soluciones de ciberseguridad de naturaleza y complejidad comparables con la presente contratación.

Cada contrato deberá acreditar un monto ejecutado mínimo equivalente a USD 5 000 000 (cinco millones de dólares de los Estados Unidos de América).

Para uno (1) de los dos (2) contratos requeridos se permitirá acumular hasta dos (2) contratos ejecutados por el mismo Licitante o por el mismo integrante de la APCA, siempre que el monto acumulado sea igual o superior a USD 5 000 000.

Para ser considerado similar, el contrato deberá incluir como mínimo el suministro e implementación y, adicionalmente, al menos dos (2) de los siguientes grupos:

a) Networking/red LAN o data center;
b) Servidores, almacenamiento, hiperconvergencia o backup;
c) Equipamiento informático/ofimático; y
d) Seguridad de red o ciberseguridad.

Al menos uno (01) de los contratos acreditados deberá incluir componentes de networking/red LAN, data center o ciberseguridad.

La experiencia deberá acreditarse mediante copia del contrato u orden de compra y, adicionalmente, acta de conformidad, certificado de recepción, constancia de prestación satisfactoria, comprobante de pago cancelado u otro documento equivalente que permita verificar de manera fehaciente el objeto, monto ejecutado, período y culminación satisfactoria del contrato.

Cuando el documento se encuentre expresado en una moneda distinta del dólar estadounidense, se aplicará el tipo de cambio previsto en los DDL para fines de comparación.

En caso de APCA, la experiencia podrá acreditarse conjuntamente. El integrante líder deberá acreditar por sí mismo al menos uno (01) de los contratos requeridos.

Los contratos aportados deberán corresponder al integrante que efectivamente los ejecutó.

No se sumarán contratos ejecutados por distintos integrantes para alcanzar el monto mínimo exigido para un contrato. La acumulación excepcional de hasta dos (2) contratos prevista en este numeral únicamente podrá efectuarse respecto de contratos ejecutados por un mismo integrante.

Para determinar el cumplimiento del número mínimo de contratos, se considerará el total de contratos válidamente acreditados por los integrantes de la APCA, de conformidad con las reglas establecidas en el presente numeral.

3.1.3 CONFORMIDAD TÉCNICA Y TRAZABILIDAD DOCUMENTAL

El Licitante deberá acreditar el cumplimiento de las características técnicas identificadas para sustento documental en los Anexos de la Sección IV.

Para cada bien o solución ofertada deberá identificar, según corresponda, fabricante, marca, modelo, versión, SKU y/o Part Number, de modo que el bien o solución ofertada quede inequívocamente individualizado.

El sustento deberá realizarse mediante documentación técnica pública oficial del fabricante, tal como ficha técnica, data sheet, catálogo, manual, certificado, u otra documentación pública del fabricante.

El Licitante deberá señalar, para cada requisito que requiera sustento documental del **Anexo 02**, el documento, página, sección o enlace/referencia técnica exacta donde pueda verificarse su cumplimiento.

Una declaración genérica del Licitante no sustituirá la evidencia técnica del fabricante cuando el requisito exija expresamente documentación oficial del fabricante.

3.1.4 VIGENCIA TECNOLÓGICA

Para los bienes respecto de los cuales la Sección VII o los DDL exijan respaldo del fabricante, no se requerirá acreditar experiencia comercial mínima del fabricante en la fabricación o provisión de la familia de productos ofertada.

La evaluación se centrará en la vigencia tecnológica de los bienes ofertados, a fin de garantizar su disponibilidad de soporte y continuidad tecnológica durante el período requerido.

a) **Vigencia tecnológica**. Cuando corresponda, de conformidad con la IAL 16.4 y la Sección VII, los bienes ofertados no deberán encontrarse ni ingresar en condición de End of Life (EOL) o End of Support (EOS) durante los cinco (5) años siguientes a la fecha límite de presentación de

Ofertas. Esta condición deberá acreditarse mediante documentación oficial del fabricante.

b) **Correspondencia documental**. La documentación presentada deberá corresponder exactamente a la marca, familia, modelo o versión ofertada y deberá ser verificable por el Comprador.

3.1.5 CAPACIDAD PARA IMPLEMENTAR SOLUCIONES DE CIBERSEGURIDAD

Dada la criticidad operativa de la Central 911 y la inclusión de soluciones de seguridad previstas en la Sección VII, el Licitante deberá demostrar capacidad para implementar o integrar componentes de seguridad de red y/o ciberseguridad.

Este requisito se considerará cumplido cuando dicha capacidad se encuentre acreditada en al menos uno (1) de los contratos válidos presentados para acreditar la experiencia específica prevista en el numeral 3.1.2, o mediante un contrato adicional ejecutado satisfactoriamente de naturaleza equivalente.

La experiencia contractual no podrá ser sustituida por una certificación del fabricante.

Las certificaciones técnicas, cuando sean exigidas por la Sección VII para personal o soluciones específicas, acreditarán competencia técnica, pero no reemplazarán la experiencia contractual del Licitante exigida en el presente numeral.

3.1.6 ACREDITACIÓN DEL LICITANTE

El Licitante que no sea fabricante deberá acreditar su condición de distribuidor, representante comercial, integrador, revendedor autorizado o proveedor habitual de los bienes ofertados, según corresponda.

La acreditación podrá realizarse mediante certificados de distribución autorizada, cartas emitidas por el fabricante, acuerdos comerciales vigentes, registros de socios comerciales, contratos de suministro, órdenes de compra ejecutadas u otra documentación equivalente aceptable para el Comprador, que permita verificar razonablemente la capacidad del Licitante para suministrar los bienes ofertados.

3.1.7 CAPACIDAD DE SOPORTE TÉCNICO, GARANTÍA Y SERVICIO POSTVENTA

El Licitante deberá acreditar que cuenta con capacidad para brindar soporte técnico, atención de garantías, mantenimiento y reposición de componentes durante el período de garantía establecido en los Documentos de Licitación.

La acreditación podrá realizarse mediante la presentación de certificados de soporte autorizado, cartas de respaldo del fabricante, relación de centros de servicio autorizados, personal técnico certificado, contratos de soporte o documentación equivalente.

3.1.8 PERSONAL CLAVE

El Licitante deberá demostrar que cuenta con el personal requerido para ocupar las posiciones claves, debidamente calificado y en cantidad suficiente, conforme a lo establecido en los numerales 4.2, 4.3, 4.4 y 4.5 de las Especificaciones Técnicas de la Sección VII.

El Licitante deberá proporcionar la información del personal propuesto para la ejecución del Contrato, incluyendo sus calificaciones académicas, experiencia laboral y demás información requerida en los formularios correspondientes. Para tal efecto, el Licitante deberá completar y presentar los formularios establecidos en la Sección IV, Formularios de Licitación, correspondientes al Personal Clave.

La evaluación verificará que la Oferta no contenga reservas, exclusiones, limitaciones o condiciones que reduzcan los niveles de servicio exigidos en el Documento de Licitación.

Únicamente las Ofertas que cumplan sustancialmente con los requisitos del Documento de Licitación y cuyos Licitantes cumplan los criterios de calificación establecidos en los numerales 3.1.1 a 3.1.8 podrán continuar a la comparación del costo evaluado y, de corresponder, a la determinación de la Oferta con el costo evaluado más bajo, de conformidad con las IAL aplicables.

Sección IV. Formularios de la Oferta

Índice de Formularios

Carta de la Oferta 55

Formulario de Información sobre el Licitante 58

Formulario de información sobre los miembros de la APCA 60

Formulario de la Oferta Lista de Precios de los Bienes (1) 61

Formulario para Solicitud de Aclaración 103

Declaración de Desempeño sobre Explotación y Abuso Sexual (EAS) y/o Acoso Sexual (ASx) 104

Formulario de Declaración de Mantenimiento de Oferta 105

Autorización del Fabricante 107

Carta de la Oferta

INSTRUCCIONES A LOS LICITANTES: ELIMINE ESTE RECUADRO UNA VEZ QUE HAYA COMPLETADO EL DOCUMENTO

El Licitante deberá preparar esta Carta de la Oferta en papel con membrete que indique claramente el nombre completo del Licitante y su dirección comercial.

Nota: El texto en cursiva se incluye para ayudar a los Licitantes en la preparación de este formulario.

Fecha de presentación de esta Oferta: *[Indique día, mes y año de la presentación de la Oferta]*.
SDO n.°: *[Indique el número del proceso de la SDO]*.
Solicitud de Oferta n.°: *[Indique identificación]*.

Para: ***[Indique el nombre del Comprador]***.

(a) **Sin reservas:** Hemos examinado el documento de licitación, incluidas las enmiendas emitidas de conformidad con la IAL 8, y no tenemos reserva alguna al respecto.

(b) **Elegibilidad:** Cumplimos los requisitos de elegibilidad y no tenemos conflictos de intereses, de acuerdo con la IAL 4.

(c) **Declaración de Mantenimiento de Oferta/Propuesta:** No hemos sido suspendidos ni declarados inelegibles por el Comprador sobre la base de la suscripción de una Declaración de Mantenimiento de Oferta/Propuesta en el País del Comprador de acuerdo con la IAL 4.7.

(d) **Explotación y Abuso Sexual (EAS) y/o Acoso Sexual (ASx):** [*seleccione la opción apropiada de (i) a (iii) a continuación y elimine las demás. En caso de los miembros de una APCA y/o subcontratistas, indicar la situación de descalificación por parte del Banco de cada miembro de la APCA y/o subcontratista.]*

Nosotros, incluyendo todos nuestros subcontratistas:

(i) [no hemos sido objeto de descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS/ASx.]

(ii) [estamos sujetos a descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS/ASx]

(iii) [habíamos sido descalificados por el Banco por incumplimiento de las obligaciones sobre EAS/ASx. Se ha dictado un laudo arbitral en el caso de descalificación a nuestro favor.]

(e) **Conformidad:** Ofrecemos proveer los siguientes bienes de conformidad con el documento de licitación y de acuerdo con el Cronograma de Entregas establecido en los

Requisitos de los Bienes y Servicios Conexos: *[proporcione una descripción breve de los Bienes y Servicios Conexos]*.

(f) **Precio de la Oferta:** El precio total de nuestra Oferta, excluyendo cualquier descuento ofrecido en el artículo (f) a continuación es:

el precio total es *[indique el precio total de la Oferta en letras y en cifras, indicando los diferentes montos y las respectivas monedas]*.

(g) **Descuentos:** Los descuentos ofrecidos y la metodología para su aplicación son los siguientes:

(i) Los descuentos ofrecidos son: *[especifique cada descuento ofrecido]*.

(ii) El método de cálculo exacto para determinar el precio neto luego de aplicados los descuentos se detalla a continuación: *[detalle la metodología que se usará para aplicar los descuentos]*.

(h) **Validez de la Oferta:** Nuestra Oferta será válida hasta *[ingresar el día, mes y año de conformidad con la IAL 18.1]*, y seguirá teniendo carácter vinculante para nosotros y podrá ser aceptada en cualquier momento antes del vencimiento de dicho período.

(i) **Garantía de Cumplimiento:** Si nuestra oferta es aceptada, nos comprometemos a obtener una Garantía de Cumplimiento del Contrato de conformidad con el documento de licitación.

(j) **Una Oferta por Licitante:** No estamos presentando ninguna otra Oferta como Licitantes individuales, y no estamos participando en ninguna otra Oferta ni como miembros de una APCA ni como subcontratistas, y cumplimos con los requisitos de la IAL 4.3, sin considerar las Ofertas Alternativas presentadas de acuerdo con la IAL 13.

(k) **Suspensión e inhabilitación:** Nosotros, junto con todos nuestros subcontratistas, proveedores, consultores, fabricantes o prestadores de servicios requeridos para ejecutar cualquier parte del contrato, no dependemos de ninguna entidad o persona, ni somos controlados por ninguna entidad o persona, que esté sujeta a una suspensión o inhabilitación temporal impuesta por el Grupo Banco Mundial ni a una inhabilitación impuesta por el Grupo Banco Mundial de conformidad con el Acuerdo de Aplicación Mutua de las Decisiones de Inhabilitación, suscrito por el Banco Mundial y otros bancos de fomento. Asimismo, no somos inelegibles en virtud de las leyes o regulaciones oficiales del País del Comprador ni en virtud de una decisión del Consejo de Seguridad de las Naciones Unidas.

(l) **Empresa o ente de propiedad estatal:** *[Seleccione la opción correspondiente y elimine la otra]*. *[No somos una empresa o ente de propiedad estatal]*/*[Somos una empresa o ente de propiedad estatal, pero cumplimos con los requisitos de la IAL 4.6]*.

(m) **Comisiones, gratificaciones, honorarios:** Hemos pagado o pagaremos los siguientes honorarios, comisiones o gratificaciones en relación con el Proceso de Licitación o la ejecución del Contrato: *[proporcione el nombre completo de cada receptor, su dirección*

completa, la razón por la cual se pagó cada comisión o gratificación, y la cantidad y moneda de cada comisión o gratificación a la que se haga referencia].

Nombre del receptor	Dirección	Concepto	Monto

(Si no ha efectuado o no se efectuará pago alguno, escriba "ninguno").

(n) **Contrato vinculante:** Entendemos que esta Oferta, junto con su debida aceptación por escrito incluida en su Carta de Aceptación, constituirá una obligación contractual entre nosotros hasta que las partes hayan preparado y perfeccionado un contrato formal.

(o) **Comprador no obligado a aceptar:** Entendemos que ustedes no están obligados a aceptar la Oferta con el costo evaluado más bajo, la Oferta más Conveniente ni ninguna otra Oferta que reciban.

(p) **Fraude y Corrupción:** Por el presente, certificamos que hemos tomado las medidas necesarias para garantizar que ninguna persona que actúe en nuestro nombre o representación incurra en prácticas fraudulentas o corruptas.

Nombre del Licitante*: *[proporcione el nombre completo del Licitante]*.

Nombre de la persona debidamente autorizada para firmar la Oferta en nombre del Licitante:** *[proporcione el nombre completo de la persona debidamente autorizada a firmar el Formulario de la Oferta]*.

Cargo de la persona firmante del Formulario de la Oferta: *[indique el cargo de la persona que firma el Formulario de la Oferta]*

Firma de la persona nombrada anteriormente: *[indique la firma de la persona cuyo nombre y capacidad se indican en los párrafos anteriores]*.

Fecha de la firma: El día *[indique la fecha de la firma]* **del mes** *[indique mes]* **del año** *[indique año]*.

***** En el caso de las Ofertas presentadas por una APCA, especifique el nombre de la APCA que actúa como Licitante.

** La persona que firme la Oferta deberá contar con el poder otorgado por el Licitante. El poder deberá adjuntarse a los Formularios de la Oferta.

Formulario de Información sobre el Licitante

[El Licitante deberá completar este formulario de acuerdo con las instrucciones indicadas a continuación. No se aceptará ninguna alteración a este formulario ni se aceptarán substitutos].

Fecha: *[indique día, mes y año de la presentación de la Oferta]*.
SDO n.°: *[Indique el número del proceso de la SDO]*.
Alternativa n.°: *[indique el n.° de identificación, si esta es una oferta por una alternativa]*.

Página _____ de _____ páginas

1. Nombre del Licitante: *[indique el nombre jurídico del Licitante]*.
2. Si se trata de una APCA, nombre jurídico de cada miembro: *[indique el nombre jurídico de cada miembro de la APCA]*.
3. País donde está registrado el Licitante en la actualidad o país donde intenta registrarse: *[indique el país donde está registrado el Licitante en la actualidad o país donde intenta registrarse]*.
4. Año de registro del Licitante: *[indique el año de registro del Licitante]*.
5. Dirección del Licitante en el país donde está registrado: *[indique el domicilio legal del Licitante en el país donde está registrado]*.
6. Información del representante autorizado del Licitante: Nombre: *[indique el nombre del representante autorizado]*. Dirección: *[indique la dirección del representante autorizado]*. Números de teléfono y fax*: [indique los números de teléfono y fax del representante autorizado]*. Dirección de correo electrónico: *[indique la dirección de correo electrónico del representante autorizado]*.
7. Se adjuntan copias de los siguientes documentos originales: *[marque las casillas que correspondan]* ☐ Estatutos de la Sociedad (o documentos equivalentes de constitución o asociación), o documentos de registro de la persona jurídica antes mencionada, y de conformidad con la IAL 4.4. ☐ Si se trata de una APCA, carta de intención de formar la APCA, o el Convenio de APCA, de conformidad con la IAL 4.1. ☐ Si se trata de una empresa o ente de propiedad estatal, de conformidad con la IAL 4.6, documentación que acredite: • su autonomía jurídica y financiera, • su operación conforme al Derecho comercial, • que el Licitante no se encuentra bajo la supervisión del Comprador.

8. Se incluye el organigrama, la lista de los miembros del Directorio y la propiedad efectiva.

Formulario de información sobre los miembros de la APCA

[El Licitante deberá completar este formulario de acuerdo con las instrucciones indicadas a continuación. El siguiente cuadro deberá ser completado por el Licitante y por cada uno de los miembros de la APCA].

Fecha: *[indique día, mes y año de la presentación de la Oferta]*.
SDO n.°: *[indique el número del proceso de Licitación]*.
Alternativa n.°: *[indique el n.° de identificación, si esta es una oferta por una alternativa]*.

Página ____ de ____ páginas

1. Nombre del Licitante *[indique el nombre jurídico del Licitante]*.
2. Nombre jurídico del miembro de la APCA *[indique el nombre jurídico del miembro de la APCA]*.
3. Nombre del país de registro del miembro de la APCA *[indique el nombre del país de registro del miembro de la APCA]*.
4. Año de registro del miembro de la APCA: *[indique el año de registro del miembro de la APCA]*.
5. Dirección del miembro de la APCA en el país donde está registrado: *[domicilio legal del miembro de la APCA en el país donde está registrado]*.
6. Información sobre el representante autorizado del miembro de la APCA: Nombre: *[indique el nombre del representante autorizado del miembro de la APCA]*. Dirección: *[indique la dirección del representante autorizado del miembro de la APCA]*. Números de teléfono y fax: *[indique los números de teléfono y fax del representante autorizado del miembro de la APCA]*. Dirección de correo electrónico: *[indique la dirección de correo electrónico del representante autorizado del miembro de la APCA]*.
7. Se adjuntan copias de los siguientes documentos originales: *[marque las casillas que correspondan]*. ☐ Estatutos de la Sociedad (o documentos equivalentes de constitución o asociación) o documentos de registro de la persona jurídica antes mencionada, y de conformidad con la IAL 4.4. ☐ Si se trata de una empresa o ente de propiedad estatal, documentación que acredite su autonomía jurídica y financiera, su operación de conformidad con el Derecho comercial y que no se encuentra bajo la supervisión del Comprador, de conformidad con la IAL 4.6. 8. Se incluye el organigrama, la lista de los miembros del Directorio y la propiedad efectiva.

Formulario de la Oferta
Lista de Precios de los Bienes (1)
(Lote Unico)

(El Licitante deberá completar el presente formulario de conformidad con las instrucciones establecidas en el Documento de Licitación. La identificación, descripción y numeración de los artículos deberán corresponder exactamente a las establecidas por el Comprador en la Sección VII – Lista de Requisitos de los Bienes y Servicios Conexos).

Señores
COMITÉ DE EVALUACION
PROCESO SDO Nº PE-PRONATEL-561608-GO-RFB

Lote Nº	**Artículo Nº**	**DESCRIPCIÓN**	**UNIDAD DE MEDIDA**	**CANTIDAD**	**PRECIO UNITARIO DDP** (incluye IGV y demás tributos aplicables) *(indicar moneda)*	**PRECIO TOTAL** (incluye IGV y demás tributos aplicables) *(indicar moneda)*
Único	1	Computadora de Escritorio Tipo 1	Und.	210		
	2	Computadora de Escritorio Tipo 2	Und.	71		
	3	Monitor para Computadoras	Und.	696		
	4	Teclado y Mouse	Und.	281		
	5	Soporte para 03 Monitores Computadoras de Escritorio Tipo 1	Und.	210		
	6	Equipo Portátil	Und.	9		
	7	Auricular Monoaural	Und.	210		
	8	Micrófono	Und.	115		
	9	Altavoces	Und.	115		
	10	PPT de pie	Und.	210		
	11	Cámara Web	Und.	281		
	12	Teléfonos IP Tipo 1	Und.	201		
	13	Teléfonos IP Tipo 2	Und.	62		
	14	Teléfonos IP Tipo 3	Und.	16		
	15	Teléfonos IP Tipo 4	Und.	4		
	16	Botonera para teléfono IP 4	Und.	1		
	17	Pantalla para Monitoreo	Und.	2		
	18	Videoconferencia	Und.	4		
	19	Impresora tipo personal	Und.	13		
	20	Impresora tipo mediano volumen	Und.	5		
	21	Proyector Multimedia	Und.	4		
	22	Tabletas Rugerizadas	Und.	37		
	23	Switches Spine Data Center	Und.	2		
	24	Switches Leaf Data Center	Und.	8		
	25	Solución de Orquestador DC	Und.	1		

	26	Switch Core LAN Campus	Und.	2		
	27	Switch de acceso 48 puertos PoE	Und.	23		
	28	Switch de acceso 24 puertos PoE	Und.	4		
	29	Switch DMZ	Und.	2		
	30	Switch de Gestión Fuera de Banda	Und.	2		
	31	Controlador inalámbrico	Und.	2		
	32	Access Point	Und.	47		
	33	Solución de Administración y Gestión Campus	Und.	1		
	34	Solución de Control de Acceso	Und.	1		
	35	Hardware de Hiperconvergencia	Und.	4		
	36	Software Hiperconvergencia	Und.	1		
	37	Servidor para backup	Und.	1		
	38	Servidor de inmutabilidad	Und.	1		
	39	Almacenamiento para backup	Und.	1		
	40	Librería de backup	Und.	1		
	41	Software de backup	Und.	1		
	42	Firewall NGFW (Perimetral)	Und.	2		
	43	Firewall Interno	Und.	2		
	44	Consola de analítica y reportes	Und.	1		
	45	XDR (Extended Detection & Response)	Und.	1		
	46	ZTNA (Zero Trust Network Access)	Und.	1		
	47	Seguridad para correo electronico	Und.	1		
	48	WAF - Seguridad para Aplicaciones Web	Und.	1		
	49	SIEM	Und.	1		
	50	Plataforma de detección y respuesta de amenazas externas e internas	Und.	1		
	51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	Und.	1		
	52	ADC (application Delivery Controller)	Und.	2		
	53	Anti - DDos	Und.	2		
	54	MFA - Administración de identidad y acceso	Und.	1		
	55	PAM - Administración de acceso privilegiado	Und.	1		
	56	NDR (Network Detection and Response)	Und.	1		
	57	Sandboxing	Und.	1		
	58	Solución de Análisis de Tráfico de Red	Und.	1		
Total						

Condiciones de Cotización:

Los bienes deberán cotizarse bajo la condición **DDP (Delivered Duty Paid – Entregado Derechos Pagados)**. El precio ofertado deberá incluir todos los costos necesarios para suministrar y entregar los bienes en el lugar de destino final indicado por el Comprador, incluyendo el valor de los bienes, embalaje, transporte internacional, seguros, derechos e impuestos de importación, nacionalización, manipuleo, transporte interno, descarga, entrega en destino y todos los tributos, tasas y demás gastos aplicables hasta la recepción conforme de los bienes.

Los precios consignados en el presente formulario corresponden exclusivamente al suministro de los bienes. Los **Servicios Conexos** requeridos en las Especificaciones Técnicas deberán ser cotizados en el **Formulario N.° 02 – Precio y Cronograma de Cumplimiento de los Servicios Conexos**, formando parte de la oferta económica integral.

Lugar y Plazo de Entrega:

Lugar de entrega: _____

Tiempo de entrega máximo requerido[1]: _____

Tiempo de Entrega ofrecido: _____
[De acuerdo a la subcláusula 13.9 de la Sección I, las ofertas que presenten un plazo de entrega mayor al máximo requerido serán rechazadas.]

Datos del Licitante:

Razón Social: _____

RUC: _____

Dirección: _____

Teléfono: _____

Correo electrónico: _____

Lugar y Fecha: _____

Firma del Representante Legal y sello de la Empresa

[1] *Las ofertas que excedan el plazo máximo requerido serán rechazadas conforme a lo establecido en el Documento de Licitación.*

Precio y cronograma de cumplimiento: Servicios conexos[2]

(El Licitante deberá completar el presente formulario de conformidad con las instrucciones establecidas en el Documento de Licitación. Los servicios conexos ofertados deberán corresponder a los requeridos en la Sección VII – Lista de Requisitos de los Bienes y Servicios Conexos y en las Especificaciones Técnicas.)

Monedas de conformidad con la IAL 15					**Fecha:_____ _____ SDO n.º _____ Página n.º _____ de _____**	
1	2	3	4	5	6	7
Servicio n.º	**Plazo de prestación del servicio**	**Plazo de prestación del servicio**	**Unidad de medida**	**Cantidad**	**Precio unitario (incluye todos los tributos aplicables)**	**Precio total por servicio (Col. 5 x 6 o un estimado) (incluye todos los tributos aplicables)**
[Indique número del servicio].	*[Indique el nombre de los servicios].*	*[Indique la fecha de entrega al lugar de destino final por servicio].*			*[Indique el precio unitario por servicio].*	*[Indique el precio total por servicio].*
1	Servicio de implementación (instalación, configuración, pruebas y comisionamiento)	90 días	Servicio	1		
2	Mesa de Servicio	12 meses	Meses	12		
3	Centro de Operaciones de Seguridad	12 meses	Meses	12		

[2] *Este formulario corresponde al Lote Único y está destinado exclusivamente a la valorización de los Servicios Conexos. La unidad de contratación se establece como "Servicio" y la cantidad como "1", debido a que cada prestación corresponde a un servicio integral con un alcance y plazo definido en las Especificaciones Técnicas. Los bienes serán valorizados separadamente en el Formulario de Lista de Precios de los Bienes bajo condición DDP.*

4	Garantía y Soporte de los Bienes	12 meses	Meses	12		
			Precio total Servicios Conexos de la oferta			

Declaración del Licitante:

Los precios ofertados en el presente formulario corresponden exclusivamente a los **Servicios Conexos** requeridos por el Comprador y comprenden todos los costos necesarios para su ejecución integral, incluyendo personal especializado, herramientas, equipos, materiales, licencias, gestión operativa, gastos administrativos, tributos aplicables y cualquier otro costo relacionado con la prestación de los servicios.

Los precios consignados incluyen todos los costos directos e indirectos necesarios para la correcta ejecución de los Servicios Conexos durante el plazo establecido en las Especificaciones Técnicas.

Cronograma de Cumplimiento de los Servicios Conexos

Servicio Conexos	Fecha de Inicio	Fecha de Culminación
Servicio de implementación (instalación, configuración, pruebas y comisionamiento)		
Mesa de Servicio		
Centro de Operaciones de Seguridad (SOC)		
Garantía y Soporte de los Bienes		

Firmada: [firma del representante autorizado]. En capacidad de [indique el cargo]

Nombre: [indique el nombre en letra de molde o mecanografiado]

Debidamente autorizado para firmar la Oferta por y en nombre de: [indique el nombre la entidad que autoriza]

Fechada el [indique el día] día de [indique el mes] de [indique el año]

ANEXO N° 01

Declaración Jurada / Hoja de Presentación Equipos sobre Cumplimiento de las Características Técnicas de las Especificaciones Técnicas.

Señores
COMITÉ DE EVALUACION
PROCESO SDO Nº PE-PRONATEL-569321-GO-RFB

Presente. -

En calidad de postor, luego de haber examinado los documentos del procedimiento de selección SOLICITUD DE OFERTA SDO Nº PE-PRONATEL-569321-GO-RFB, conociendo todas las condiciones existentes, el suscrito adjunta declaración Jurada sobre el Cumplimiento de acuerdo con los Requerimientos Técnicos Mínimos y demás condiciones que se indican en la sección VII de las especificaciones técnicas de las Bases.

DECLARACION JURADA DE CUMPLIMIENTO DE LAS CARACTERISTICAS TÉCNICAS DE LAS ESPECIFICACIONES TECNICAS
NOMBRE O RAZÓN SOCIAL DEL LICITANTE Y/O APCA:
REPRESENTANTE LEGAL:
FECHA:

RESUMEN DE LOS BIENES OFERTADOS

Ítem	**Descripción del bien**	**Cantidad**	**Marca**	**Modelo**	**País de origen**	**Año de fabricación**	**Cumple (Sí/No)**
1							
2							
3							
…							
7…							

DETALLE DEL CUMPLIMIENTO POR ÍTEM

Ítem N.° ___
Descripción del bien:

N.°	**Requerimiento técnico mínimo EETT**	**Datos del equipo ofertado**	**Cumple (Si/No)**	**Sustento de corresponder (Folio Nº)**
1		• Marca: • Modelo: • Fabricante: • País de origen: • Año de fabricación:		

2				
3				
…				

(Repetir la misma estructura para cada uno de los ítems del lote).

En ese sentido, declaro que toda la información consignada es veraz y que los bienes ofertados cumplen con las especificaciones técnicas establecidas en la Sección VII de la Solicitud de Ofertas, que forman parte integral de las Bases del procedimiento de selección, y de resultar adjudicatario me comprometo a entregar los bienes y servicios conexos según las características técnicas requerido y en las condiciones señaladas, en la forma y detalles especificados.

Ciudad, ……..de …….de……..

_____

Firma y Sello del Representante Legal
Sello del postor/ Razón Social del Proveedor

ANEXO N° 02

Sustento de Cumplimiento obligatorio de las Características Técnicas de las Especificaciones Técnicas.

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Switch Spine Data Center (02 Unidades)			
Debe contar con 32 puertos QSFP28 (con capacidad de conectar transceivers a 40 o 100 Gbps).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 16GB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 64GB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer no menor a 32MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de conmutación no menor a 6.4 Tbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío de paquetes no menor a 2 Bpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 90K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 130K y rutas IPv6 de 30K	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
EEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1p y DSCP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN dinámica mediante BGP-EVPN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
BFD y ECMP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
DCBx, PFC, ETS, ECN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VRF.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch Leaf Data Center (08 Unidades)			
Debe contar con 48 puertos SFP28 (con capacidad de conectar transceiver a 1, 10 ó 25 Gbps) y 6 puertos QSFP28 (con capacidad de conectar transceiver a 40 ó 100 Gbps	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 32GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 64GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer no menor a 32MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Capacidad de conmutación no menor a 3.6 Tbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío de paquetes no menor a 2 Bpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 98K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 130K y rutas IPv6 de 30K	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN dinámica mediante BGP-EVPN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
BFD y ECMP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
DCBx, PFC, ETS, ECN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VRF.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Solución de Orquestador DC (01 Unidad)			
La solución deberá contar con la capacidad de orquestar los switches de Data Center spine y leaf ofertados como un único fabric, simplificando las operaciones y la resolución de problemas en infraestructura de red de Centros de Datos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Debe permitir la automatización de las configuraciones VXLAN entre varias sedes	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Debe permitir la creación de políticas basadas en etiquetas de vSphere o nombres de MV.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch Core LAN Campus (02 Unidades)			
Debe contar con 32 puertos SFP28 (con capacidad de conectar transceiver a 1, 10 ó 25 Gbps) y 4 puertos QSFP28 (con capacidad de conectar transceiver a 40 ó 100 Gbps).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer no menor a 32MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de conmutación no menor a 2.4 Tbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío de paquetes no menor a 1.7 Bpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 80K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 130K y rutas IPv6 de 30K	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1p y DSCP	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN dinámica mediante BGP-EVPN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
BFD y ECMP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
DCBx, PFC, ETS, ECN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VRF.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch de acceso 48 puertos PoE (22 Unidades + 01 unidad en spare)			
El switch debe contar con 48 puertos RJ45 10/100/1000 Base-T con soporte de PoE 802.3at Clase 4 y 04 puertos de uplink SFP+ (con capacidad de conectar transceivers a 1 o 10 Gbps).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 8 GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 8 GB.	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
	documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío no menor a 130 Mpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de switching no menor a 176 Gbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer mínimo de 6 MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 32K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1p y DSCP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN estática	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por RADIUS, para los usuarios de	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
la red que se autentican vía 802.1x.	documentación técnica pública y oficial del fabricante.		
RADIUS y RADIUS CoA.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch de acceso 24 puertos PoE (04 Unidades)			
El switch debe contar con 24 puertos RJ45 10/100/1000 Base-T con soporte de PoE 802.3at Clase 4 y 04 puertos de uplink SFP+ (con capacidad de conectar transceivers a 1 o 10 Gbps).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 8 GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 8 GB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío no menor a 95 Mpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de switching no menor a 128 Gbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer mínimo de 6 MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 32K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
	documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN estática	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por RADIUS, para los usuarios de la red que se autentican vía 802.1x.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
RADIUS y RADIUS CoA.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch DMZ (02 Unidades)			
Debe contar con 24 puertos SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps) y 04 puertos SFP56 (con capacidad de conectar transceivers a 1, 10, 25 ó 50 Gbps	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 8 GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 32 GB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío no menor a 654 Mpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de switching no menor a 880 Gbps.	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
	documentación técnica pública y oficial del fabricante.		
Buffer mínimo de 8 MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 32K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 32K y rutas IPv6 de 16K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1p y DSCP	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN estática	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VRF	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch de Gestión Fuera de Banda (02 Unidades)			

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
El switch debe contar con 48 puertos RJ-45 10/100/1000 Base T con y 04 puertos SFP+ (con capacidad de conectar transceivers a 1 o 10 Gbps).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 8 GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 8 GB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío no menor a 130 Mpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de switching no menor a 176 Gbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer mínimo de 6 MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 32K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
	documentación técnica pública y oficial del fabricante.		
IEEE 802.1p y DSCP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN estática	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Controlador Inalámbrico (02 Unidades)			
Características de controlador en formato appliance hardware: • Mínimo cuatro (04) puertos SFP+ (con capacidad de conectar transceivers a 1 o 10 Gbps). Se deberá incluir dos (02) transceivers 10GE-SR por cada equipo ofertado.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
• Un (01) puerto consola RJ45 o similar.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
• Fuente redundante de energía.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
• Capacidad de poder registrar/controlar al menos 3000 dispositivos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
• Capacidad de mantener conectados al menos 9000 clientes/endpoints simultáneos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
▪ Capacidad de manejar 30,000 túneles	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
• Throughput no menor de 10 Gbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Access Point (43 Unidades + 04 Unidades en Spare			

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Antenas omnidireccionales integradas para MIMO 2x2	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Access point para interiores de tres radios: 2.4Ghz, 5Ghz y 6Ghz	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Ganancia de antena mínimo de 4 dBi en 2.4GHz, 7 dBi en 5GHz y 6 dBi en 6Ghz.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
ACC (Advanced Cellular Coexistence)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
MRC (Maximum Ratio Combining)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
CDD/CSD (Cyclic Delay/Shift Diversity)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
STBC (Space-Time Block Coding)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
LDPC (Low-Density Parity Check)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
TxBF (transmit beam-forming)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
TWT (Target Wait Time)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
FTM (Fine Timing Measurement	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
A-MPDU, A-MSDU	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Dos interfaces 100/1000/2500 BASE-T Ethernet (RJ-45)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Radio BLE (Bluetooth Low Energy) y Zigbee (802.15.4	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Solución de Administración y Gestión de Campus			
En el caso de una solución en premisa, deberá incluir alta disponibilidad de todos sus servicios. Cada appliance físico deberá tener: Dos (02) interfaces de 10Gbps Fuente de poder redundante Altura no mayor a dos (02) Rack Units (RUs) Kit para poder ser instalado en rack de 19”	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
En el caso de una solución en nube, se deberá presentar documentación o carta del fabricante que indique un SLA no menor a 99.95%. No se aceptarán soluciones basadas en VMs que obliguen a la institución a gestionar o contratar un Tenant de nube pública.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Debe realizar el aprovisionamiento de los dispositivos de red por medio de PnP (Plug and Play) o ZTP (Zero Touch Provisioning)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
La solución debe mostrar el mapa topológico de la red.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Debe incluir integración por medio de APIs.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Solución de Control de Acceso (01 Unidad)			
- La solución debe centralizar el control de acceso de usuarios administradores a dispositivos de red de la entidad vía TACACS+ para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
- La solución debe basarse en un esquema AAA (autenticación, autorización y accounting).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
- La solución debe soportar y tener habilitados los siguientes	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
métodos de autenticación como mínimo: ▪ PAP ▪ OAuth2	documentación técnica pública y oficial del fabricante.		
▪ CHAP			
▪ EAP-MSCHAPv2			
▪ EAP-MD5			
▪ PEAP			
▪ EAP-TLS			
▪ EAP-GTC			
▪ MAC Authentication			
▪ WEB Authentication			
▪ EAP-FAST			
▪ EAP-PWD			
▪ SAML			
- Identificación y clasificación (profiling) basada en datos contextuales tales como: ▪ MAC OUIs	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
▪ Nmap Scan			
▪ DHCP fingerprints			
▪ TCP fingerprints			
▪ HTTP user agent			
▪ SNMP traps			
▪ LLDP			
▪ Netflow / IPFIX			
▪ WMI			
▪ Span Port			
Plataforma de la solución en formato appliance, mínimo de dos (02) nodos (appliances físicos) redundantes, con capacidad de soportar cada uno al menos 60,000 dispositivos endpoints autenticados simultáneamente.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Cada nodo deberá tener dos (02) conexiones 10GE-SR para conectarse con la red.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Deberá soportar Microsoft Active Directory Deberá soportar base de datos internas.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Deberá soportar Kerberos	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Deberá soportar LDAP	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
	documentación técnica pública y oficial del fabricante.		
Deberá soportar SQL server compatible con ODBC	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Deberá soportar listas estáticas	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Deberá soportar listas estáticas	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

HIPERCONVERGENCIA

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Hardware de Hiperconvergencia		
La solución hiperconvergente por definición es cómputo, virtualización y storage totalmente definido por software. Los nodos HCI deben encontrarse en la matriz de compatibilidad e interoperabilidad del fabricante del software. Los nodos HCI deben estar identificado en el portal del fabricante del hardware como appliance o sistema hiperconvergente.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de que el hardware sea certificado por el software hiperconvergente. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Dos (02) procesadores x86 de la última generación, con fecha de lanzamiento 2025 como mínimo, de 12 cores como mínimo, de al menos 2.2GHz de frecuencia base y mínimo 48MB de cache L3. Debe soportar la tecnología Hyper-Threading o Multithreading	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de que los procesadores sean de última generación. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Cada servidor o nodo HCI deberá contar con discos SSD NVMe intercambiables en caliente, deberá incluir al menos 10 bahías para discos SSD NVMe. La solución hiperconvergente (HCI) debe ser configurada para permitir la tolerancia de fallos ante la caída de un (01) servidor o nodo (N+1) La capacidad efectiva o usable total de almacenamiento de la solución HCI deberá ser de al menos 50TiB SSD NVMe en RF2 o RAID 1 o mirror, sin considerar factores de eficiencia como compresión y de duplicación.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de las capacidades. No se aceptarán cartas de fabricante para dicho cumplimiento.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
El dimensionamiento deberá ser sobre arquitectura de acceso directo a la capa de almacenamiento NVMe. La solución debe realizar réplicas de datos almacenados a través de los nodos de clúster.		
Cuatro (04) puertos Ethernet de 25Gb SFP28, deben incluir sus respectivos transceivers SR SFP28 y cables de fibra LC-LC MM OM3 de mínimo 3 metros. los cuales se utilizarán para garantizar redundancia de conectividad LAN y para la interconexión de la solución hiperconvergente.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de la cantidad de puertos y velocidades. No se aceptarán cartas de fabricante para dicho cumplimiento.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Software Hiperconvergencia		
El licenciamiento del software debe ser por suscripción, del tipo OPEN, de forma que no esté vinculado a un solo fabricante de hardware.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	
La solución deberá ser agnóstica al hipervisor y debe soportar distintos hipervisores como: VMware ESXi y basados en Linux KVM.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Deberá soportar el crecimiento scale-out en nodos heterogéneos, o diferentes modelos para maximizar recursos de procesamiento, memoria o almacenamiento según requiera.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Servidor para backup		
Un (01) procesador x86 de la última generación, con fecha de lanzamiento 2025 como mínimo, cada procesador de 12 cores como mínimo, de al menos 2.2 GHz de frecuencia base y mínimo 48 MB de cache L3.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
El servidor debe soportar el crecimiento hasta dos (02) procesadores.	de fabricante para dicho cumplimiento.	
Dos (02) puertos Ethernet de 25Gb SFP28, deben incluir sus respectivos transceivers SR SFP28 y cables de fibra LC-LC MM OM3 de mínimo 5 metros.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de la cantidad de puertos y velocidades. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Dos (02) discos SSD de 3.84TB como mínimo configurados en RAID 1. Los discos deben poder ser intercambiables en caliente. Deberá incluir el backplane con soporte de al menos ocho (08) discos.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de la capacidad solicitada y de la cantidad de puertos, así como también las velocidades. No se aceptarán cartas de fabricante para dicho cumplimiento.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Almacenamiento para backup		
Deberá estar diseñado para una disponibilidad de 99.9999%, deberá poder ser verificado en la documentación pública del fabricante del sistema de almacenamiento.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Dos controladoras en configuración activo-activo con balanceo de carga automático.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Dos (02) puertos iSCSI de 10/25 Gb, deben incluir sus respectivos transceivers.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Librería de backup		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
La librería deberá incluir cuarenta (40) slots para cartuchos de cinta magnética LTO en su máxima configuración.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Cada tape drive LTO9 debe incluir como mínimo un (01) puerto en fibra canal (FC) para conectarse al servidor de backup solicitado, cada uno de estos puertos debe ser de 8 Gbps como mínimo.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	

CIBERSEGURIDAD

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Firewall NGFW Perimetral (02 Unidades)		
Deberá tener un rendimiento de Prevención de Amenazas de 28 Gbps cuando opera en simultáneo: Application Control, firewall, IPS, Antivirus/Anti-Bot/Antispyware o 14 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7) teniendo las siguientes funcionalidades habilitadas de manera simultánea: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. La solución debe operar bajo una arquitectura de procesamiento único donde todas las funciones de seguridad se apliquen simultáneamente sobre el mismo flujo de tráfico.	El postor deberá presentar documentación pública del fabricante que sustente el cumplimiento del performance y condiciones de medición requeridas. No se aceptarán cartas de fabricante como sustentos para el cumplimiento del performance y condiciones de medición solicitadas.	
El equipo debe soportar como mínimo 20 millones de sesiones concurrentes medidas con transacciones TCP o 2.5 millones medidas con transacciones HTTP. El equipo debe soportar 800 mil nuevas sesiones por segundo medidas con transacciones TCP o 200 mil nuevas sesiones por segundo medidas con transacciones HTTP.	El postor deberá presentar documentación pública que sustente expresamente la metodología de medición de sesiones concurrentes y sesiones por segundo utilizada por el fabricante, precisando si corresponde a transacciones TCP (L4) o HTTP (L7). No se aceptarán equivalencias sustentadas mediante cartas de fabricante.	
Debe incluir mínimo 12 interfaces de 1G/2.5G/5G/10G RJ-45, 10 interfaces de	Las interfaces requeridas deberán encontrarse activas, soportadas y	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
10Gbps SFP/ SFP+, 4 interfaces de 25Gbps SFP28 y 2 interfaces de 40G/100GGbps QSFP28.	documentadas públicamente por el fabricante. No se aceptarán habilitaciones futuras, roadmap de producto ni cartas de compromiso.	
Capacidad de inspeccionar el contenido en túneles GRE, opcionalmente GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.	Esto deberá encontrarse expresamente documentado en información pública del fabricante	
Debe incluir capacidades de identificación y perfilado de dispositivos conectados a la red (incluyendo dispositivos IoT/OT), permitiendo su clasificación, evaluación de riesgo y aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, sin requerir la instalación de agentes adicionales	Las capacidades de identificación y perfilado de dispositivos IoT, asi como la aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, deberán sustentarse con documentación públicamente del fabricante, no se aceptará integración con otros componentes ni carta de fabricante para sustentar lo solicitado.	
Firewall Interno (02 Unidades)		
- Deberá tener un rendimiento de Prevención de Amenazas de 110 Gbps cuando opera en simultáneo: Application Control, firewall, IPS, Antivirus/Anti-Bot/Antispyware o 48 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7) teniendo las siguientes funcionalidades habilitadas de manera simultánea: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. La solución debe operar bajo una arquitectura de procesamiento único donde todas las funciones de seguridad se apliquen simultaneamente sobre el mismo flujo de tráfico.	El postor deberá presentar documentación pública del fabricante que sustente el cumplimiento del performance y condiciones de medición requeridas. No se aceptarán cartas de fabricante como sustentos para el cumplimiento del performance y condiciones de medición solicitadas.	
El equipo debe soportar como mínimo 80 millones de sesiones concurrentes medidas con transacciones TCP o 7 millones medidas con transacciones HTTP. El equipo debe soportar 1.2 millones de nuevas sesiones por segundo medidas con transacciones TCP o 370 mil nuevas sesiones por segundo medidas con transacciones HTTP.	El postor deberá presentar documentación pública que sustente expresamente la metodología de medición de sesiones concurrentes y sesiones por segundo utilizada por el fabricante, precisando si corresponde a transacciones TCP (L4) o HTTP (L7). No se aceptarán equivalencias sustentadas mediante cartas de fabricante.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Debe incluir mínimo 8 interfaces de 1G/2.5G/5G/10G RJ-45, 12 interfaces de 1G/10G SFP/ SFP+, 4 interfaces de 25Gbps SFP28 y 4 interfaces de 40G/100GGbps QSFP28.	Las interfaces requeridas deberán encontrarse activas, soportadas y documentadas públicamente por el fabricante. No se aceptarán habilitaciones futuras, roadmap de producto ni cartas de compromiso.	
Capacidad de inspeccionar el contenido en túneles GRE, opcionalmente GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.	Esto deberá encontrarse expresamente documentada en información pública del fabricante.	
Debe incluir capacidades de identificación y perfilado de dispositivos conectados a la red (incluyendo dispositivos IoT/OT), permitiendo su clasificación, evaluación de riesgo y aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, sin requerir la instalación de agentes adicionales.	Las capacidades de identificación y perfilado de dispositivos IoT, así como la aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, deberán sustentarse con documentación públicamente del fabricante, no se aceptará integración con otros componentes ni carta de fabricante para sustentar lo solicitado	
Consola de analítica y reportes		
La solución deberá contar con una plataforma de almacenamiento centralizado de logs de seguridad, que permita la ingesta continua de telemetría sin restricciones por volumen de datos y que incluya una capacidad de retención de logs de al menos un (01) año.	La capacidad de retención de logs requerida deberá estar expresamente sustentada mediante documentación pública y oficial del fabricante, incluyendo las condiciones de licenciamiento y operación correspondientes. No se aceptarán declaraciones comerciales ni cartas de fabricante como sustento único	
Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red.	Las capacidades de evaluación automática de buenas prácticas, gráficas de adopción de los módulos de seguridad y el módulo de filtrado y depuración de reglas deberán ser expresamente sustentadas con información pública y oficial del fabricante	
XDR (Extended Detection & Response) – 1 solución		
La solución deberá ser de tipo XDR (Extended Detection & Response) y permitir la operación centralizada de capacidades de detección, análisis y respuesta para endpoints, formando parte de una plataforma unificada de operaciones de seguridad que integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la	Estas capacidades deberán encontrarse expresamente documentadas en información pública y oficial del fabricante, no se aceptará integración con otros componentes ni carta de fabricante para sustentar lo solicitado	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.		
La solución XDR deberá permitir la integración con la solución SIEM propuesta o formar parte de la misma plataforma, habilitando el envío y consumo de telemetría de seguridad, de forma nativa y estructurada, sin requerir desarrollos personalizados o procesos complejos de normalización, garantizando su uso para correlación, análisis y respuesta automatizada	La capacidad de integración nativa, intercambio estructurado de telemetría y correlación y respuesta automatizada entre la solución XDR y la solución SIEM deberá encontrarse expresamente documentada mediante documentación pública y oficial del fabricante.	
El mismo agente de Endpoint Protectión deberá ser capaz de colectar la siguiente telemetría para equipos MacOS y Linux: • Logs de eventos de autenticación • Actividades de creación, escritura, renombre, eliminación, modificación de archivos. • Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma digital. • Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP). • Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.	Las capacidades de recolección de telemetría continua, almacenamiento estructurado y disponibilidad de telemetría para analítica y threat hunting deberán sustentarse expresamente mediante información pública y oficial del fabricante. No se aceptarán cartas de fabricante, declaraciones juradas ni documentos emitidos específicamente para el presente proceso.	
Con base en el comportamiento aprendido, el módulo de UEBA deberá ser capaz de detectar y alertar actividades inusuales o desviaciones significativas respecto al perfil base establecido. Deberá tener al menos 150 casos de uso nativos, generados por machine learning, incluyendo los siguientes: • Comandos anómalos ejecutados en el endpoint • Múltiples procesos LOLBINs ejecutados • Procesos raros ejecutados sobre el endpoint	Toda capacidad asociada a aprendizaje automático no supervisado, perfiles base, UEBA, modelos analíticos, generación automática de comportamientos y casos de uso nativos deberá sustentarse expresamente mediante documentación pública y oficial del fabricante, en caso no pueda ser verificada bajo dicho criterio, será considerada como no sustentada para fines de evaluación técnica.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
• Eventos de Pass the ticket • Proceso conectándose a un sitio externo inusual • Comandos de powershell inusuales • Cifrado de datos sospechoso en el endpoint • Carga de driver inusual • Conexión anómala usando WMI • Servicio detenido de manera inusual • Tráfico LDAP generado desde un proceso inusual • Transferencia inusual de archivos por SMB		
ZTNA (Zero Trust Network Access) – 01 Solución		
Las políticas de validación de postura del endpoint deberán poder ser aplicadas a un grupo de usuarios o direcciones IP.	Las capacidades de validación de postura de seguridad del endpoint deberán sustentarse mediante documentación pública oficial del fabricante.	
La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada, de manera manual y automática. Los equipos en cuarentena no deberán tener conexión con ningún recurso de red protegido por la solución. Esta capacidad deberá tener cobertura dentro de la red interna, sin necesidad de hacer túneles VPN	Deberá sustentarse mediante documentación pública oficial del fabricante, no se aceptará cartas de fabricante.	
Este navegador web debe permitir el acceso seguro desde dispositivos no gestionados o de terceros, garantizando el aislamiento de la sesión y la protección de la información accedida.	La capacidad de acceso seguro mediante navegador web sin instalación de agentes (agentless), así como los mecanismos de aislamiento y control de acceso asociados, deberán encontrarse debidamente sustentados mediante documentación pública y oficial del fabricante.	
Seguridad para correo electrónico – 01 solución		
El servicio de correo electrónico es Zimbra, por lo que la solución deberá integrarse mediante protocolos SMTP, operando como gateway de correo electrónico a través de registros MX, permitiendo la inspección completa del tráfico entrante y saliente antes de su entrega.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
La solución deberá contar con mecanismos avanzados de protección de URLs que permitan analizar los enlaces contenidos en los correos electrónicos mediante técnicas como reescritura de URLs, evaluación de reputación en tiempo	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
real y análisis dinámico en el momento de interacción del usuario (time-of-click), con el fin de identificar y bloquear enlaces maliciosos antes y después de su entrega al usuario final.		
La solución deberá contar con capacidades de análisis avanzado de archivos adjuntos mediante tecnología de sandboxing, integrada dentro de un modelo de protección multicapa que combine técnicas de análisis estático, reputación, machine learning y análisis dinámico selectivo, permitiendo la detección de amenazas conocidas y desconocidas en archivos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
La solución deberá garantizar que los procesos de análisis de archivos adjuntos se realicen sin alterar su estructura ni contenido original, utilizando mecanismos de análisis seguros como entornos aislados (sandbox) y técnicas de inspección que operen sobre copias del archivo, manteniendo la integridad del contenido original	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
La solución deberá operar mediante un modelo Secure Email Gateway (SEG) en modo inline, integrándose con el servicio de correo mediante registros MX, permitiendo la prevención de amenazas en tránsito antes de la entrega al usuario final.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
WAF - Seguridad para Aplicaciones Web		
Modalidad del Servicio		
Tipo de Despliegue: La solución debe ser entregada bajo la modalidad de Software as a Service (SaaS) basado en la nube.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Licenciamiento		
Mitigación de DDoS en Capa 7: Debe incluir protección nativa contra ataques de denegación de servicio distribuidos dirigidos específicamente a la capa de aplicación (HTTP/HTTPS).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Capacidades de Seguridad		
Protección contra Top 10 de OWASP: Debe mitigar de forma automática amenazas como Inyección SQL, Cross-Site Scripting (XSS), rotura de autenticación, entre otros.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Políticas de Seguridad Positiva y Negativa: Capacidad de combinar firmas de ataque conocidas con modelos de comportamiento para detectar amenazas "Zero-day".	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
SIEM (01 Solución)		
La solución deberá realizar monitoreo, correlación y análisis de eventos de seguridad (SIEM), formando parte de una plataforma unificada de operaciones de seguridad que	Esto deberá sustentarse expresamente mediante documentación pública y oficial del fabricante	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.		
Deberá ser capaz de recolectar y almacenar centralizadamente logs y telemetría de endpoints provenientes de agentes EDR/XDR, ya sean del mismo fabricante o de terceros. El Postor deberá incluir el licenciamiento necesario para habilitar esta capacidad. Se entiende por telemetría no solo las alertas generadas por el EDR/XDR, sino también la actividad detallada del endpoint, incluyendo como mínimo: procesos (creación/árbol/command-line), archivos (creación/modificación/lectura), registro (Windows Registry), sesiones e identidad (logon/logoff), actividad de red (conexiones/DNS), y otros eventos relevantes de seguridad	La capacidad de recolección de telemetría detallada de endpoint y compatibilidad con EDR/XDR de terceros deberá ser sustentada mediante documentación pública oficial del fabricante.	
Deberá tener conectores nativos para más de 1000 plataformas de terceros y ser capaz de normalizar los eventos de manera nativa, sin necesidad de escribir reglas de correlación	Debe sustentarse expresamente mediante documentación pública y oficial del fabricante, no se aceptarán como sustento cartas de fabricante, declaraciones juradas ni documentos emitidos específicamente para el presente proceso.	
Debe contar con al menos 500 casos de uso de detección de amenazas. Todos estos casos de uso deberán estar activados de manera automática, sin necesidad de construir una regla de correlación o afinamiento manual.	La capacidad de analítica para la construcción de línea base, generación de alertas de anomalías y detección de amenazas deberá ser sustentada mediante documentación pública oficial del fabricante.	
Plataforma de Detección y Respuesta de Amenazas Externas e Internas (01 Solución)		
La solución deberá formar parte de una plataforma unificada de operaciones de seguridad que permita complementar estas capacidades con la detección y respuesta de amenazas internas, mediante la integración y correlación de telemetría proveniente de diferentes fuentes de seguridad	Esto deberá sustentarse expresamente mediante documentación pública y oficial del fabricante, no se aceptarán como sustento cartas de fabricante, declaraciones juradas ni documentos emitidos específicamente para el presente proceso.	
Deberá descubrir servicios cloud expuestos a Internet que no estén gestionados y/o no sean conocidos por la Entidad.	Las técnicas de descubrimiento requeridas deberán encontrarse expresamente documentados	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
	mediante información pública oficial del fabricante.	
Deberá permitir administrar los test de escaneo, permitiendo habilitar o deshabilitar los test. Por cada test deberá mostrar información como software afectado, identificadores de vulnerabilidad (CVE/CWE), score de severidad (CVSS), probabilidad de explotación (EPSS), referencias, guía de remediación, estado de habilitación y cantidad de servicios confirmados como vulnerables.	Las capacidades de escaneo solicitadas deberán ser sustentadas mediante mediante documentación pública oficial del fabricante.	
SOAR – Solución de Orquestación de Seguridad, Automatización y Respuesta (01 Solución)		
La solución deberá contar con un catálogo de al menos 800 playbooks predefinidos, orientados a automatizar la respuesta ante incidentes de seguridad. Dichos playbooks deberán poder personalizarse según las necesidades de la Entidad.	La cantidad mínima de playbooks predefinidos y las capacidades de personalización deberán sustentarse mediante información pública y oficial del fabricante. No se aceptarán cartas de fabricante como sustento.	
La solución deberá permitir crear bucles dentro de un playbook principal mediante sub-playbooks, donde cada iteración calcule sus valores usando los datos del sub-playbook	Esto deberá sustentarse expresamente mediante documentación pública y oficial del fabricante, no se aceptarán como sustento cartas de fabricante, declaraciones juradas ni documentos emitidos específicamente para el presente proceso.	
Los playbooks deben poder ser ejecutados como tareas programadas, es decir, sin necesidad de que exista una alerta o incidente de seguridad un playbook puede ejecutarse de manera periódica (permitiendo especificar la periodicidad) para automatizar alguna tarea.	Esto deberá sustentarse expresamente mediante documentación pública y oficial del fabricante, no se aceptarán como sustento cartas de fabricante, declaraciones juradas ni documentos emitidos específicamente para el presente proceso.	
La plataforma deberá ofrecer una interfaz unificada para interactuar con agentes de IA predefinidos y personalizados, capaces de planificar y ejecutar flujos de trabajo de múltiples pasos	Esto deberá sustentarse expresamente mediante documentación pública y oficial del fabricante.	
ADC (application Delivery Controller) (02 Unidades)		
Arquitectura y Capacidad de Hardware		
Chasis Físico: El equipo debe ser un appliance de propósito específico (Hardware-based) con una capacidad física de cómputo (throughput) de hasta 40 Gbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Procesamiento: Debe contar con una arquitectura multi-core optimizada, incluyendo un procesador de al menos 12 núcleos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Rendimiento y Licenciamiento		
Capacidad de Sesiones: Debe soportar un mínimo de 46 millones de conexiones concurrentes en Capa 4.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Transacciones por Segundo: Capacidad para procesar al menos 1.8 millones de peticiones por segundo (RPS) en Capa 7.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Conectividad Física y Escalabilidad		
Puertos de Cobre: Al menos ocho (08) puertos 10/100/1000 Mbps Base-T (RJ45) para gestión y servicios auxiliares.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Puertos de Fibra (Acceso/Agregación): Al menos ocho (08) puertos con soporte nativo para 10 GbE (SFP+).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Puertos de Alta Velocidad (Core): Al menos cuatro (04) puertos con soporte nativo para 25 GbE (SFP28) para interconexión de alta velocidad.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Anti – DDoS (02 Unidades)		
Arquitectura y Componentes de la Solución		
Mecanismo de Bypass: Los puertos de cobre deben contar con un mecanismo de derivación (bypass) físico incorporado para garantizar la continuidad del tráfico en caso de fallo del equipo.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Rendimiento y Performance		
Rendimiento de Mitigación: La solución debe admitir un rendimiento total de inspección y mitigación de hasta 10 Gbps al 100% de la carga.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Latencia Máxima: La inspección del tráfico debe mantener una latencia ultra-baja, no superior a los 70 microsegundos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Capacidades de Detección y Mitigación		
Firmas en Tiempo Real: Capacidad de generar firmas automáticas (Real-Time Signatures) para ataques de día cero en un tiempo inferior a los 15 segundos sin intervención humana.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Licenciamiento y Servicios Críticos		
Cloud Signaling: El licenciamiento debe permitir la comunicación automática entre el equipo on-premise y el centro de inteligencia del fabricante.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Solución de Análisis de Tráfico de Red - (01 Solución)		
Debe contar con una vista de alto nivel del estado de la infraestructura que permita agrupar y explorar dinámicamente nodos, identificando de inmediato los puntos conflictivos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Debe permitir el monitoreo de métricas clave de salud del sistema operativo y rendimiento de	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
aplicaciones mediante protocolos estándar o agentes.		
Debe presentar el rendimiento a nivel de dispositivo y a nivel de puerto/interfaz mediante gráficos de línea y estadísticas de entrada/salida.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
MFA – Administración de Identidad y Acceso (01 Solución)		
La solución se debe basar en algoritmos de aprendizaje de máquina (machine learning) no supervisados. Es decir, los modelos estadísticos con los casos de uso ya deben estar listos y calibrados.	Esta capacidad deberá sustentarse expresamente mediante documentación pública y oficial del fabricante.	
La solución debe ofrecer un componente/software para intermediar el SSO en aplicaciones web que se encuentren en el centro de procesamiento de datos de la entidad, sin necesidad de exponer a estas aplicaciones al uso de internet o de VPN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Soporte para SSO mediante IWA (Integrated Windows Authentication), que reutiliza el login de red para autenticación en las aplicaciones web sin necesidad de ingresar con usuario y contraseña nuevamente	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante, no se aceptarán cartas de fabricante como sustento.	
PAM – Administración de Acceso Privilegiado (01 Solución)		
La solución propuesta deberá tener la capacidad de cifrar, en reposo y en tránsito todos los datos que utilice. Incluyendo contraseñas, reportes almacenados, grabaciones y registros de usuarios. Lo anterior utilizando algoritmos que cumplan con los estándares en FIPS 140-2, como AES-256 y RSA-2048.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
La solución propuesta deberá tener mecanismos de detección y alerta cuando se detecta una desviación en el patrón de comportamiento de un usuario humano al recuperar/obtener un secreto de la bóveda digital o de la plataforma. Esta detección puede indicar un abuso de la plataforma de identidades y la vulnerabilidad o brecha de la identidad del usuario.	La arquitectura de la bóveda digital, incluidas sus capacidades, deberán sustentarse mediante documentación técnica pública y oficial del fabricante.	
La solución debe tener la capacidad de entregar un acceso remoto seguro (externo a la red corporativa) a los usuarios sin necesidad de instalación de clientes VPN en los dispositivos de usuarios remotos y garantizando un acceso seguro con MFA sin necesidad de modificar los recursos de autenticación corporativos como el AD.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
NDR (Network Detection and Response) (01 Solución)		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
El sensor debe ser capaz de recolectar y enviar automáticamente la siguiente telemetría de red: o Logs avanzados o telemetría detallada, es decir eventos que incluyan contenido de la aplicación de red en capa 7, cabecera HTTP, querys de DNS, información del tráfico DHCP y otros datos de la telemetría de red. o Eventos del tráfico mostrando: IP y puerto origen y destino, nombre de la aplicación en capa 7, país origen y destino, IP NAT de origen y destino, usuario de dominio, Bytes enviados y recibidos, Paquetes enviados y recibidos, DNS Querys, información sobre tráfico DHCP. o Nombre, serial number, nombre de la política y/o regla de seguridad de los Firewalls. o Nombre, tipo, categoría y severidad de la amenaza identificada. o Nombre del archivo transferido a través del tráfico de red. o Logs de tráfico URL, detallando URL accedida, categoría, severidad, hora, IP origen/destino, usuario, país de la URL, User-Agent de los paquetes HTTP. o Atributos de los dispositivos de red, tales como tipo de dispositivo, categoría, marca, sistema operativo, fabricante del dispositivo.	Las capacidades de extracción de telemetría, análisis de tráfico y mecanismos utilizados para la obtención de información de red deberán sustentarse mediante información pública oficial del fabricante	
La solución deberá emplear algoritmos avanzados de inteligencia artificial y aprendizaje automático, incluyendo como mínimo Machine Learning supervisado, no supervisado y técnicas de Deep Learning, orientados a la detección de amenazas conocidas y desconocidas	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Sandboxing (01 Solución)		

Característica Técnicas a sustentar de las EETT	**Acreditación documental requerida**	**Documento Sustento que lo acredita / Sustento (Folio Nº)**
Los firewalls deberán ser capaces de enviar 5000 archivos por hora al sandbox.	Esto deberá sustentarse mediante documentación técnica pública y oficial del fabricante, no se aceptará carta de fabricante para el sustento.	
Deberá contar con al menos 20 técnicas patentadas para realizar el análisis del malware.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante	

En ese sentido, me comprometo a entregar el bien con las características, en la forma y detalles especificados.

Ciudad, ……..de …….de……..

_____

Firma y Sello del Representante Legal
Sello del postor/ Razón Social del Proveedor

Nota: *Consignar el número de folio del sustento de la característica técnicas, deberá presentar un formato por cada bien y/o equipo ofertado.*

ANEXO N° 03

Declaración Jurada de Compromiso de Garantía, Soporte y Mantenimiento de los Bienes y Licencias Ofertados

Señores
COMITÉ DE EVALUACIÓN
PROCESO SDO Nº PE-PRONATEL-569321-GO-RFB

Presente. -

El que suscribe, _____, identificado con DNI Nº _____, en calidad de Representante Legal de _____, con RUC Nº _____, declaro bajo juramento que, de resultar adjudicado, mi representada se compromete a otorgar la garantía, soporte y mantenimiento de los bienes, licencias y servicios asociados ofertados, conforme a las condiciones establecidas en las Especificaciones Técnicas de la presente contratación.

La garantía comprenderá la atención de fallas, defectos de fabricación, reemplazo o reparación de componentes, actualización de versiones, parches de seguridad y demás prestaciones requeridas para asegurar la continuidad operativa de la solución implementada durante el período de garantía establecido.

Nº	BIENES / SOLUCIONES	GARANTÍA Y SOPORTE MÍNIMO	ACREDITACIÓN
1	Todos los bienes, equipos, software y soluciones comprendidos en el Lote Único, según corresponda.	Doce (12) meses, 24x7 on-site, con tiempo de respuesta de cuatro (04) horas, más las condiciones particulares establecidas en el Anexo 3 de las EETT.	Declaración Jurada de Compromiso y respaldo del fabricante/canal autorizado cuando corresponda.

Asimismo, declaro que mi representada garantizará:

- La disponibilidad de soporte técnico durante el período establecido en las Especificaciones Técnicas, incluyendo atención bajo modalidad **24x7**, generación de tickets y tiempos de respuesta conforme a los niveles de servicio requeridos.
- La atención de incidencias, mantenimiento preventivo y correctivo, así como la aplicación de actualizaciones y parches de seguridad proporcionados por los fabricantes.
- La continuidad operativa de la solución implementada durante el período de garantía, incluyendo los bienes, licencias, configuraciones e integraciones realizadas como parte del contrato.

La vigencia de la garantía y servicios asociados iniciará a partir de la suscripción del Acta de Aceptación Operativa, cconforme a lo establecido en las Especificaciones Técnicas.

La presente declaración será respaldada, de corresponder, mediante las cartas de garantía, soporte y respaldo emitidas por los fabricantes de los bienes ofertados, conforme a los requisitos establecidos en los Documentos de Licitación.
En señal de conformidad, suscribo la presente declaración.

Nombre del Licitante*:

Nombre de la persona debidamente autorizada para firmar la Oferta en nombre del Licitante**: _____

Cargo de la persona firmante del Formulario de la Oferta: _____

Firma de la persona nombrada anteriormente: _____

Fecha de la firma: El día _____ del mes _____ del año _____.

***** En el caso de las Ofertas presentadas por una APCA, especifique el nombre de la APCA que actúa como Licitante.

** La persona que firme la Oferta deberá contar con el poder otorgado por el Licitante. El poder deberá adjuntarse a los Formularios de la Oferta.

[Nota: En caso de que se trate de una APCA, la Declaración de Mantenimiento de Oferta deberá emitirse en nombre de todos los miembros de la APCA que presenta la Oferta].

Formulario PER – 1
Personal Clave propuesto
Formulario

Los Licitantes deberán suministrar los nombres y otros detalles de las personas clave debidamente calificadas para cumplir con el Contrato. La información sobre su experiencia se deberá consignar utilizando el Formulario PER-2 de los que aparecen más abajo para cada candidato.

Personal Clave

1.	**Título de la posición:** *[insertar título]*	
	Nombre del candidato:	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*
	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*
2.	**Título de la posición:** *[insertar título]*	
	Nombre del candidato:	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*
	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*
3.	**Título de la posición:** *[insertar título]*	
	Nombre del candidato:	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*
	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*
4.	**Título de la posición:** *[insertar título]*	
	Nombre del candidato:	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*

	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*
5	**Título de la posición:** *[insertar título]* *[**Cuando los riesgos EAS de un Proyecto sean sustanciales o altos, el Personal clave debe incluir un especialista** en Explotación Sexual, Abuso y Acoso Sexual **con experiencia pertinente en tratar casos de** en explotación sexual, abuso y acoso sexual]*	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*
	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*
6.	**Título de la posición:** *[insertar título]*	
	Nombre del candidato:	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*
	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*

Formulario PER – 2:
Currículum Vítae del Personal Propuesto

Nombre del Licitante

Cargo ***[#1] [título del puesto según Formulario PER-1]***		
Información personal	**Nombre***	**Fecha de nacimiento**
	Dirección:	**Correo electrónico:**
	Calificaciones profesionales	
	Calificaciones académicas:	
	Conocimiento de idiomas: ***(idiomas y nivel de conversación, lectura y escritura)***	
Detalles		
	Dirección del empleador	
	Teléfono	**Persona de contacto (gerente / funcionario de personal)**
	Fax	
	Denominación del cargo	**Años con el empleador actual**

Resuma la experiencia profesional en orden cronológico inverso. Indique la experiencia particular, técnica y gerencial pertinente para este proyecto.

Proyecto	**Posición**	**Duración**	**Experiencia pertinente**
[principales características del proyecto]	*[posición y responsabilidades en el proyecto]*	*[tiempo en la posición]*	*[describir la experiencia pertinente de esta posición]*

Declaración

Yo, en mi calidad de miembro del personal clave abajo firmante, certifico que, a mi leal saber y entender, la información contenida en este Formulario PER-2 me describe correctamente, así como a mis calificaciones y a mi experiencia.

Confirmo que estoy disponible como certifico en la siguiente tabla y en todo el calendario previsto para esta posición, según lo dispuesto en la Oferta:

Compromiso	**Detalles**
Compromiso con la duración del contrato:	*[Indicar el período (fechas de inicio y de finalización) para el cual este personal clave está disponible para trabajar en este contrato]*
Compromiso de tiempo:	*[Inserte el número de días / semana / meses / que este personal clave será contratado]*

Entiendo que cualquier declaración falsa u omisión en este Formulario puede:

(a) que se tome en consideración durante la evaluación de la Oferta;

(b) causar mi descalificación para participar en la Oferta;

(c) causar mi despido del contrato.

Nombre del personal clave: ***[insertar nombre]***

Firma: _____

Fecha: (día/ mes/ año): _____

Firma del representante autorizado del Licitante:

Firma: _____

Fecha: (día/ mes/ año): _____

ANEXO N° 04

Formulario para Solicitud de Aclaración

SDO Nº PE-PRONATEL-569321-GO-RFB

“Adquisición de Equipamiento Ofimático y de Redes Lan para la Central 911 en el Marco del Proyecto Creación de un Sistema de Atención de Emergencias, Urgencias e Información Mediante un Número Único en Lima Metropolitana y El Callao - Proyecto 911”

LICITANTE:
……

CONSULTA N° 1
Referente a las bases: Sección: Numeral: Página: Consulta:

(i) Puede adicionar más bloques de filas según lo requiera.

Firmada: [firma del representante autorizado]. En capacidad de [indique el cargo]

Nombre: [indique el nombre en letra de molde o mecanografiado]

Debidamente autorizado para firmar la Oferta por y en nombre de: [indique el nombre la entidad que autoriza]

Fechada el [indique el día] día de [indique el mes] de [indique el año]

Declaración de Desempeño sobre Explotación y Abuso Sexual (EAS) y/o Acoso Sexual (ASx)

[El siguiente cuadro debe ser completada por el Licitante y cada miembro de la APCA o JV y cada subcontratista propuesto por el Licitante]

Nombre del Licitante: *[indicar el nombre completo]*
Fecha: *[insertar día, mes, año]*
SDO No. y Título: *[insertar la referencia de la SDO]*
Página *[insertar número de página] de [insertar número total] páginas*

Declaración EAS y /o ASx
Nosotros: ☐ (a) no hemos sido objeto de descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS/ASx. ☐ (b) no estamos sujetos a descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS/ASx ☐ (c) hemos sido descalificados por el Banco por incumplimiento de las obligaciones sobre EAS/ASx pero fuimos excluidos de las empresas descalificadas Se ha dictado un laudo arbitral en el caso de descalificación a nuestro favor.
[Si (c) anterior es aplicable, adjunte evidencia de un laudo arbitral que revierta las conclusiones sobre los problemas subyacentes a la descalificación.]

Formulario de Declaración de Mantenimiento de Oferta

[El Licitante completará este Formulario de Declaración de Mantenimiento de Oferta de acuerdo con las instrucciones indicadas].

Fecha: *[indique día, mes y año de presentación de la oferta]*.
Oferta n.°: *[número del proceso de la SDO]*.
Alternativa n.°: *[indique el n.° de identificación si se trata de una oferta por una alternativa]*.

Para: *[indique el nombre completo del Comprador]*.

Los suscriptos declaramos que:

Entendemos que, de acuerdo con sus condiciones, las Ofertas deberán estar respaldadas por una Declaración de Mantenimiento de Oferta.

Aceptamos que seremos declarados automáticamente inelegibles para participar en cualquier licitación de contrato con el Comprador por un período especificado en la Sección II - Datos de la Licitación (DDL), si incumplimos nuestras obligaciones derivadas de las condiciones de la oferta, a saber:

(a) si retiramos nuestra Oferta antes de la fecha de expiración de la validez de la Oferta especificado en la Carta de la Oferta, o cualquier fecha extendida otorgada por nosotros, o

(b) si, una vez que el Comprador nos ha notificado de la aceptación de nuestra Oferta antes de la fecha de expiración de la validez de la Oferta especificada en la Carta de la Oferta, o cualquier fecha extendida otorgada por nosotros, (i) no firmamos o nos negamos a firmar el Contrato, o (ii) no suministramos o nos negamos a suministrar la Garantía de Cumplimiento de conformidad con las IAL.

Entendemos que esta Declaración de Mantenimiento de Oferta expirará en el caso de que no seamos seleccionados, y (i) si recibimos una notificación con el nombre del Licitante seleccionado, o (ii) han transcurrido 28 días después de la fecha de expiración de la validez de nuestra Oferta, lo que ocurra primero.

Nombre del Licitante*:

Nombre de la persona debidamente autorizada para firmar la Oferta en nombre del Licitante**: _____

Cargo de la persona firmante del Formulario de la Oferta: _____

Firma de la persona nombrada anteriormente: _____

Fecha de la firma: El día _____ del mes _____ del año _____.

***** En el caso de las Ofertas presentadas por una APCA, especifique el nombre de la APCA que actúa como Licitante.

** La persona que firme la Oferta deberá contar con el poder otorgado por el Licitante. El poder deberá adjuntarse a los Formularios de la Oferta.

[Nota: En caso de que se trate de una APCA, la Declaración de Mantenimiento de Oferta deberá emitirse en nombre de todos los miembros de la APCA que presenta la Oferta].

Autorización del Fabricante

[NO APLICA]

[El Licitante solicitará al Fabricante que complete este formulario de acuerdo con las instrucciones indicadas. Esta carta de autorización deberá estar escrita en papel membretado del Fabricante y deberá estar firmada por una persona debidamente autorizada para firmar documentos que comprometan jurídicamente al Fabricante. El Licitante lo deberá incluirá en su Oferta, si así se establece en los DDL].

Fecha: *[indique día, mes y año de presentación de la oferta]*.
SDO n.°: *[Indique el número del proceso de la SDO]*.
Alternativa n.°: *[indique el n.° de identificación si se trata de una oferta por una alternativa]*.

Para: *[indique el nombre completo del Comprador]*.

POR CUANTO

Nosotros *[indique nombre completo del Fabricante]*, como fabricantes oficiales de *[indique el nombre de los bienes fabricados]*, con fábricas ubicadas en *[indique la dirección completa de las fábricas]*, autorizamos mediante el presente a *[indique el nombre completo del Licitante]* a presentar una Oferta con el propósito de suministrar los siguientes Bienes de nuestra fabricación *[nombre y breve descripción de los bienes]*, y a posteriormente negociar y firmar el Contrato.

Por este medio extendemos nuestro aval y plena garantía, conforme a la IAL 28 de las Condiciones Generales del Contrato, respecto de los Bienes ofrecidos por la firma antes mencionada.

Nosotros confirmamos que no hemos incurrido o empleado trabajo forzoso o personas sujetas a trata de personas o trabajo infantil de conformidad con la Cláusula 14 de las Condiciones Generales del Contrato.

Firma: *[indique firma de los representantes autorizados del Fabricante]*.

Nombre: *[indique el nombre completo de los representantes autorizados del Fabricante]*.

Cargo: *[indique el cargo]*.

Fechado el día _____ de _____del año _____ *[fecha de la firma]*.

Sección V. Países Elegibles

Elegibilidad para el suministro de bienes, obras y servicios distintos de los de consultoría en adquisiciones financiadas por el Banco

Con referencia a las IAL 4.8 y 5.1 de las Instrucciones a los Licitantes (IAL), para información de los Licitantes, las firmas, los bienes y los servicios de los siguientes países están excluidos actualmente de participar en este Proceso de Licitación:

En virtud de las IAL 4.8 (a) y 5.1: *"ninguno".*

En virtud de las IAL 4.8 (b) y 5.1: *"ninguno".*

Sección VI. Fraude y Corrupción

(La Sección VI no deberá modificarse)

1. Propósito

1.1 Las Directrices del Banco de Lucha Contra el Fraude y la Corrupción y esta sección se aplicarán a las adquisiciones en el marco de las operaciones de Financiamiento para Proyectos de Inversión del Banco.

2. Requisitos

2.1 El Banco exige que los Prestatarios (incluidos los beneficiarios del financiamiento del Banco), licitantes (postulantes / proponentes) , consultores, contratistas y proveedores, todo subcontratista, subconsultor, prestadores de servicios o proveedores, todo agente (haya sido declarado o no), y todo miembro de su personal, observen las más elevadas normas éticas durante el proceso de adquisición, la selección y la ejecución de contratos financiados por el Banco, y se abstengan de prácticas fraudulentas y corruptas.

2.2 Con ese fin, el Banco:

a. Define de la siguiente manera, a los efectos de esta disposición, las expresiones que se indican a continuación:

i. Por “práctica corrupta” se entiende el ofrecimiento, entrega, aceptación o solicitud directa o indirecta de cualquier cosa de valor con el fin de influir indebidamente en el accionar de otra parte.

ii. Por “práctica fraudulenta” se entiende cualquier acto u omisión, incluida la tergiversación de información, con el que se engañe o se intente engañar en forma deliberada o imprudente a una parte con el fin de obtener un beneficio financiero o de otra índole, o para evadir una obligación.

iii. Por “práctica colusoria” se entiende todo arreglo entre dos o más partes realizado con la intención de alcanzar un propósito ilícito, como el de influir de forma indebida en el accionar de otra parte.

iv. Por “práctica coercitiva” se entiende el perjuicio o daño o la amenaza de causar perjuicio o daño directa o indirectamente a cualquiera de las partes o a sus bienes para influir de forma indebida en su accionar.

v. Por “práctica obstructiva” se entiende:

(a) la destrucción, falsificación, alteración u ocultamiento deliberado de pruebas materiales referidas a una investigación o el acto de dar falsos testimonios a los investigadores para impedir materialmente que el Banco investigue denuncias de prácticas corruptas, fraudulentas, coercitivas o colusorias, o la amenaza, persecución o intimidación de otra parte para evitar

que revele lo que conoce sobre asuntos relacionados con una investigación o lleve a cabo la investigación, o

(b) los actos destinados a impedir materialmente que el Banco ejerza sus derechos de inspección y auditoría establecidos en el párrafo 2.2 e, que figura a continuación.

b. Rechazará toda propuesta de adjudicación si determina que la empresa o persona recomendada para la adjudicación, los miembros de su personal, sus agentes, subconsultores, subcontratistas, prestadores de servicios, proveedores o empleados han participado, directa o indirectamente, en prácticas corruptas, fraudulentas, colusorias, coercitivas u obstructivas para competir por el contrato en cuestión.

c. Además de utilizar los recursos legales establecidos en el convenio legal pertinente, podrá adoptar otras medidas adecuadas, entre ellas declarar que las adquisiciones están viciadas, si determina en cualquier momento que los representantes del prestatario o de un receptor de una parte de los fondos del préstamo participaron en prácticas corruptas, fraudulentas, colusorias, coercitivas u obstructivas durante el proceso de adquisición, o la selección o ejecución del contrato en cuestión, y que el prestatario no tomó medidas oportunas y adecuadas, satisfactorias para el Banco, para abordar dichas prácticas cuando estas ocurrieron, como informar en tiempo y forma a este último al tomar conocimiento de los hechos.

d. Podrá sancionar, conforme a lo establecido en las Directrices del Banco de Lucha Contra la Corrupción y a sus políticas y procedimientos de sanciones vigentes, a cualquier empresa o persona en forma indefinida o durante un período determinado, lo que incluye declarar a dicha empresa o persona inelegibles públicamente para: (i) obtener la adjudicación o recibir cualquier beneficio, ya sea financiero o de otra índole, de un contrato financiado por el Banco[1]; (ii) ser nominada[2] como subcontratista, consultor, fabricante o proveedor, o prestador de servicios de una firma que de lo contrario sería elegible a la cual se le haya adjudicado un contrato financiado por el Banco, y (iii) recibir los fondos de un préstamo del Banco o participar más activamente en la preparación o la ejecución de cualquier proyecto financiado por el Banco.

e. Exigirá que en los documentos de solicitud de ofertas/propuestas y en los contratos financiados con préstamos del Banco se incluya una cláusula en la

---

1 A fin de disipar toda duda al respecto, la inelegibilidad de una parte sancionada en relación con la adjudicación de un contrato implica, entre otras cosas, que la empresa o persona no podrá: (i) presentar una solicitud de precalificación, expresar interés en una consultoría, y participar en una licitación, ya sea directamente o en calidad de subcontratista nominado, consultor nominado, fabricante o proveedor nominado, o prestador de servicios nominado, con respecto a dicho contrato, ni (ii) firmar una enmienda mediante la cual se introduzca una modificación sustancial en cualquier contrato existente.

2 Un subcontratista nominado, consultor nominado, fabricante o proveedor nominado, o prestador de servicios nominado (se utilizan diferentes nombres según el documento de licitación del que se trate) es aquel que: (i) ha sido incluido por el licitante en su solicitud de precalificación u oferta por aportar experiencia y conocimientos técnicos específicos y esenciales que permiten al licitante cumplir con los requisitos de calificación para la oferta particular; o (ii) ha sido designado por el Prestatario.

que se exija que los licitantes (postulantes / proponentes), consultores, contratistas y proveedores, así como sus respectivos subcontratistas, subconsultores, prestadores de servicios, proveedores, agentes y personal, permitan al Banco inspeccionar[3] todas las cuentas, registros y otros documentos referidos a la presentación de ofertas y la ejecución de contratos, y someterlos a la auditoría de profesionales nombrados por este.

[3] Las inspecciones que se llevan a cabo en este contexto suelen ser de carácter investigativo (ej. forense). Consisten en actividades de constatación realizadas por el Banco o por personas nombradas por este para abordar asuntos específicos relativos a las investigaciones/auditorías, como determinar la veracidad de una denuncia de fraude y corrupción a través de los mecanismos adecuados. Dicha actividad incluye, entre otras cosas, acceder a la información y los registros financieros de una empresa o persona, examinarlos y hacer las copias que corresponda; acceder a cualquier otro tipo de documentos, datos o información (ya sea en formato impreso o electrónico) que se considere pertinente para la investigación/auditoría, examinarlos y hacer las copias que corresponda; entrevistar al personal y otras personas; realizar inspecciones físicas y visitas al emplazamiento, y someter la información a la verificación de terceros.

PARTE 2. Requisitos de los Bienes y Servicios Conexos

Sección VII. Requisitos de los Bienes y Servicios Conexos

Índice

1. Lista de Bienes y Cronograma de Entregas 116
2. Lista de servicios conexos y cronograma de cumplimiento…...……..125
3. Especificaciones Técnicas..... 126

1. Lista de bienes y Cronograma de entregas

[El comprador completará este cuadro, excepto la columna "Fecha de entrega ofrecida por el Licitante", la cual será completada por el Licitante].

N.º de artículo	Descripción de los bienes	Cantidad	Unidad física	Lugar de entrega final, según se indica en los DDL	Fecha de entrega[6] (de acuerdo con los Incoterms)		
					Fecha más temprana de entrega	Fecha límite de entrega	Fecha de entrega ofrecida por el licitante *[la proporcionará el Licitante]*
[Indique el n.º].	*[Indique la descripción de los bienes].*	*[Indique la cantidad de los artículos por suministrar].*	*[Indique la unidad física de medida de la cantidad].*	*[Indique el lugar de entrega].*	*[Indique el número de días después de la fecha de entrada en vigor del Contrato].*	*[Indique el número de días después de la fecha de entrada en vigor del Contrato].*	*[Indique el número de días después de la fecha de entrada en vigor del Contrato].*
1	Computadora de Escritorio Tipo 1	210	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
2	Computadora de Escritorio Tipo 2	71	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

[6] El plazo máximo para la entrega de los bienes será de hasta setenta y cinco (75) días calendario contados desde el día siguiente de la firma del Contrato. Los Licitantes podrán ofertar un plazo menor, el cual será considerado como factor de evaluación conforme al Plan de Entregas de los Bienes (IAL 34.6), aplicándose el ajuste económico correspondiente para efectos de comparación de Ofertas, según lo establecido en las Bases de Licitación.

3	Monitor para Computadoras	696	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
4	Teclado y Mouse	281	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
5	Soporte para 03 Monitores para Computadoras de Escritorio Tipo 1	210	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
6	Equipo Portátil	09	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
7	Auricular Monoaural	210	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
8	Micrófono	115	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
9	Altavoces	115	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
10	PPT de pie	210	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

11	Cámara Web	281	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
12	Teléfonos IP Tipo 1	201	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
13	Teléfonos IP Tipo 2	62	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
14	Teléfonos IP Tipo 3	16	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
15	Teléfonos IP Tipo 4	4	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
16	Botonera para teléfono IP 4	1	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
17	Pantalla para Monitoreo	2	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
18	Videoconferencia	4	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

19	Impresora tipo personal	13	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
20	Impresora tipo mediano volumen	5	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
21	Proyector Multimedia	4	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
22	Tabletas Rugerizadas	37	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
23	Switches Spine Data Center	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
24	Switches Leaf Data Center	8	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
25	Solución de Orquestador DC	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
26	Switch Core LAN Campus	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

27	Switch de acceso 48 puertos PoE	23	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
28	Switch de acceso 24 puertos PoE	4	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
29	Switch DMZ	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
30	Switch de Gestión Fuera de Banda	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
31	Controlador inalámbrico	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
32	Access Point	47	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
33	Solución de Administración y Gestión Campus	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
34	Solución de Control de Acceso	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

35	Hardware de Hiperconvergencia	4	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
36	Software Hiperconvergencia	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
37	Servidor para backup	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
38	Servidor de inmutabilidad	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
39	Almacenamiento para backup	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
40	Librería de backup	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
41	Software de backup	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
42	Firewall NGFW (Perimetral)	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

43	Firewall Interno	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
44	Consola de analítica y reportes	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
45	XDR (Extended Detection & Response)	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
46	ZTNA (Zero Trust Network Access)	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
47	Seguridad para correo electronico	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
48	WAF - Seguridad para Aplicaciones Web	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
49	SIEM	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
50	Plataforma de detección y respuesta de amenazas externas e internas	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
52	ADC (application Delivery Controller)	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
53	Anti - DDos	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
54	MFA - Administración de identidad y acceso	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
55	PAM - Administración de acceso privilegiado	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
56	NDR (Network Detection and Response)	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
57	Sandboxing	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
58	Solución de Análisis de Tráfico de Red	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

2. Lista de servicios conexos y cronograma de cumplimiento

Servicio	Descripción del servicio	Cantidad[1]	Unidad física	Lugar donde los servicios serán prestados	Fecha(s) final(es) de ejecución de los servicios
[Indique el n.º del servicio].	*[Indique descripción de los servicios conexos].*	*[Indique la cantidad de rubros de servicios por proveer].*	*[Indique la unidad física de medida de los rubros de servicios].*	*[Indique el nombre del lugar].*	*[Indique la(s) fecha(s) de entrega requerida(s)].*
1	Servicio de implementación (instalación, configuración, pruebas y comisionamiento)	1	Servicios	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta noventa (90) días calendario para la implementación integral de la solución, incluyendo instalación, configuración, integración, pruebas y puesta en operación, contabilizados a partir del día siguiente de la suscripción del Contrato.
2	Mesa de Servicio	12	Meses	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	12 meses, contabilizado a partir del dia siguiente de la aceptacion operativa.
3	SOC	12	Meses	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	12 meses, contabilizado a partir del dia siguiente de la aceptacion operativa.
4	Garantía y Soporte de los Bienes	12	Meses	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	12 meses, contabilizado a partir del dia siguiente de la aceptacion operativa.

3. Especificaciones Técnicas



"Año de la Esperanza y el Fortalecimiento de la Democracia"

ADQUISICIÓN DE EQUIPAMIENTO OFIMÁTICO Y DE REDES LAN PARA LA CENTRAL 911 EN EL MARCO DEL PROYECTO CREACIÓN DE UN SISTEMA DE ATENCIÓN DE EMERGENCIAS, URGENCIAS E INFORMACIÓN MEDIANTE UN NÚMERO ÚNICO EN LIMA METROPOLITANA Y EL CALLAO – PROYECTO 911





Índice

1. Marco General ... 3
1.1. Base Normativa ... 3
1.2. Objetivo de la Contratación ... 3
1.3. Glosario de Términos ... 4
1.4. Información General ... 5
2. Alcance, Descripción de la Solución y Arquitectura Tecnológica ... 8
2.1. Equipamiento Ofimático ... 10
2.2. Red LAN ... 13
3. Soporte y Ciberseguridad ... 20
3.1. Mesa de Servicio ... 20
3.2. SOC ... 24
4. Implementación, Planificación y Gestión del Proyecto ... 32
4.1. Gestión del Proyecto ... 32
4.2. Personal Clave para la gestión ... 32
4.3. Personal clave para la Implementación. ... 33
4.4. Personal Clave para la administración de las soluciones tecnológicas durante el periodo de soporte y garantía. ... 34
4.5. Personal Clave para el soporte a usuario final durante el periodo de soporte y garantía ... 35
4.6. Personal NO Clave ... 35
4.7. Implementación ... 35
4.8. Aceptación Operativa ... 35
4.9. Recursos y Servicios para entregar por el Comprador ... 36
4.10. Gestión de Activos ... 36
4.11. Embalaje y/o Rotulado ... 36
4.12. Salud y Seguridad ... 36
4.13. Logistica y Control ... 36
4.14. Acreditación y Control de Acceso ... 37
4.15. Integraciones ... 37
4.16. Entrenamiento Técnico ... 37
4.17. Lugar y Plazo de Entrega ... 37
ANEXO 1 – CARACTERÍSTICAS TECNICAS ... 39
ANEXO 2 – DIAGRAMA TOPOLOGICO ... 123
ANEXO 3 – GARANTÍA Y SOPORTE DE LOS BIENES ... 124
ANEXO 4 – ACCESORIOS / CONSUMIBLES ... 126

1. Marco General

El Proyecto de implementación de la Central de Atención y Gestión de Emergencias 911 constituye una iniciativa estratégica del Estado Peruano, orientada a garantizar la atención oportuna, continua y coordinada de emergencias para Lima Metropolitana y el Callao. Dada la naturaleza crítica del servicio, la Central 911 ha sido concebida para operar de manera ininterrumpida (24x7x365), incluso ante escenarios de desastre, lo que exige una infraestructura tecnológica altamente disponible, resiliente, segura y escalable.

El Edificio de la Central 911 ha sido diseñado bajo estándares de misión crítica, incorporando redundancia en energía, comunicaciones, climatización y estabilidad estructural, así como un Centro de Datos y sistemas tecnológicos especializados. En este contexto, la experiencia en proyectos similares y los análisis técnicos realizados evidencian que la confiabilidad del servicio depende directamente de contar con una red LAN moderna y equipamiento informático adecuadamente dimensionados, capaces de soportar plataformas críticas como el sistema SAGE, videovigilancia, radiocomunicaciones, telecomunicaciones, hiperconvergencia y ciberseguridad avanzada.

Asimismo, la complejidad del ecosistema tecnológico, la necesidad de integración con múltiples soluciones provistas por terceros y el cumplimiento de principios de seguridad como Zero Trust, hacen indispensable establecer especificaciones técnicas claras, homogéneas y verificables. La ausencia de estos lineamientos podría generar riesgos de indisponibilidad, vulnerabilidades de seguridad, sobrecostos operativos y afectación directa a la continuidad del servicio de atención de emergencias.

En virtud de lo expuesto, las presentes Especificaciones Técnicas se sustentan en la criticidad del servicio 911, en los antecedentes técnicos del proyecto y en la necesidad de garantizar una plataforma tecnológica confiable, segura y sostenible, que asegure la correcta implementación, operación y transferencia de las soluciones tecnológicas que soportan la atención de emergencias a nivel metropolitano.

1.1. Base Normativa

- Contrato de Préstamo Nº 9039-PE, para el Financiamiento del Proyecto 911, suscrito el 16 de julio de 2020 entre el Banco Internacional de Reconstrucción y Fomento y la Republica del Perú.
- Regulaciones de Adquisiciones para prestatarios de Inversión: Bienes, Obras, Servicios de No consultoría y Servicios de Consultoría, julio 2016, Revisión noviembre 2017 y agosto 2018 aprobado por Resolución Ejecutiva N° 097-2020-MTC/24 y sus modificatorias.
- Manual de Operaciones, disposiciones para la ejecución del Proyecto 911
- Resolución Ministerial Nº 0311-2020-MTC/01.03, que aprueba el Manual de Operaciones del Programa Nacional de Telecomunicaciones – PRONATEL.

1.2. Objetivo de la Contratación

El objetivo de la presente contratación es adquirir e implementar de manera integral el equipamiento ofimático y la red LAN de la Central de Atención y Gestión de Emergencias 911, garantizando una infraestructura tecnológica de misión crítica, segura, altamente disponible y escalable, que asegure la operación continua 24x7x365 de los sistemas y servicios esenciales de atención de emergencias, su correcta integración con las plataformas existentes y el cumplimiento de los estándares técnicos y normativos aplicables.

1. Marco General

El Proyecto de implementación de la Central de Atención y Gestión de Emergencias 911 constituye una iniciativa estratégica del Estado Peruano, orientada a garantizar la atención oportuna, continua y coordinada de emergencias para Lima Metropolitana y el Callao. Dada la naturaleza crítica del servicio, la Central 911 ha sido concebida para operar de manera ininterrumpida (24x7x365), incluso ante escenarios de desastre, lo que exige una infraestructura tecnológica altamente disponible, resiliente, segura y escalable.

El Edificio de la Central 911 ha sido diseñado bajo estándares de misión crítica, incorporando redundancia en energía, comunicaciones, climatización y estabilidad estructural, así como un Centro de Datos y sistemas tecnológicos especializados. En este contexto, la experiencia en proyectos similares y los análisis técnicos realizados evidencian que la confiabilidad del servicio depende directamente de contar con una red LAN moderna y equipamiento informático adecuadamente dimensionados, capaces de soportar plataformas críticas como el sistema SAGE, videovigilancia, radiocomunicaciones, telecomunicaciones, hiperconvergencia y ciberseguridad avanzada.

Asimismo, la complejidad del ecosistema tecnológico, la necesidad de integración con múltiples soluciones provistas por terceros y el cumplimiento de principios de seguridad como Zero Trust, hacen indispensable establecer especificaciones técnicas claras, homogéneas y verificables. La ausencia de estos lineamientos podría generar riesgos de indisponibilidad, vulnerabilidades de seguridad, sobrecostos operativos y afectación directa a la continuidad del servicio de atención de emergencias.

En virtud de lo expuesto, las presentes Especificaciones Técnicas se sustentan en la criticidad del servicio 911, en los antecedentes técnicos del proyecto y en la necesidad de garantizar una plataforma tecnológica confiable, segura y sostenible, que asegure la correcta implementación, operación y transferencia de las soluciones tecnológicas que soportan la atención de emergencias a nivel metropolitano.

1.1. Base Normativa

- Contrato de Préstamo N° 9039-PE, para el Financiamiento del Proyecto 911, suscrito el 16 de julio de 2020 entre el Banco Internacional de Reconstrucción y Fomento y la Republica del Perú.
- Regulaciones de Adquisiciones para prestatarios de Inversión: Bienes, Obras, Servicios de No consultoría y Servicios de Consultoría, julio 2016, Revisión noviembre 2017 y agosto 2018 aprobado por Resolución Ejecutiva N° 097-2020-MTC/24 y sus modificatorias.
- Manual de Operaciones, disposiciones para la ejecución del Proyecto 911
- Resolución Ministerial Nº 0311-2020-MTC/01.03, que aprueba el Manual de Operaciones del Programa Nacional de Telecomunicaciones – PRONATEL.

1.2. Objetivo de la Contratación

El objetivo de la presente contratación es adquirir e implementar de manera integral el equipamiento ofimático y la red LAN de la Central de Atención y Gestión de Emergencias 911, garantizando una infraestructura tecnológica de misión crítica, segura, altamente disponible y escalable, que asegure la operación continua 24x7x365 de los sistemas y servicios esenciales de atención de emergencias, su correcta integración con las plataformas existentes y el cumplimiento de los estándares técnicos y normativos aplicables.

1.3. Glosario de Términos

A continuación, se lista el glosario de términos que permitirán el entendimiento de aspectos particulares para tener en cuenta para la lectura del presente requerimiento técnico:

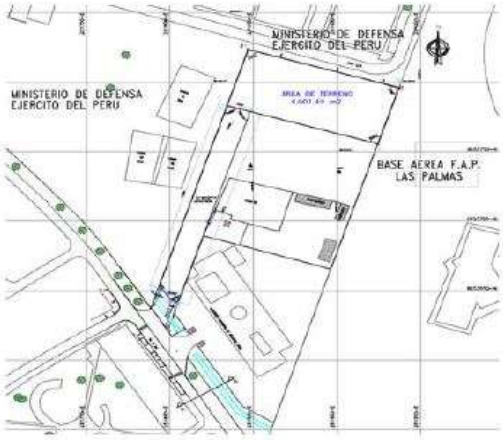
- **Centro de Atención de Llamadas:** Es un área donde operadores, reguladores, despachadores, supervisores o ejecutivos, especializados en servicio al usuario, realizan o reciben llamadas desde o hacia las personas (ciudadanía) u otras entidades.
- **Comprador**: Es la Entidad Contratante, Programa Nacional de Telecomunicaciones.
- **Contratista Obra:** Es la empresa constructora del edificio de la Central 911.
- **Despachador:** Personal de una entidad de primera respuesta – EPR, encargado de asignar los recursos necesarios, coordinar, dar seguimiento y soporte para la atención eficiente y oportuna de una emergencia o urgencia.
- **Edificio de la Central 911:** Esta locación es el sitio donde se realizará la implementación del presente requerimiento, y está ubicada en Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.
- **EPR:** Conjunto de las Entidades de Primer Respuesta (PNP, SAMU y Bomberos).
- **Implementación:** Hace referencia a la instalación, configuración, pruebas individuales y pruebas integrales que realizará el proveedor del presente requerimiento.
- **Línea 100:** Servicio especializado en atención telefónica gratuita a nivel nacional que tiene como finalidad brindar información, orientación, consejería y soporte emocional a las personas afectadas o involucradas en hechos de violencia familiar o sexual y a quienes conozcan sobre algún caso de maltrato en su entorno.
- **Médico Regulador:** Médico capacitado y entrenado en la atención prehospitalario, encargado del triaje telefónico, clasificará las prioridades de la atención médica y discriminará el uso de recursos para la atención (envío de ambulancia para prioridad I y II, y/o la asistencia médica en las prioridades III y IV).
- **Operador Telefónico:** Profesional que trabaja en un centro de atención telefónica que se encarga de atender y recibir las llamadas de los ciudadanos que marcan a la línea de emergencia, está encargado de determinar la pertinencia de la llamada.
- **Proveedor:** Es la empresa que se adjudique el presente requerimiento.
- **Proveedor SAGE:** Es la empresa que provee el software SAGE, que incluye hardware y software dedicado de la solución del SAGE.
- **Proveedor Servicios de Telecomunicaciones:** Es la empresa que provee los servicios de telecomunicaciones a la Central 911 (Servicio de Internet, Servicio de Telefonía fija y Servicios de Enlaces Dedicados).
- **Proveedor de Solución TETRA:** Es la empresa que provee la solución de TETRA en el Edificio de la Central 911.
- **SAGE:** El Sistema de Atención y Gestión de Emergencias – SAGE, es componente fundamental de la plataforma tecnológica y como sistema informático, está compuesto entre otros, por un sistema de despacho asistido por computadora (CAD- Computer-Aided Dispatch), un sistema de comunicaciones, sistema de geolocalización, sistema de información geográfica, entre otros sistemas, que permiten la atención centralizada y despacho descentralizado de emergencias, urgencias e información; que integra servicios como la geolocalización de las llamadas, la gestión de los recursos para la asistencia, la integración de las cámaras de vigilancia, la integración de las comunicaciones de radio, telefonía celular y analógica y el completo registro de la información (audio y video) generada como consecuencia de la atención.
- **Supervisor Obra:** Es la empresa especializada y dedicada a la Supervisión de las actividades del Contratista de Obra.
- **Spare:** Contingencia en bienes.
- **Gerente de Proyectos:** Será asignado por el comprador, y será el responsable de dirigir, coordinar y controlar la implementación del presente requerimiento en la Central 911, asegurando que los componentes de infraestructura, comunicaciones, plataformas, servicios TI, integración de sistemas y soporte operativo se ejecuten conforme al alcance, cronograma, calidad, seguridad y objetivos institucionales definidos en el presente requerimiento.

1.4. Información General

Edificio de la Central 911

Con la finalidad de contextualizar el proyecto general se describe que el Edificio de la Central 911 se ubica en la Avenida el Sol S/N, Distrito de Chorrillos, Provincia y departamento de Lima, con un área de 4,001.49 m2. Tiene los siguientes linderos y medida perimétricas:

- Por el Norte con Ministerio de Defensa Ejercito del Perú con 94.50 ml.
- Por el Oeste con la Ministerio de Defensa Ejercito del Perú con 41.99 ml.
- Por el Sur con la pista de acceso y terreno de INDECI con 94.50 ml.
- Por el este con la Base Aérea de Las Palmas con 42.70 ml.



El edificio tiene la función de estar operativo durante las 24 horas del día los 365 días del año, incluso cuando haya habido un evento devastador en la ciudad. Por lo tanto, tiene redundancia de servicios de comunicaciones, energía y abastecimiento de agua y desagüe, como también una estabilidad estructural a prueba de sismos de gran magnitud, por lo que cuenta con aisladores sísmicos.

La función principal del edificio es albergar al personal que reciba las llamadas de emergencia y éstas, luego de ser verificadas, serán canalizadas a las Entidades de Primera Respuesta (EPR) como la Policía Nacional, los Bomberos, el SAMU y la Línea 100, quienes se encargarán de darle solución a las diferentes emergencias.

El edificio se ha distribuido en un sótano y tres pisos distribuido de la siguiente manera:

Sótano:

Se accede desde la pista de acceso por una rampa al nivel -3.75 y cuenta con 48 estacionamientos de autos (incluyendo 2 para discapacitados), 2 ambulancias, 1 estacionamiento para descarga de materiales, 1 estacionamiento para un vehículo de abastecimiento a la cocina y estacionamientos para 16 motos y 20 bicicletas se ha considerado también una toma de energía para la carga de 2 unidades de autos eléctricos.

Cuenta con una Subestación Eléctrica y Área para Tableros, un Área para Grupos Electrógenos (3), Depósito General, Cuarto de Comunicaciones, Cuarto de Sistema Ininterrumpido, Área de mantenimiento con Baño, Área de Soporte Técnico, Camerinos para hombres y mujeres destinado a los ciclistas, 2 baños, un

depósito y un área para lavar las camillas que está destinado para las ambulancias del SAMU, Cuarto de basura, Cuarto para desechos eléctricos (RAEE), Ductos de Comunicaciones 1 y 2, Cuarto y Ducto Eléctrico y Hall de ascensores y escalera. También se ubica un área de camerinos y baños para el personal de la cocina con montacargas para abastecimiento de esta y una escalera de escape.

En el mismo nivel, pero ingresando desde el primer piso del estacionamiento de personalidades se encuentran las Cisternas de Consumo Humano divididas en 2, con dotaciones que permiten el uso ininterrumpido del edificio en caso de un desabastecimiento, un Cuarto de Bombas para 2 grupos de bombas de presión constante y una motobomba contra incendios y una Cisterna de Agua Contra Incendio.

Bajo el nivel de sótano se encuentra la cimentación del edificio, la cual está dotada de aisladores sísmicos que deben ser monitoreados permanentemente y al cual se accede mediante las trincheras que se encuentran alrededor del edificio, en este nivel se ha ubicado un ambiente para un acelerografo. Estas trincheras tendrán un tratamiento paisajístico con muros verdes dotadas de especies con poca necesidad de agua para generar vistas agradables a los ambientes que tiene acceso a ellas.

El aforo permanente de este piso son 6 personas.

Primer Piso:

En el Primer Piso se ubica una Garita de control vehicular y peatonal, el Ingreso Vehicular se realiza a través de una rampa y el Ingreso Peatonal accede a una plaza interior que da acceso al Lobby, en donde se encuentra la Recepción y el Hall Principal de ascensores que lleva a los diferentes niveles. En este nivel también se encuentra un Ingreso Vehicular desde la Base Aérea de las Palmas dejando un pase también al Terreno del futuro Proyecto del Edificio de Defensa Civil destinado a personalidades VIP, las cuales tienen la misión de tomar las decisiones en caso de emergencia. Este acceso está destinado a 10 vehículos.

Por otro lado, se encuentra el Data Center como el ambiente técnico más importante del proyecto y el cual debe garantizar el funcionamiento del edificio en caso de un desastre, este ambiente tiene un piso técnico de 45 cm.

También se encuentran ambientes como la sala de prensa, la cual tiene conexión a la Plaza de acceso, el Salón de Usos Múltiples, el cual se puede dividir en 3 salones menores mediante tabiques acústicos móviles, para capacitaciones o reuniones y un área de ampliación destinada a la PNP. Frente a ellos se encuentra la Cafetería con capacidad para 120 personas la cual tendrá vista hacia un muro verde y la cocina.

Todas estas áreas están complementadas con un Tópico, un Lactario y los Servicios Higiénicos para hombres y mujeres, así como Servicios higiénicos para discapacitados y Cuarto de Limpieza.

También se ubican 2 Ductos de Comunicaciones y 2 Cuartos Eléctricos, ubicados en el mismo lugar en todos los pisos para poder distribuir flexiblemente y con seguridad las instalaciones de comunicaciones y energía y un segundo ambiente para un acelerógrafo.

Finalmente, en este nivel también se encuentra la Sala de Control y Monitoreo con baño.

El aforo de esta planta es de 354 personas.

Segundo Piso:
En el Segundo nivel se encuentran las Salas de Operadores (90 personas) y Despachadores de las Entidades de Primera Respuesta (EPR) como la Policía Nacional (40 personas), el Cuerpo de Bomberos (15 personas) y el SAMU (30 personas) así como la Línea 100 (15 personas), a las cuales se accede desde una esclusa de doble altura con una escalera helicoidal que relaciona funcional y espacialmente los ambientes del segundo y tercer piso. La sala de Despachadores tiene un techo escalonado para mantener las alturas máximas que establece el estudio aeronáutico exigido para el lote. Toda el área se ha diseñado con una gran integración visual entre los ambientes mediante tabiquerías de vidrio debido a la gran interacción entre el personal de esta área que demanda una coordinación constante.

El área de operadores y despachadores cuenta con un piso técnico de 30 cm de manera de ofrecer flexibilidad en las distribuciones de ellos puestos de trabajo debido a la gran cantidad de cables que se necesitan ya que cada puesto de trabajo deberá contar con redundancia en el suministro de datos y energía.

En este nivel también se encuentra la Sala de Descanso 1, la cual consta de un área para lockers, 7 dormitorios con 2 camarotes cada uno (pudiendo albergar 1 más cada 1) incluyendo uno de ellos habilitado para recibir personas con discapacidad, vestuarios para hombres y mujeres, así como el área propiamente de descanso con kitchenette.

Finalmente se ubican también tres módulos de Baños para hombres, mujeres, discapacitados y Cuarto de Limpieza, así como 2 Ductos de Comunicaciones y 2 Cuartos Eléctricos.

El aforo total de este piso es de 205 personas.

Tercer Piso:
En el Tercer nivel se encuentran la Sala de Crisis, la cual tiene contacto visual con la doble altura de la Sala de Operadores y su Video Wall para una mejor comunicación. A ellas se accede desde la esclusa de doble altura que relaciona espacialmente los ambientes mediante una escalera, también se accede desde el vestíbulo de ascensores. En este piso se ubica una sala para el Cuerpo de Bomberos y una sala para la Policía Nacional, así como un área de mesa de ayuda y un área para oficina de SAMU con depósito y dos terrazas, la cual permite el ingreso de iluminación a la doble altura reforzando la iluminación natural.

En este nivel también se encuentra el Área Administrativa con Archivo, la Alta Dirección, la Sala de Descanso 2 y el Cuarto de radiocomunicaciones.

Finalmente se ubican también un módulo de Baños para hombres, mujeres, discapacitados y Cuarto de limpieza.

El aforo total de este piso es de 81 personas.

Azotea:
En este nivel se considera el acceso desde la escalera de evacuación, los ductos de comunicaciones y energía, ductos de ventilación, un ambiente para la ubicación de un acelerógrafo, los equipos de aire acondicionado de precisión de la data Center los equipos de aire acondicionado del Edificio (Chillers), así como un cuarto para los equipos de radiocomunicaciones y una torre de radiocomunicaciones.

2. Alcance, Descripción de la Solución y Arquitectura Tecnológica

La presente contratación tiene por objeto la adquisición, suministro, entrega, instalación (cuando corresponda) y puesta en funcionamiento de equipamiento tecnológico, agrupados por especialidad:

- Equipamiento Ofimático
- Equipamiento para la Red LAN

Cuadro Nro. 01 – Lista total del equipamiento

Nro	Bienes Equipamiento Ofimático	Cantidad	Spare	Cantidad Total (*) (**)
1	Computadora de Escritorio Tipo 1	198	12	210
2	Computadora de Escritorio Tipo 2	70	1	71
3	Monitor para Computadoras	664	32	696
4	Teclado y Mouse	268	13	281
5	Soporte para 03 Monitores Computadoras de Escritorio Tipo 1	198	12	210
6	Equipo Portátil	8	1	9
7	Auricular Monoaural	198	12	210
8	Micrófono	108	7	115
9	Altavoces	108	7	115
10	PPT de pie	198	12	210
11	Cámara Web	268	13	281
12	Teléfonos IP Tipo 1	190	11	201
13	Teléfonos IP Tipo 2	60	2	62
14	Teléfonos IP Tipo 3	14	2	16
15	Teléfonos IP Tipo 4	2	2	4
16	Botonera para teléfono IP 4	1	0	1
17	Pantalla para Monitoreo	2	0	2
18	Videoconferencia	4	0	4
19	Impresora tipo personal	13	0	13
20	Impresora tipo mediano volumen	5	0	5
21	Proyector Multimedia	4	0	4
22	Tabletas Rugerizadas	35	2	37
Nro	**Bienes Equipamiento Red LAN**	**Cantidad**	**Spare**	**Cantidad Total (*) (**)**
23	Switches Spine Data Center	2	0	2
24	Switches Leaf Data Center	8	0	8
25	Solución de Orquestador DC	1	0	1
26	Switch Core LAN Campus	2	0	2
27	Switch de acceso 48 puertos PoE	22	1	23
28	Switch de acceso 24 puertos PoE	4	0	4
29	Switch DMZ	2	0	2
30	Switch de Gestión Fuera de Banda	2	0	2
31	Controlador inalámbrico	2	0	2
32	Access Point	43	4	47
33	Solución de Administración y Gestión Campus	1	0	1
34	Solución de Control de Acceso	1	0	1
35	Hardware de Hiperconvergencia	4	0	4
36	Software Hiperconvergencia	1	0	1
37	Servidor para backup	1	0	1
38	Servidor de inmutabilidad	1	0	1
39	Almacenamiento para backup	1	0	1
40	Librería de backup	1	0	1
41	Software de backup	1	0	1
42	Firewall NGFW (Perimetral)	2	0	2
43	Firewall Interno	2	0	2

44	Consola de analítica y reportes	1	0	1
45	XDR (Extended Detection & Response)	1	0	1
46	ZTNA (Zero Trust Network Access)	1	0	1
47	Seguridad para correo electronico	1	0	1
48	WAF - Seguridad para Aplicaciones Web	1	0	1
49	SIEM	1	0	1
50	Plataforma de detección y respuesta de amenazas externas e internas	1	0	1
51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	1	0	1
52	ADC (application Delivery Controller)	2	0	2
53	Anti - DDos	2	0	2
54	MFA - Administración de identidad y acceso	1	0	1
55	PAM - Administración de acceso privilegiado	1	0	1
56	NDR (Network Detection and Response)	1	0	1
57	Sandboxing	1	0	1
58	Solución de Análisis de Tráfico de Red	1	0	1

(*) Las cantidades totales, incluyen las unidades operativas y de spare, según corresponda.
(**) Todos los bienes a suministrar, incluido los spare, deben incluir sus accesorios o elementos necesarios para la instalación, interconexión y puesta en operación, tales como tranceivers, cables de energía, ventiladores entre otros necesarios para su puesta en operación de forma integral.

Para la presentación de propuestas, los postores deberán adjuntar una relación de los bienes ofertados, indicando: marca, modelo y año de fabricación.

Los bienes propuestos no deberán ingresar en condición de "fuera de soporte" ni "fin de vida" (End of Support / End of Life) durante los próximos cinco (5) años, contados a partir de la fecha de presentación de propuestas. Para acreditar lo anterior, el postor deberá presentar una carta emitida por el fabricante como sustento.

Para la implementación, el Proveedor deberá presentar un matriz de cumplimiento de cada una de las características técnicas del Anexo 1, la cual será revisada y aprobada por el equipo de implementación del Contratante. En caso alguna de las características no cumpla, esta será rechazada, por lo que Proveedor será responsable de reemplazar con un bien que si cumpla. El retraso que generé esto será de responsabilidad única y exclusiva del Proveedor.

A continuación, se realiza la descripción general de los bienes que conforman el presente requerimiento con el desagregado de cantidades de spare. El detalle de las características técnicas se describe en el Anexo 1 del presente documento.

2.1. Equipamiento Ofimático

A continuación, se describe de forma general todos los bienes, accesorios, y otros que forman parte del presente requerimiento referente al equipamiento ofimático a proveer.

Cuadro Nro. 02 – Lista total del equipamiento Ofimático

Nro	Bien	Cantidad	Spare	Cantidad Total
1	Computadora de Escritorio Tipo 1	198	12	210
2	Computadora de Escritorio Tipo 2	70	1	71
3	Monitor para Computadoras	664	32	696
4	Teclado y Mouse	268	13	281
5	Soporte para 03 Monitores para Computadoras de Escritorio Tipo 1	198	12	210
6	Equipo Portátil	8	1	9
7	Auricular Monoaural	198	12	210
8	Micrófono	108	7	115
9	Altavoces	108	7	115
10	PPT de pie	198	12	210
11	Cámara Web	268	13	281
12	Teléfonos IP Tipo 1	190	11	201
13	Teléfonos IP Tipo 2	60	2	62
14	Teléfonos IP Tipo 3	14	2	16
15	Teléfonos IP Tipo 4	2	2	4
16	Botonera para teléfono IP 4	1	0	1
17	Pantalla para Monitoreo	2	0	2
18	Videoconferencia	4	0	4
19	Impresora tipo personal	13	0	13
20	Impresora tipo mediano volumen	5	0	5
21	Proyector Multimedia	4	0	4
22	Tabletas Rugerizadas	35	2	37

2.1.1. Estaciones de Trabajo

Los equipos de cómputo serán dotados para las posiciones operativas y administrativas de la Central 911, conforme a la distribución definida por ambientes y turnos establecidos, asegurando un estándar homogéneo de configuración, continuidad operativa y soporte.

Todas las estaciones de trabajo serán aprovisionadas con una imagen base institucional, debidamente configuradas y agregadas a un dominio de red, con las aplicaciones autorizadas para operación (CAD, GIS, radiocomunicación, video y herramientas complementarias), y con endurecimiento (hardening) acorde a lineamientos de seguridad para puestos de operadores, despachadores y supervisores que se entregarán al Proveedor durante la implementación.

La preparación de los equipos comprende como mínimo lo siguiente:

- Configuración estándar (imagen base), inventario y etiquetado patrimonial.
- Unión a dominio, políticas de seguridad (GPO), control de privilegios y actualización.
- Lista de software base y parámetros de hardening entregados para despliegue y auditoría.
- Preparado para soporte 24x7 (mesa de ayuda, reposición y mantenimiento).
- Redundancia con doble tarjeta de red.

Computadoras de Escritorio Tipo 1 y 2

Se han definido dos tipos de computadora, de acuerdo a los perfiles del personal de la Central 911. Las cuales deberán considerar su accesorios generales y soporte para monitores, según el tipo de computadora. Para las computadoras tipo 1 se ha

considerado 03 monitores con su soporte para estos, mientras que las computadoras tipo 2 no se considera el componente de soporte. Las características técnicas se detallan en el Anexo 1 del presente documento, siendo las cantidades resumidas en el siguiente cuadro:

Cuadro Nro. 03

Nro	Tipo del componente	Cantidad	Spare	Total
1	Computadora de Escritorio Tipo 1	198	12	210
2	Computadora de Escritorio Tipo 2	70	1	71
3	Monitor para Computadoras	664	32	696
4	Teclado y Mouse	268	13	281
5	Soporte para 03 Monitores para Computadoras de Escritorio Tipo 1	198	12	210

Computadoras Portátiles

Como parte del parque informático, también se ha definido equipamiento portátil, siendo lo requerido un total de 09 unidades. Las características técnicas se detallan en el Anexo 1 del presente documento.

2.1.2. Periféricos Especializados

Componentes críticos de las posiciones operativas para asegurar la operación continua 24x7 de la Central 911, orientados a la atención de emergencias y a la integración con los módulos de CAD, GIS y radiocomunicación. Los periféricos especializados son: cámaras web, interruptores PTT (Push-To-Talk), micrófonos, altavoces y auriculares monoaurales, los cuales deberán ser compatibles con las estaciones de trabajo y plataformas de comunicaciones, contar con controladores estables y garantía local, para facilitar soporte, reposición y continuidad operativa.

La preparación de los periféricos comprende como mínimo lo siguiente:

- Instalación integral de los componentes periféricos.
- Compatibilidad técnica con estaciones, puertos y aplicaciones (audio/video/Radio).
- Calidad y confiabilidad para uso intensivo por turnos (misión crítica).
- Estandarización para reducir fallas recurrentes y tiempos de restauración.
- Considerar stock mínimo/backup para reemplazo inmediato y continuidad 24x7.

Las características técnicas se detallan en el Anexo 1 del presente documento, siendo las cantidades resumidas en el siguiente cuadro:

Cuadro Nro. 04

Nro	Tipo del componente	Cantidad	Spare	Cantidad Total
7	Auricular Monoaural	198	12	210
8	Micrófono	108	7	115
9	Altavoces	108	7	115
10	PPT de pie	198	12	210
11	Cámara Web	268	13	281

2.1.3. Teléfonos IP

Los teléfonos IP serán desplegados en la central 911 para las comunicaciones por voz que se requieran. Las características técnicas se detallan en el Anexo 1 del presente documento, siendo las cantidades resumidas en el siguiente cuadro:

Cuadro Nro. 05

Nro	Tipo del componente	Cantidad	Spare	Cantidad Total
12	Teléfonos IP Tipo 1	190	11	201
13	Teléfonos IP Tipo 2	60	2	62
14	Teléfonos IP Tipo 3	14	2	16
15	Teléfonos IP Tipo 4	2	2	4
16	Botonera para teléfono IP 4	1	0	1

2.1.4. Pantalla de Monitoreo

Se requiere la provisión de dos (02) pantallas para monitoreo, las cuales estarán ubicadas en la sala NOC de TI. Las características técnicas se detallan en el Anexo 1 del presente documento.

2.1.5. Videoconferencia

Se incorporará cuatro (04) soluciones de videoconferencia para coordinación interinstitucional, gestión operativa y soporte durante la operación de las actividades de la Central 911 garantizando audio y video de calidad, estabilidad y seguridad. La solución deberá integrarse al entorno de red, contemplar administración y configuración controlada, y operar bajo políticas institucionales de ciberseguridad.

La solución de videoconferencia comprende como mínimo lo siguiente:

- Cámara, audio, codec/terminal y accesorios según sala y aforo las cuales deben estar integrados.
- Conectividad y segmentación de red conforme a arquitectura aprobada.
- Cifrado/seguridad y actualización de firmware bajo control.
- Soporte y mantenimiento alineado a disponibilidad 24x7.

2.1.6. Impresoras/Suministros/consumibles

Los equipos de impresión monocromáticos de tipo personal y de mediano volumen, atenderán las necesidades operativas y administrativas de la Central 911, asegurando disponibilidad, rendimiento y control. Las impresoras deberán soportar carga de trabajo acorde al volumen esperado, conectividad segura a la red institucional y administración centralizada, permitiendo trazabilidad y reducción de riesgos por uso no controlado.

La preparación de los periféricos comprende como mínimo lo siguiente:

- Conectividad de red, gestión central y control de acceso.
- Impresión dúplex y rendimiento (ciclo mensual) alineado al uso real.
- Seguridad básica: credenciales, actualizaciones y segmentación según diseño.
- Soporte y repuestos con tiempos acordes a operación 24x7.

Del mismo modo, se considerarán suministros y consumibles necesarios para el inicio de las operaciones de la Central 911. Los suministros deberán corresponder a los modelos adquiridos y contemplar rendimiento por página y rotación, de forma que se garantice disponibilidad sin impactar la operación.

- Tóner/tinta, kits y repuestos consumibles según especificación del fabricante.

- Rendimiento declarado (yield) y control de inventario (kardex).
- Stock mínimo y reposición planificada para operación continua.
- Registro de consumo para control y proyección de demanda.

Las características técnicas se detallan en el Anexo 1 del presente documento, siendo las cantidades resumidas en el siguiente cuadro:

Cuadro Nro. 06

Nro	Tipo del componente	Cantidad Total
19	Impresora tipo personal	13
20	Impresora tipo mediano volumen	5

Estos equipos no tienen spare

2.1.7. Proyectores Multimedia

Se realizará el suministro, instalación, configuración y puesta en funcionamiento de tres (03) sistemas de proyección multimedia para salas de usos múltiples divisibles mediante tabiques móviles, permitiendo la operación independiente de cada ambiente o la operación conjunta de los tres ambientes como una sola sala. Asimismo, un (01) sistema de proyección para la Sala de Prensa.

2.1.8. Tabletas para SAMU

Se adquirirán treinta y siete (37) tabletas para uso operativo del SAMU orientadas a movilidad y continuidad de servicio en campo, permitiendo acceso a información y aplicaciones autorizadas vinculadas a la atención de emergencias. Los equipos deberán contar con controles de seguridad, conectividad estable y accesorios que aseguren operación segura en ambientes exigentes.

La preparación de los equipos comprende como mínimo lo siguiente:

- Cifrado, control de aplicaciones y borrado remoto.
- Conectividad (Wi-Fi/LTE según corresponda), GPS y autonomía.
- Accesorios: fundas, cargadores y soportes.
- Integración con procesos de mesa de ayuda (inventario, incidentes y reposición).
- Servicio de datos por el periodo de soporte y garantía (Consumo promedio 50 GB en alta velocidad mensual por dispositivo).

2.2. Red LAN

La Red LAN de la Central 911 constituye la plataforma de conectividad principal que soportará la operación continua, segura y de alta disponibilidad de los servicios tecnológicos y operativos del proyecto, incluyendo el equipamiento de usuario final, la telefonía IP, la red inalámbrica, la plataforma SAGE, la infraestructura de centro de datos, los servicios de respaldo, las plataformas de ciberseguridad y los demás componentes que forman parte del ecosistema tecnológico de la Central 911. Dada la naturaleza del servicio 911, esta infraestructura ha sido concebida y deberá implementarse como una red para un entorno de misión crítica, preparada para operar de manera ininterrumpida 24x7x365, con tolerancia a fallas, continuidad operativa ante incidentes, eventos adversos o mantenimientos programados, y con niveles de resiliencia acordes al carácter estratégico de la atención de emergencias.

De manera general, la solución esta diseñada en una arquitectura integrada de Campus y Data Center, conformada por un fabric de centro de datos tipo Spine-Leaf, un núcleo de red LAN Campus (Core LAN), una capa de acceso cableado PoE, una red inalámbrica con administración centralizada, una zona DMZ y una red de gestión fuera de banda (OOB), permitiendo la segregación funcional y lógica de los distintos servicios, así como la integración ordenada de las plataformas tecnológicas del proyecto. Esta arquitectura ha sido definida para un centro de misión crítica, por lo que prioriza la

eliminación de puntos únicos de falla, el crecimiento horizontal, la recuperación rápida ante contingencias y el soporte estable del tráfico asociado a la atención de emergencias, la coordinación interinstitucional, los sistemas de despacho, voz, video, monitoreo y los servicios internos del centro de datos.

La solución contempla mecanismos de alta disponibilidad en los componentes críticos mediante redundancia de equipos, enlaces duales, agregación de enlaces, balanceo de tráfico y esquemas de operación que garanticen continuidad aun ante la falla de dispositivos, enlaces o módulos individuales. Del mismo modo, deberá soportar capacidades avanzadas de conmutación y enrutamiento para la segmentación lógica de la red, la separación de dominios de tráfico y la aplicación de políticas centralizadas de acceso y seguridad, asegurando la convivencia ordenada de redes de usuarios, voz, video, administración, servicios críticos, respaldo, seguridad y demás segmentos requeridos para la operación de la Central 911, sin comprometer el desempeño, la disponibilidad ni los tiempos de respuesta esperados en una operación de misión crítica.

Como parte del alcance del presente requerimiento, la Red LAN deberá integrarse de forma nativa con la plataforma de hiperconvergencia, la solución de backup e inmutabilidad, los componentes de ciberseguridad multicapa, la infraestructura inalámbrica, la solución de control de acceso a la red (NAC), así como con las plataformas institucionales y de terceros que forman parte de la operación integral de la Central 911. Esta integración deberá permitir visibilidad, telemetría, monitoreo, trazabilidad, administración centralizada y operación coordinada entre todos los componentes tecnológicos, manteniendo el desempeño requerido para una infraestructura de misión crítica y asegurando que los servicios esenciales del 911 dispongan de conectividad confiable, segura y permanentemente disponible.

Asimismo, la solución deberá contemplar una gestión centralizada, capacidades de automatización, monitoreo permanente, control de versiones de firmware, registro de eventos, analítica y operación segregada mediante red de administración fuera de banda, con la finalidad de facilitar la implementación, operación, mantenimiento, soporte y crecimiento futuro de la plataforma tecnológica. Todo ello deberá realizarse considerando la operación de la infraestructura en doble pila IPv4/IPv6, sin afectar el desempeño integral de la red y conforme a los lineamientos establecidos en el presente requerimiento. En concordancia con el enfoque de misión crítica del proyecto, la red deberá facilitar actividades de operación y soporte sin introducir indisponibilidades no planificadas y con capacidad de administración segura ante escenarios degradados.

La topología base de referencia de la solución se presenta en el Anexo 2 – Diagrama Topológico, en el cual se muestra, de manera referencial, la interconexión general entre los componentes de campus, centro de datos, seguridad, respaldo, acceso inalámbrico, gestión y servicios asociados. Dicho anexo deberá entenderse como la representación de la arquitectura objetivo del proyecto para un entorno de misión crítica y servirá como insumo para la ingeniería de detalle que desarrollará el Proveedor durante la fase de implementación, sin perjuicio del cumplimiento íntegro de las características técnicas, funcionales y de desempeño establecidas en el presente documento.

A continuación, se describe de forma general todos los bienes y accesorios que forman parte de la Red LAN, el cual será provisto en el presente requerimiento.

Cuadro Nro. 07 – Lista total del equipamiento de Red LAN

Nro	Bien	Cantidad	Spare	Cantidad Total
23	Switches Spine Data Center	2	0	2
24	Switches Leaf Data Center	8	0	8
25	Solución de Orquestador DC	1	0	1
26	Switch Core LAN Campus	2	0	2
27	Switch de acceso 48 puertos PoE	22	1	23
28	Switch de acceso 24 puertos PoE	4	0	4
29	Switch DMZ	2	0	2

Nro	Bien	Cantidad	Spare	Cantidad Total
30	Switch de Gestión Fuera de Banda	2	0	2
31	Controlador inalámbrico	2	0	2
32	Access Point	43	4	47
33	Solución de Administración y Gestión Campus	1	0	1
34	Solución de Control de Acceso	1	0	1
35	Hardware de Hiperconvergencia	4	0	4
36	Software Hiperconvergencia	1	0	1
37	Servidor para backup	1	0	1
38	Servidor de inmutabilidad	1	0	1
39	Almacenamiento para backup	1	0	1
40	Librería de backup	1	0	1
41	Software de backup	1	0	1
42	Firewall NGFW (Perimetral)	2	0	2
43	Firewall Interno	2	0	2
44	Consola de analítica y reportes	1	0	1
45	XDR (Extended Detection & Response)	1	0	1
46	ZTNA (Zero Trust Network Access)	1	0	1
47	Seguridad para correo electronico	1	0	1
48	WAF - Seguridad para Aplicaciones Web	1	0	1
49	SIEM	1	0	1
50	Plataforma de detección y respuesta de amenazas externas e internas	1	0	1
51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	1	0	1
52	ADC (application Delivery Controller)	2	0	2
53	Anti - DDos	2	0	2
54	MFA - Administración de identidad y acceso	1	0	1
55	PAM - Administración de acceso privilegiado	1	0	1
56	NDR (Network Detection and Response)	1	0	1
57	Sandboxing	1	0	1
58	Solución de Análisis de Tráfico de Red	1	0	1

2.2.1.Switching

A continuación, se describe los aspectos del diseño considerados para este equipamiento. Siendo estos detallados en la ingeniería a detalle a realizarse previo a la implementación por parte del Proveedor. Asimismo, en el Anexo 2, se adjunta el diagrama de conexión definido como diseño base para la implementación de todas las soluciones.

- **Alta disponibilidad:** Redundancia N+1 en equipos críticos y enlaces duales hacia el fabric.
- **Simplicidad y Escalabilidad:** Topología Spine-Leaf con ECMP y crecimiento horizontal.
- **Segmentación y Seguridad: VRF**, **VXLAN/EVPN**, y control de acceso centralizado (NAC/TACACS+).
- **Operabilidad:** Orquestación, versiones controladas de firmware y telemetría continua.

- **Gestión segregada:** Red OOB independiente del plano de datos

Vista Lógica del Centro de Datos (Fabric Spine-Leaf)

- **Rol y ubicación de equipos**
  - **Spine Data Center (2 unidades):** En sala del Centro de datos; switch de agregación de alto rendimiento.
  - **Leaf Data Center (8 unidades, en pares MLAG):** En racks del DC; acceso a HCI, servicios y firewalls.
  - **Leaf Border (incluido en los Leaf):** Switch Leaf designado como frontera del fabric, responsable de la interconexión con redes y servicios externos (Firewall Interno, Firewall Perimetral, DMZ, SAGE y/o WAN), asegurando la aplicación de políticas de seguridad y segmentación definidas.
  - **Switch OOB (2 unidades):** Gestión fuera de banda para todos los equipos.

- **Interconexiones Obligatorias**
  - Cada Leaf deberá conectarse a ambos Spine mediante dos (2) enlaces de 100Gbps por cada Spine (mínimo), soportando ECMP.
  - Cada Leaf formará MLAG con su par/virtualización equivalente.
  - Cada nodo HCI contará con al menos cuatro (4) enlaces de 25Gbps hacia los Leaf (LACP), y un (1) enlace hacia el switch de gestión OOB.
  - Leaf Border conectará hacia Firewall Interno y DMZ.

- **Servicios L2/L3 del Fabric**
  - **Underlay:** BGP/OSPF para accesibilidad entre Spine/Leaf.
  - **Overlay:** VXLAN/EVPN (estático o dinámico) para extensibilidad L2 y movilidad de cargas.
  - **Gateway distribuido:** ARP/ND suppression, IRB y Anycast Gateway.
  - **Multicast:** IGMP/MLD snooping y PIM/EVPN-Multicast (según fabricante).

Vista Lógica del Campus

- **Core LAN (2 unidades, núcleo colapsado):** Conectado a los firewalls internos mediante enlaces de 10 Gbps.
- **Acceso (22 unidades × 48p PoE + 1 spare = 23 total; + 4 × 24p PoE):** Uplinks 10 Gbps al Core con stack hasta 8 equipos.
- **DMZ (02 unidades)**

2.2.2. Red Inalámbrica

La solución inalámbrica deberá proporcionar conectividad de alta disponibilidad mediante controladores WLAN en configuración N+1, con administración centralizada, políticas homogéneas y optimización automática del entorno radioeléctrico. La arquitectura deberá considerar:

- **Controladoras WLAN en HA (N+1)**
  - Con capacidad para manejar la totalidad de los APs y crecimiento proyectado.
  - Gestión centralizada de políticas de seguridad (WIPS/WIDS, detección de interferencias, optimización automática de canales y potencia).
  - Integración nativa con NAC (802.1X, MAB, perfiles basados en rol, segmentación dinámica).
  - Soporte para SSID corporativo, invitado, BYOD y servicios de localización.
  - Integración con la plataforma de analítica y telemetría

- **Equipamiento WLAN**
  La solución deberá incluir:
  - **43 Access Points + 4 en spare (total 47)** Wi-Fi 6/6E, MIMO 2x2, compatibles con PoE 802.3bt, soporte BLE/Zigbee y servicios IoT.

- Controladores WLAN en N+1, con puertos 10Gbps, DPI, WIPS, WIDS y firewall L7 integrado o deducible por políticas.
- Licenciamiento para toda la solución (AP + Controller + Analytics).

- **Interconexiones mínimas**
  La solución inalámbrica deberá cumplir con las siguientes interconexiones mínimas:
  - Cada controlador WLAN deberá conectarse al Core de la red LAN mediante dos (2) interfaces de 10Gbps, en configuración de alta disponibilidad.
  - Cada controlador WLAN deberá incluir una interfaz adicional para gestión fuera de banda (OOB).
  - Los puntos de acceso deberán conectarse a los puertos PoE de los switches de acceso los cuales deberán tener uplinks de mínimo 10Gbps hacia el Core de la Red LAN.
  - La solución deberá integrarse con la plataforma de control de acceso a red (NAC) mediante mecanismos estándar.
  - La solución deberá integrarse con la plataforma institucional de analítica, telemetría y monitoreo mediante protocolos estándar (Syslog, NetFlow/sFlow, APIs, o equivalentes).

2.2.3. Hiperconvergencia (HCI) - Arquitectura y Equipamiento

La solución de hiperconvergencia deberá integrar cómputo, virtualización y almacenamiento bajo un modelo totalmente definido por software, con administración centralizada y escalabilidad horizontal.

- **Requerimientos:**
  - Mínimo 4 nodos HCI, operando en clúster.
  - Soporte nativo para replicación, alta disponibilidad y auto-recuperación.
  - Conectividad a la red mediante cuatro (4) interfaces de 25Gbps agregadas vía LACP, distribuidas en pares MLAG a dos switches Leaf distintos.
  - Gestión fuera de banda obligatoria mediante Switch OOB.
  - Integración con la solución de respaldo para protección de máquinas virtuales.

- **Equipamiento HCI**
  - Nodos HCI con CPU de gama empresarial, almacenamiento SSD/NVMe, duplicación de controladoras, fuentes redundantes y hypervisor integrado.
  - Licencias completas para virtualización, administración y soporte del fabricante.

- **Interconexiones mínimas**
  La solución de hiperconvergencia deberá de cumplir con las siguientes interconexiones mínimas:
  - Cada nodo HCI deberá conectarse al fabric del centro de datos mediante cuatro (4) interfaces de 25Gbps, agregadas mediante LACP y distribuidas en pares hacia dos (2) switches Leaf distintos, asegurando alta disponibilidad y continuidad operativa ante la falla de uno de los dispositivos o enlaces.
  - Cada nodo HCI deberá contar con una interfaz adicional dirigida a la red de gestión fuera de banda (OOB), conectada a los switches de administración correspondientes.
  - Las interconexiones deberán permitir el tráfico simultáneo requerido por el clúster, incluyendo almacenamiento distribuido, replicación interna, sincronización del clúster, migración de máquinas virtuales y tráfico del hipervisor, sin generación de cuellos de botella.
  - La solución HCI deberá integrarse con la plataforma de respaldo mediante APIs, agentes o mecanismos equivalentes, garantizando

consistencia a nivel de hipervisor para operaciones de copia, restauración y protección.
- Todo el tráfico interno del clúster deberá operar en redes o segmentos específicos del centro de datos (Fabric / VRF correspondientes), evitando mezclarse con redes de usuarios, acceso o tráfico no relacionado al funcionamiento del clúster.

- **Servicios de red**
  El Proveedor deberá realizar el despliegue de servicios de red en los servidores como el AD, NTP, DNS, DHCP y entre otros que se requieran para poner en producción los servicios. Asimismo, deberá de garantizar su operación durante el año de soporte requerido en el presente requerimiento.

  Las características técnicas de todo el equipamiento de la solución de hiperconvergencia se detallan en el Anexo 1 del presente documento.

2.2.4.Sistema de Respaldo

El sistema de respaldo deberá garantizar la protección integral de cargas virtualizadas, servidores físicos y servicios críticos mediante una arquitectura escalable, segura y alineada a buenas prácticas internacionales.

La arquitectura deberá considerar:
- Servidor dedicado de Backup con recursos suficientes para procesamiento de tareas concurrentes.
- Repositorio de almacenamiento optimizado para operaciones de respaldo y restauración, incluyendo disco, inmutabilidad y/o cinta.
- Software de gestión de copias con retenciones configurables, verificación automática de integridad (health check) y compatibilidad con hipervisores, servidores, bases de datos y aplicaciones.
- Integración nativa con la plataforma HCI, servidores físicos, bases de datos y componentes críticos mediante APIs y agentes.
- Capacidad para realizar backups completos, incrementales y diferenciales, con optimización del tráfico.
- Definición de políticas de retención, ventanas de respaldo y mecanismos de restauración granular.

Equipamiento de Respaldo

El equipamiento mínimo requerido para la solución de respaldo incluye:
- Servidor de backup con almacenamiento interno de alto rendimiento, procesador empresarial, memoria suficiente y redundancia de energía.
- Repositorio de almacenamiento en disco dedicado para respaldos, con soporte para cifrado, protocolo NFS/SMB o S3 compatible, y capacidad dimensionada según la retención proyectada.
- Librería de almacenamiento en cinta, con capacidad dimensionada para retención prolongada y compatibilidad con tecnología LTO.
- Software de Backup licenciado para máquinas virtuales, servidores físicos, base de datos y aplicaciones, incluyendo módulos de replicación, verificación de integridad e integración con inmutabilidad.

Almacenamiento para Backups en Disco e Inmutabilidad (WORM)

Incorporar un repositorio de respaldo en disco on-premise para restauraciones rápidas y un repositorio inmutable que impida la eliminación o modificación de copias durante el período de retención definido.

Deberá incluir:
- **Repositorio en disco para backup**
  - Compatible con el software de backup propuesto (bloque/NFS/SMB o S3-compatible, según aplique).
  - Cifrado en reposo (AES-256) y en tránsito (TLS 1.2/1.3).
  - RBAC, autenticación multifactor y segregación de accesos.

- **Repositorio Inmutable**
  - Soporte de Object Lock / WORM en modo Compliance o equivalente, con retenciones y legal hold configurables.
  - Protección total contra eliminación o sobrescritura de backups durante la retención, incluso por administradores.
  - MFA-Delete o mecanismos equivalentes; auditoría inalterable exportable a SIEM.
  - Separación estricta de credenciales, dominios y funciones administrativas.
  - Integración nativa con el software de backup para aplicar inmutabilidad por política o por conjunto de trabajos.

- **Buenas Prácticas 3-2-1-1-0:** mantener 3 copias de datos, en 2 tipos de medios distintos, 1 copia off-site (o logical-airgap), 1 copia inmutable, y garantizar 0 errores mediante verificaciones automáticas de integridad del software de respaldo.

- **Telemetría y monitoreo:** exportación de eventos (retenciones, expiraciones, intentos de borrado) vía Syslog hacia el SIEM.

Interconexiones mínimas

La solución de respaldo deberá de cumplir con las siguientes interconexiones mínimas:

- El servidor de backup deberá conectarse al fabric del centro de datos mediante un mínimo de dos (2) interfaces de 10/25Gbps, configuradas en alta disponibilidad, para garantizar el rendimiento en operaciones de copia y restauración.
- El servidor de backup deberá contar con una interfaz adicional dedicada a la red de gestión fuera de banda (OOB) para operación y mantenimiento independiente del plano de datos.
- El repositorio de almacenamiento en disco deberá conectarse al fabric mediante interfaces de 10/25Gbps, utilizando protocolos estándar (NFS, SMB o S3-compatible), asegurando suficiente ancho de banda para respaldos y restauraciones de alta velocidad.
- La librería de cintas deberá conectarse directamente al servidor de backup mediante interfaces SAS, según lo requerido para operaciones de copia a largo plazo.
- Todo el tráfico asociado a operaciones de respaldo deberá operar sobre redes o segmentos específicos del centro de datos, evitando mezclarse con redes de producción, acceso o tráfico de usuario.
- Los eventos del sistema de respaldo (retenciones, expiraciones, verificaciones de integridad e intentos de eliminación) deberán enviarse mediante Syslog o mecanismo equivalente hacia la plataforma de monitoreo o SIEM.

2.2.5. Ciberseguridad

La solución de seguridad deberá cumplir los principios de Zero Trust Architecture (ZTA), garantizando inspección en múltiples capas, segmentación dinámica, autenticación continua, visibilidad completa del tráfico, y respuesta automatizada ante incidentes.

Incluye los siguientes componentes:

- **Firewall Perimetral NGFW en HA,** con IPS avanzado, inspección TLS/SSL, control de aplicaciones y filtrado web.
- **Firewall Interno** segmentando dominios críticos
- **Consola de Analítica y Reportes** para visibilidad unificada y cumplimiento.
- **XDR (Extended Detection & Response)** para endpoints, con análisis de comportamiento y respuesta integrada.

- **ZTNA (Zero Trust Network Access)** para accesos remotos basados en identidad y postura del dispositivo.
- **Seguridad para Correo Electrónico** con (antiexploit, antiphishing, sandboxing), reputacion y análisis avanzado.
- **WAF** para aplicaciones Web institucionales
- **SIEM** para correlación centralizada
- **Plataforma de Detección y Respuesta de Amenazas Externas e Internas,** para detección temprana de intrusiones.
- **SOAR** para automatización de flujos de respuesta y orquestación de incidentes.
- **ADC (application Delivery Controller)** para balanceo L4/L7, offloading SSL, optimización de aplicaciones y continuidad del servicio.
- **Anti-DDos** para mitigación de ataques volumétricos y de aplicación.
- **MFA** para administración de identidad y acceso.
- **PAM** para administración de acceso privilegiado
- **NDR (Network Detection and Response)** para detección avanzada basado en tráfico y comportamiento.
- **Sandboxing** para análisis dinámico de archivos sospechosos.
- **Solución de Análisis de Tráfico de Red**

3. Soporte y Ciberseguridad

3.1. Mesa de Servicio

En una operación de misión crítica como la Central 911, la Mesa de Servicio 24x7 no es un "soporte adicional", sino un control operativo esencial para asegurar la continuidad y disponibilidad de la infraestructura tecnológica implementada para la atención y gestión de emergencias. Este servicio debe considerarse porque habilita atención permanente con (3) tres niveles de escalamiento, gestión integral de incidentes y requerimientos con trazabilidad, mantenimiento preventivo/correctivo, y gestión de garantías/repuestos, reduciendo la probabilidad y el tiempo de indisponibilidad. Además, permite cumplir acuerdos de niveles de servicio con tiempos objetivo exigentes, respuesta en minutos y restauración en horas para criticidad alta, y asegurar control, evidencia y mejora continua, elementos indispensables para gobernar la operación 24x7 y evitar puntos únicos de falla. Este servicio deberá estar activo desde el inicio del soporte y garantía para el presente requerimiento.

Alcance

Asegurar la continuidad operativa del equipamiento tecnológico del presente requerimiento para la operación de la Central 911 mediante un servicio de Mesa de Servicio especializado, con atención permanente, escalamiento por niveles y cumplimiento de acuerdos de niveles de servicio.

- Atención permanente 24x7 para incidentes y requerimientos asociados al equipamiento tecnológico.
- Soporte nivel 1: registro, categorización, priorización, diagnóstico inicial, solución remota y escalamiento.
- Soporte nivel 2: diagnóstico avanzado, intervención presencial cuando corresponda, reinstalación, configuración, reemplazo de componentes y coordinación de garantías.
- Soporte nivel 3: resolución de fallas complejas, soporte a configuraciones avanzadas, análisis de causa raíz y coordinación con fabricantes o proveedores especializados.
- Mantenimiento preventivo planificado, mantenimiento correctivo y verificación de salud de equipos.
- Gestión de inventario y control de activos, incluyendo evidencia de intervenciones y cambios.
- Reportes operativos, seguimiento y plan de mejora continua.
- Catálogo de Servicios: definido por el proveedor en base todo al presente requerimiento, y actualizado durante el soporte y garantía.

Dotación de personal mínima

Cuadro Nro. 08

Nivel	Cobertura	Modalidad	Posición simultanea	Dotación total recomendada	Rol principal
Nivel 1	Atención continua	Presencial	Tres (3)	Once (11) 2 por turno (3x3=9) + 2 de relevo (descansos, vacaciones y contingencias).	Registro, diagnóstico inicial, solución remota y escalamiento
Nivel 2	Atención continua	Presencial	Cuatro (4)	Catorce (14) 2 por turno (4x3=12) + 2 de relevo (descansos, vacaciones y contingencias)	Soporte avanzado, intervención presencial, reemplazos y coordinación de garantías
Nivel 3	Atención continua	Presencial	Dos (2)	Ocho (8) 1 por turno (2x3=6) + 2 de relevo (descansos, vacaciones y contingencias)	Especialistas, análisis de causa raíz y coordinación con fabricantes

Turnos Operativos mínimos

Cuadro Nro. 09

Turno	Horario	Observación
Primer Turno	Turno de ocho (8) horas	Incluye traslape de quince minutos para transferencia de posición.
Segundo Turno	Turno de ocho (8) horas	Incluye traslape de quince minutos para transferencia de posición.
Tercer Turno	Turno de ocho (8) horas	Incluye traslape de quince minutos para transferencia de posición.

Nivel 1 Funciones mínimas de Analista de mesa de ayuda

- Recepción multicanal, registro y clasificación.
- Priorización según matriz de impacto y urgencia.
- Diagnóstico inicial y solución remota cuando aplique.
- Comunicación al usuario y escalamiento controlado.
- Gestión de base de conocimiento y cierre con evidencia.

Nivel 2 Funciones mínimas de Soporte Técnico

- Atención de incidencias de software, hardware, periféricos y conectividad del puesto.
- Atención presencial y/o remoto, reinstalación, configuración, reemplazo y pruebas.
- Gestión de repuestos y coordinación de garantías.
- Estandarización y control de configuraciones de estaciones y periféricos.

Nivel 3 Funciones mínimas de Soporte Especialista

- Resolución de fallas complejas no resueltas en niveles previos.
- Análisis de causa raíz, corrección permanente y prevención de recurrencia.
- Coordinación con fabricantes y proveedores especializados.
- Validación técnica de cambios que afecten continuidad operativa.

Gestión de componentes, repuestos, garantías y cambios

- Diagnóstico y evidencia: confirmar falla con checklist, registros y evidencia.
- Contención: reasignación de puesto o componente.
- Reemplazo: cambio por unidad equivalente y actualización de inventario con número de serie.
- Verificación: pruebas funcionales y conformidad del usuario.
- Cierre y trazabilidad: registro completo en el Nivel 1 y actualización de activos.
- Gestión de garantía: trámite de reparación o reemplazo del componente retirado para reconstituir stock mínimo.

Características generales del Software de Mesa de Servicio:

Cuadro Nro. 10

Componente funcional	Carácter	Descripción técnica	Resultado esperado
Gestión de tickets	Obligatorio	Registro, categorización, asignación, bitácora, adjuntos y estados.	Trazabilidad completa
Acuerdos de niveles de servicio	Obligatorio	Cálculo automático, alertas, escalamiento y semáforos por prioridad.	Control de cumplimiento
Catálogo de servicios	Obligatorio	Formularios, validaciones y aprobaciones por tipo de requerimiento.	Atención estandarizada
Gestión de activos	Obligatorio	Inventario con número de serie, ubicación, usuario, garantía y relación con tickets.	Inventario consistente
Base de conocimiento	Obligatorio	Artículos, versionado, revisión y publicación para nivel 1.	Resolución más rápida
Reportes	Obligatorio	Tableros de desempeño, tendencias, exportación y reportes programados.	Gobierno del servicio
Auditoría y seguridad	Obligatorio	Roles, permisos, bitácora de cambios y trazabilidad por usuario.	Cumplimiento y control

Módulo de Soporte Remoto	Obligatorio	Conexión segura, grabación de sesión Multisesión	Atención estandarizada
Aplicación IA/ Chatbot	Obligatorio	Triaje inteligente, resolución autónoma, traspaso fluido	Atención estandarizada

Alcance de implementación – entregables y criterios minimos de aceptación

Cuadro Nro. 11

Fase	Entregables	Criterios mínimos de aceptación	Cumplimiento
Planificación	Plan de despliegue; matriz de riesgos; plan de comunicaciones; plan de pruebas; matriz de roles y responsabilidades.	Aprobación formal; cronograma validado.	La planificación para la implementación de la mesa de servicio formará parte del Plan del Proyecto. El Proveedor deberá de implementar la mesa de servicio, detallando los procedimientos, catálogo de servicio, recursos, software, entre otros previo a la aceptación operativa del presente requerimiento, considerando lo establecido en el presente documento. El software de mesa de servicio podrá ser on-premise o en nube.
Preparación	Imágenes, configuraciones estándar, etiquetado, inventario inicial.	Muestra representativa validada; inventario trazable.	
Despliegue	Instalación física y lógica; checklist por puesto; evidencias.	Pruebas de aceptación aprobadas; incidencias registradas.	
Transferencia	Documentación técnica; capacitación; acta de transferencia.	Transferencia formal; base de conocimiento inicial.	

Indicadores mínimos para control del servicio durante el primer año de soporte y garantía:

Cuadro Nro. 12

Indicador	Definición	Meta referencial
Cumplimiento del tiempo máximo de respuesta	Porcentaje de tickets atendidos dentro del tiempo máximo de respuesta por prioridad	95% o superior
Cumplimiento del tiempo objetivo de restauración	Porcentaje de incidentes restaurados dentro del tiempo objetivo por prioridad	90% o superior en prioridad crítica
Tiempo promedio de restauración en prioridad crítica	Promedio desde registro hasta restauración para prioridad crítica	2 horas o menor

Resolución en primer contacto	Porcentaje de tickets resueltos por nivel 1 sin escalamiento	60% o superior (objetivo creciente)
Reincidencia de incidentes	Cantidad de incidentes repetidos por misma causa	Tendencia decreciente
Disponibilidad de la Mesa de Servicios	Disponibilidad efectiva del canal de atención y registro	99.9% o superior
Antigüedad de tickets abiertos	Tickets abiertos con más de 72 horas	Controlado y justificado
Satisfacción del usuario	Encuesta posterior al cierre	4 sobre 5 o superior
Cumplimiento de mantenimiento preventivo	Actividades preventivas ejecutadas frente a plan	95% o superior
Tiempo de reposición de periféricos o equipos con spare en sitio	Tiempo desde diagnóstico hasta reemplazo para periféricos o equipos con spare en sitio	1 hora

3.2. SOC

El Centro de Operaciones de Seguridad (SOC) constituye un control operativo esencial para asegurar la confidencialidad, integridad y disponibilidad de los activos tecnológicos que soportan la atención de emergencias. El SOC permite la vigilancia continua 24x7 de eventos de ciberseguridad, la detección temprana de actividades anómalas y amenazas (internas y externas), y la respuesta coordinada a incidentes de seguridad antes de que escalen a afectaciones operativas, para lo cual coordina permanentemente con la mesa de servicio para el registro respectivo de la incidencia u otro relacionado al alcance del SOC. Asimismo, el SOC asegura el cumplimiento de objetivos de seguridad operacional, y se integra con el servicio de seguridad del SAGE, de tal forma se tenga una seguridad de extremo a extremo con equipos multidiscplinarios y herramientas diversas para minimizar cualquier tipo de ataque o vulneración a la seguridad del 911.

El servicio SOC y todo lo inidicado debe estar implementado antes de la aceptación operativa, por lo que el Proveedor deberá presentar el plan de implementación de este servicio en el "Plan del Proyecto".

El Proveedor debe proporcionar un SOC con las siguientes características:

- Analizar y clasificar eventos mediante playbooks, clasificadores de severidad y la base de datos de amenazas y vulnerabilidades del laboratorio de amenazas de las soluciones adquiridas.
- Notificar a la Central 911 y otros Proveedores sobre amenazas verificadas y entregar recomendaciones de remediación a través del portal del servicio.
- Brindar acceso a un portal del servicio para visualizar eventos verificados, estatus de incidentes y descargar reportes.
- Escalar incidentes críticos a la Central 911 dentro de los 15 minutos posteriores a su confirmación, a través de correo electrónico y llamada telefónica.
- Escalar incidentes de alta severidad en máximo 45 minutos vía correo electrónico; de severidad media en 90 minutos y de severidad baja en un máximo de 6 horas.
- Proporcionar informes semanales resumidos de alertas, notificaciones y tickets del portal.
- Procesar y evaluar todos los eventos de seguridad recibidos de los dispositivos monitoreados para filtrar falsos positivos y generar notificaciones verificadas.
- Analizar y validar eventos, clasificándolos como incidentes verificados y notificando por correo electrónico.

- Generar tickets de incidente de seguridad con notificación inmediata según la matriz de escalamiento acordada.
- Registrar todas las interacciones y recomendaciones en los tickets creados.
- Brindar acceso al historial de eventos y tickets, con visualización de estado y detalle de incidentes.
- Permitir la visualización de reportes e informes generados por el servicio.
- Permitir el envío de solicitudes de ajuste de monitoreo o cambios en la recolección de logs mediante el portal proporcionado.
- Clasificar los incidentes de seguridad de acuerdo con su impacto potencial, utilizando la tabla de severidad descrita (Crítico, Alto, Medio, Bajo).
- Ajustar la prioridad del ticket de incidente conforme cambie el estado o impacto del incidente.
- Mantener abiertos los tickets el tiempo necesario para la evaluación.
- Permitir solicitudes de incorporación de nuevos dispositivos a través del portal.
- Debe de considerar alguno de los siguientes casos de uso alineados a MITRE:

Cuadro Nro. 13

Reconocimiento	
Reconocimiento: Casos de uso que detectan técnicas de recopilación de información de forma activa o pasiva.	
T1595	Escaneo activo
Militarización	
Ejecución: Casos de uso que detectan técnicas que implican crear, comprar o comprometer/robar recursos externos con el fin de comprometer las vulnerabilidades de la víctima.	
T1047	Instrumental de administración de Windows
Entrega	
Acceso inicial: Casos de uso que detectan sitios web, aplicaciones, acceso remoto, servicios o ataques de phishing comprometidos.	
T1133	Servicios Remotos Externos
T1189	Compromiso de intrusión
T1190	Aprovechar la aplicación de cara al público
T1566	Phishing
Explotación	
Ejecución: Casos de uso que detectan cuando se habilita código o software no autorizado en un sistema.	
T1072	Herramientas de implementación de software
T1059	Intérprete de comandos y secuencias de comandos
T1203	Explotación para la ejecución del cliente
Acceso a credenciales: Casos de uso que detectan intentos de robo de credenciales, como keyloggers o ataques de volcado de credenciales.	
T1003	Volcado de credenciales del sistema operativo
T1056	Captura de entrada
T1083	Detección de archivos y directorios
T1110	Fuerza bruta
Descubrimiento: Casos de uso que detectan cuándo los atacantes intentan obtener conocimientos sobre el sistema y las redes internas.	
T1018	Detección remota de sistemas
T1046	Escaneo de servicios de red
T1082	Descubrimiento de información del sistema
T1083	Detección de archivos y directorios
T1087	Descubrimiento de Cuentas
T1135	Detección de recursos compartidos de red
Evasión de la defensa: Casos de uso que detectan cuándo los atacantes intentan eludir los controles de protección.	
T1014	Rootkit

T1027	Archivos o información ofuscados
T1055	Inyección de proceso
T1070	Eliminación del indicador en el host
T1140	Desofuscar / Decodificar archivos o información
T1211	Explotación para la evasión de la defensa
T1212	Explotación para el acceso a credenciales
T1218	Ejecución de proxy binario firmado
T1497	Virtualización / Evasión de sandbox
T1539	Robar código de sesión web
T1548	Mecanismo de control de elevación de abuso
T1562	Deteriorar las defensas
T15740	Flujo de ejecución de secuestro
Escalada de privilegios: Casos de uso que detectan intentos de obtener permisos de nivel superior en un sistema o red.	
T1055	Inyección de proceso
T1068	Explotación para la escalada de privilegios
T1078	Cuentas válidas
T1134	Manipulación de tokens de acceso
T1548	Mecanismo de control de elevación de abuso
T1574	Flujo de ejecución de secuestro
Instalación	
Movimiento lateral: Casos de uso que detectan intentos de obtener acceso no autorizado a los sistemas de una red desde una fuente presuntamente confiable en la misma red.	
T1021	Servicios Remotos
T1072	Herramientas de implementación de software
T1210	Explotación de servicios remotos
T1534	Spearphishing interno
T1570	Transferencia lateral de herramientas
Persistencia: Casos de uso que detectan intentos de mantener el acceso a los sistemas a través de reinicios, credenciales modificadas y otras interrupciones que podrían cortar el acceso del adversario.	
T1176	Extensiones de navegador
T1133	Servicios Remotos Externos
T1136	Crear una cuenta
T1574	Flujo de ejecución de secuestro
Colección: Casos de uso que detectan técnicas utilizadas por los atacantes para recopilar información con fines de exfiltración.	
T1185	Secuestro de sesión del navegador
T1574	Captura de entrada
T1602	Datos del repositorio de configuración
Comando y control	
Comando y control: Casos de uso que detectan tráfico sospechoso que se origina desde el sistema interno a destinos externos.	
T1001	Ofuscación de datos
T1008	Canales de reserva
T1071	Protocolo de capa de aplicación
T1092	Comunicación a través de medios extraíbles
T1095	Protocolo de capa no aplicativa
T1104	Canales de varias etapas
T1105	Transferencia de herramientas de entrada
T1132	Codificación de datos
T1219	Software de acceso remoto
T1568	Resolución dinámica
T1571	Puerto no estándar
T1573	Canal encriptado
Acciones sobre objetivos	

Exfiltración: Casos de uso que detectan técnicas que los adversarios pueden utilizar para robar datos y evitar la detección mientras los eliminan.	
T1041	Exfiltración a través del canal C2
T1048	Exfiltración sobre protocolo alternativo
T1052	Exfiltración sobre medio físico
T1537	Transferir datos a una cuenta en la nube
T1567	Exfiltración a través del servicio web
Impacto: Casos de uso que detectan técnicas que los adversarios pueden utilizar para interrumpir la disponibilidad o comprometer la integridad mediante la manipulación de los procesos comerciales y operativos.	
T1485	Destrucción de datos
T1486	Datos encriptados para lograr un impacto
T1498	Denegación de servicio de red
T1499	Denegación de servicio de endpoints
T1561	Borrado de disco

- Se debe proporcionar un servicio complementario al SOC, el cual debe ser provisto por un fabricante de ciberseguridad e incluir servicios para preparación y respuesta ante incidentes, con las siguientes características:
  - Proporcionar un servicio de preparación y respuesta ante incidentes del fabricante de seguridad de las soluciones adquiridas que contemple asesoría y acompañamiento remoto en actividades de forense digital, análisis, contención y remediación de incidentes de ciberseguridad.
  - Garantizar 100 horas de análisis forense digital y respuesta a incidentes, debiendo ser provista por algunos de los fabricantes de las soluciones XDR, SIEM o SOAR adquiridas, por el periodo de soporte y garantía. De no ser usado el servicio, antes del término del contrato, se podrá acceder a un catálogo de opciones asesoría especializada.
  - Asegurar la disponibilidad de recursos técnicos especializados para la atención de incidentes y ejercicios proactivos de preparación durante toda la vigencia del servicio contratado.
  - Realizar una reunión remota inicial de onboarding para establecer los puntos de contacto, presentar el portal de gestión de incidentes y explicar las opciones de servicios disponibles.
  - Ejecutar una reunión remota de capacitación forense, explicando en detalle los procesos de respuesta a incidentes, capacidades y alcance, así como resolver todas las consultas relevantes.
  - Garantizar un tiempo de respuesta máximo de 02 horas desde la apertura del ticket de incidente crítico.
  - Brindar acceso continuo a servicios de soporte y asesoría para respuesta a incidentes durante toda la vigencia del contrato.
  - Realizar revisión integral del sistema de seguridad de la Central 911, incluyendo identificación de componentes comprometidos en caso de incidente.
  - Analizar logs relevantes provenientes de soluciones firewall/NetFlow, VPN, proxy web, IDS/IPS, SIEM y artefactos forenses complementarios.
  - Ejecutar análisis detallado de archivos y memoria con el fin de descubrir cargas maliciosas y técnicas utilizadas en el incidente.
  - Identificar y documentar hosts comprometidos, cuentas comprometidas, indicadores de compromiso (IOC), indicadores de exfiltración de datos, métodos de acceso inicial y paciente cero.
  - El servicio deberá evaluar el estado actual de preparación de la entidad ante incidentes y ataques. Esta evaluación se deberá realizar en conjunto con los expertos de la marca para evaluar la postura de seguridad actual.
  - Este servicio deberá Identificar y priorizar las mejoras más críticas. Desde la implementación completa de programas hasta la orientación estratégica para ayudarnos a establecer una ciberdefensa de primer nivel.

- Deberá establecer una base sólida, desarrollando las bases para una ciberdefensa sólida, incluidas políticas, procedimientos, estándares, flujos de trabajo, cuadros de personal y hojas de ruta estratégicas.
- Deberá descubrir y priorizar los riesgos de seguridad en toda la institución en términos de ciberdefensa.
- Adicionalmente deberá trabajar colaborativamente con el personal de la entidad para actuar ante los siguientes escenarios a demanda:

Cuadro Nro. 14

Tipo de Servicio	Servicio y Descripción
Servicio de Respuesta a Incidentes	Respuesta al incidente • Investigar y recuperarse de incidentes de seguridad y violaciones de datos: ▪ Contener y erradicar la amenaza ▪ Determinar el punto de acceso inicial ▪ Determinar el alcance de la actividad no autorizada ▪ Determinar a qué datos, si los hubo, se accedió o se robaron • Análisis de malware e ingeniería inversa Investigación de ransomware • Involucrar al actor de amenazas en nombre de la Entidad. • Buscar pruebas de que el atacante puede descifrar los datos • Remitir a la Entidad y a los proveedores de servicios de pago para adquirir claves de cifrado para la recuperación de datos. • Aplicar ingeniería inversa a la utilidad de descifrado proporcionada por el atacante para garantizar que no exista ningún código malicioso • Proporcionar tutorial al equipo de la Entidad para demostrar cómo descifrar archivos • Proporcionar soporte remoto para la resolución de problemas Compromiso de correo electrónico corporativo • Contener el incidente y recomendar medidas de seguridad adicionales; Investigue y determine la causa raíz, la ventana de compromiso, la actividad del atacante y revise los datos a los que se accede para cuantificar la información confidencial. Compromiso web • Contenga amenazas e implemente salvaguardas, analice registros, revise código, cuantifique la exposición o pérdida de información confidencial y recomiende contramedidas de refuerzo de diseño. Respuesta a la brecha en la nube • Identifique el vector de ataque inicial y el alcance del acceso no autorizado y la exfiltración, contenga el incidente, identifique el alcance de los sistemas para la remediación y recomiende/implemente medidas de seguridad adicionales y verificaciones continuas. Investigación PCI • Contenga los incidentesdispo e implemente medidas de seguridad, navegue por el proceso de PFI, responda a supuestas violaciones, identifique el vector de ataque y la ventana de compromiso, cuantifique la cantidad de tarjetas expuestas

Análisis Forense Digital	• Investigaciones digitales, incluidos asuntos relacionados con amenazas internas, empleados que se han ido y robo de propiedad intelectual. • Análisis forenses de medios digitales, incluidas computadoras de escritorio/portátiles, servidores, teléfonos móviles/tabletas y/o datos de registro para cumplir objetivos específicos, incluida la identificación del acceso, movimiento, exfiltración y/o destrucción de datos. • Análisis forense de hardware para determinar la funcionalidad de un dispositivo o extraer datos de dispositivos IoT, nuevas tecnologías o hardware creado por atacantes • Investigaciones de datos estructurados ▪ Asesorar sobre la recopilación y liderar el análisis de entornos de bases de datos SQL y NoSQL, incluidos, entre otros, la revisión de esquemas, tablas, procedimientos y registros recopilados de los sistemas de bases de datos afectados, para evaluar la actividad de los actores de amenazas y el riesgo de exposición de datos.
Servicios de Prueba y Evaluación	Revisión de preparación para infracciones (BRR) • Evaluación de riesgos de ciberseguridad específica centrada en controles de detección, personas, procesos y tecnologías necesarios para responder de manera efectiva a las amenazas cibernéticas. • Incluye recomendaciones de remediación, mejoras de control y una hoja de ruta estratégica para lograr un estado objetivo de preparación para infracciones. Desarrollo del Programa de Respuesta a Incidentes • Facilitar el desarrollo de un programa de respuesta a incidentes para ayudar a establecer o mejorar el plan, las políticas, los procedimientos y los manuales de respuesta a incidentes actuales. Pruebas de penetración (Penetration Test): ejercicios de equipo morado y rojo • Simula un ciberataque del mundo real para evaluar la fuerza de las contramedidas e identificar vulnerabilidades de seguridad ocultas. • Defina un alcance, reglas de compromiso y establezca objetivos, y luego identifique rutas de ataque y cadenas de explotación que un actor de amenazas probablemente aprovecharía para obtener acceso a datos confidenciales o aplicaciones comerciales críticas. Análisis de vulnerabilidades • Evaluación técnica interna y/o externa diseñada para generar tantas vulnerabilidades como sea posible en el entorno, junto con la gravedad y la prioridad de remediación recomendada. Análisis de Aplicaciones Web • Evalúe las aplicaciones web en busca de vulnerabilidades, incluidas las fallas en el desarrollo, la configuración, la implementación, el proceso de actualización, las integraciones de API, el mantenimiento o los complementos de terceros. Evaluaciones de aplicaciones móviles • Probar y mejorar la seguridad de las aplicaciones móviles. Enumere la superficie de ataque, buscando vulnerabilidades,

	configuraciones incorrectas o fallas lógicas que conduzcan a caminos probables de compromiso y/o exfiltración de datos. Ejercicios de phishing por correo electrónico • Probar y mejorar la conciencia de seguridad cibernética en la Entidad y reduzca la susceptibilidad a los ataques de phishing. Evaluación de Compromisos / Cacería de Amenazas (Threat Hunting) • Revisar las redes de la Central 911 y los comportamientos de los terminales para determinar si hay evidencia de acceso o actividad no autorizados. Evaluación de la seguridad del correo electrónico • Llevar a cabo una revisión exhaustiva de la configuración de seguridad del entorno de correo electrónico que incluya la revisión de la administración de la cuenta, las reglas de reenvío de correo electrónico, las políticas de la bandeja de entrada, los controles de autenticación.
Servicios de Asesoría Estratégica	Director virtual de seguridad de la información (vCISO) • Un vCISO de El fabricante ayuda a desarrollar e implementar una estrategia de seguridad cibernética, identificar riesgos y proporcionar recomendaciones para medidas de reducción de riesgos. • Un vCISO puede responder a las preguntas de la junta directiva o de la alta dirección sobre los puntos de referencia y la madurez del programa de seguridad, la preparación para infracciones, la eficacia y la idoneidad, etc. • Estrategia de riesgo cibernético y hojas de ruta de mitigación • Desarrolle planes estratégicos personalizados que establezcan un camino, un cronograma y un presupuesto para lograr los objetivos de resiliencia cibernética de una organización. • Revisión de la estrategia de seguridad del Directorio (Board of Directors o BoD) • Evaluación y revisión para identificar el riesgo cibernético, crear un perfil de estado actual y crear una estrategia de seguridad clara para compartir con sus ejecutivos y la Junta. • Maduración del desarrollo de programas cibernéticos, políticas y estándares • Desarrollar o mejorar políticas y estándares de ciberseguridad. Teniendo en cuenta los estándares específicos de la industria, los objetivos de la Central 911 y las metas futuras. • Evaluación SOC • Diseñar y asesorar sobre la construcción de un centro de operaciones de seguridad de próxima generación y/o un programa de seguridad de la información basado en las mejores prácticas. • Implementación discreta de proyectos cibernéticos • Asistencia experta con la arquitectura, la supervisión de la implementación y el ajuste de un proyecto crítico de ciberseguridad. • Servicios estratégicos y tácticos, por ejemplo, asesoramiento sobre el fortalecimiento de aplicaciones comerciales críticas, correo electrónico empresarial y controles de detección de última generación. • Servicios de asesoramiento de remediación y recuperación estratégica posterior a la vulneración • Orientación y priorización de remediación estratégica para evitar una mayor propagación de cualquier persistencia relacionada con el Incidente.

	• Evaluación del estado de los controles de seguridad, sistemas, proveedores de servicios gestionados, diseño de equipos y procedimientos destinados a identificar y prevenir el Incidente específico. • Con base en la evaluación, desarrollar y entregar un plan de remediación estratégico que incluya objetivos priorizados a corto, mediano y largo plazo para abordar las debilidades de seguridad expuestas por un incidente específico y reducir el riesgo de cualquier incidente continuo o recurrente.
Servicios de Gobierno, Riesgo y Cumplimiento	Evaluación CIS V8 • Informe CIS V8 y recomendaciones personalizadas. • Roadmap (hoja de ruta) de implementación de 12 a 24 meses. Evaluación del marco de ciberseguridad del NIST (NIST CSF) • Libro de trabajo de resultados del LCR del NIST. • Informe Ejecutivo de Hallazgos Temáticos. • Hoja de ruta de implementación de 12 a 24 meses. Evaluaciones de ciberseguridad reguladas y basadas en contratos (por ejemplo, CCPA, NYDFS, HIPAA, FINRA, PCI DSS, C2M2, GDPR) • Realizar un mapeo de evaluación a los requisitos de control de los marcos contractuales, estatales y/o regulatorios. • Evalúe los requisitos de control, encuentre y solucióne las brechas y demuestre el cumplimiento. Revisiones de debida diligencia cibernética de fusiones y adquisiciones • Evaluación específica en relación con la actividad pendiente de fusión/adquisición. Enfocada y táctica, esta evaluación está diseñada para brindar transparencia a los participantes del trato. • Identifique posibles señales de alerta, resalte los riesgos de ciberseguridad ocultos y obtenga una evaluación independiente de la madurez general del programa de seguridad de la información. Evaluación de riesgos de ciberseguridad de proveedores externos • Evaluación del riesgo de ciberseguridad basado en proveedores externos. • Evaluar y mejorar los requisitos del contrato relacionados con la seguridad de la información. • Desarrollar y/o mejorar las operaciones de seguridad relacionadas con el cumplimiento de los requisitos de seguridad por parte de proveedores externos.

4. Implementación, Planificación y Gestión del Proyecto

4.1. Gestión del Proyecto

El Proveedor deberá presentar el plan del proyecto a los quince (15) días calendarios contabilizados al día siguiente de firmado el Contrato. Este documento tiene que contener como mínimo las siguientes áreas de conocimiento:

- Gestión del Alcance
- Gestión del Cronograma
- Gestión de recursos
- Gestión de Calidad
- Gestión de las comunicaciones
- Gestión de riesgos
- Gestión de los interesados

Dicho plan será revisado por el Gerente del Proyecto del Comprador asignado a este contrato y será aprobado en un plazo no mayor de cinco (05) días calendarios después de haber sido presentado por el Proveedor en el caso de no existir observaciones. De existir observaciones, están deberán ser levantadas en un plazo no mayor de dos (2) días calendario y ser enviado nuevamente para revisión con el mismo plazo de aprobación. Asimismo, el Proveedor deberá habilitar en una herramienta en línea para 05 usuarios que permita visualizar todas estas áreas de conocimiento, con el cronograma en línea, estableciendo KPI de seguimiento. Asimismo, la gestión de riesgos debe ser una actividad semanal, con la finalidad de generar alertas tempranas de la ejecución del proyecto en todas sus áreas de conocimiento y propias del Contrato, visualizando el estado de la procura desde su requerimiento hasta la llegada a los almacenes del Proveedor y su traslado al almacén en la Central 911, con la finalidad de tener el tracking de estos.

Se establecerán semanalmente reuniones con el personal clave del Proveedor y el personal del equipo del proyecto 911 para realizar el seguimiento a las actividades.

El Proveedor deberá contar con un equipo de profesionales para realizar la gestión de proyectos, principalmente el Jefe de Proyectos y un Controller del Proyecto, quienes deberán generar y mantener en un repositorio en línea compartido con toda la documentación desde la firma del contrato. Asimismo, elaborar todas las actas de reuniones que se realicen durante la ejecución de estas. Este repositorio será de acceso restringido.

4.2. Personal Clave para la gestión

- ***01 Jefe de Proyecto:***

  Nivel Académico

  - Con título profesional en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. Colegiado y habilitado (para la firma de contrato se presentará la habilitación)

  Certificaciones

  - Certificación vigente PMP emitido institución PMI o Certificación SCRUM Máster.
  - Certificación ITIL V4
  - Certificación ISO27001 Seguridad de la información.
  - Certificación ISO22301 Continuidad del negocio.

  Experiencia

  - Con mínimo de diez (10) años de experiencia como jefe o gerente de proyecto en implementación de soluciones TIC.

  Nota: los licitantes en su propuesta deben considerar un controller del proyecto.

4.3. Personal clave para la Implementación.

Cuadro Nro. 15

Especialista	Perfil
01 Especialista en Networking	**Formación académica:** Con título profesional o bachiller en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante en Switching de la solución ofertada. **Experiencia:** Con mínimo cinco (05) años de experiencia como Especialista en Networking.
01 Especialista en Ciberseguridad	**Formación académica:** Con título profesional o bachiller en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes y/o Comunicaciones. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante de la solución de Firewall ofertada. **Experiencia:** Con mínimo cinco (05) años de experiencia como Especialista en Seguridad.
01 Especialista en Servidores	**Formación académica:** Con título profesional o bachiller en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante de la solución de Hardware y/o Software ofertada. **Experiencia:** Con mínimo cinco (05) años de experiencia como Especialista en Servidores.
01 Especialista en Servicios de TI	**Formación académica:** Con título profesional o bachiller en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. **Capacitaciones:** Capacitación mínima en 1 certificación en algunas de las soluciones ofertadas por el fabricante de la solución ofertada.

	Certificación en ITIL **Experiencia:** Con mínimo cinco (05) años de experiencia como Especialista en Gestión de Servicios de TI.

4.4. Personal Clave para la administración de las soluciones tecnológicas durante el periodo de soporte y garantía.

Cuadro Nro. 16

Especialista	Perfil	Cantidad
Jefe de Soporte TI	**Formación académica:** Con título profesional en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Ingeniero Administrativo, **Capacitación** • Curso o taller o Certificación en Dirección de Proyectos • Curso o taller o Certificación ITIL V4 • Curso o Taller Certificación SCRUM Máster. **Experiencia:** • Con mínimo de cinco (05) años de experiencia como Coordinador o Gerente de Servicio de soluciones TIC. Colegiado y habilitado (para la firma de contrato se presentará la habilitación)	01
Soporte en redes	**Formación académica:** Con título profesional o bachiller o técnico en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante en Switching de la solución ofertada. **Experiencia:** Con mínimo dos (02) años de experiencia como Especialista en Networking.	03
Soporte en Ciberseguridad	**Formación académica:** Con título profesional o bachiller o técnico en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes y/o Comunicaciones. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante de la solución de Firewall ofertada. **Experiencia:**	03

	Con mínimo dos (02) años de experiencia como Especialista en Seguridad.	
Soporte en Servidores	**Formación académica:** Con título profesional o bachiller o técnico en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante de la solución ofertada. **Experiencia:** Con mínimo dos (02) años de experiencia como Especialista en Servidores.	03

4.5. Personal Clave para el soporte a usuario final durante el periodo de soporte y garantía

Para el primer año el soporte y garantía, el Proveedor debe brindar el soporte 24x7, para lo cual deberá considerar 3 turnos.

El servicio debe estar estructurado como mínimo en tres niveles de atención, con escalamiento controlado y responsabilidades diferenciadas. La dotación se proyecta considerando continuidad 24x7 y una base instalada de equipamiento para operación.

El personal deberá considerar como mínimo los siguientes puestos para brindar el soporte requerido en 03 turnos con la finalidad de cubrir el servicio de 24x7:

- Analista de mesa de servicio,
- Soporte técnico para las diversas especialidades a nivel de usuario final.

4.6. Personal NO Clave

El Proveedor puede considerar otro personal al exigido de forma complementaria, sin que reemplace las actividades del personal clave, para la gestión, implementación y soporte y garantía.

4.7. Implementación

El Proveedor, previo a la instalación, configuración y pruebas, deberá presentar la topología final, plan de numeración en IPv4 e IPv6, plan de configuración, planes de despliegue, planes de rollback, plan de pruebas final, entre otros documentos que considere para su implementación. Esto deberá presentarlo por equipo o solución integral tres (03) días antes de su implementación en la Central 911, y será aprobado mediante acta por el Gerente de Proyectos asignado por el Comprador.

Finalizada la instalación, configuración y pruebas, deberá actualizar los documentos finales, y entregarlos en sobre lacrado para la "Aceptación Operativa".

Nota: Todas las soluciones deberán ser configuradas en doble pila (IPv4/IPv6), para lo cual el Proveedor deberá considerar los complementos tecnológicos (hardware y/o software) necesarios para su operatividad y correcta operación, sin afectar el performance de la red en su integridad.

4.8. Aceptación Operativa

Finalizada la implementación, el comprador (Pronatel), a través del Gerente de Proyectos asignado a este requerimiento, solicita al Proveedor toda la documentación desde el diseño hasta las pruebas finales integrales, y de considerar solicitar pruebas adicionales. Asimismo, se revisa que el Proveedor presente toda la documentación

para la operación como planes BCP, DRP, SLAs, mesa de servicio y SOC 7x24, manuales, y que todos los sistemas estén debidamente integrados con las demás soluciones y operativas.

La Aceptación Operativa será realizada mediante acta firmada entre el Gerente del Proyecto del Comprador y el Jefe de proyectos del Proveedor. Esta acta con toda la documentación que forma parte de la aceptación operativa, deberá ser presentada por el Proveedor en la mesa de partes del Comprador para el proceso de pago final.

4.9. Recursos y Servicios para entregar por el Comprador

El Comprador, dará todas las facilidades de acceso a la Central 911, los planos finales del sistema de cableado estructurado, centro de datos y demás soluciones tecnológicas que requiera el Proveedor para el cumplimiento del presente requerimiento.

4.10. Gestión de Activos

El Proveedor es responsable de todo lo suministrado en el presente requerimiento desde su adquisición, traslado a sus almacenes, traslado a la Central 911, todo el proceso de implementación, hasta la aceptación operativa final otorgada por el Gerente de Proyectos del Comprador.

Deberán considerar el etiquetado de todo el equipamiento a entregar, para lo cual cargará en el software de mesa de servicio todos los activos, donde se detalle, ubicación, área, usuarios, marca, modelo, # serie, entre otros datos de los bienes provistos por el Proveedor en este requerimiento.

4.11. Embalaje y/o Rotulado

El proveedor será responsable de que el embalaje, rotulado, identificación y documentación de los bienes objeto de la contratación sean adecuados, completos y suficientes para garantizar su correcta protección, identificación y control durante el transporte, almacenamiento y entrega.

El embalaje deberá ser nuevo y apropiado para equipos de TI. El rotulado deberá ser claro, legible e indeleble, colocado en el interior y exterior de los paquetes, e incluir como mínimo la identificación del proveedor, descripción del bien, cantidad, número de serie (cuando corresponda) y referencias del contrato y del Proyecto 911.

El incumplimiento de lo señalado será causal de observación, rechazo o no conformidad de los bienes, sin perjuicio de las acciones correctivas que correspondan, siendo de exclusiva responsabilidad del proveedor, sin generar costos adicionales para el Comprador.

4.12. Salud y Seguridad

El personal del Proveedor deberá tener SCTR en salud y pensión, desde el inicio de los trabajos, con los Equipos de Protección Personal (EPP) según el tipo de trabajo, para lo cual deberá de presentar su Plan de Seguridad, Salud y Trabajo en el Plan de Proyecto, con la matriz IPERC.

Previo a los trabajos en la Central 911, deberá recibir la charla de inducción respectiva. Este será dado por el Especialista SSOMA del Proveedor, quien lidera y coordina con sus pares del Contratista de la Obra, la Supervisión de la Obra y con el personal del Comprador.

4.13. Logistica y Control

Traslado y entrega

El Proveedor será plenamente responsable del traslado, transporte y entrega de los bienes objeto del contrato hasta el lugar de la Central 911, incluyendo las maniobras de carga, descarga, estibas necesarias e incluso el almacenaje con seguridad del Proveedor.

Seguro de Transporte
El Proveedor deberá contratar, bajo su exclusivo costo y responsabilidad, un seguro de transporte que cubra los bienes desde el punto de origen hasta su entrega final y conformidad, amparando los riesgos de pérdida, robo, daño, deterioro, siniestro, accidente u otros riesgos habituales durante el traslado o almacenaje.

Transporte y Almacenaje
Cualquier daño, pérdida o menoscabo que sufran los bienes durante el transporte, almacenaje, instalación hasta la aceptación operativa será responsabilidad exclusiva del Proveedor, quien deberá proceder a la reposición inmediata de los bienes afectados, sin costo adicional para el Comprador y sin perjuicio de la aplicación de las penalidades que correspondan.

4.14. Acreditación y Control de Acceso
El personal del Proveedor deberá estar debidamente identificado con su fotocheck y vestimenta con los logos que identifiquen al Proveedor, tanto en camisa, chalecos, polos y casco.

Para el acceso, el Proveedor deberá enviar una semana antes del inicio de sus actividades en la Central 911, la lista del personal adjuntado DNI y antecedentes penales.

4.15. Integraciones
El Proveedor en su plan de proyecto deberá incluir un acápite para las integraciones tecnológicas con las soluciones implementadas en la Central 911, para lo cual el Proveedor podrá solicitar las reuniones de coordinación y técnicas necesarias al Gerente de Proyectos del Comprador para que sean realizadas con el Contratista de la Obra, la Supervisión de la Obra y el resto de Los proveedores presentes en la Central 911.

Estas integraciones son:
- Integración entre la red LAN y Equipamiento Ofimático
- Integración entre la red LAN y el SAGE
- Integración entre la red LAN y el Centro de datos
- Integración entre la red LAN y los servicios de Telecomunicaciones
- Integración entre la red LAN y el Sistema TETRA

4.16. Entrenamiento Técnico
El Proveedor deberá presentar el plan de entrenamiento técnico para su aceptación operativa, el cual será realizado para 2 personas por cada solución que se lista a continuación: Switches, Red inalámbrica, Firewall, Hiperconvergencia, XDR, SIEM, SOAR, NDR, PAM y la Solución de respaldo.

El entrenamiento técnico será realizado en el primer semestre del soporte y garantía, y serán cursos oficiales a nivel fundamentos emitidos por cada fabricante propuesto. Siendo responsabilidad del Proveedor asumir todos los gastos como traslados, impuestos, y otros que se consideren para la correcta ejecución del entrenamiento técnico.

4.17. Lugar y Plazo de Entrega

Lugar:
La entrega de los equipos previo a la instalación será realizada en la Central 911, para lo cual el Proveedor deberá instalar un almacen con todas las condiciones físicas, ambientales y de seguridad para su posterior implementación, previa coordinación con el Gerente de Proyecto del Contrato.

El servicio se realizará en las instalaciones del Edificio de la Central 911 se ubica en la Avenida el Sol S/N, Distrito de Chorrillos, Provincia y departamento de Lima de forma presencial.

Plazo:
El plazo de entrega de bienes es de hasta 75 días calendarios contabilizados al día siguiente de la firma del Contrato.

El plazo para la implementación es de 90 días calendarios contabilizados al día siguiente de la firma del Contrato.

La garantía y soporte del Proveedor están indicados en el Anexo 3 del presente documento. Con relación a la mesa de servicio y SOC, estas inician con el soporte y garantía por un periodo de 12 meses, y estarán habilitados para garantizar la continuidad del Proyecto y su correcta transferencia al MININTER.

El entrenamiento se realizará dentro del primer semestre de año de garantía y soporte.

La puesta en Operación del servicio será posterior a la aceptación operativa y a través de un acta firmada entre el Jefe de Proyectos del Proveedor y el Gerente de Proyectos del Comprador en donde se establecerá la fecha de inicio para el Soporte y Garantía.

"Año de la Esperanza y el Fortalecimiento de la Democracia"

ANEXO 1 – CARACTERÍSTICAS TECNICAS

Equipamiento Ofimático

Estaciones de trabajo

1. Computadora de Escritorio Tipo 1 (210 Unidades)

Factor de forma	Mini
Sistema Operativo	Windows 11 LTSC
Procesador	Intel Core i7 de última generación
Memoria RAM	16GB DDR5 5600MHz
Tarjeta de Video	Dedicada PCIe de 4Gb DDR6 Compatible con DirectX 10.0 con 256 MB.
Unidad de Almacenamiento	500Gb PCIe M.2 SSD.
Bios	Instalado UEFI BIOS, de la misma marca del fabricante del equipo. -Precargado el número de serie de la computadora. -Herramienta de diagnóstico capaz de generar análisis de sistema y códigos de error. -Actualización del BIOS del equipo mediante descarga de software de la WEB del fabricante
Puertos	3x HDMI y/o MiniHDMI (con sus adaptadores) y/o 3x Displayport y/o 3x MiniDP 6x USB SuperSpeed Tipo A 10Gbps. 1x USB 3.2, 1x USB-C.
Audio	Integrado de Alta Definición soporta múltiple transmisión. 1x mini-jack universal de 3.5mm.
Conectividad	2x puertos de red RJ45, 10/100/1000 Mbps.
Certificación	Energy Star.
Fuente de Alimentación	CA 120/230 V (50/60 HZ). Estándar de 200 Watts certificada.

2. Computadora de Escritorio Tipo 2 (71 Unidades)

Factor de forma	Mini / SFF
Sistema Operativo	Windows 11 Profesional de 64 bits OEM
Procesador	Intel Core i7 de última generación
Memoria RAM	16Gb. DDR5 5600MHz
Unidad de Almacenamiento	500Gb PCIe M.2 SSD.
Bios	Instalado UEFI BIOS, de la misma marca del fabricante del equipo. -Precargado el número de serie de la computadora. -Herramienta de diagnóstico capaz de generar análisis de sistema y códigos de error. -Actualización del BIOS del equipo mediante descarga de software de la WEB del fabricante
Puertos	1 x HDMI 1 x DisplayPort 1.4 integrado 4 x USB-A de 5Gbps delanteros 4 x USB-A de 5Gbps traseros

	2 x Ethernet 1GbE RJ-45 1 x USB-C
Audio	Integrado de Alta Definición soporta múltiple transmisión. 1x mini-jack universal de 3.5mm.
Conectividad	2x puertos de red RJ45, 10/100/1000 Mbps. Wi-Fi integrada. Bluetooth 5.0.
Ofimática	Office LTSC 2024
Certificación	Energy Star
Fuente de Alimentación	Estándar de 200 Watts certificada.

3. Monitor para Computadoras (696 Unidades)

Tamaño	23-24 pulgadas
Tipo:	LED
Resolución	1920x1080p
Tipo de Panel	TN
Tiempo de Respuesta	<5 ms
Brillo	250 cd/m2
Interfaz	HDMI y/o Displayport
Fuente de Alimentación	CA 120/230 V (50/60 HZ).
Certificación	Energy Star

4. Teclado y Mouse (281 Unidades)

Teclado	Alámbrico en español.
Mouse	Alámbrico tres botones Sensor óptico Ambidiestro y/o Ergonómico
Conexión	USB
Compatible	Windows 11 professional

5. Soporte para 03 Monitores para Computadoras de Escritorio Tipo 1 (210 Unidades)

Compatibilidad	De 13 a 24 pulgadas.
VESA compatible	75x75, 100x100mm
Carga	7 kg (Por pantalla)
Giro	+90°~-90°
Inclinación	+45°~-45°
Rotación	+180°~-180°
Extensión del Brazo	658mm
Altura del Poste	443mm
Material	Acero, plástico.
Color	Negro
Gestión de cables	SI
Cantidad de Monitores	03 por soporte. Los monitores a soportar son los que se proveerán en el numeral 1.3 de este Anexo.

6. Equipo Portátil (09 Unidades)

Procesador	Intel Core I9 (Décimo cuarta generación) y/o su equivalente en AMD
Memoria RAM	16GB.
Almacenamiento	Disco SSD 512 GB
Pantalla	LCD retroiluminación LED, HD de 14".
Puertos	USB, HDMI, RJ45/Ethernet, Audio y Micrófono 3.5mm
Teclado	En español.
Multimedia	Cámara WEB HD, Micrófono integrado, altavoces.
Conectividad	Wifi, 10/100/1000 Mbps.
Fuente de alimentación	Adaptador de alimentación de 220V.
Software	Windows 11 professional (64bits en español). Office 2024.

Perifericos Especializados

7. Auricular Monoaural (210 Unidades)

Tipo de conexión	USB (audio y alimentación)
Material almohadillas	Cuero Sintético y/o similar
Micrófono	Omnidireccional, 35 Hz a 21 kHz Sensibilidad -40 ± 3dB
Parlante	< 6 mm, 20Hz a 20 KHz
Tasa señal / ruido	> 50dB
Peso	< 55 gramos
Longitud de Cable	> 2 metros

8. Micrófono (115 Unidades)

Tipo de Micrófono	Cuello de ganso flexible
Tipo de Conexión	USB (audio y alimentación)
Frecuencia	150 - 12500 Hz a 48 KHz de tasa de muestreo
Distorsión Armónica	<5%
Cancelación de ruido	20dB de cancelación activa
Longitud de Cable	> 2 metros

9. Altavoces (115 Unidades)

Tipo de Conexión	USB 3 (audio y alimentación)
Respuesta en frecuencia	120 - 10300 Hz a 48 KHz de tasa de muestreo
Frecuencia	150 - 12500 Hz a 48 KHz de tasa de muestreo
Distorsión Armónica	<5%
Nivel de potencia de audio máxima	95 dB SPL a 50 cm (aproximadamente 10W)
Control de Volumen	Dedicado
Montaje	Opciones de montaje flexible
Longitud de cable	> 2 metros

10. PPT de pie (210 Unidades)

Tipo de Conexión	USB 3 (audio y alimentación)
Material	Hierro fundido pesado
Base	Antideslizante
Longitud de cable	> 3 metros
Homologación	*El sistema ha sido homologado con pedaleras Kinesis FS22AJ-JSB. Modelos adicionales deben ser validados*

	previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.
Control de Volumen	Dedicado
Montaje	Opciones de montaje flexible
Longitud de cable	> 2 metros

11. Cámara Web (281 Unidades)

Tipo de Conexión	USB 3 (audio y alimentación)
Resolución	1080p
Micrófono	Micrófono omnidireccional estéreo
Cable	1.15 m.

Teléfonos IP

12. Teléfonos IP Tipo 1 (201 Unidades)

Marca	Mitel
Modelo	6865i
Pantalla	LCD monocromática 3.4" (128×48) con retroiluminación
Teclas físicas	8 teclas programables con LED; 2 teclas de línea "hard" con LED
Red	Doble puerto Gigabit Ethernet (10/100/1000) con switch integrado (LAN + PC)
Auriculares	Soporte nativo DHSG/EHS para headset analógico
Alimentación	PoE IEEE 802.3af Clase 2 o adaptador de corriente
Capacidad de líneas (call lines)	Hasta 24 call lines con LED
Homologación	Compatibilidad con el modelo de la central telefónica MX-ONE y versión del sistema operativo 7.7.1.0.15. Modelos adicionales deben ser validados previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.

13. Teléfonos IP Tipo 2 (62 Unidades)

Marca	Mitel
Modelo	6920w
Protocolos	SIP y MiNet
Pantalla	LCD color 3.5" (QVGA, 320×240)
Líneas	Hasta 20 líneas
Teclas	18 teclas de función programables; 4 teclas contextuales
Wi-Fi	Dual band 802.11 a/b/g/n
Bluetooth	Bluetooth 5.2 (documentación reciente / quick reference)
Red	2× puertos Gigabit Ethernet (LAN + PC)
Audio	Altavoz full-duplex; "HD audio"; lista de códecs incluye G.711/G.729/G.722, etc.
Puertos / expansión	USB 2.0 host (500 mA); puerto "sidecar/expansion"
Seguridad / QoS	Voz cifrada; IEEE 802.1p/Q (VLAN/priority); IEEE 802.1X
Alimentación	PoE IEEE 802.3az (en este datasheet figura Clase 3) y soporte de fuente 48V
Homologación	Compatibilidad con el modelo de la central telefónica MX-ONE y versión del sistema operativo 7.7.1.0.15. Modelos adicionales deben ser validados previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.

14. Teléfonos IP Tipo 3 (16 Unidades)

Marca	Mitel
Modelo	6930t
Enfoque	Plásticos con tratamiento antimicrobiano
Protocolos	MiNet y SIP
Pantalla	4.3" color (480×272)
Líneas	Hasta 24 call lines
Teclas	Teclas programables + contextuales
Bluetooth	Bluetooth 4.1 (MobileLink)
Wi-Fi	No integrado
Red	2× puertos Gigabit Ethernet (LAN + PC)
Headset	USB + puerto analógico EHS/DHSG (y puerto modular 4-pin convertible)
USB host	USB 2.0 host (500 mA)
Alimentación	PoE Clase 2 + 48V local
Homologación	Compatibilidad con el modelo de la central telefónica MX-ONE y versión del sistema operativo 7.7.1.0.15. Modelos adicionales deben ser validados previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.

15. Teléfonos IP Tipo 4 (4 Unidades)

Marca	Mitel
Modelo	6940w
Pantalla	7" color touch (800×480)
Wi-Fi	Dual band 802.11 a/b/g/n
Bluetooth	Bluetooth 5.2
Líneas / teclas	Acceso mediante teclas programables "soft" a hasta 96 líneas (según plataforma)
Red	2× Gigabit Ethernet (LAN + PC)
USB	USB 2.0 host (500 mA)
QoS / Seguridad	QoS 802.1p/Q, 802.1X, voz cifrada
Alimentación	PoE Clase 3; soporte de fuente 48V. Ojo: si instalas DECT integrado y/o M695, requiere alimentación por adaptador 48V
Homologación	Compatibilidad con el modelo de la central telefónica MX-ONE y versión del sistema operativo 7.7.1.0.15. Modelos adicionales deben ser validados previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.

16. Botonera para teléfono IP 4 (1 Unidad)

Marca	Mitel
Modelo	Botonera
Pantalla del módulo	4.3" LCD color
Teclas	28 teclas programables × 3 páginas
Encadenamiento	Hasta 3 módulos enlazables
Compatibilidad	Soportado en 6920w / 6930w / 6940w
Alimentación	Se alimenta desde el teléfono, pero el fabricante recomienda/indica uso de adaptador de escritorio (no sólo PoE) para ciertos escenarios con accesorios
Homologación	Compatibilidad con el modelo de la central telefónica MX-ONE y versión del sistema operativo 7.7.1.0.15.

	Modelos adicionales deben ser validados previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.

17. Pantalla para Monitoreo (02 Unidades)

Pantalla:	Full HD (1920 x 1080) o superior.
Dimensiones:	55" diagonal o superior.
Tecnología:	IPS y/o D-LED o LCD
Vida útil:	50 mil horas o superior.
Entradas de video:	2 entradas DP 1.2, 2 entradas HDMI 2.0 o superior.
Salidas de video:	1 salida DP 1.2 o superior.
Puerto Ethernet:	Si
Wifi:	Si

18. Videoconferencia (04 Unidades)
Especificación técnica Sala 08 personas (01 Unidad)

Camara	• Resolución: 4K, 1440p, 1080p, 900p, 720p y SD a 30fps • Panorámica: Robotizada ±25° • Inclinación: Robotizada ±15° • Zoom: Zoom digital HD 4x • Campo visual diagonal: 120°, Campo visual horizontal: 113°, Campo visual vertical: 80.7° • Cobertura total de sala (campo visual + panorámica e inclinación): 163° horizontal x 110° vertical
Parlante Subwoofer	• Transductor: 70 mm • Sensibilidad: 92 dB SPL a 1 W, 99 dB SPL a 8.0 W, ambos +/-2 dB a 0.5 m • Potencia nominal: 8W • THD: 1 kHz < 2% a 1 W • Frecuencia de muestreo de bocina: 48 kHz • Impedancia: 4 ohmios
Parlante Altavoces	• Transductores: 2 de 43 mm • Sensibilidad: 84 dB SPL a 1 W/1 M • Potencia nominal: 4W • THD: 1 kHz < 2% a 1 W • Frecuencia de muestreo de bocina: 48 kHz • Impedancia: 4 ohmios
Micrófonos	• Respuesta de frecuencia: 90 Hz – 16 kHz • Sensibilidad: >-36 dBFS +/-1 dB a 1 Pa • Velocidad de salida de datos de micrófono: 48 kHz • Radio de captación: Hasta 7 m • Elementos de formación de haces: 6 micrófonos MEMS digitales omnidireccionales que forman 5 haces de difusión acústica adaptativa • Procesamiento de audio: AEC (Acoustic Echo Cancellation), VAD (Voice Activity Detector) • Supresión de ruido: Algoritmo de supresión de ruido basado en inteligencia artificial • Micrófonos adicionales: Admite hasta tres micrófonos adicionales

	• Visualización en cuadrícula: Detecta y encuadra a todos los participantes de la reunión para crear experiencias de reunión híbridas equitativas.
Interfaces	• Salida HDMI: 2 • Entrada HDMI: 1 • USB: 3 x Tipo A, 1x Tipo C • Red: Ethernet 10/100/1G • WiFi: 802.11a/b/g/n/ac • Entrada de micrófono externo: Sí • Control remoto: Bluetooth® Low Energy
Alimentación y cables	• Fuente de alimentación: Detección automática • Alimentación/Voltaje de servicio: 100-240 V, 19 V, 4,74 A • Cable de CC: 1,5 m, Cable de CA: 1 m, Cable HDMI 1.4: 2 m, Cable USB A a USB C 3.0: 2,2 m
Medioambiente	• Temperatura de funcionamiento: 0 °C a 40 °C • Temperatura de almacenamiento: -40 a 70°C • Humedad: 10 % a 95 % • BTU/h: 57 (en inactividad), 64 (durante reuniones)
Seguridad	• Cifrado de disco completo: AES-128 • Cifrado de datos: Claves simétricas, infraestructura de clave pública (PKI) • Identidad de dispositivos: Protección mediante atestación de estado de dispositivos • Acceso a dispositivos: Autenticación mediante API • Protección mediante clave: Arm TrustZone, RPMP
Accesorios	• Piezas de montaje: Pieza de montaje en pared para barras de video, pieza de montaje en TV para barras de video
Compatibilidad	• Sistemas operativos Windows 11 professional, macOS: 10.10 o posteriores y Chrome OS™ • El Proveedor debe garantizar la compatibilidad de todos sus accesorios y elementos que conforman la solución de videoconferencia para su correcta operación 24x7.
Pantalla	• LED 75" con sus accesorios a pared, y puerto red LAN / Wifi

Especificación técnica Sala 16 personas (02 Unidades):

Cámara	• Resolución: 4K, 1440p, 1080p, 900p, 720p y SD a 30fps • Panorámica: Robotizada ±25° • Inclinación: Robotizada ±15° • Zoom: Zoom 15X HD (óptico 5X y digital 3X) • Campo visual diagonal: 90°, Campo visual horizontal: 82,1°, Campo visual vertical: 52,2° • Cobertura total de sala (campo visual + panorámica e inclinación): 132,1° horizontal x 82,2° vertical
Altavoces	• Transductores: 2x 70 mm • Sensibilidad: 92 dB SPL a 1 W, 99 dB SPL a 8.0 W, ambos +/-2 dB a 0.5 m • Potencia nominal: 8W • THD: 1 kHz < 2% a 1 W • Frecuencia de muestreo de bocina: 48 kHz • Impedancia: 4 ohmios

Micrófonos	• Respuesta de frecuencia: 90 Hz - 16 kHz • Sensibilidad: >-36 dBFS +/-1 dB a 1 Pa • Velocidad de salida de datos de micrófono: 48 kHz • Radio de captación: Hasta 7 m • Elementos de formación de haces: 6 micrófonos MEMS digitales omnidireccionales que forman 5 haces de difusión acústica adaptativa • Procesamiento de audio: AEC (Acoustic Echo Cancellation), VAD (Voice Activity Detector) • Supresión de ruido: Algoritmo de supresión de ruido basado en inteligencia artificial • Micrófonos adicionales: Admite hasta cuatro micrófonos adicionales
Interfaces	• Salida HDMI: 2 • Entrada HDMI: 1 • USB: 3 x Tipo A, 1x Tipo C • Red: Ethernet 10/100/1G • WiFi: 802.11a/b/g/n/ac • Entrada de micrófono externo: Sí • Control remoto: Bluetooth® Low Energy
Alimentación y cables	• Fuente de alimentación: Detección automática • Alimentación/Voltaje de servicio: 100-240 V, 19 V, 4,74 A • Cable de CC: 1,5 m, Cable de CA: 1 m, Cable HDMI 1.4: 2 m, Cable USB A a USB C 3.0: 2,2 m
Medioambiente	• Temperatura de funcionamiento: 0 °C a 40 °C • Temperatura de almacenamiento: -40 a 70°C • Humedad: 10 % a 95 % • BTU/h: 57 (en inactividad), 64 (durante reuniones)
Seguridad	• Cifrado de disco completo: AES-128 • Cifrado de datos: Claves simétricas, infraestructura de clave pública (PKI) • Identidad de dispositivos: Protección mediante atestación de estado de dispositivos • Acceso a dispositivos: Autenticación mediante API • Protección mediante clave: Arm TrustZone, RPMP
Accesorios	• Pieza de montaje en pared para barras de video, pieza de montaje en TV para barras de video
Compatibilidad	• Sistemas operativos Windows 11 professional, macOS: 10.10 o posteriores y Chrome OS™. • El Proveedor debe garantizar la compatibilidad de todos sus accesorios y elementos que conforman la solución de videoconferencia para su correcta operación 24x7.
Pantalla	• LED 86" con sus accesorios a pared, y puerto red LAN / Wifi

Especificación técnica Sala 30 personas (01 Unidad):

Camara	• Zoom: - Zoom 15x HD (óptico 5x + digital 3x) • Panorámica: 180° (±90°) • Inclinación: 140° (+50° / -90°) • Campo visual • Diagonal: 90°

	• Horizontal: 82° • Vertical: 52° • Cobertura total de sala: 262° ancho x 192° alto (campo visual + panorámica e inclinación) Resoluciones @ 30fps: 4K Ultra HD, 1440p, 1080p, 900p, 720p, y SD Resoluciones @ 60fps: 1080p, 720p • Rango dinámico amplio (WDR), compensación de poca luz, reducción de ruido de video, optimización de saturación con poca luz • Privacidad: En modo de suspensión, la lente permanece en ángulo de -90° para garantizar la privacidad
Parlante	• Transductor de 76 mm de alto desempeño con imán de tierras raras • El sistema de suspensión pendiente de patente elimina el temblor de la cámara por vibración y las interferencias de audio • El cable Mini XLR se conecta al controlador de pantalla para proporcionar señal y alimentación • Volumen de bocina: 95 dB SPL a 1 W, 100 dB SPL a 7,5 W, ambos +/-2 dB a ½ metro • Sensibilidad: 95+/-2 dB SPL a ½ metro • Distorsión: 200 Hz–300 Hz <2,5%, 300 Hz– 10 kHz <1% a 7,5 W • Frecuencia de muestreo: 48 kHz
Micrófonos	• Radio de captación: 7 m de diámetro • Cuatro micrófonos omnidireccionales forman ocho haces acústicos • AEC: Cancelación de eco acústico • VAD: Voice Activity Detector (VAD), Supresión de ruido de fondo, Botón de silencio con LED indicador de estado, Cable cautivo de 12 patillas y 2,95 m, Conexión en serie de hasta 7 bases de micrófono • Respuesta de frecuencia: 90 Hz – 16 kHz • Sensibilidad: >-27 dB +/-1 dB a 1 Pa • Velocidad de datos de micrófono: 48 kHz
Interfaces	• Salida HDMI: 2 • Entrada HDMI: 1 • USB: 3 x Tipo A, 1x Tipo C • Red: Ethernet 10/100/1G • WiFi: 802.11a/b/g/n/ac • Entrada de micrófono externo: Sí • Control remoto: Bluetooth® Low Energy
Alimentación y cables	• USB 3.1 Tipo C a USB 3.1 Tipo C (2 m) • Computadora de sala de conferencias a controlador de pantalla o de sobremesa • USB 3.1 Tipo A a USB Tipo B (2 m)
Controlador de sobremesa	• Conexión de cable CAT6A individual • Detección de hablante activo: analiza cada 8 ms el audio de hasta 7 bases de micrófono y 56 haces • Conector de 12 patillas para base de micrófono • Paso de HDMI Tipo A a controlador de pantalla (x2) • Debe tener interfaz USB Tipo C, USB Tipo A, USB Tipo B y RJ45

Controlador de pantalla	• HDMI Tipo A: (x2) (conexión a pantallas), USB C (conexión a cámara), USB Tipo B (conexión a computadora de sala de reuniones) • Debe tener interfaz RJ45 y Mini XLR que alimenta una o dos bocinas
Accesorios	• Pieza de montaje en pared para barras de video, pieza de montaje en TV para barras de video
Compatibilidad	• Sistemas operativos Windows 11 professional, macOS: 10.10 o posteriores y Chrome OS™ • El Proveedor debe garantizar la compatibilidad de todos sus accesorios y elementos que conforman la solución de videoconferencia para su correcta operación 24x7.

19. Impresora tipo personal (13 Unidades)

Funciones Principales	Copia, impresión y escáner de red
Velocidad	40ppm
Tecnología de Impresión	Láser monocromático (blanco y negro)
Resolución de Impresión	1200 x 1200 ppp
Velocidad de escaneo	40 ipm
Tamaño de papel	Hasta A4
Memoria RAM	Hasta 512 MB
Tipo de escaneo y copia	Cama plana y alimentadora de documentos (adf)
Sistemas operativos soportados	Windows 10, Windows 11 en todas sus versiones
Conectividad	USB 2.0.
	LAN, WIFI
Impresión a doble cara	Automática (estándar)
Ciclo mensual de trabajo	Hasta 10 000
Voltaje de operación	220 V / 50/60 Hz.

20. Impresora tipo mediano volumen (05 Unidades)

Funciones Principales	Copia, impresión y escáner de red
Velocidad	Desde 50ppm
Tecnología de Impresión	Láser monocromático (blanco y negro)
Resolución de Impresión	1200 x 1200 ppp
Tamaño de papel	Hasta A4
Memoria RAM	2 GB
Tipo de escaneo y copia	Cama plana y alimentadora de documentos (adf)
Sistemas operativos soportados	Windows 10, Windows 11 en todas sus versiones
Conectividad	USB 2.0.
	LAN, WIFI
Impresión a doble cara	Automática (estándar)
Voltaje de operación	220 V / 50/60 Hz.

21. Proyector Multimedia (04 Unidades)

Proyector Multimedia	• Tecnología de proyección: Fuente de luz láser de estado sólido, basada en tecnología 3LCD, LCD, DLP o equivalente. • Resolución nativa mínima: WUXGA (1920 x 1200 píxeles). • Brillo mínimo: 7,000 lúmenes ANSI o ISO. • Relación de aspecto nativa: 16:10. • Compatibilidad con formatos 16:9 y Full HD. • Contraste dinámico mínimo: 2,500,000:1. • Vida útil de la fuente de luz: mínimo 20,000 horas. • Zoom óptico mínimo: 1.6x. • Lens Shift horizontal y vertical. • Corrección trapezoid • al horizontal y vertical. • Tamaño de imagen compatible con pantallas de 150 pulgadas o superiores. • Entradas mínimas: dos (02) HDMI, un (01) USB y un (01) puerto RJ45. • Administración y monitoreo mediante red. • Nivel de ruido máximo: 38 dB. • Alimentación eléctrica: 220 VCA, 60 Hz. • Instalación fija en techo mediante soporte metálico.
Ecran Motorizado	• Tipo: Pantalla de proyección motorizada eléctrica. • Formato: 16:9. • Tamaño mínimo: 150 pulgadas diagonales. • Área útil mínima de proyección: 3.30 m x 1.85 m. • Material de proyección: Tela blanca mate (Matte White) o equivalente. • Ganancia mínima: 1.0. • Ángulo de visión mínimo: 160°. • Bordes negros perimetrales. • Operación mediante motor eléctrico integrado. • Accionamiento mediante interruptor de pared. • Carcasa metálica de alta resistencia. • Instalación en techo o pared. • Operación silenciosa. • Tela resistente a deformaciones, arrugas y humedad.
Sistema de Distribución Audiovisual	• Matriz audiovisual digital profesional de cuatro (04) entradas por cuatro (04) salidas como mínimo. • Entradas mínimas: cuatro (04) puertos HDMI. • Salidas mínimas: cuatro (04) salidas HDBaseT o equivalente, pudiendo incluir salidas HDMI locales. • Resolución soportada mínima: 4K UHD. • Compatibilidad HDCP. • Capacidad de conmutación, distribución y replicación simultánea de una misma señal audiovisual hacia los proyectores instalados. • Capacidad de operación independiente por sala o en modo combinado para los tres ambientes. • Administración mediante panel frontal, interfaz web, red IP, RS-232 o equivalente. • Instalación en rack estándar de 19 pulgadas. • Transmisión de video, audio y señales de control mediante cableado estructurado categoría 6A o superior.

	• Deberá incluir receptores HDBaseT o interfaces equivalentes cuando los proyectores no cuenten con entrada HDBaseT integrada. • Deberá permitir la conexión de fuentes audiovisuales como computadoras portátiles, computadoras de sala, sistemas de videoconferencia, reproductores multimedia u otros equipos similares.
Accesorios	• Soportes de techo para proyectores. • Pantallas motorizadas. • Matriz audiovisual. • Receptores HDBaseT o interfaces equivalentes cuando sean requeridos por la solución propuesta. • Cableado de energía, señal y control. • Accesorios de fijación y montaje.

22. Tabletas Rugerizadas (37 Unidades)

Pantalla	Tamaño: 10" a 12". Resolución: >= 1920 x 1200.
Procesador / GPU	(Octa-core) o superior.
Memoria RAM	6 GB.
Almacenamiento	128 GB.
Conectividad	Wi-Fi 6, Bluetooth >= 5.0. 4G LTE + Nano-SIM y/o eSIM
Puertos	USB Type-C para carga y transferencia de datos.
Cámaras	Frontal >= 5 MP. Posterior >= 12 MP.
Audio	Altavoces estéreo. Micrófonos integrados para videollamadas.
Batería	Capacidad típica 7,000 mAh.
Sistema operativo	Android 11 o superior
Seguridad	Bloqueo biométrico (huella o reconocimiento facial). Cifrado del dispositivo.
Accesorios	Cargador (o fuente) y cable. Funda protectora.

Red LAN

Switching
23. Switches Spine Data Center (02 Unidades)

Características de Hardware	- Debe contar con 32 puertos QSFP28 (con capacidad de conectar transceivers a 40 ó 100 Gbps). - Factor de forma: Una unidad de rack. - Un (1) Puerto USB (USB-A o USB 2.0 o USB similar) para gestión de archivos. - Un (1) puerto de gestión fuera de banda RJ45. - Administración por Consola RJ-45 o USB-C. - Memoria RAM: Mínimo 16GB. - Memoria Flash o SSD: Mínimo 64GB. - Debe contar con fuentes de poder redundantes removibles en caliente y en la máxima configuración disponible tanto en cantidad de fuentes y de potencia de cada fuente. - Ventiladores redundantes. Mínimo 4 bandejas removibles en caliente. Flujo de aire Front-to-Back. - Se deberá incluir ocho (08) transceivers ópticos 100GE-SR4 con conectores LC en cada uno de los switches propuestos.
Capacidades de Procesamiento	- Buffer no menor a 32MB. - Capacidad de conmutación no menor a 6.4 Tbps. - Capacidad de reenvío de paquetes no menor a 2 Bpps. - Capacidad de tabla de direcciones MAC no menor a 90K. - Capacidad de rutas IPv4 mínima de 130K y rutas IPv6 de 30K.
Características del Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecientes al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso de APIs de tipo REST o similar. - Debe permitir el apilamiento de dos switches mediante la tecnología MC-LAG o similar manteniendo planos de control separados de modo que se maximice la alta disponibilidad del servicio. Estos dos switches apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. - Debe contar con una consola de configuración por la línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI ó web UI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la Consola Gráfica de Administración Integrada	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Deberá mostrar de manera gráfica el equipo, visualizando la distribución de puertos y el factor de forma.
Funcionalidades de Capa 2, Capa	- Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q)

3, de Seguridad y Gestión	- Spanning Tree (802.1w, 802.1s y 802.1d). - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad). - IEEE 802.1ab LLDP. - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping. - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP. - VXLAN estática. - VXLAN dinámica mediante BGP-EVPN. - Protocolos de enrutamiento: PBR, VRRP, RIPv2, RIPng, OSPFv2 y v3, BGP4 y MP-BGP. - BFD y ECMP. - DCBx, PFC, ETS, ECN. - VRF. - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP server para IPv4 e IPv6 y DNS. - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Soporte de "port mirroring" por puerto o grupo de puertos. - Jumbo Frames de al menos 9K bytes.

24. Switches Leaf Data Center (08 unidades)

Características de hardware	- Debe contar con 48 puertos SFP28 (con capacidad de conectar transceiver a 1, 10 ó 25 Gbps) y 6 puertos QSFP28 (con capacidad de conectar transceiver a 40 ó 100 Gbps) - Factor de forma: Una unidad de rack - Un (1) Puerto USB (USB-A o USB 2.0, etc). - Un (1) puerto de gestión fuera de banda RJ45 - Administración por Consola RJ-45 o USB-C. - Memoria RAM: Mínimo 32GB - Memoria Flash o SSD: Mínimo 64GB - Debe contar con fuentes de poder redundantes removibles en caliente y en la máxima configuración disponible tanto en cantidad de fuentes y de potencia de cada fuente. - Ventiladores redundantes. Mínimo 5 bandejas removibles en caliente. Flujo de aire Front-to-Back. - Se deberá incluir dieciséis (16) transceivers ópticos 100GE-SR4 con conectores LC a ser distribuidos entre los switches solicitados. - Se deberá incluir treinta y cuatro (34) transceivers ópticos 25GE-SR con conectores LC a ser distribuidos entre los switches solicitados. - Se deberá incluir cuatro (04) transceivers ópticos 10GE-SR con conectores LC a ser distribuidos entre los switches solicitados.

	- Se deberá incluir doce (12) transceivers 1000Base-T con conector RJ-45 a ser distribuidos entre los switches solicitados. - Se deberá incluir un (01) cable de apilamiento a 100 Gbps por cada switch para virtualizar/apilar los switches solicitados.
Capacidades de procesamiento	- Buffer no menor a 32 MB. - Capacidad de conmutación no menor a 3.6 Tbps. - Capacidad de reenvío de paquetes no menor a 2 Bpps. - Capacidad de tabla de direcciones MAC no menor a 98 K - Capacidad de rutas IPv4 mínima de 130 K y rutas IPv6 de 30 K.
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso APIs del tipo REST o similar. - Debe permitir el apilamiento de dos switches mediante la tecnología MC-LAG o similar manteniendo planos de control y enrutamiento separados de modo que se maximice la alta disponibilidad del servicio. Estos dos switches deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. - Soporte del balanceo de servidores de aplicaciones mediante Microsoft Network Load Balancer (NLB). - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola externa de administración de políticas	- La plataforma podrá estar compuesta por más de un software del mismo fabricante y en conjunto deberá como mínimo: ▪ Basarse en appliance físico o virtual. En caso de ser virtual, se deberá considerar todo el componente de hardware y software necesario para el funcionamiento de la herramienta. ▪ Debe incluir APIs que permita el desarrollo de futuras integraciones. ▪ Debe brindar visibilidad de los hosts conectados, máquinas virtuales, VLANs, servicios y cargas de trabajo ▪ Debe proveer una orquestación unificada para segmentación, seguridad y configuración de políticas ▪ Debe dar visibilidad sobre la red física y las cargas de trabajo que la utilizan ▪ Debe realizar optimización de las rutas de datos creando políticas de optimización de red para satisfacer las necesidades de las cargas de trabajo de aplicaciones críticas ▪ Debe permitir visualizar el estado de salud de los switches ▪ Permitir el descubrimiento de dispositivos de red
Funcionalidades de Capa 2, Capa 3, de seguridad y gestión	- Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d). - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad). - IEEE 802.1ab LLDP. - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping. - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP.

	- VXLAN estática. - VXLAN dinámica mediante BGP-EVPN. - Protocolos de enrutamiento: PBR, VRRP, RIPv2, RIPng, OSPFv2 y v3, BGP4 y MP-BGP. - BFD y ECMP. - DCBx, PFC, ETS, ECN. - VRF - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. No se aceptarán protocolos similares y/o propietarios. - Incluir TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos - Jumbo Frames de al menos 9K bytes

25. Solución de Orquestador DC (01 Unidad)

Características Generales	- La solución de orquestación debe ser definida por software y basada en APIs de modo que simplifique y acelere el aprovisionamiento de redes, la gestión de la seguridad y las operaciones diarias en infraestructura de red de Centros de Datos. - La solución deberá contar con la capacidad de orquestar los switches de Data Center spine y leaf ofertados como un único fabric, simplificando las operaciones y la resolución de problemas en infraestructura de red de Centros de Datos. - La solución deberá implementarse en alta disponibilidad.
Arquitectura y Capacidades Principales	- Debe permitir la definición y creación de topologías de centro de datos mediante software. - Debe permitir la automatización de las configuraciones VXLAN entre varias sedes. - Debe permitir la gestión unificada de múltiples fabrics a través de ubicaciones geográficas. - Debe permitir la visualización integral de mallas, VLANs, hosts, MVs y seguridad. - Debe contar con un mapa en tiempo real auto-documentado del entorno de red. - Debe brindar visibilidad integral, desde las MVs hasta los puertos físicos de switch. - Debe contar con una interfaz gráfica que permita señalar y hace clicks, para eliminar complejidades en su uso. - Debe contar con configuración asistida o guiada para implementaciones complejas. - Debe contar con asistentes intuitivos que permitan la automatización de EVPN.

	- Debe contar con APIs RESTful para integración con sistemas de orquestación de terceros y otros repositorios. - La solución deberá ser capaz de aprovisionar, configurar y optimizar la red propuesta en tiempo real, respondiendo a eventos de sistemas de terceros sin intervención manual.
Funcionalidades de Orquestación	- Debe permitir la configuración de virtualización/stacking de switches Leaf del DC. - Debe permitir la implementación de topologías Leaf and Spine en el DC. - Debe permitir la configuración de redes subyacentes (underlay) basadas en al menos BGP/OSPF u otros protocolos similares no propietarios. - Debe permitir la configuración de redes superpuestas (overlay) basadas en al menos BGP EVPN u otros protocolos similares no propietarios. - Debe permitir la gestión de la agregación de enlaces y de grupos VLANs. - Debe permitir la gestión de VRFs y EVPN - Debe permitir la gestión del firmware de los switches de DC.
Capacidades de Integración	- La solución debe ser compatible con los siguientes sistemas: SimpliVity, VMware vSphere, ESX, NSX, VSAN, Nutanix Prism y las soluciones de gestión del fabricante propuesto. - Debe permitir el descubrimiento y visualización de infraestructura virtual. - Debe permitir la respuesta automática a eventos del ciclo de vida de MVs. - Debe permitir la creación de políticas basadas en etiquetas de vSphere o nombres de MV.
Vistas Disponibles	- Debe contar con una "Vista de Host" que permita visualizar la conectividad integral desde MVs hasta NIC físicos. - Debe contar con una "Vista de Red" que permita visualizar la conectividad Spine and Leaf y la de los conmutadores virtuales.
Capacidades de Monitoreo	- Debe contar con capacidad de análisis de red para un monitoreo amplio de problemas. - Debe permitir el monitoreo de alertas de estado de hardware, CPU/memoria, transceptores. - Debe permitir la recolección de alertas syslog. - Debe permitir la gestión de telemetría continua/integral/distribuida/pervasiva para resolución de problemas.

26. Switch Core LAN Campus (02 Unidades)

Características de hardware	- Debe contar con 32 puertos SFP28 (con capacidad de conectar transceiver a 1, 10 ó 25 Gbps) y 4 puertos QSFP28 (con capacidad de conectar transceiver a 40 ó 100 Gbps). - Factor de forma: Una unidad de rack - Un (1) Puerto USB (USB-A o USB 2.0 o USB similar) para gestión de archivos. - Un (1) puerto de gestión fuera de banda RJ45 - Administración por Consola RJ-45 o USB-C. - Memoria RAM: Mínimo 16GB - Memoria Flash o SSD: Mínimo 32GB - Debe contar con fuentes de poder redundantes removibles en caliente y en la máxima configuración disponible tanto en cantidad de fuentes y de potencia de cada fuente. - Bandeja de ventiladores redundantes (mínimo 3 bandejas) removibles en caliente. Flujo de aire Front-to-Back. - Se deberá incluir un (01) transceiver óptico 25GE-SR con conectores LC en cada uno de los switches solicitados - Se deberá incluir ocho (08) transceivers ópticos 10GE-LR con conectores LC en cada uno de los switches solicitados. - Se deberá incluir cuatro (04) transceivers ópticos 10GE-SR con conectores LC en cada uno de los switches solicitados.

	- Se deberá incluir dos (02) transceivers ópticos 1000Base-T con conectores RJ-45 en cada uno de los switches solicitados. - Se deberá incluir un (01) cable de apilamiento a 100Gbps por cada switch para virtualizar/apilar los switches solicitados.
Capacidades de procesamiento	- Buffer no menor a 32MB - Capacidad de conmutación no menor a 2.4Tbps - Capacidad de reenvío de paquetes no menor a 1.7Bpps - Capacidad de tabla de direcciones MAC no menor a 80k - Capacidad de rutas IPv4 mínima de 130k y rutas IPv6 de 30k
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecientes al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso de APIs de tipo REST o similar. - Debe permitir el apilamiento de dos switches mediante la tecnología MC-LAG o similar manteniendo planos de control separados de modo que se maximice la alta disponibilidad del servicio. Estos dos switches apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI ó web UI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola grafica de administración integrada	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Deberá mostrar de manera gráfica el equipo, indicando la distribución de puertos y el factor de forma.
Funcionalidades requeridas de Capa 2, Capa 3, de seguridad y gestión	- Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d). - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad). - IEEE 802.1ab LLDP. - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping. - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP. - VXLAN estática. - VXLAN dinámica mediante BGP-EVPN. - Protocolos de enrutamiento: PBR, VRRP, RIPv2, RIPng, OSPFv2 y v3, BGP4 y MP-BGP. - BFD y ECMP.. - DCBx, PFC, ETS, ECN. - VRF. - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS.

	- Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos - Jumbo Frames de al menos 9K bytes

27. Switch de acceso 48 puertos PoE (22 Unidades + 01 unidad en spare)

Características de hardware	- El switch debe contar con 48 puertos RJ45 10/100/1000 Base-T con soporte de PoE 802.3at Clase 4 y 04 puertos de uplink SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps). - El switch debe contar con una capacidad PoE disponible ("PoE Budget") de 740W de modo que cualquiera de los 48 puertos RJ45 10/100/1000 Base-T pueda brindar hasta 30 W de potencia PSE mientras no se agote dicha capacidad PoE. - El switch debe contar con dicha capacidad PoE disponible ("PoE Budget") de 740W bajo cualquier situación de falla de una de las dos (02) fuentes de energía solicitadas. - Factor de forma: una (01) unidad de rack (RU: Rack Unit). - El switch debe contar con ASIC del mismo fabricante. - Un (01) puerto auxiliar USB (USB-A o USB 2.0 o similar). - Un (01) puerto de gestión fuera de banda 10/100/1000 RJ-45. - Administración por Consola RJ-45 o USB-C. - Capacidad de mantener el flujo de energización por los puertos Ethernet a los dispositivos cliente (Ej. Teléfono IP, cámaras IP, access point, etc.) incluso durante el proceso de reinicio del switch (PoE permanente). - Memoria RAM: Mínimo 8 GB. - Memoria Flash o SSD: Mínimo 8 GB. - Fuentes de poder reduntantes intercambiables en caliente (incluir fuente redundante). - Bandejas/Módulos de ventiladores redundantes, al menos dos, intercambiables en caliente. - Se deberá incluir once (11) transceivers ópticos 10GE-LR con conectores LC a ser distribuidos entre los switches solicitados. - Se deberá incluir dieciocho (18) cables de apilamiento de 1m de longitud a 10 Gbps a ser distribuidos entre los switches solicitados. - Se deberá incluir cuatro (04) cables de apilamiento de 3m de longitud a 10 Gbps a ser distribuidos entre los switches solicitados.
Capacidades de procesamiento	- Capacidad de reenvío no menor a 130 Mpps. - Capacidad de switching no menor a 176 Gbps. - Buffer mínimo de 6 MB. - Capacidad de tabla de direcciones MAC no menor a 32K. - Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K.
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecientes al mismo fabricante. El Motor de Analítica debe

	incluir monitoreo y diagnósticos avanzados mediante el uso de APIs de tipo REST o similar. - Debe permitir el apilamiento o stack clásico de hasta 8 switches de la misma familia. Se permitirá el uso de back plane stacking o de máximo dos de los puertos de uplink solicitados. Estos switches en stack o apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. Se debe incluir el hardware necesario para realizar el apilamiento o stack. - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola grafica de administración integrada	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Revisión del estado del PoE (cuando aplique), estatus, prioridad y uso por puerto. - Deberá mostrar de manera gráfica el equipo, indicando la distribución de puertos y el factor de forma. - Mostrar información de los dispositivos conectados al equipo. Se aceptará una consola de gestión externa licenciada con su respectivo hardware para cubrir dicho requerimiento.
Funcionalidades requeridas Capa 2, Capa 3, de seguridad y gestión	- Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d). - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad).. - IEEE 802.1ab LLDP. - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping. - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP. - Protocolos de enrutamiento: RIPv2, RIPng, OSPFv2 y v3. - VXLAN estática. - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS. - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - Control de acceso centralizado por RADIUS, para los usuarios de la red que se autentican vía 802.1x. - RADIUS y RADIUS CoA. - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo.

	- Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN. - Jumbo Frames de al menos 9K bytes.

28. Switch de acceso 24 puertos PoE (04 Unidades)

Características de hardware	- El switch debe contar con 24 puertos RJ45 10/100/1000 Base-T con soporte de PoE 802.3at Clase 4 y 04 puertos de uplink SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps). - El switch debe contar con una capacidad PoE disponible ("PoE Budget") de 740W de modo que cualquiera de los 24 puertos RJ45 10/100/1000 Base-T pueda brindar hasta 30 W de potencia PSE mientras no se agote dicha capacidad PoE. - El switch debe contar con dicha capacidad PoE disponible ("PoE Budget") de 740W bajo cualquier situación de falla de una de las dos (02) fuentes de energía solicitadas. - Factor de forma: una (01) unidad de rack (RU: Rack Unit). - El switch debe contar con ASIC del mismo fabricante. - Un (01) puerto auxiliar USB (USB-A o USB 2.0 o similar). - Un (01) puerto de gestión fuera de banda 10/100/1000 RJ-45. - Administración por Consola RJ-45 o USB-C. - Capacidad de mantener el flujo de energización por los puertos Ethernet a los dispositivos cliente (Ej. Teléfono IP, cámaras IP, access point, etc.) incluso durante el proceso de reinicio del switch (PoE permanente). - Memoria RAM: Mínimo 8 GB. - Memoria Flash o SSD: Mínimo 8 GB. - Fuentes de poder reduntantes intercambiables en caliente (incluir fuente redundante). - Bandejas/Módulos de ventiladores redundantes, al menos dos, intercambiables en caliente. - Se deberá incluir cinco (05) transceivers ópticos 10GE-LR con conectores LC a ser distribuidos entre los switches solicitados. - Se deberá incluir cuatro (04) cables de apilamiento de 3m de longitud a 10 Gbps a ser distribuidos entre los switches solicitados.
Capacidades de procesamiento	- Capacidad de reenvío no menor a 95 Mpps. - Capacidad de switching no menor a 128 Gbps. - Buffer mínimo de 6 MB. - Capacidad de tabla de direcciones MAC no menor a 32K. - Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K.
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecientes al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso de APIs de tipo REST o similar. - Debe permitir el apilamiento o stack clásico de hasta 8 switches de la misma familia. Se permitirá el uso de back plane stacking o de máximo dos de los puertos de uplink solicitados. Estos switches en stack o apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. Se debe incluir el hardware necesario para realizar el apilamiento o stack. - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola grafica	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el

de administración integrada	estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Revisión del estado del PoE (cuando aplique), estatus, prioridad y uso por puerto. - Deberá mostrar de manera gráfica el equipo, indicando la distribución de puertos y el factor de forma. - Mostrar información de los dispositivos conectados al equipo. Se aceptará una consola de gestión externa licenciada con su respectivo hardware para cubrir dicho requerimiento.
Funcionalidades requeridas Capa 2, Capa 3, de seguridad y gestión	- Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d). - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad). - IEEE 802.1ab LLDP. - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping. - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP. - Protocolos de enrutamiento: RIPv2, RIPng, OSPFv2 y v3. - VXLAN estática. - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS. - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - Control de acceso centralizado por RADIUS, para los usuarios de la red que se autentican vía 802.1x. - RADIUS y RADIUS CoA. - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN. - Jumbo Frames de al menos 9K bytes. -

29. Switch DMZ (02 Unidades)

Características de hardware	- Debe contar con 24 puertos SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps) y 04 puertos SFP56 (con capacidad de conectar transceivers a 1, 10, 25 ó 50 Gbps). - Factor de forma: Una unidad de rack - El switch debe contar con ASIC del mismo fabricante. - Un (01) Puerto USB (USB-A o USB 2.0 o similar).

	- Un (01) puerto de gestión fuera de banda RJ45. - Administración por Consola RJ-45 o USB-C. - Memoria RAM: Mínimo 8GB - Memoria Flash o SSD: Mínimo 32GB - Debe contar con fuentes de poder redundantes removibles en caliente y en la máxima configuración disponible tanto en cantidad de fuentes y de potencia de cada fuente. - Ventiladores redundantes, al menos dos módulos/bandejas de ventiladores, intercambiables en caliente. - Se deberá incluir ocho (08) transceivers ópticos 10GE-SR con conectores LC a ser distribuidos entre los switches solicitados. - Se deberá incluir ocho (08) transceivers 1000 Base-T con conectores RJ-45 a ser distribuidos entre los switches solicitados. - Se deberá incluir un (01) cable de apilamiento a 50Gbps por cada switch para virtualizar/apilar los switches solicitados.
Capacidades de procesamiento	- Capacidad de reenvío no menor a 654 Mpps. - Capacidad de switching no menor a 880 Gbps. - Buffer mínimo de 8MB - Capacidad de tabla de direcciones MAC no menor a 32K - Capacidad de rutas IPv4 mínima de 32K y rutas IPv6 de 16K
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso APIs del tipo REST o similar. - Debe permitir el apilamiento o stack clásico de hasta 8 switches de la misma familia. Se permitirá el uso de back plane stacking o de máximo dos de los puertos de uplink solicitados. Estos switches en stack o apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. Se debe incluir el hardware necesario para realizar el apilamiento o stack. - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola grafica de administración integrada	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Deberá mostrar de manera gráfica el equipo, indicando la distribución de puertos y el factor de forma. - Mostrar información de los dispositivos conectados al equipo. Se aceptará una consola de gestión externa licenciada con su respectivo hardware para cubrir dicho requerimiento.
Funcionalidades requeridas Capa 2, Capa 3, de seguridad y gestión	- Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d) - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad) - IEEE 802.1ab LLDP - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping

	- Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP - Protocolos de enrutamiento: PBR, VRRP, RIPv2, RIPng, OSPFv2 y v3, BGP4 y MP-BGP. - VXLAN estática. - VRF - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP - Control de acceso centralizado por RADIUS, para los usuarios de la red que se autentifican vía 802.1x. - RADIUS y RADIUS CoA - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN - Jumbo Frames de al menos 9K bytes

30. Switch de Gestión Fuera de Banda (02 Unidades)

Características de hardware	- El switch debe contar con 48 puertos RJ-45 10/100/1000 Base T con y 04 puertos SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps). - Factor de forma: una (01) unidad de rack (RU: Rack Unit). - El switch debe contar con ASIC del mismo fabricante. - Un (01) puerto auxiliar USB (USB-A o USB 2.0 o similar). - Un (01) puerto de gestión fuera de banda 10/100/1000 RJ-45. - Administración por Consola RJ-45 o USB-C. - Memoria RAM: Mínimo 8GB - Memoria Flash o SSD: Mínimo 8GB - Fuente de poder y ventiladores embebidos (fijos). - Se deberá incluir un (01) cable de apilamiento a 10Gbps por cada switch para virtualizar/apilar los switches solicitados.
Capacidades de procesamiento	- Capacidad de reenvío no menor a 130 Mpps. - Capacidad de switching no menor a 176 Gbps. - Buffer mínimo de 6MB - Capacidad de tabla de direcciones MAC no menor a 32K - Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso APIs del tipo REST o similar.

	- Debe permitir el apilamiento o stack clásico de hasta 8 switches de la misma familia. Se permitirá el uso de back plane stacking o de máximo dos de los puertos de uplink solicitados. Estos switches en stack o apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. Se debe incluir el hardware necesario para realizar el apilamiento o stack. - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola grafica de administración integrada	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Deberá mostrar de manera gráfica el equipo, indicando la distribución de puertos y el factor de forma. - Mostrar información de los dispositivos conectados al equipo. Se aceptará una consola de gestión externa licenciada con su respectivo hardware para cubrir dicho requerimiento.
Funcionalidades requeridas Capa 2, Capa 3, de seguridad y gestión	- Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d) - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad) - IEEE 802.1ab LLDP - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP - Protocolos de enrutamiento: RIPv2, RIPng, OSPFv2 y v3. - VXLAN estática - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP - Control de acceso centralizado por RADIUS, para los usuarios de la red que se autentifican vía 802.1x. - RADIUS y RADIUS CoA - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN - Jumbo Frames de al menos 9K bytes.

Red Inalámbrica

31. Controlador Inalámbrico (02 Unidades)

- Deberá ser del tipo appliance y trabajar en conjunto con un servicio o software externo del mismo fabricante on-premise o en nube el cual se encargará de la gestión, monitoreo y la capa de control.
- Deberá ser una solución que permita extender el mismo registro/control que se realiza en la red inalámbrica a la red cableada (switches) propuesta.
- Características de controlador en formato appliance hardware:
  - Mínimo cuatro (04) puertos SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps). Se deberá incluir dos (02) transceivers 10GE-SR por cada equipo ofertado.
  - Un (01) puerto consola RJ45 o similar.
  - Fuente redundante de energía.
  - Capacidad de poder registrar/controlar al menos 3000 dispositivos.
  - Capacidad de mantener conectados al menos 9000 clientes/endpoints simultáneos.
  - Capacidad de manejar 30,000 túneles.
  - Throughput no menor de 10 Gbps.
- La solución de controladores inalámbricos deberá implementarse bajo un esquema de redundancia N+1, de modo que, en caso de falla de un controlador, se pueda mantener conectados al menos 9000 clientes.
- En caso que en el futuro se requiera aumentar la capacidad de clientes conectados, la solución deberá permitirlo mediante la adición de más controladores.
- Debe manejar los estándares 802.11 a/b/g/n/ac/ax.
- Debe de operar conjuntamente con el resto de los equipos de la solución inalámbrica y cableada para soportar las aplicaciones de datos, voz y video.
- Deberá de contar con software o servicio que le permita adaptarse y administrar en tiempo real el entorno de RF. Entre estas funciones deberá de encontrarse:
  - Asignación dinámica de canales para optimizar la cobertura y desempeño.
  - Balanceo de carga de usuarios entre múltiples puntos de acceso inalámbricos.
  - Detección y corrección de huecos en la cobertura inalámbrica.
  - Control dinámico de potencia de acuerdo con las condiciones de la red.
- Incluir un firewall stateful embebido de al menos 2M de sesiones, con la capacidad de aplicar políticas basadas en L3, L4 y L7 o de lo contrario incluir un firewall de la misma marca de los switches y access points con las siguientes características:
  - Firewall stateful de 2M de sesiones
  - Throughput 10Gbps
  - 2 puertos SFP+ con dos (02) transceivers 10GE-SR
- Detección y clasificación de puntos de acceso inalámbricos no legítimos de manera automática, con opción a llevar acciones de contención como alguna de las siguientes:
  - Contención en el aire. Los puntos de acceso de la solución permiten contener al rogue incrementando su señal u otro mecanismo similar para que el cliente se asocie a la red adecuada.
  - Contención en la red. Integración con la plataforma de switches que permita identificar con la información de la red inalámbrica el punto de red a la cual se ha conectado el rogue. Debe de poder inclusive, realizar un apagado de puerto o bloquear el tráfico del AP no autorizado.
  - Enviar paquetes de interferencia al dispositivo ilegítimo para desconectarlo de la red inalámbrica.
- Capacidad de poder manejar autenticaciones basadas en web que pueda servir para la autenticación de usuarios invitados.
- Bloqueo de tráfico entre clientes asociados a un mismo SSID.
- Soporte de AAA mediante un servidor de RADIUS y TACACS+ para manejar las políticas de usuarios.
- Debe incluir o estar integrado a una solución DPI (Deep Packet Inspection) con la cual se pueda visualizar, analizar y controlar el uso de tráfico a nivel capa 7 (aplicación).
- Debe poder identificar las aplicaciones que usan los clientes con la finalidad de permitir o restringir su uso además de establecer la velocidad de carga y descarga de cada una (shaping).
- Deberá soportar y tener habilitada las siguientes funcionalidades de calidad de servicio:

  - Soporte de Wi-Fi Multimedia (WMM)
  - Soporte de DSCP
- Soporte de asignación de ancho de banda por perfil de usuario de acuerdo con su rol en la red o grupo en el directorio activo
- Debe tener la capacidad de funcionar como servidor de DHCP o DHCP Proxy o DHCP Relay.
- Para la administración como mínimo debe de soportar el acceso via HTTPS, SSH, SNMP v2 o v2c y v3.
- Debe manejar los estándares 802.11 d/e/h.
- Debe estar integrado con sistemas WIPS o WIDS o tener uno embebido en el mismo equipo que como mínimo permita:
  - Contar con mecanismos precisos y automáticos para la clasificación real de Access Points intrusos que se encuentren en la red.
  - Proveer mecanismos automáticos y eficientes de contención de Access Points intrusos.
  - Detección de ataques avanzados, habilitar acciones de contención o mitigación de amenazas avanzadas y colección de datos del WLAN.
  - Incluir la integración con un sistema de prevención de intrusos avanzado y completo, que permita tener total visibilidad de amenazas, identificación de firmas de ataques reconocidos, tomar acciones correctivas de mitigación y contención.
  - Detección y clasificación de puntos de acceso inalámbricos no legítimos (rogue) de manera automática, con opción a llevar acciones de contención.
- El equipo deberá permitir la aplicación política de red de forma automática según el usuario o dispositivo, eliminando la necesidad de configurar VLANs, ACLs o subredes manualmente, garantizando la separación y la seguridad del tráfico mediante segmentación dinámica.

32. Access Point (43 Unidades + 04 Unidades en Spare)

Especificaciones de radio WiFi	- Antenas omnidireccionales integradas para MIMO 2x2 - Access point para interiores de tres radios: 2.4Ghz, 5Ghz y 6Ghz. - Ganancia de antena mínimo de 4 dBi en 2.4GHz, 7 dBi en 5GHz y 6 dBi en 6Ghz. - Radio 5 GHz: 2 flujos espaciales con una tasa de datos de hasta 1.2 Gbps - Radio 2.4 GHz: 2 flujos espaciales con una tasa de datos de hasta 287 Mbps - Radio 6 GHz: 2 flujos espaciales con una tasa de datos de hasta 2.4 Gbps - DFS (Dynamic Frequency Selection) - Tecnologías de radio: ▪ 802.11b: DSSS (Direct-Sequence Spread-Spectrum) ▪ 802.11a/g/n/ac: OFDM (Orthogonal frequency-division multiplexing) ▪ OFDMA en 802.11 ax - Tipos de modulación: ▪ 802.11b: BPSK, QPSK, CCK ▪ 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM ▪ 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256- QAM ▪ 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256- QAM, 1024-QAM - Máxima potencia de transmisión : ▪ Por radio/banda de 2.4 GHz, 5 GHz y 6 GHz: +18 dBm por cadena, +21 dBm agregado.
Especificaciones de protocolos	- ACC (Advanced Cellular Coexistence) - MRC (Maximum Ratio Combining) - CDD/CSD (Cyclic Delay/Shift Diversity) - STBC (Space-Time Block Coding) - LDPC (Low-Density Parity Check) - TxBF (transmit beam-forming) - TWT (Target Wait Time) - FTM (Fine Timing Measurement)

	- BSS Coloring - Tasas de datos soportadas (Mbps): ▪ 802.11b: 1, 2, 5.5, 11 ▪ 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 ▪ 802.11n: 6.5 hasta 300 (MCS0 a MCS15, HT20 a HT40) ▪ 802.11ac: 6.5 hasta 867 (MCS0 a MCS9, NSS = 1 a 2, VHT20 a VHT80). ▪ 802.11ax: (2.4GHz): 3.6 hasta 574 (MCS0 a MCS11, NSS = 1 to 2, HE20 a HE40) ▪ 802.11ax (5GHz): 3.6 hasta 1,201 (MCS0 a MCS11, NSS = 1 to 2, HE20 a HE80) ▪ 802.11ax (6GHz): 3.6 a 2,402 (MCS0 a MCS11, NSS = 1 a 2, HE20 a HE160) - A-MPDU, A-MSDU
Interfaces	- Dos interfaces 100/1000/2500 BASE-T Ethernet (RJ-45) - Velocidad de enlace auto-sensing y MDI/MDX - EEE (Energy Efficient Ethernet) 802.3az - - PoE-PD (entrada): 48 Vdc (nominal) 802.3bt PoE - Radio BLE (Bluetooth Low Energy) y Zigbee (802.15.4) - Interface host USB 2.0 (conector Tipo A) - Interface serial de la consola
Características adicionales	- Módulo TPM o TAM para asegurar la autenticidad del hardware y del código del access point. - Debe incluir kit para instalación en techo o pared. - En caso se necesite, el AP debe poder funcionar sin necesidad de un controlador centralizado, es decir, mediante un controlador embebido. - Aspectos Regulatorios: ▪ FCC/ISED ▪ CE Marked ▪ Low Voltage Directive 2014/35/EU ▪ UL/IEC/EN 60950 o 62368-1 ▪ EN 60601-1-2 - Certificaciones: ▪ UL2043 plenum rating ▪ Wi-Fi Alliance (WFA) certificado 802.11a/b/g/n/ac/ax (incluyendo radio 6Ghz) ▪ WPA, WPA2 y WPA3 – Enterprise with CNSA option, Personal(SAE), Enhanced Open (OWE)

33. Solución de Administración y Gestión Campus (01 Unidad)

Características Generales	- La solución de administración y gestión de la infraestructura campus podrá ser implementada en premisa con appliance de propósito específico o en la nube. - En el caso de una solución en premisa, deberá incluir alta disponibilidad de todos sus servicios. Cada appliance físico deberá tener: ▪ Dos (02) interfaces de 10Gbps ▪ Fuente de poder redundante ▪ Altura no mayor a dos (02) Rack Units (RUs) ▪ Kit para poder ser instalado en rack de 19" - En el caso de una solución en nube, se deberá presentar documentación o carta del fabricante que indique un SLA no menor a 99.95%. No se aceptarán soluciones basadas en VMs que obliguen a la institución a gestionar o contratar un Tenant de nube pública. - Debe administrar tanto la infraestructura de switching como la de Wireless. No se aceptarán herramientas independientes con cross launch. - Debe realizar el aprovisionamiento de los dispositivos de red por medio de PnP (Plug and Play) o ZTP (Zero Touch Provisioning)

	- El licenciamiento debe ser perpetuo. En caso de estar basado en suscripción deberá considerarse por 12 meses contados desde la fecha que inicie la garantía y soporte.
Monitoreo	- La solución debe contar con una interfaz fácil de utilizar. - La solución debe mostrar información actualizada sobre el uso de la red y métricas de rendimiento de la misma. - La solución debe mostrar el mapa topológico de la red. - La solución debe proveer vistas de red de cada dispositivo (por ejemplo, puntos de acceso, switches, etc) bajo su gestión: ▪ En el caso de la red inalámbrica para cada dispositivo o radio se deberá contar cómo mínimo con información sobre la cantidad de dispositivos conectados, ancho de banda (bajada y subida), modelo y versión de software, utilización de canales, ruido, pérdidas, errores y retransmisiones, dirección IP, serie, y dirección MAC. ▪ En el caso de la red cableada para cada dispositivo deberá contar cómo mínimo con información sobre modelo, serie, dirección MAC, dirección IP, versión de software, estado de puertos (estado, utilización de subida y bajada, vlans configuradas, información de paquetes unicast, multicas, broadcast, errores y descartes), PoE consumido y disponible, utilización de CPU y memoria, estado de ventiladores y fuentes. - Debe proveer información sobre los clientes inalámbricos y cableados conectados a los dispositivos de red gestionados como: ▪ En el caso de los clientes inalámbricos se deberá mostrar como mínimo el nombre de usuario o hostname, dirección IP, MAC, vlan, estado (en línea, fuera de línea o fallido especificando el por qué) radio y canal de conexión inalámbrica, velocidad, throughput de subida y bajada. ▪ En el caso de los clientes cableados se deberá mostrar como mínimo el nombre de usuario o hostname, dirección IP, MAC, vlan, puerto y switch al cual está conectado, throughput de subida y bajada. - Incluir visibilidad de las aplicaciones en capa 7, con capacidad de al menos 3000 para usuarios conectados vía LAN y/o WLAN.
Diagnóstico y alertas	- Debe permitir la habilitación y configuración de alertas - Las alertas deben poder ser categorizadas por severidad. - Las alertas deben poder ser personalizadas de tal forma que se puedan definir umbrales y severidades. - Las alertas deben poder ser enviadas por correo electrónico. - Incluir IA que detecte posibles problemas que afecten el rendimiento de la red y ofrecer pistas sobre la causa raíz del problema para ayudar al administrador en la resolución (Insights) - Contar con una IA que permita analizar el desempeño de la red basado en SLAs o baselines obtenidos de otros sitios de modo que se pueda afinar la configuración de manera manual o automática. - Contar con una IA que permita determinar la calidad de la cobertura basado en el análisis del roaming de los clientes inalámbricos u otros parámetros. - Debe permitir el monitoreo de servicio de red, como mínimo AAA, DHCP y DNS, de modo que se pueda conocer si las transacciones contra estos servicios se están dando de manera exitosa o no. - Debe permitir la integración con soluciones terceras por medio de Webhooks para el envío de notificaciones.
Administración de configuraciones y firmware	- La plataforma deberá poder hacer cambios de configuración en la infraestructura de red ya sea de manera global, por grupos de equipos o de manera específica a un dispositivo en particular. - Debe manejar el inventario de los dispositivos de red, recopilando la dirección IP, la MAC Address

	- Debe permitir la creación de tags o etiquetas (labels) para realizar la agrupación o identificación de dispositivos que tengan alguna característica en común - Debe permitir la organización de los dispositivos de red en ubicaciones geográficas de modo que se pueda contar con el detalle de las redes por sitio. - Debe ser capaz de generar una plantilla de configuración o grupo de configuración. Este debe poder ser aplicada a uno o varios dispositivos de red. - Creación de SSID y configuración de parámetros de RF - Carga de planos para la visualización del mapa de calor de la red inalámbrica - Debe proveer información de auditoria para todos los cambios realizados en la red que incluya el nombre del usuario que hizo el cambio, así como la fecha/horas y detalle del cambio. - Debe proveer la opción de actualizar el firmware de uno o más dispositivos a la vez de manera inmediata o programada. - Se debe poder definir versiones de firmware mínimas aceptables por tipo de equipamiento o grupo de dispositivos. - Debe indicar si es que hay una versión de firmware superior a la utilizada en los dispositivos. Asimismo, debe recomendar una versión de firmware por tipo de dispositivo. - Clasificación de dispositivos finales utilizando capacidades de Machine Learning (ML) - Debe incluir workflows intuitivos - Debe incluir integración por medio de APIs. - Deberá poder definir perfiles de acceso para distintos tipos de usuarios de tal manera que se puedan asignar distintos privilegios de acceso a cada una de las secciones o módulos de la consola.
Seguridad	- La solución deberá utilizar todos los dispositivos de red inalámbrica bajo su gestión para detectar dispositivos no autorizados tales como puntos de acceso "rogue". - La solución deberá ser capaz de monitorear eventos de IDS tales como el descubrimiento de dispositivos no autorizados o interferencias. - Debe tener la capacidad de permitir o denegar tráfico basado en aplicaciones, categoría de aplicaciones, reputación y categorías de sitios web. - La solución deberá proveer mecanismos para remediar o contener dispositivos no autorizados encontrados en la red.
Reportes	- La solución deberá generar reportes. - Los reportes deberán poder generarse y enviarse vía correo electrónico de manera diaria, semanal o mensual. - Los reportes generados deberán poder ser exportados en formato pdf o csv.

34. Solución de Control de Acceso (01 Unidad)

Características generales	- Se requiere una solución de control de acceso redundante con la cual se puedan aplicar políticas de acceso basadas en usuario, dispositivo, lugar y medio de conexión a todos los dispositivos que se conectan a la red. - Deberá soportar la aplicación de políticas de control de acceso para redes de cualquier tipo (LAN, WLAN y VPN) - La solución debe centralizar el control de acceso de usuarios administradores a dispositivos de red de la entidad vía TACACS+ para autenticación, autorización y accounting. - La solución debe basarse en un esquema AAA (autenticación, autorización y accounting). - Interfaz basada en WEB para la configuración de políticas y troubleshooting.

	- El sistema deberá contar con funcionalidad habilitada para proporcionar integración con las siguientes fuentes de autenticación externas: Directorio Activo de Microsoft, Mobile Device Management (MDM), servidores RADIUS y RADIUS token server, entre otros. - El sistema deberá contar con funcionalidad habilitada de integrarse con soluciones de terceros de modo que se puedan compartir contextos e interoperar con el fin de realizar acciones de enforcement en conjunto. - Deberá soportar Auto Sign-On y/o single sign-on (SSO) mediante SAML - Deberá permitir autenticación 802.1x, no 802.1x y acceso basado en portal web. - Soporte de varias fuentes de autenticación tales como RADIUS, LDAP, AD, HTTP, SQL, Kerberos y Okta. - Los tipos de enforcements aplicados para cada uno de los servicios de autenticación deben ser como mínimo: ▪ RADIUS enforcement permit / deny / CoA ▪ Policy assignment ▪ SNMP enforcement ▪ DACL ▪ TACACS+ ▪ HTTP ▪ Filter Id - El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multi dominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario. - La solución debe soportar y tener habilitados los siguientes métodos de autenticación como mínimo: ▪ PAP ▪ CHAP ▪ EAP-MSCHAPv2 ▪ EAP-MD5 ▪ PEAP ▪ EAP-TLS ▪ EAP-GTC ▪ MAC Authentication ▪ WEB Authentication ▪ EAP-FAST ▪ EAP-PWD ▪ SAML ▪ OAuth2 - La solución debe, dependiendo del perfil del usuario autenticado, poder asignarle políticas de manera granular de acuerdo a las siguientes condiciones combinadas o independientes: ▪ Acceso a la red basado en tiempos: determinación de intervalos de tiempo en donde está permitido el usuario en la red. ▪ Acceso de red basado en la localización del usuario en la red: en determinados lugares de la red debe permitir el acceso del usuario. ▪ Acceso de red basado en el tipo de acceso:aAnte determinados medios de acceso como WLAN, VPN, LAN, etc., si el usuario está autorizado, darle acceso a la red. ▪ Atributos extraídos del directorio activo o personalizaciones vía APIs. - De acuerdo a las condiciones descritas anteriormente, poder aplicar algún tipo de política al usuario. Como mínimo las siguientes: ▪ Asignación dinámica de vlans ▪ Asignación dinámica de listas de control de acceso. ▪ Redirección hacia una URL. - Deberá permitir utilizar atributos de múltiples repositorios de identidad tales como Microsoft Active Directory, LDAP, base de datos SQL compatibles con OBDC, servidores de Token y base de datos interna, con

	el objetivo de utilizar estos atributos dentro de una política para un control granular.
Reconocimiento de dispositivos (profiling)	- Descubrir y clasificar los dispositivos finales, independientemente del tipo de dispositivo. Por ejemplo: Impresora, dispositivo móvil, computadora, teléfono, entre otros. - Identificación y clasificación (profiling) basada en datos contextuales tales como: ▪ MAC OUIs ▪ Nmap Scan ▪ DHCP fingerprints ▪ TCP fingerprints ▪ HTTP user agent ▪ SNMP traps ▪ LLDP ▪ Netflow / IPFIX ▪ WMI ▪ Span Port - La funcionalidad de profiling debe estar licenciada para el 100% de conexiones simultáneas, debe ser capaz de identificar cambios en perfilamiento y modificar dinámicamente la autorización de privilegios. Es decir, si una impresora que ya había sido autenticada en el pasado aparece como una Laptop Windows, el sistema de control de acceso debe denegar el acceso de manera automática. - Debe permitir al administrador sobrescribir la clasificación de perfilamiento hecha por el sistema, o agregar una nueva regla de clasificación para los atributos aprendidos, a modo de permitir que endpoints desconocidos sean categorizados de manera adecuada.
Administración de acceso para dispositivos headless	- Deberá permitir identificar a los dispositivos no administrados no 802.1x (headless) –impresoras, teléfonos y cámaras IP y clasificarlos como conocido o desconocido. - Esta funcionalidad deberá estar disponible y habilitada para su despliegue.
Gestión de visitantes	- Deberá permitir crear perfiles de accesos y la creación de cuentas temporales de invitados para el acceso a la red WIFI y cableada. - Deberá permitir la creación de más de un portal cautivo - El portal cautivo incluirá funcionalidades avanzadas de auto-registro, mediante las cuales el invitado podrá generar su propia cuenta de invitado sin comprometer la seguridad de la red. - El portal proporcionará diversos métodos para la entrega de credenciales de invitado: email, SMS o impresión de tickets. - El portal proporcionará métodos avanzados de aprobación de la visita por parte de la persona que recibe al invitado que permitan autorizar la visita de manera flexible y sin intervención de personal de IT. Es importante que los usuarios que aprueban el acceso no deban contar con ningún tipo autorización con privilegios de administración hacia la plataforma de control de acceso/guest. - Para la autenticación vía portal o Portal Authentication es necesario que el protocolo usado por el portal o captive portal sea el estándar y no uno propietario lo cual impide que la solución inalámbrica se integre con soluciones de control de acceso de terceros.
Control de salud de los dispositivos	- Deberá soportar la validación de la salud del dispositivo mediante el uso de agentes instalados en el dispositivo final. - Deberá informar sobre la integridad del dispositivo final como el estado del antivirus, anti-spyware, firewall, aplicaciones peer-to-peer, a los cuales se les definirá la autorización de su uso. - Deberá soportar la auto-remediación para los dispositivos que no cumplen las políticas de salud. - Deberá soportar la clasificación de los dispositivos como saludable o cuarentena.

	- El sistema deberá proporcionar un agente ligero NAC (Network Access Control) que garantice la integridad de los dispositivos. Este agente comprobará el estado y actualización de anti-virus, anti-spyware, firewalls, etc., y proporcionará instrucciones de remediación en caso de que el dispositivo viole las políticas corporativas. El agente deberá ser compatible con, al menos: Windows, Linux y MacOS - También debe realizar comprobaciones avanzadas como detección de programas P2P, utilización de llaves USB como dispositivos de almacenamiento y valores dentro de las llaves del REGEDIT.
Aprovisionamiento automático de dispositivos móviles corporativos (BYOD)	- Se deberá ser capaz de comportarse como una Entidad Certificadora (CA) la cual genere e instale automáticamente certificados digitales en los dispositivos móviles entregados por la empresa a sus colaboradores. - Deberá proveer un portal de auto-servicio para que los usuarios puedas aprovisionar sus dispositivos sin intervención de TI - Deberá incluir de manera embebida la funcionalidad de Autoridad Certificadora (CA), que permita generar certificados que incluya la información específica de los usuarios y sus dispositivos. - Deberá incluir dentro de sus workflows, la opción de integrarse con sistemas MDM/EMM y MFA para incrementar los niveles de seguridad - Deberá permitir limitar la cantidad de dispositivos por usuario - Deberá soportar el aprovisionamiento para dispositivos con los siguientes sistemas operativos: Windows, Mac OS X, iOS, Android y Ubuntu - Deberá ser capaz de configurar de manera automática los parámetros de red en los dispositivos personales, para que éstos se puedan conectar de manera segura a la red corporativa con 802.1x - Deberá realizar perfilamiento automático para identificar tipo de dispositivo, fabricante, modelo y sistema operativo - Deberá proveer estadísticas de uso e inventario de los dispositivos móviles - Deberá permitir la personalización de los workflows de aprovisionamiento, para que, por ejemplo, un miembro del staff de TI deba aprobar la solicitud antes de que el usuario pueda conectar su dispositivo.
Plataforma	- Plataforma de la solución en formato appliance, mínimo de dos (02) nodos (appliances físicos) redundantes, con capacidad de soportar cada uno al menos 60,000 dispositivos endpoints autenticados simultáneamente. - Cada nodo deberá tener dos (02) conexiones 10GE-SR para conectarse con la red. - Cada nodo (appliance físico) deberá contar con: un procesador de por lo menos 32 cores y 32 threads, RAM de al menos 128 GB y storage de 960 GB SSD. - Licenciamiento a perpetuidad. - Se deberá considerar que se tendrán 2,000 dispositivos finales (endpoints) conectados de manera concurrente/simultánea a la red, cantidad que será independiente del tipo de autenticación que usen (por usuario y password, por MAC, por certificado, via portal, etc.). Se deberá considerar incluir para esta cantidad de dispositivos finales todas las funcionalidades descritas en las secciones "características generales", "reconocimiento de dispositivos", "administración de acceso para dispositivos headless", y "gestión de visitantes". - Se deberá considerar que 500 usuarios podrán conectar a la red empresarial dispositivos BYOD hasta un máximo de un smartphone, una tablet y una computadora portátil por usuario, los cuales deberán aprovisionarse automáticamente con los certificados correspondientes. Se deberá considerar incluir para esta cantidad de usuarios todas las funcionalidades descritas en la sección "aprovisionamiento automático de dispositivos móviles corporativos (BYOD)". - Se deberá considerar que existirán 2000 dispositivos finales (endpoints) sobre los cuales se deberá realizar una evaluación avanzada de postura (control de salud) ya sea si su conexión es cableada, inalámbrica y/o por VPN. Se deberá considerar incluir para esta cantidad de usuarios todas

	las funcionalidades descritas en la sección "control de salud de los dispositivos".
Repositorios de identidad soportados	- Deberá soportar Microsoft Active Directory - Deberá soportar Kerberos - Deberá soportar LDAP - Deberá soportar SQL server compatible con ODBC - Deberá soportar listas estáticas - Deberá soportar base de datos internas.

Hiperconvergencia

35. Hardware de Hiperconvergencia (04 Unidades)

Descripción	Características técnicas mínimas
Cantidad	Cuatro (04) unidades.
Solución Hiperconvergente (HCI)	La solución hiperconvergente por definición es cómputo, virtualización y storage totalmente definido por software. Los nodos HCI deben encontrarse en la matriz de compatibilidad e interoperabilidad del fabricante del software. Los nodos HCI deben estar identificado en el portal del fabricante del hardware como appliance o sistema hiperconvergente.
Factor de forma	Rackeable, debe incluir los accesorios de rackeo.
Procesadores	Dos (02) procesadores x86 de la última generación, con fecha de lanzamiento 2026 como mínimo, de 12 cores como mínimo, de al menos 2.2GHz de frecuencia base y mínimo 48MB de cache L3. Debe soportar la tecnología Hyper-Threading o Multithreading.
Memoria RAM	512GB de memoria RAM de tecnología DDR5, en módulos de mínimo 64GB 6,400MHz RDIMM. Deberá soportar un crecimiento de al menos hasta 2TB de memoria RAM en su máxima configuración, añadiendo módulos de memoria, sin reemplazar los módulos solicitados. Deberá soportar como mínimo 32 slots DIMM.
Boot de hipervisor	Dos (02) discos M.2 SSD NVMe de mínimo 480GB configurados en RAID 1 por hardware.
Almacenamiento	Cada servidor o nodo HCI deberá contar con discos SSD NVMe intercambiables en caliente, deberá incluir al menos 10 bahías para discos SSD NVMe. La solución hiperconvergente (HCI) debe ser configurada para permitir la tolerancia de fallos ante la caída de un (01) servidor o nodo (N+1) La capacidad efectiva o usable total de almacenamiento de la solución HCI deberá ser de al menos 50TiB SSD NVMe en RF2 o RAID 1 o mirror, sin considerar factores de eficiencia como compresión y deduplicación. El dimensionamiento deberá ser sobre arquitectura de acceso directo a la capa de almacenamiento NVMe. La solución debe realizar réplicas de datos almacenados a través de los nodos de clúster.
Puertos de conectividad	Cuatro (04) puertos Ethernet de 25Gb SFP28, deben incluir sus respectivos transceivers SR SFP28 y cables de fibra LC-LC MM OM3 de mínimo 3 metros. los cuales se utilizarán para garantizar redundancia de conectividad LAN y para la interconexión de la solución hiperconvergente. La solución debe garantizar conectividad redundante hacia los switches de data center, el postor deberá considerar la configuración y compatibilidad de la solución con dicha infraestructura.
Fuentes de poder	Dos (02) fuentes poder redundantes de 220VAC de intercambio en caliente de mínimo 1,300W, con sus respectivos cables de poder C13-C14 de al menos 2 metros.

Seguridad	Soporte de TPM 2.0. La gestión del hardware del nodo HCI debe cumplir con los estándares FIPS 140-2 y NIST 0800-053. Debe contar con un sistema de arranque (boot) seguro, que garantice que solo se cargue software inmutable y firmado durante el tiempo de arranque, evitando que se cargue código malicioso y ayudando a prevenir ataques como la instalación de rootkits. Debe contar con una tapa de seguridad frontal con llave.
Análisis predictivo de fallas	Debe soportar análisis predictivo de fallas de componentes como: procesador, discos, memoria, ventiladores y fuentes de poder; y debe poder solicitarse el cambio por garantía desde el momento que se presenta una alerta de este tipo en algunos de estos componentes.
Puerto de gestión	Deberá incluir un (01) puerto de gestión de 1GbE RJ45, que proporcionen una interfaz de administración web, desde la cual se podrá supervisar y gestionar todos los componentes internos del servidor. Debe contar con todas sus funcionalidades habilitadas.
Software de administración de hardware	Factor de forma: máquina o appliance virtual. Deberá incluir el software y todas las licencias necesarias que permitan la administración centralizada de los servidores solicitados. Este software debe permitir la administración, control, gestión y manejo de toda la infraestructura de cómputo y realizar las siguientes funciones como mínimo: - Descubrir todo el hardware. - Realizar un inventario de la infraestructura de servidores. - Monitoreo del estado de la salud de los componentes. - Actualizaciones de firmware. - Configuración de patrones de los servidores. - El software deberá soportar la administración remota gráfica de cada servidor independientemente del sistema operativo del servidor. - Proveer acceso detallado a problemas de fallas del sistema. - Deberá de ser capaz de contactar al fabricante automáticamente para abrir un ticket y enviar datos de servicio siempre que el equipo notifique un error de hardware. - Capacidad de instalación remota de un servidor o grupo de servidores. - Capacidad de actualización del firmware remota de un servidor o grupo de servidores. - Funcionalidad de acceso remoto compartido entre por lo menos tres usuarios concurrentemente, independiente del sistema operativo del servidor. - Integración con herramientas de administración de recursos como basadas en Ansible, Chef y Puppet. - Las características descritas deberán entenderse como requerimientos funcionales abiertos, no vinculados a un fabricante específico, permitiendo la participación de soluciones equivalentes que cumplan o superen las funcionalidades solicitadas.
Consideraciones	Se deberá incluir la instalación física y configuración de la Solución Hiperconvergente (HCI) por parte del fabricante de los servidores o del software HCI. Todos los componentes, partes y accesorios deben ser originales y nuevos. El año de fabricación de los servidores o nodos HCI deberá ser como mínimo 2026.

36. Software Hiperconvergencia (01 Unidad)

Descripción	Características técnicas mínimas
Licencias	El licenciamiento del software debe ser por suscripción, del tipo OPEN, de forma que no esté vinculado a un solo fabricante de hardware.
Características del almacenamiento definido por software	La infraestructura de cómputo y almacenamiento deberá ser distribuida y completamente definida por software, armando un clúster con las siguientes características: - La solución deberá soportar tolerancia a fallas equivalente a un esquema de redundancia N+1, permitiendo la continuidad operativa del clúster ante la caída simultánea de hasta dos nodos sin pérdida de información ni indisponibilidad de servicios críticos. - La protección de datos deberá realizarse entre los múltiples nodos que componen el clúster, de manera distribuida. - Deberá tener la capacidad de distribuir los datos dentro del clúster y adicionalmente poder replicarlos internamente, para asegurar su disponibilidad. - En caso de una falla, la solución basada en software debe actuar de manera automática creando nuevas copias múltiples de los datos, de manera de mantener el nivel de protección hasta tanto se reemplace el componente que haya fallado. - Capacidad de generar almacenamiento compartido (distribuido) usando los discos internos de cada uno de los nodos generando un almacenamiento virtual, el cual pueda ser presentado a la capa de hypervisor para que los diferentes Hosts puedan hacer uso del almacenamiento de manera transparente y homogénea. - Los recursos de cómputo (CPU y memoria) deberán mantenerse dedicados a cada nodo físico. En el caso del almacenamiento, la solución deberá permitir la conformación de una malla o fabric de almacenamiento distribuido, donde los discos locales de cada nodo se integren en un pool lógico unificado presentado al clúster, garantizando distribución de datos, resiliencia y balanceo automático. - Cada nodo deberá contar con su propia controladora de almacenamiento virtual. - La solución debe escalar como mínimo hasta 16 nodos por clúster. - Debe incluir el soporte de vGPU y GPU Passthrough. - La solución deberá ser agnóstica al hipervisor y debe soportar distintos hipervisores como: VMware ESXi y basados en Linux KVM. - La solución deberá de ser capaz de actualizar el hipervisor en forma desatendida y automatizada. Así mismo la solución deberá de tener la capacidad de convertir la infraestructura de un hipervisor a otro en forma desatendida. - La solución deberá permitir las actualizaciones centralizadas del software en caliente, sin salida de servicio de las cargas (máquinas virtuales) que están corriendo. - La solución debe tener la capacidad de expandir la infraestructura en cualquiera de los tres componentes, procesamiento, memoria, y almacenamiento, sin que las cargas

	(máquinas virtuales) salgan de servicio. El software debe reconocer los recursos cuando se agregue un nodo. - Deberá soportar el crecimiento scale-out en nodos heterogéneos, o diferentes modelos para maximizar recursos de procesamiento, memoria o almacenamiento según requiera. - Proveer un crecimiento lineal, estable y predecible en su rendimiento a medida que se agreguen nodos. - Proveer alto rendimiento al presentar recursos de almacenamiento desde el mismo nodo en el que la máquina virtual se encuentra atendiendo los requerimientos de IOPS. Esto significa que el almacenamiento virtualizado, puede entregar recursos para administrar los requerimientos de I/O hecho por la máquina virtual local a cada nodo. - Cada nodo deberá manejar los IOPS de sus máquinas virtuales en forma local. Independientemente de que la máquina virtual sea original a ese nodo, o haya sido desplazada desde otro nodo. - Debe incluir la funcionalidad de asignar y redistribuir cargas de trabajo a los nodos que mejor se adapten a sus requisitos específicos de almacenamiento, ya sea en términos de rendimiento, latencia o capacidad, asegurando así una óptima utilización de los recursos disponibles. - La solución de almacenamiento deberá ser definida por software e incluir las siguientes funcionalidades: o Deduplicación y compresión. o Thin provisioning. o Snapshots ilimitados basados en punteros. o Sistemas de clones de máquinas virtuales sin consumo de espacio adicional. o Replicación asíncrona. - La solución de almacenamiento no requerirá de switches Fibra Canal, ni FCoE para su funcionamiento. Solamente utilizará switches para Data Center que trabajen stack TCP/IP sobre Ethernet. - La solución debe ser 100% definida por software, desacoplando la inteligencia del hardware y evitando la dependencia de componentes propietarios. Debe integrar en una sola plataforma recursos de cómputo, almacenamiento, virtualización y gestión centralizada, permitiendo una experiencia operativa coherente en centros de datos locales y nubes públicas. - La solución deberá incluir al menos 1 TiB de almacenamiento para servicios de archivos (NFS, SMB) u objetos compatibles con S3, incorporando funcionalidades de analítica que permitan visualizar comportamiento de usuarios y consumo. También podrá ser ofertado con Hardware y Software de terceros que se integren dentro de la solución.
Características del software virtualización	- El software de virtualización debe instalarse para todos los nodos que conforman el clúster. - El hipervisor debe ser compatible con servidores tipo x86 basados en procesadores multinúcleo compatibles con la arquitectura x86 de 64 bits. - El hipervisor deberá instalarse en cada servidor físico como parte de la arquitectura del clúster hiperconvergente, pudiendo coexistir con controladoras virtuales de almacenamiento distribuidas propias de la solución propuesta, siempre que no

	se comprometa el rendimiento, disponibilidad y seguridad de la plataforma. - Debe incluir el soporte para la migración de máquinas virtuales apagadas (Power off) de un servidor físico a otro tan solo indicando la acción de la máquina virtual seleccionada en la consola de administración. - Debe incluir el soporte para la migración de máquinas virtuales en ejecución o encendidas (Power On) desde un servidor físico a otro similar, sin interrupciones para los usuarios ni pérdidas de servicio, eliminando la necesidad de planificar tiempo fuera de servicio de aplicaciones para realizar el mantenimiento planificado de los servidores. - La solución de virtualización debe incluir alta disponibilidad, se entiende la capacidad que debe tener la plataforma de iniciar una máquina virtual en cualquier nodo disponible, en el caso de que el nodo que la alberga falle. - El software de virtualización debe permitir el reinicio de manera automatizada de todas las máquinas virtuales en forma inmediata en caso de un fallo de hardware. - La solución de virtualización debe tener la capacidad de creación y ejecución simultánea de múltiples máquinas virtuales sobre un mismo nodo. Con soporte de sistemas operativos como: o Microsoft Windows Server 2016, 2019 y 2022. o Red Hat Enterprise Linux 6, 7, 8 y 9. o SUSE Linux Enterprise 12 y 15. o Canonical Ubuntu 14, 16, 18, 19, 20 y 22.
Características del software de administración de la Plataforma Virtual	La solución deberá proveer una consola de administración única la cual deberá: - Ser accedida mediante un browser y estar basada en HTML5. - Proveer una única vista para todo el entorno (sistema) manteniendo múltiples puntos de acceso. - La consola permitirá administrar y monitorear a todo el stack que compone la solución, almacenamiento, hipervisor, redes, los nodos que conforman el clúster hiperconvergente. - La consola de Administración deberá ejecutarse sobre los mismos nodos del clúster que administra, aprovechando la tolerancia a fallos de este. La consola debe permanecer disponible ante la falla de cualquiera de los nodos. - Proveer accesos alternativos basados en SSH y/o interfaces seriales remotas estilo IPMI. - Contener autenticación LDAP, Active Directory, CAC Prompt y certificados firmados por SSL. - Gestión automática de dependencias. - Proceso de actualización unificado. - La consola facilitará la ejecución de las tareas de mantenimiento de la plataforma, actualizaciones del software, upgrades de hipervisor, upgrades de firmware de manera no disruptiva. - Permitir reportes y panel de control personalizable. - Permitir analizar de manera predictiva, el uso de los recursos del clúster (memoria, discos y procesamiento). - Permitir el análisis del comportamiento de una máquina virtual. - Permitir su optimización automatizada en caso no esté usando los recursos de manera eficiente.

	- Permitir analizar de manera gráfica, la estadística de las cargas de trabajo, permitir proyectar crecimientos, para luego recomendar un upgrade de recursos (memoria, disco y procesamiento) que soporte ese crecimiento futuro (Capacity Planning).
Seguridad	- Microsegmentación de la red: Debe incluir capacidades nativas de redes definidas por software para aplicar políticas de seguridad de «confianza cero» a nivel de la interfaz de red virtual, aislando las cargas de trabajo y las aplicaciones sin necesidad de realizar cambios en la red, también esta funcionalidad podrá ser ofertada con Hardware y Software de terceros que se integren dentro de la solución. - La solución debe incluir una funcionalidad nativa para análisis y gestión de políticas de seguridad que proporcione: o Monitoreo y visibilidad de VMs y políticas aplicadas. o Auditoría y remediación mediante análisis en tiempo real y acciones automatizadas para corregir desviaciones. o Cumplimiento continuo, automatizando verificaciones y validaciones normativas. o Planificación de seguridad, con visualización y clasificación del tráfico de red. o Investigación de incidentes y generación de mapas de calor para evaluar la postura de seguridad. o Pruebas automatizadas basadas en mejores prácticas. o Políticas listas para usar para cumplir normativas como HIPAA, PCI-DSS, CIS, entre otras. o Todo gestionado desde una única consola, sin recurrir a herramientas externas ni integraciones adicionales. - La solución de hiperconvergencia debe proveer la capacidad para la encripción de datos en reposo sin requerir un Key Management Server externo, sino entregar el manejo de las llaves de encriptación. También esta funcionalidad podrá ser ofertada con Hardware y Software de terceros que se integren dentro de la solución. - La solución debe contar con un nivel de aseguramiento (hardening) aplicado de fábrica y disponer de un mecanismo nativo que automatice la remediación de cualquier desviación respecto a dicho hardening durante todo el ciclo de vida, sin requerir tareas manuales por parte del administrador.
Sistema Operativo	- Windows Server 2025 Datacenter segurando el licenciamiento total de los cores físicos (2 paquetes de 12 cores). Adicionalmente, se requiere la compra de 300 CALs de Usuario de Windows Server 2025, las cuales deben cubrir al total de usuarios que interactuarán con el Directorio Activo y los servicios de red.

Sistema de Respaldo

37. Servidor para backup (01 Unidad)

Descripción	Características técnicas mínimas
Cantidad	Una (01) unidad.
Factor de forma	Rackeable, debe incluir los accesorios de rackeo.
Procesadores	Un (01) procesador x86 de la última generación, con fecha de lanzamiento 2025 como mínimo, cada procesador de 12 cores como mínimo, de al menos 2.2 GHz de frecuencia base y mínimo 48 MB de cache L3. El servidor debe soportar el crecimiento hasta dos (02) procesadores. Debe soportar la tecnología Hyper-Threading o Multithreading.
Memoria RAM	64GB de memoria RAM, de tecnología DDR5, en módulos de mínimo 16GB 6,400MHz RDIMM o superior. Deberá soportar como mínimo 32 slots DIMM.
Puertos de conectividad	Dos (02) puertos Ethernet de 25Gb SFP28, deben incluir sus respectivos transceivers SR SFP28 y cables de fibra LC-LC MM OM3 de mínimo 5 metros. Dos (02) puertos Fibra Canal (FC) de 32Gb, deben incluir sus respectivos transceivers y cables de fibra LC-LC MM OM3 de mínimo 5 metros, para la conexión con la Librería de Cintas solicitada.
Discos	Dos (02) discos SSD de 3.84TB configurados en RAID 1. Los discos deben poder ser intercambiables en caliente. Deberá incluir el backplane con soporte de al menos ocho (08) discos.
Tarjeta de arreglo	Con soporte de RAID 0, 11 10, 5, 50 y 60 como mínimo. Deberá tener 4GB de caché flash integrada Soporte de discos HDD y SSD.
Fuentes de poder	Dos (02) fuentes poder redundantes de 220VAC de intercambio en caliente de mínimo 1,300W, con sus respectivos cables de poder C13-C14 de al menos 2 metros.
Sistemas operativos soportado	Microsoft Windows Server 2022 y 2025 Red Hat Enterprise Linux 9 y 10. SUSE Linux Enterprise Server 15 y 16. VMware vSphere (ESXi) 8 y 9.
Licencia de Sistema Operativo	Deberá incluir la suscripción o licencia OEM del Sistema Operativo de 64 bits. Esta deberá ser compatible con el Software de Backup solicitado.
Análisis predictivo de fallas	Debe soportar análisis predictivo de fallas de componentes internos como: procesador, discos, memoria, ventiladores y fuentes de poder; y debe poder solicitarse el cambio por garantía desde el momento que se presenta una alerta de este tipo en algunos de estos componentes.
Seguridad	Soporte de TPM 2.0. El servidor debe cumplir con los estándares NIST SP800-193, NIST SP800-131A y NIST SP800-147B. Debe contar con un sistema de arranque (boot) seguro, que garantice que solo se cargue software inmutable y firmado durante el tiempo de arranque, evitando que se cargue código malicioso y ayudando a prevenir ataques como la instalación de rootkits.

	Debe contar con protección contra actualizaciones de firmware no autorizadas y corrupción, restaurando el firmware a un estado integral y monitoreo del firmware en busca de posibles compromisos de ataques cibernéticos.
Puerto de gestión	Deberá incluir un puerto de gestión fuera de banda, que proporcionen una interfaz de administración web, desde la cual se podrá supervisar y gestionar todos los componentes internos del servidor, así mismo deberá contar con mecanismos de despliegue o provisionamiento del sistema operativo, estas funciones deberán ser independientes al sistema operativo. Deberá ser un puerto de gestión dedicado de 1Gb RJ45 y con todas sus funcionalidades habilitadas.
Software de administración de hardware	Factor de forma: máquina o appliance virtual. Deberá incluir el software y todas las licencias necesarias que permitan la administración centralizada de los servidores solicitados. Este software debe permitir la administración, control, gestión y manejo de toda la infraestructura de cómputo y realizar las siguientes funciones como mínimo: - Descubrir todo el hardware. - Realizar un inventario de la infraestructura de servidores. - Monitoreo del estado de la salud de los componentes. - Actualizaciones de firmware. - Configuración de patrones de los servidores. - El software deberá soportar la administración remota gráfica de cada servidor independientemente del sistema operativo del servidor. - Proveer acceso detallado a problemas de fallas del sistema. - Deberá de ser capaz de contactar al fabricante automáticamente para abrir un ticket y enviar datos de servicio siempre que el equipo notifique un error de hardware. - Capacidad de instalación remota de un servidor o grupo de servidores. - Capacidad de actualización del firmware remota de un servidor o grupo de servidores. - Funcionalidad de acceso remoto compartido entre por lo menos tres usuarios concurrentemente, independiente del sistema operativo del servidor. - Integración con herramientas de administración de recursos como basadas en Ansible, Chef y Puppet.
Sostenibilidad	Certificado de no perjudicar la salud y/o presentar un impacto negativo al medio ambiente EPEAT. Certificado de eficiencia de energía (Energy Star).
Consideraciones	Todos los componentes, partes y accesorios, deben ser originales y nuevos. El año de fabricación del servidor deberá ser como mínimo 2026.

38. Servidor de inmutabilidad (01 Unidad)

Descripción	Características técnicas mínimas
Factor de forma	Rackeable, debe incluir los accesorios de rackeo.
Procesadores	Un (01) procesador x86 de la última generación, con fecha de lanzamiento 2025 como mínimo, cada procesador de 12 cores como mínimo, de al menos 2.2 GHz de frecuencia base y mínimo 48 MB de cache L3. El servidor debe soportar el crecimiento hasta dos (02) procesadores. Debe soportar la tecnología Hyper-Threading o Multithreading.
Memoria RAM	64GB de memoria RAM, de tecnología DDR5, en módulos de mínimo 16GB 6,400MHz RDIMM o superior. Deberá soportar como mínimo 32 slots DIMM.
Puertos de conectividad	Dos (02) puertos Ethernet de 25Gb SFP28, deben incluir sus respectivos transceivers SR SFP28 y cables de fibra LC-LC MM OM3 de mínimo 5 metros. Dos (02) puertos Fibra Canal (FC) de 32Gb, deben incluir sus respectivos transceivers y cables de fibra LC-LC MM OM3 de mínimo 5 metros, para la conexión con el Almacenamiento de Backup solicitado.
Discos	Dos (02) discos SSD de 1.92TB configurados en RAID 1. Los discos deben poder ser intercambiables en caliente. Deberá incluir el backplane con soporte de al menos ocho (08) discos.
Tarjeta de arreglo	Con soporte de RAID 0, 11 10, 5, 50 y 60 como mínimo. Deberá tener 4GB de caché flash integrada Soporte de discos HDD y SSD.
Fuentes de poder	Dos (02) fuentes poder redundantes de 220VAC de intercambio en caliente de mínimo 1,300W, con sus respectivos cables de poder C13-C14 de al menos 2 metros.
Sistemas operativos soportado	Microsoft Windows Server 2022 y 2025 Red Hat Enterprise Linux 9 y 10. SUSE Linux Enterprise Server 15 y 16. VMware vSphere (ESXi) 8 y 9.
Licencia de Sistema Operativo	Deberá incluir la suscripción del Sistema Operativo Linux de 64 bits, necesarias para la inmutabilidad del backup a disco.
Análisis predictivo de fallas	Debe soportar análisis predictivo de fallas de componentes internos como: procesador, discos, memoria, ventiladores y fuentes de poder; y debe poder solicitarse el cambio por garantía desde el momento que se presenta una alerta de este tipo en algunos de estos componentes.
Seguridad	Soporte de TPM 2.0. El servidor debe cumplir con los estándares NIST SP800-193, NIST SP800-131A y NIST SP800-147B. Debe contar con un sistema de arranque (boot) seguro, que garantice que solo se cargue software inmutable y firmado durante el tiempo de arranque, evitando que se cargue código malicioso y ayudando a prevenir ataques como la instalación de rootkits. Debe contar con protección contra actualizaciones de firmware no autorizadas y corrupción, restaurando el firmware a un estado integral y monitoreo del firmware en busca de posibles compromisos de ataques cibernéticos.

Puerto de gestión	Deberá incluir un puerto de gestión fuera de banda, que proporcionen una interfaz de administración web, desde la cual se podrá supervisar y gestionar todos los componentes internos del servidor, así mismo deberá contar con mecanismos de despliegue o provisionamiento del sistema operativo, estas funciones deberán ser independientes al sistema operativo. Deberá ser un puerto de gestión dedicado de 1Gb RJ45 y con todas sus funcionalidades habilitadas.
Software de administración de hardware	Factor de forma: máquina o appliance virtual. Deberá incluir el software y todas las licencias necesarias que permitan la administración centralizada de los servidores solicitados. Deberá contar con soporte y suscripción por el periodo de 12 meses. Este software debe permitir la administración, control, gestión y manejo de toda la infraestructura de cómputo y realizar las siguientes funciones como mínimo: - Descubrir todo el hardware. - Realizar un inventario de la infraestructura de servidores. - Monitoreo del estado de la salud de los componentes. - Actualizaciones de firmware. - Configuración de patrones de los servidores. - El software deberá soportar la administración remota gráfica de cada servidor independientemente del sistema operativo del servidor. - Proveer acceso detallado a problemas de fallas del sistema. - Deberá de ser capaz de contactar al fabricante automáticamente para abrir un ticket y enviar datos de servicio siempre que el equipo notifique un error de hardware. - Capacidad de instalación remota de un servidor o grupo de servidores. - Capacidad de actualización del firmware remota de un servidor o grupo de servidores. - Funcionalidad de acceso remoto compartido entre por lo menos tres usuarios concurrentemente, independiente del sistema operativo del servidor. - Integración con herramientas de administración de recursos como basadas en Ansible, Chef y Puppet.
Sostenibilidad	Certificado de no perjudicar la salud y/o presentar un impacto negativo al medio ambiente EPEAT. Certificado de eficiencia de energía (Energy Star).
Consideraciones	Todos los componentes, partes y accesorios, deben ser originales y nuevos. El año de fabricación del servidor deberá ser como mínimo 2026.

39. Almacenamiento para backup (01 Unidad)

Descripción	Características técnicas mínimas
Formato	Rackeable, deberá incluir su kit de montaje en rack. Si es necesario expansiones de discos se deben agregar y cada expansión debe ser en formato rack e incluir su kit de montaje en rack.

Disponibilidad	Deberá estar diseñado para una disponibilidad de 99.9999%, deberá poder ser verificado en la documentación pública del fabricante del sistema de almacenamiento. Deberá soportar actualizaciones de firmware sin interrupciones.
Controladoras	Dos controladoras en configuración activo-activo con balanceo de carga automático. La arquitectura de las controladoras debe estar basado en tecnología de procesadores x86.
Memoria cache	64GB como mínimo de memoria cache nativa por sistema. No se aceptará tarjetas o discos flash u otro elemento no nativo como componentes de cache.
Conectividad	iSCSI y Fibra Canal.
Puertos por controlador	Dos (02) puertos iSCSI de 10/25 Gb, deben incluir sus respectivos transceivers. Cuatro (04) puertos Fibra Canal a 32 Gb, deben incluir sus respectivos transceivers. Un (01) puerto 1GbE RJ45 para gestión.
RAID	Debe soportar RAID 0, 1, 5, 6 y 10 como mínimo. Soporte de Pool de discos dinámicos o similar.
Escalabilidad	Mínimo 3 expansiones de discos. Debe soportar escalar al menos hasta 1 PB RAW.
Tipo de discos soportados	SSD SAS o superior. HDD SAS. HDD NL-SAS. Los discos deberán ser reemplazables en caliente.
Capacidad instalada	Deberá contar como mínimo con 100TiB de capacidad usable, sin considerar funcionalidades de eficiencia de datos, con discos de estado sólido (SSD), deberá configurarse doble paridad y al menos un disco o capacidad spare.
Interoperabilidad	Deberá ser compatible con la conexión directa (DAS)
Fuentes de poder redundantes	Dos (02) fuentes de poder AC, Hot-Swap, activas y redundantes.
Sistemas Operativos Soportados	Microsoft Windows Server. Red Hat Enterprise Linux. SUSE Linux Enterprise Server. VMware vSphere.
Administración	La consola de administración deberá permitir: - La gestión centralizada vía web con distintos perfiles y privilegios de usuarios. - Visualizar datos de rendimiento, incluida la latencia de E/S, IOPS, la utilización de la CPU y el rendimiento. - Suministrar almacenamiento mediante conjuntos o grupos de volumen y crear cargas de trabajo de aplicaciones. - Realizar copias de seguridad y recuperación ante desastres mediante capturas y copias de volúmenes. - Comprobar el estado de los componentes. - Notificar a los administradores acerca de sucesos importantes que se producen en el almacenamiento. Las alertas se deberán enviar mediante correo electrónico, capturas SNMP y syslog. - Configurar la autenticación de los usuarios y funciones de rendimiento del sistema.

	- Ver datos de diagnóstico, gestionar actualizaciones y configurar el soporte automático, que permitirá supervisar el estado del almacenamiento y enviarlo automáticamente al centro de soporte técnico.
Funcionalidades incluidas	- Deberá incluir la funcionalidad de thin provisioning para generar volúmenes de espacio virtual sobre el espacio físico disponible. - Deberá incluir la capacidad de realizar snapshots. - Deberá incluir la capacidad de realizar copia de volúmenes. - Estas funcionalidades deberán incluir el licenciamiento por toda la capacidad soportada del sistema de almacenamiento.
Software de gestión de hardware	Deberá incluir el software y todas las licencias necesarias que permitan la administración centralizada de los servidores y almacenamiento solicitados. También se podrá proponer un software de terceros para esta funcionalidad.
Consideraciones	Todos los componentes, partes y accesorios, deben ser originales y nuevos. El año de fabricación del almacenamiento deberá ser como mínimo 2026.

40. Librería de backup (01 Unidad)

Descripción	Características técnicas mínimas
Formato físico	Debe ser modular y escalable. El módulo base debe ser en formato rack. Debe ser de tipo rackeable y debe incluir los accesorios para su montaje.
Unidades de lectura/escritura	La configuración de la librería debe incluir mínimo dos (02) tapes drives LTO9, cada uno con un (01) puerto de fibra canal (FC) de 8 Gbps como mínimo. - La configuración de la librería debe incluir la capacidad de instalar y sustituir los tapes drives en caliente sin afectar la operatividad de la librería. - El modelo de la librería debe soportar tape drives y cartuchos de tecnologías LTO8 y LTO9 en forma concurrente. - La librería requerida deberá soportar escalar hasta 21 tapes drives como mínimo, a partir de módulos de expansiones adicionales.
Slots y estaciones de Ingreso/Salida de cintas	- La librería deberá incluir cuarenta (40) slots para cartuchos de cinta magnética LTO en su máxima configuración.
Lector de barras y brazo robótico	- La configuración de la librería ofertada debe incluir la automatización de la manipulación, identificación (mediante etiquetas de código de barras) e inventario de cartuchos de cinta magnética LTO. - La configuración de la librería ofertada deberá incluir mínimo un (01) brazo robótico.
Cartuchos de cintas	- Debe incluir diez (10) cartuchos de cintas Ultrium 9 con sus etiquetas de código de barras. - Debe incluir como mínimo un (02) cartucho de limpieza.

Fuentes de poder y ventiladores	- Debe incluir fuentes de poder redundantes con la capacidad de instalar y sustituir las fuentes de poder en caliente.
Conectividad	- Cada tape drive LTO9 debe incluir como mínimo un (01) puerto en fibra canal (FC) para conectarse al servidor de backup solicitado, cada uno de estos puertos debe ser de 8 Gbps como mínimo. - Debe incluir como mínimo dos (02) puertos Ethernet para la gestión, cada uno de estos puertos debe ser de 10/100/1000 BASE-T como mínimo y deben tener soporte de protocolos IPv4 e IPv6.
Compatibilidad y actualización de firmware	- Debe ser compatible con el sistema operativo del servidor de backup solicitado. - Debe incluir la función de actualización del firmware de la Librería y de los tapes drives, sin que esta actividad afecte la operatividad de la totalidad de la Librería. - Compatibilidad con el software de backup solicitado.
Interfaces de administración y monitoreo	- Debe incluir una consola de administración. - Debe incluir una interfase de administración web browser y/o GUI. - La interface de administración de la librería debe incluir la función de mostrar el estado de la Librería y tapes drives. - Debe incluir la función de monitoreo y comunicación de alertas.
Consideraciones	- Todos los componentes, partes y accesorios, deben ser originales y nuevos. - El año de fabricación deberá ser como mínimo 2026.

41. Software de backup (01 Unidad)

- Tipo de licenciamiento por suscripción por 12 meses.
- Licenciamiento para proteger mínimo 80 cargas de trabajo (VMs, servidores físicos y estaciones).
- Debe ser compatible con software de hiperconvergencia.
- Compatibilidad con otros entornos como Microsoft Hyper-V, Windows Server (2016/2019/2022/2025) y distribuciones Linux (RHEL, SUSE, Ubuntu), etc.
- Soporte nativo para unidades de cinta LTO (hasta LTO-9) conectadas vía SAS o FC.
- Destinos de respaldo a disco, cinta, almacenamiento en red y nubes compatibles.
- La solución debería facilitar la recuperación de una copia de seguridad basada en agentes directamente en Google Platform, Amazon AWS o Microsoft Azure y Microsoft Azure Stack.
- Métodos de respaldo deben ser completos, incrementales y sintéticos. Programación flexible de tareas.
- Recuperación o restauración granular de archivos, VMs completas, objetos de aplicaciones.
- Optimizaciones como compresión, deduplicación, cambio por bloque, exclusiones, balanceo de carga.
- Cifrado en tránsito y en reposo. Control de acceso por roles. Registro de auditoría.
- La solución debe integrar analítica de seguridad a su consola proporcionada.
- La solución deberá asegurar las copias de seguridad en repositorios reforzados a prueba de malware y hackers con copias de seguridad inmutables, para prevenir el cifrado o eliminación por ransomware y debe admitir credenciales que se usan una sola vez y no ser almacenadas en la infraestructura de respaldo, así si el servidor de respaldo se ve comprometido, un atacante no puede obtener las credenciales y conectarse al repositorio reforzado.

- La solución debe ofrecer una Incident API que pueda ser consumida por cualquier herramienta de seguridad que al detectar un ataque o incidente pueda notificar del incidente y poder hacer un quick backup del equipo que está bajo ataque.
- La solución deberá asegurar las copias de seguridad en repositorios reforzados a prueba de malware y hackers con copias de seguridad inmutables, para prevenir el cifrado o eliminación por ransomware y debe admitir credenciales que se usan una sola vez y no ser almacenadas en la infraestructura de respaldo, así si el servidor de respaldo se ve comprometido, un atacante no puede obtener las credenciales y conectarse al repositorio reforzado
- La solución debe permitir el escaneo in-line de los backups con bajo impacto utilizando una base de datos de más de 4000 cepas de malware que se actualiza automáticamente.
- Consola de gestión gráfica web o cliente local. Reportes, alertas y administración centralizada.
- Escalabilidad, capacidad de ampliar licencias sin reinstalación.

Ciberseguridad

42. Firewalles NGFW Perimetral (02 Unidades)

- La solución debe ser ofrecida en alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones técnicas.
- Deberá tener un rendimiento de Prevención de Amenazas de 28 Gbps cuando opera en simultáneo: Application Control, firewall, IPS, Antivirus/Anti-Bot/Antispyware o 14 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7) teniendo las siguientes funcionalidades habilitadas de manera simultánea: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. La solución debe operar bajo una arquitectura de procesamiento único donde todas las funciones de seguridad se apliquen simultaneamente sobre el mismo flujo de tráfico. El postor deberá presentar documentación pública del fabricante que sustente el cumplimiento de la medición. No se aceptarán cartas de fabricante como sustentos para el cumplimiento del performance y condiciones de medición solicitadas.
- El equipo debe soportar como mínimo 20 millones de sesiones concurrentes medidas con transacciones TCP o 2.5 millones medidas con transacciones HTTP.
- El equipo debe soportar 800 mil nuevas sesiones por segundo medidas con transacciones TCP o 200 mil nuevas sesiones por segundo medidas con transacciones HTTP.
- Debe incluir mínimo 12 interfaces de 1G/2.5G/5G/10G RJ-45, 10 interfaces de 10Gbps SFP/ SFP+, 4 interfaces de 25Gbps SFP28 y 2 interfaces de 40G/100GGbps QSFP28.
- Debe contar con una interfaz de cobre RJ45 dedicada para la gestión del equipo
- Debe contar con 02 interfaces dedicadas para la alta disponibilidad.
- Debe contar con disco interno de estado sólido de 480 SSD.
- Debe contar con dos fuentes de poder redundantes.
- Debe estar licenciado y habilitado en simultaneo las funcionalidades: Firewall, IPS, Antivirus de red, Filtrado URL, Control de aplicaciones, identificación de usuarios, identificación y perfilado de dispositivos IoT/OT, prevención de Bots y amenazas DNS, SDWAN y Sandboxing cloud.
- El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- Capacidad de inspeccionar el contenido en túneles GRE, opcionalmente GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.
- Deberá soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based

forwarding, dual-stack, QoS y/o DSCP, NAT64, LLDP, BFD, DHCPv6 Relay, SNMP, opcionalmente ECMP y SLAAC

- La plataforma propuesta por el fabricante debe contar con certificación USGv6-r1 para las pruebas de Firewall, IDS e IPS.
- Debe realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas.
- Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.
- La solución deberá contar con capacidades nativas de auditoría y versionado de cambios de reglas de seguridad, permitiendo visualizar el historial de modificaciones, identificar usuario, fecha y acción realizada, así como consultar el estado previo y posterior de las reglas y comparar versiones de configuración. Estas funcionalidades deberán estar integradas en el propio equipo, sin requerir herramientas externas.
- Debe soportar la configuración de alta disponibilidad Activo/Pasivo, con despliegues de los equipos tanto en modo transparente y/o como en modo capa 3 (L3).
- Deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, RC4, AES128, AES256, CHACHA20-POLY1305; MD5, SHA1, SHA256, SHA384.
- Capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos y/o no fiables, a pesar de no descifrar el tráfico.
- Debe contar con un dashboard que muestre gráficamente la proporción del tráfico descifrado, aplicaciones y dominios con descifrado correcto, errores de descifrado.
- Debe contar con un panel de logs dedicados a monitorear el tráfico de descifrado SSL/TLS, estos logs deberán permitir una identificación rápida de problemas del descifrado.
- Desde la consola gráfica deberá mostrar todo el detalle de la sesión SSL/TLS identificada, tales como IP origen y destino, subject common name, issuer common name, server name indication, datos del certificado digital (fecha de expiración, serial number), versión de TLS, algoritmo asimétrico, algoritmo simétrico, hash, estado del descifrado (correcto o con error), motivo del error del descifrado. Este detalle de logs no deberá afectar el performance del equipo.
- Reconocer por lo menos 4500 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
- Las aplicaciones deberán estar clasificadas en al menos 30 categorias y/o subcategorias, de tal manera que se puedan configurar políticas en base al tipo de aplicación.
- Las aplicaciones deberán contar con atributos descriptivos tales como tipo, nivel de riesgo y etiqueta.
- Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.
- Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión y/o a través de una herramienta tercera del fabricante.
- Deberá contar con un módulo de aprendizaje que permita migrar las políticas basadas en puertos específicos y políticas con puertos ALL/ANY, a políticas basadas en aplicaciones.
- El módulo de aprendizaje deberá ser específico por cada política de seguridad.
- El módulo de aprendizaje deberá mostrar el nombre de la(s) aplicación(es) que han pasado por una política de seguridad, fecha de primera y última ocurrencia y volumen de datos transferido por cada aplicación.
- Deberá contar con un wizard que permita convertir una política basada en puertos (capa 4) a una política basada en aplicaciones (capa 7) en base al aprendizaje realizado.

- La solución debe permitir la creación de políticas de seguridad basadas en la identidad del usuario y grupo al cual pertenece, a través de la integración de servicios de autenticación como Active Directory, Novell eDirectory, Open LDAP y base de datos local.
- Debe contar con varios mecanismos para la identificación del usuario y la dirección IP del equipo en donde se encuentra autenticado. Como mínimo deberá poder integrarse a las siguientes plataformas para cubrir este requerimiento:
    - Eventos de login gestionados en Domain Controller y/o Microsoft Exchange.
    - Capacidad de leer eventos de login y logout usando el protocolo WinRM.
    - Terminal Server de Microsoft o Citrix
    - Consultando directamente a cada estación de trabajo a través del protocolo WMI
    - Lectura de la cabecera XFF al integrarse con soluciones terceras de Proxy
    - Capacidad de extraer la información de IP y usuarios a través de la lectura y extracción de datos del tráfico syslog.
- Deberá contar con un componente que permita integrarse a diversas plataformas de identidades tales como Azure LDAP, Google Directory, Okta, Cisco Duo, PingID.
- Deberá contar con un mecanismo que permita identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, inclusive si el tráfico entre la potencial víctima y su servidor DNS utilizado no pasa por el NGFW.
- Los algoritmos basados en inteligencia artificial deberán ser capaces de prevenir ataques como DGA (Domain Generation Algorithm) Random y de Diccionario, DNS Tunneling, Fast Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS.
- Soportar proteger contra ataques de día cero y malware desconocido a través de un servicio de sandboxing del fabricante provisto desde su nube (Debe soportar emulacion en Windows, MacOS y Linux).
- El sandbox debe identificar los ataques de phishing al momento de emular los potenciales archivos maliciosos en: swf, html, lnk y js.
- Luego del análisis realizado por el sandbox, éste deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.
- El análisis en tiempo real deberá determinar si la página web desconocida (no categorizada en la base de datos del fabricante), tiene contenido javascript malicioso, phishing, actividad de command and control y otros tipos de contenido malicioso.
- Debe contar con medidas de antievasión como Cloaking, Captcha falsos, codificación de caracteres HTML, entre otros.
- Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de robo de credenciales.
- Debe incluir capacidades de identificación y perfilado de dispositivos conectados a la red (incluyendo dispositivos IoT/OT), permitiendo su clasificación, evaluación de riesgo y aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, sin requerir la instalación de agentes adicionales.
- La solución debe incluir la capacidad de poder monitorear la salud de los enlaces en términos de jitter, latencia y pérdida de paquetes, tomando decisiones inteligentes de enrutamiento basado en la condición de los enlaces de manera dinámica.
- Debe permitir realizar la detección y bloqueo de archivos por su extensión.
- Deberá integrarse de forma nativa con la plataforma SIEM, proporcionando telemetría de seguridad enriquecida y correlacionada en tiempo cercano a real, incluyendo como mínimo información de aplicaciones de red en capa 7, cabeceras HTTP, consultas DNS, tráfico DHCP y atributos de dispositivos (tipo, categoría, fabricante y sistema operativo). Dicha telemetría deberá ser consistente y utilizable directamente para análisis, correlación y automatización, sin requerir procesos adicionales de normalización, parsing complejo o integraciones personalizadas.
- En total para la solución de Firewall externo, se debe incluir 04 transceiver de SFP+ 10Gbps MMF.

- En total para la solución de Firewall externo, se debe incluir 04 transceiver de SFP28 25Gbps MMF.

43. Firewall Interno (02 Unidades)

- La solución debe ser ofrecida en alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones técnicas.
- Deberá tener un rendimiento de Prevención de Amenazas de 110 Gbps cuando opera en simultáneo: Application Control, firewall, IPS, Antivirus/Anti-Bot/Antispyware o 48 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7) teniendo las siguientes funcionalidades habilitadas de manera simultánea: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. La solución debe operar bajo una arquitectura de procesamiento único donde todas las funciones de seguridad se apliquen simultaneamente sobre el mismo flujo de tráfico. El postor deberá presentar documentación pública del fabricante que sustente el cumplimiento de la medición, el cual será validado durante la implementación, según la metodología que sustente el Proveedor.
- El equipo debe soportar como mínimo 80 millones de sesiones concurrentes medidas con transacciones TCP o 7 millones medidas con transacciones HTTP.
- El equipo debe soportar 1.2 millones de nuevas sesiones por segundo medidas con transacciones TCP o 370 mil nuevas sesiones por segundo medidas con transacciones HTTP.
- Debe incluir mínimo 8 interfaces de 1G/2.5G/5G/10G RJ-45, 12 interfaces de 1G/10G SFP/ SFP+, 4 interfaces de 25Gbps SFP28 y 4 interfaces de 40G/100GGbps QSFP28.
- Debe contar con una interfaz de cobre RJ45 dedicada para la gestión del equipo
- Debe contar con 02 interfaces dedicadas para la alta disponibilidad.
- Debe contar con disco interno de estado sólido de 480 SSD.
- Debe contar con dos fuentes de poder redundantes.
- Debe estar licenciado y habilitado en simultaneo las funcionalidades: Firewall, IPS, Antivirus de red, Control de aplicaciones, identificación de usuarios, identificación y perfilado de dispositivos IoT/OT, prevención de Bots y amenazas DNS y Sandboxing cloud.
- El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- Capacidad de inspeccionar el contenido en túneles GRE, opcionalmente GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.
- Deberá soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based forwarding, dual-stack, QoS y/o DSCP, NAT64, LLDP, BFD, DHCPv6 Relay, SNMP, opcionalmente ECMP y SLAAC
- La plataforma propuesta por el fabricante debe contar con certificación USGv6-r1 para las pruebas de Firewall, IDS e IPS.
- Debe realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas.
- Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.
- La solución deberá contar con capacidades nativas de auditoría y versionado de cambios de reglas de seguridad, permitiendo visualizar el historial de modificaciones, identificar usuario, fecha y acción realizada, así como consultar el estado previo y posterior de las reglas y comparar versiones de configuración. Estas funcionalidades deberán estar integradas en el propio equipo, sin requerir herramientas externas.

- Debe soportar la configuración de alta disponibilidad Activo/Pasivo, con despliegues de los equipos tanto en modo transparente y/o como en modo capa 3 (L3).
- Deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, RC4, AES128, AES256, CHACHA20-POLY1305; MD5, SHA1, SHA256, SHA384.
- Capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos y/o no fiables, a pesar de no descifrar el tráfico.
- Debe contar con un dashboard que muestre gráficamente la proporción del tráfico descifrado, aplicaciones y dominios con descifrado correcto, errores de descifrado.
- Debe contar con un panel de logs dedicados a monitorear el tráfico de descifrado SSL/TLS, estos logs deberán permitir una identificación rápida de problemas del descifrado.
- Desde la consola gráfica deberá mostrar todo el detalle de la sesión SSL/TLS identificada, tales como IP origen y destino, subject common name, issuer common name, server name indication, datos del certificado digital (fecha de expiración, serial number), versión de TLS, algoritmo asimétrico, algoritmo simétrico, hash, estado del descifrado (correcto o con error), motivo del error del descifrado. Este detalle de logs no deberá afectar el performance del equipo.
- Reconocer por lo menos 4500 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
- Las aplicaciones deberán estar clasificadas en al menos 30 categorias y/o subcategorias, de tal manera que se puedan configurar políticas en base al tipo de aplicación.
- Las aplicaciones deberán contar con atributos descriptivos tales como tipo, nivel de riesgo y etiqueta.
- Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.
- Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión y/o a través de una herramienta tercera del fabricante.
- Deberá contar con un módulo de aprendizaje que permita migrar las políticas basadas en puertos específicos y políticas con puertos ALL/ANY, a políticas basadas en aplicaciones.
- El módulo de aprendizaje deberá ser específico por cada política de seguridad.
- El módulo de aprendizaje deberá mostrar el nombre de la(s) aplicación(es) que han pasado por una política de seguridad, fecha de primera y última ocurrencia y volumen de datos transferido por cada aplicación.
- Deberá contar con un wizard que permita convertir una política basada en puertos (capa 4) a una política basada en aplicaciones (capa 7) en base al aprendizaje realizado.
- La solución debe permitir la creación de políticas de seguridad basadas en la identidad del usuario y grupo al cual pertenece, a través de la integración de servicios de autenticación como Active Directory, Novell eDirectory, Open LDAP y base de datos local.
- Debe contar con varios mecanismos para la identificación del usuario y la dirección IP del equipo en donde se encuentra autenticado. Como mínimo deberá poder integrarse a las siguientes plataformas para cubrir este requerimiento:
    - Eventos de login gestionados en Domain Controller y/o Microsoft Exchange.
    - Capacidad de leer eventos de login y logout usando el protocolo WinRM.
    - Terminal Server de Microsoft o Citrix
    - Consultando directamente a cada estación de trabajo a través del protocolo WMI
    - Lectura de la cabecera XFF al integrarse con soluciones terceras de Proxy
    - Capacidad de extraer la información de IP y usuarios a través de la lectura y extracción de datos del tráfico syslog.
- Deberá contar con un componente que permita integrarse a diversas plataformas de identidades tales como Azure LDAP, Google Directory, Okta, Cisco Duo, PingID.
- Deberá contar con un mecanismo que permita identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, inclusive si el tráfico entre la potencial víctima y su servidor DNS utilizado no pasa por el NGFW.
- Los algoritmos basados en inteligencia artificial deberán ser capaces de prevenir ataques como DGA (Domain Generation Algortihm) Random y de Diccionario, DNS Tunneling, Fast

Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS.

- Soportar proteger contra ataques de día cero y malware desconocido a través de un servicio de sandboxing del fabricante provisto desde su nube (Debe soportar emulacion en Windows, MacOS y Linux).
- El sandbox debe identificar los ataques de phishing al momento de emular los potenciales archivos maliciosos en: swf, html, lnk y js.
- Luego del análisis realizado por el sandbox, éste deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- Debe incluir capacidades de identificación y perfilado de dispositivos conectados a la red (incluyendo dispositivos IoT/OT), permitiendo su clasificación, evaluación de riesgo y aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, sin requerir la instalación de agentes adicionales.
- Debe permitir realizar la detección y bloqueo de archivos por su extensión.
- Deberá integrarse de forma nativa con la plataforma SIEM, proporcionando telemetría de seguridad enriquecida y correlacionada en tiempo cercano a real, incluyendo como mínimo información de aplicaciones de red en capa 7, cabeceras HTTP, consultas DNS, tráfico DHCP y atributos de dispositivos (tipo, categoría, fabricante y sistema operativo). Dicha telemetría deberá ser consistente y utilizable directamente para análisis, correlación y automatización, sin requerir procesos adicionales de normalización, parsing complejo o integraciones personalizadas.
- En total para la solución de Firewall interno, se debe incluir 08 transceiver de SFP+ 10Gbps MMF.
- En total para la solución de Firewall interno, se debe incluir 08 transceiver de SFP28 25Gbps MMF.

44. Consola de analítica y reportes (01 Unidades)

- Debe incluir una consola de analítica y reportería local provista en la nube del fabricante, que debe de estar licenciada para poder administrar todos los NGFW solicitados.
- La solución debe ser una plataforma unificada de gestión y operaciones impulsada por IA para toda la infraestructura de seguridad de red, permitiendo la gestión de politicas y gestión de eventos de los firewalls perimetrales y los firewalls internos
- La solución deberá contar con una plataforma de almacenamiento centralizado de logs de seguridad, que permita la ingesta continua de telemetría sin restricciones por volumen de datos y que incluya una capacidad de retención de logs de al menos un (01) año.
- La capacidad de almacenamiento deberá estar incluida de forma nativa en el licenciamiento de la solución, sin requerir dimensionamiento previo ni adquisición incremental de almacenamiento para cumplir con el período de retención requerido.
- Con el objetivo de que la Institución cuente con autonomía para evaluar si el NGFW se encuentra configurado acorde a las buenas prácticas y evitar que el postor sea juez y parte del control de calidad de ésta, la consola de analítia y reportes debe permitir evaluar automáticamente si el NGFW se encuentra configurado acorde a las buenas prácticas del fabricante en materia de los diferentes módulos de seguridad que se le haya activado.
- Esta plataforma deberá ser única y consolidar la información de todos los NGFW incluidos en este proyecto.
- Debe contar con gráficos ejecutivos que permitan mostrar el nivel de adopción de los módulos de seguridad del NGFW en las políticas de seguridad.
- Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red.
- La solución debe tener Alertas de Salud del Hardware, Software, Licencias
- La solución debe detectar vulnerabilidades de software de los NGFW
- La solución debe tener análisis de causa raíz para problemas de rendimiento.
- La solución debe predecir averías y evitar el impacto en la red por interrupciones del firewall y conexiones de servicio con pronósticos y recomendaciones de soluciones hasta 90 días antes de una interrupción.

- La solución debe tener Análisis de Mejores Prácticas del fabricante.
- La solución debe tener Verificaciones de Configuración Personalizadas.
- La solución debe ofrecer mejores prácticas en tiempo real y proactivas con la aplicación.
- La solución debe tener un Analizador de Políticas (ML).
- La solución debe tener Optimizador de Políticas (ML).
- La solución debe aprovechar el análisis impulsado por IA para detectar, resolver y optimizar anomalías en las políticas, como políticas ocultas y redundantes, y reglas demasiado permisivas o no utilizadas.
- La solución debe mejorar la postura de seguridad con recomendaciones de mejores prácticas integradas y mantener el cumplimiento de los estándares de la industria y de InfoSec.
- La solución debe tener verificaciones de mejores prácticas predefinidas.
- La solución debe tener verificaciones de mejores prácticas personalizadas.
- La solución debe tener recomendaciones y aplicación de mejores prácticas en línea para cerrar las brechas de seguridad existentes.
- La solución debe tener limpieza de configuración de reglas y objetos no utilizados.
- La solución debe proporcionar recomendaciones en tiempo real y análisis automatizado sobre deficiencias de implementación, configuración y seguridad para una resolución de problemas más rápida.
- La solución debe permitir evaluaciones diarias de la configuración para identificar brechas, mantener las mejores prácticas y garantizar una postura de seguridad óptima.
- La solución debe garantizar el cumplimiento de los estándares de la industria (CIS, NIST) y verificaciones personalizadas para un cumplimiento continuo, reduciendo el riesgo.
- La solución debe optimizar la gestión de configuraciones y políticas en todos los puntos de aplicación desde una única interfaz.
- La solución debe proporcionar recomendaciones de actualización de software basadas en las funciones habilitadas y las vulnerabilidades CVE conocidas para NGFW.
- La solución debe tener paneles para Resumen Ejecutivo, Sandboxing, Seguridad DNS, SD-WAN y personalizados.
- La solución debe incluir un asistente basado en inteligencia artificial que permita realizar consultas en lenguaje natural para resolución de problemas, consultas técnicas, explicación de alertas y asistencia en la configuración de políticas de seguridad.
- La solución debe incluir capacidades de asistencia basada en inteligencia artificial que permitan analizar eventos de seguridad y generar reportes mediante consultas asistidas y visualización interactiva de datos.

45. XDR (Extended Detection & Response) – 01 solución

- La solución deberá ser de tipo XDR (Extended Detection & Response) y permitir la operación centralizada de capacidades de detección, análisis y respuesta para endpoints, formando parte de una plataforma unificada de operaciones de seguridad que integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.
- La solución XDR deberá permitir la integración con la solución SIEM propuesta, habilitando el envío y consumo de telemetría de seguridad, de forma nativa y estructurada, sin requerir desarrollos personalizados o procesos complejos de normalización, garantizando su uso para correlación, análisis y respuesta automatizada.
- Se deberán licenciar 1000 agentes XDR que incluyan todas las capacidades descritas en el requerimiento.
- El agente deberá ser ligero, que incluso pueda convivir con cualquier otro software instalado en el endpoint.
- El agente deberá soportar las siguientes versiones de sistemas operativos como mínimo:
    - Windows 11 professional
    - Windows Server 2025
    - MacOS 26

- Deberá estar protegido ante intentos de desinstalación o manipulación del agente.
- Deberá ser posible definir diferentes password de seguridad para diferentes grupos de endpoints.
- Deberá contar con capacidades nativas de prevención de exploits basadas en la detección y bloqueo de técnicas de explotación que afecten a sistemas Windows (Workstations y Servidores), Linux y MacOS. No debe depender de firmas por CVEs, ni heurísticas tradicionales.
- La capacidad de bloqueo de técnicas de explotación no deberá limitarse únicamente a aplicaciones predeterminadas. La plataforma deberá permitir extender la protección a procesos adicionales, incluyendo aplicaciones desarrolladas internamente (in-house), permitiendo especificar explícitamente los nombres de los procesos a proteger.
- Deberá proteger contra la explotación de vulnerabilidades del sistema operativo y de aplicaciones, incluso cuando estas no cuenten con el parche de seguridad instalado, mitigando riesgos asociados a ventanas de exposición.
- Los mecanismos de protección contra vulnerabilidades deberán ser independientes de la existencia o identificación de un CVE, permitiendo detectar y bloquear intentos de explotación de vulnerabilidades conocidas y de día cero, aun cuando estas no cuenten con un identificador público.
- El agente dedeberá ser capaz de enviar automáticamente archivos sospechosos y/o desconocidos a un entorno de sandbox para su emulación y análisis, esta capacidad deberá estar soportada al menos para Windows, Linux y MacOS.
- El entorno de sandbox podrá ser provisto por el mismo fabricante de la solución o por un tercero, siempre que se encuentre debidamente integrado con la plataforma.
- El sandbox deberá soportar el análisis de al menos 500,000 archivos diarios y permitir el análisis de archivos de hasta 100 MB de tamaño.
- Debe permitir gestionar los puertos USB que permitan conectar dispositivos como: discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles, unidades lectoras de discos floppy externas.
- Las políticas de control de dispositivos deben poder asignar a nivel de hostnames, grupos de hosts, usuarios, grupos de Active Directory.
- Debe de permitir la creación de excepciones temporales a partir de una alerta registrada, para permitir el dispositivo solo durante un tiempo configurable
- Toda la telemetría colectada del endpoint se deberá realizar de manera continua y en línea, así exista o no exista una alerta de seguridad de por medio, el agente debe colectar la siguiente telemetría, enviarlo automáticamente y de manera cifrada hacia la nube de la solución y almacenarse en formato estructurado para labores de analítica y threat hunting.
- El agente deberá capturar, como mínimo, la siguiente telemetría para equipos Windows:
    - Ejecución de procesos, incluyendo tiempo de inicio y tamaño del archivo.
    - Operaciones sobre archivos: creación, escritura, modificación, renombrado y eliminación.
    - Carga de DLLs, incluyendo ruta completa, dirección base, ID del proceso, tamaño de imagen, firma digital y hashes MD5 y SHA256.
    - Creación y finalización de procesos, con atributos como: proceso padre, PID, ruta completa, argumentos de línea de comando, hashes y detalles de firma o certificado.
    - Inyección de hilos, incluyendo ID del hilo padre, ID del hilo creado o terminado y proceso originador.
    - Interacciones de red, incluyendo IP y puertos origen/destino, estado de conexión (exitosa o fallida), protocolo (TCP/UDP), solicitudes y respuestas de DNS y actividad HTTP.
    - Estadísticas de red, considerando volúmenes de tráfico TCP de subida y descarga.
    - Acciones sobre el Registro de Windows, incluyendo creación, modificación, eliminación, restauración y guardado de claves y valores, con ruta y datos afectados.

  - Eventos de sesión del sistema, tales como inicio y cierre de sesión, conexión y desconexión.
  - Eventos .NET, tales como carga de DLL, intentos de bypass de AMSI.
  - Llamadas RPC y llamadas al sistema (syscalls).
  - Eventos de Windows, incluyendo logs de Seguridad y Aplicación, con soporte para al menos 60 tipos de eventos, entre ellos: 4880, 4881, 4896, 4898, 6272, 6280, 4624, 4625, 4634, 4647, 4649, 4776, 4800, 4801, 4720, 4722, 4723, 4724, 4725, 4726, 4727, 4731, 4754, 4728, 4732, 4756, 4735, 4737, 4755, 4764, 4741, 4742, 4743, 4698.
- El mismo agente de Endpoint Protectión deberá ser capaz de colectar la siguiente telemetría para equipos MacOS y Linux:
  - Logs de eventos de autenticación
  - Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
  - Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma digital.
  - Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
  - Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.
- Deberá poder almacenar toda la telemetría de los endpoints por al menos 30 días.
- La solución deberá presentar una secuencia gráfica del incidente de seguridad, construida automáticamente mediante los mecanismos de inteligencia artificial de la plataforma, que correlacione múltiples alertas y eventos con el objetivo de identificar la causa raíz del incidente.
- La secuencia gráfica deberá mostrar la información de los procesos correlacionados, incluyendo como mínimo: ruta de ejecución, usuario que ejecutó el proceso, entidad firmante del ejecutable, hash SHA256, veredicto del análisis en sandbox y línea de comandos utilizada., timestamp, hostname, dirección IP local y remota, TTPs de MITRE ATT&CK, actividad de red generada por cada proceso, actividad de archivos y directorios, actividad a nivel de claves de registro, llamadas RPC, Syscalls, Event Logs generados.
- La solución deberá permitir mostrar el catálogo de reglas de detección por comportamiento predefinidas en la plataforma, de tal forma que éstas se puedan clonar y crear reglas personalizadas de detección.
- La solución deberá permitir mostrar el catálogo de reglas de detección basadas en inteligencia artificial (IA), los cuales no deberán estar basadas en reglas estáticas, sino en el aprendizaje individual de cada activo.
- La solución deberá permitir la creación de reglas personalizadas de detección, basadas en el comportamiento de usuarios y hosts. Para ello se podrá hacer uso de cualquier evento colectado de telemetría.
- Deberá poder generar un inventario de las aplicaciones instaladas en las computadoras con sistema operativo Windows, MacOS y Linux
- Deberá generar un inventario de características de hardware del endpoint, como mínimo cantidad de memoria RAM; tipo, marca y capacidad de procesador; almacenamiento del disco duro; identificar si es servidor, desktop o laptop; sistema operativo y arquitectura.
- Deberá poder listar los usuarios locales creados en el endpoint y su respectivo estado (activo o inactivo)
- Deberá poder listar los autoruns, servicios/daemons y unidades o carpetas compartidas.
- Deberá ser capaz de guardar un histórico diario de estos inventarios, para poder comparar cambios que hubiesen ocurrido. Este histórico deberá estar disponible por al menos 30 días.

- A partir de la telemetría recolectada de los endpoints y de la información contextual de usuarios y hosts obtenida mediante las integraciones, la plataforma deberá aprender de forma automática un perfil base (baseline) del comportamiento de cada activo.
- Los perfiles de comportamiento deberán ser generados dinámicamente mediante algoritmos de aprendizaje de máquina no supervisado, permitiendo modelar el comportamiento normal sin necesidad de reglas predefinidas o umbrales estáticos
- Con base en el comportamiento aprendido, el módulo de UEBA deberá ser capaz de detectar y alertar actividades inusuales o desviaciones significativas respecto al perfil base establecido. Deberá tener al menos 150 casos de uso nativos, generados por machine learning, incluyendo los siguientes:
    - Comandos anómalos ejecutados en el endpoint
    - Múltiples procesos LOLBINs ejecutados
    - Procesos raros ejecutados sobre el endpoint
    - Eventos de Pass the ticket
    - Proceso conectándose a un sitio externo inusual
    - Comandos de powershell inusuales
    - Cifrado de datos sospechoso en el endpoint
    - Carga de driver inusual
    - Conexión anómala usando WMI
    - Servicio detenido de manera inusual
    - Tráfico LDAP generado desde un proceso inusual
    - Transferencia inusual de archivos por SMB
- La plataforma deberá asignar un puntaje de riesgo (risk score) a usuarios y hosts, considerando la frecuencia, severidad y correlación de eventos sospechosos y/o anómalos, con el objetivo de facilitar el triage y la priorización de incidentes.

46. ZTNA (Zero Trust Network Access) – 01 Solución

- La solución ZTNA deberá proporcionar acceso seguro a aplicaciones mediante un cliente de acceso remoto, aplicando políticas basadas en identidad de usuario, aplicación y contexto, sin exponer la red interna.
- La solución ZTNA deberá ser una solución dedicada o formar parte los NGFW Perimetrales. Debiendo integrarse a la Consola de Analítica y Reportes para permitir la aplicación de políticas de seguridad y control de acceso de manera unificada.
- La solución ZTNA debe soportar al menos 200 usuarios, debiendo incluir el licenciamiento necesario.
- Deberá ser capaz de validar si el equipo que intenta acceder a algún recurso de red (IP o IPs destino) cuenta con una postura de seguridad adecuada.
- La restricción al recurso de red debe ser personalizable, es decir, deberá permitir acceder de manera total o parcial al recurso de red destino en base al nivel de cumplimiento de la postura de seguridad del equipo. Por ejemplo, si cumple parcialmente con la postura de seguridad únicamente se le dará acceso para hacer PING a un servidor, sí cumple completamente podrá acceder vía RDP.
- La validación de la postura de seguridad del endpoint deberá ser continua; el NGFW automáticamente deberá restringir el acceso si es que luego de la conexión establecida el equipo modifica su postura de seguridad.
- Como mínimo la postura de seguridad del endpoint deberá validar lo siguiente:
    - Sistema operativo del equipo
    - Serial number del equipo
    - Pertenencia al dominio corporativo
    - Software antivirus instalado y habilitado en tiempo real
    - Software antivirus con la base de datos de firmas actualizada en un número de días personalizable
    - Haber realizado un escaneo del malware en un equipo dentro de un número de días personalizable
    - Marca del software antivirus
    - Parche de seguridad instalado, según su nivel de criticidad, o en su defecto mostrar las vulnerabilidades del endpoint (por CVE).

  - Firewall de host habilitado
  - Permitir validaciones personalizadas en base a registros de REGEDIT
- Las políticas de validación de postura del endpoint deberán poder ser aplicadas a un grupo de usuarios o direcciones IP.
- Deberá permitir configurar un mensaje personalizado, el cual permita notificar al usuario que controles no está cumpliendo.
- Esta verificación se podrá realizar a través de un agente instalado en los endpoints. Debe tener soporte como mínimo para Windows y MacOS.
- La solución podrá integrarse a una plataforma de Network Access Control (NAC) para cumplir los requerimientos listados. Se deja libertar al postor de elegir la plataforma NAC que se pueda integrar.
- Debe tener capacidad de integrarse con plataformas de Doble Factor de Autenticación (2FA).
- Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN, incluyendo el soporte de Split DNS.
- El Split Tunnel debe permitir elegir el tipo tráfico que se enrutará por el túnel VPN, basado en el nombre de la Aplicación y el Dominio.
- Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
  - Antes del usuario se autentique en la estación.
  - Después de la autenticación del usuario en la estación usando Single Sign On (SSO).
  - A demanda, de forma manual por parte del usuario.
- El agente de VPN client-to-site debe ser compatible al menos con: Windows 10, Windows 11 professional
- , MacOS X, Linux, Android y iOS.
- La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada, de manera manual y automática. Los equipos en cuarentena no deberán tener conexión con ningún recurso de red protegido por la solución. Esta capacidad deberá tener cobertura dentro de la red interna, sin necesidad de hacer túneles VPN.
- Para el caso de usuarios externos, dispositivos no gestionados o escenarios de acceso temporal, la solución deberá permitir el acceso seguro a aplicaciones críticas mediante navegador web, sin requerir la instalación de agentes en el endpoint. Esto a fin de reducir la superficie de ataque, evitar la exposición de la red interna y garantizar un control granular sobre el acceso y uso de la información sensible.
- La solución ZTNA adicionalmente deberá incluir capacidades de acceso seguro a aplicaciones a través de navegador web (agentless), permitiendo el acceso controlado a recursos críticos sin requerir la instalación de software en el endpoint.
- El acceso ZTNA mediante navegador web seguro debe estar licenciada para un minimo de 200 usuarios.
- El acceso ZTNA mediante navegador web deberá estar basado en validación de identidad del usuario y contexto de la sesión, permitiendo aplicar políticas de seguridad consistentes con las definidas para el acceso mediante cliente.
- El acceso ZTNA mediante navegador web deberá permitir la aplicación de controles granulares sobre la sesión web, incluyendo como mínimo restricciones de descarga, carga de archivos, copiado/pegado, impresión y transferencia de información.
- Este navegador web debe permitir el acceso seguro desde dispositivos no gestionados o de terceros, garantizando el aislamiento de la sesión y la protección de la información accedida.
- El acceso mediante navegador web seguro deberá integrarse con la plataforma de analítica y reportes, permitiendo la aplicación consistente de políticas de acceso y controles de seguridad definidos para el modelo ZTNA.
- El navegador web seguro deberá permitir la visibilidad y registro de las actividades realizadas durante la sesión, incluyendo usuario, aplicación accedida, acciones ejecutadas y duración de la sesión, para fines de auditoría y análisis.
- El navegador web seguro deberá permitir la aplicación de controles basados en tipo de aplicación (por ejemplo, aplicaciones web internas o SaaS), sin exponer directamente la red interna.

47. Seguridad para Correo Electrónico – 01 solución

- El servicio de correo electrónico es Zimbra, por lo que la solución deberá integrarse mediante protocolos SMTP, operando como gateway de correo electrónico a través de registros MX, permitiendo la inspección completa del tráfico entrante y saliente antes de su entrega.
- La solución deberá proteger un mínimo de 1000 buzones de correo electrónico bajo un modelo de licenciamiento por usuario, permitiendo escalabilidad automática en arquitectura SaaS, sin requerir adquisición de infraestructura adicional ni afectar el rendimiento del servicio
- La solución deberá implementar un modelo de análisis multicapa basado en riesgo, que combine técnicas de reputación, machine learning, análisis heurístico y análisis dinámico mediante sandboxing selectivo, permitiendo evaluar los correos electrónicos y sus componentes de manera eficiente según su nivel de riesgo.
- La solución deberá analizar todas las URLs y archivos adjuntos contenidos en los correos electrónicos entrantes mediante un modelo de análisis multicapa basado en riesgo, que combine técnicas de reputación, análisis estático y análisis dinámico selectivo para la detección de amenazas conocidas y desconocidas.
- La solución deberá permitir a los administradores acceder a información detallada del análisis de cada correo electrónico procesado, incluyendo trazabilidad completa del mensaje, clasificación de la amenaza, motores de detección utilizados y las razones específicas por las cuales el correo ha sido identificado como malicioso
- La solución deberá permitir la clasificación diferenciada de tipos de correo no deseado, incluyendo spam, graymail y campañas masivas, así como la aplicación de políticas específicas para cada categoría
- La solución deberá incorporar inteligencia de amenazas global que combine fuentes internas y externas, análisis basado en aprendizaje automático y correlación de eventos a gran escala, permitiendo la detección proactiva de amenazas conocidas y desconocidas en el tráfico de correo electrónico.
- La solución deberá incorporar motores antivirus como parte de una arquitectura de seguridad multicapa, permitiendo la detección de amenazas conocidas en el tráfico de correo electrónico, complementadas con mecanismos avanzados de análisis para la identificación de amenazas emergentes y sofisticadas.
- La solución deberá incorporar capacidades avanzadas de detección que no dependan exclusivamente de firmas tradicionales, utilizando inteligencia de amenazas, aprendizaje automático, análisis de comportamiento y correlación global para identificar amenazas conocidas, variantes y campañas emergentes.
- La solución deberá ofrecer protección frente a phishing, spear phishing, robo de identidad y phishing mediante códigos QR, utilizando análisis lingüístico del contenido, visión por ordenador, aprendizaje automático, evaluación de reputación y correlación de inteligencia de amenazas para identificar intentos de engaño dirigidos a usuarios."
- La solución deberá brindar protección frente a ataques de tipo Business Email Compromise (BEC), mediante el uso de análisis contextual, comportamiento del remitente, inteligencia de amenazas y validación de mecanismos de autenticación como SPF, DKIM y DMARC.
- La solución deberá detectar y proteger contra ataques de suplantación (spoofing), incluyendo la identificación de suplantación de nombres visibles (display name spoofing), suplantación de dominios y ataques dirigidos a usuarios VIP, mediante análisis contextual y de comportamiento del remitente
- La solución deberá contar con mecanismos para proteger contra ataques de tipo zero-day y N-day, mediante el uso de análisis de comportamiento, inteligencia de amenazas, machine learning y capacidades de análisis dinámico en entornos controlados.
- La solución deberá contar con mecanismos avanzados de protección de URLs que permitan analizar los enlaces contenidos en los correos electrónicos mediante técnicas como reescritura de URLs, evaluación de reputación en tiempo real y análisis dinámico en el momento de interacción del usuario (time-of-click), con el fin de identificar y bloquear enlaces maliciosos antes y después de su entrega al usuario final.
- La solución deberá contar con capacidades de análisis avanzado de archivos adjuntos mediante tecnología de sandboxing, integrada dentro de un modelo de protección multicapa que combine técnicas de análisis estático, reputación, machine learning y

análisis dinámico selectivo, permitiendo la detección de amenazas conocidas y desconocidas en archivos

- La solución deberá garantizar que los procesos de análisis de archivos adjuntos se realicen sin alterar su estructura ni contenido original, utilizando mecanismos de análisis seguros como entornos aislados (sandbox) y técnicas de inspección que operen sobre copias del archivo, manteniendo la integridad del contenido original
- La solución deberá ser capaz de detectar macros maliciosas y contenido sospechoso dentro de documentos adjuntos, mediante el uso de análisis de comportamiento, sandboxing e inteligencia de amenazas, permitiendo identificar actividades maliciosas y vectores de ataque embebidos en archivos.
- La solución deberá proporcionar herramientas de investigación que permitan analizar correos, archivos o enlaces previamente procesados, mediante interfaces de consulta y análisis desde la consola de administración
- La solución deberá ser capaz de analizar contenido comprimido y archivos embebidos dentro de los correos electrónicos, incluyendo estructuras anidadas, permitiendo identificar archivos, documentos y enlaces ocultos para su evaluación mediante mecanismos de análisis de seguridad multicapa
- La solución deberá ser capaz de identificar archivos protegidos por contraseña dentro de los correos electrónicos y aplicar políticas de seguridad configurables para su tratamiento, tales como bloqueo, cuarentena o entrega controlada, en caso de que el contenido no pueda ser inspeccionado
- La solución deberá ser capaz de analizar archivos comprimidos contenidos en los correos electrónicos, permitiendo extraer y evaluar su contenido mediante mecanismos de análisis de seguridad multicapa, con el fin de identificar amenazas ocultas en archivos y estructuras anidada
- La solución deberá contar con reconocimiento en reportes de analistas del mercado de seguridad de correo electrónico, tales como Magic Quadrant, Forrester Wave u otros estudios equivalentes, evidenciando su posicionamiento y capacidad de ejecución en el segmento
- La solución deberá ser nativa en la nube (cloud-native), operando bajo un modelo SaaS completamente alojado en infraestructura cloud, sin requerir la instalación de componentes on-premise, y permitiendo la integración con el servicio de correo mediante mecanismos estándar como SMTP/MX.
- La solución deberá operar bajo un modelo SaaS que garantice la actualización automática y continua de sus capacidades de seguridad, motores de detección e inteligencia de amenazas, sin requerir intervención manual por parte de la Entidad.
- La solución deberá operar bajo un modelo cloud-native que permita escalar automáticamente en función de la demanda, adaptándose al crecimiento de la Entidad sin requerir la adquisición de hardware adicional, y garantizando niveles adecuados de rendimiento y experiencia de usuario.
- La solución deberá permitir su implementación en modo de prevención de amenazas en línea (inline), inspeccionando el tráfico de correo electrónico antes de su entrega a los servidores, con el fin de detectar y bloquear amenazas antes de que lleguen al usuario final.
- La solución deberá operar mediante un modelo Secure Email Gateway (SEG) en modo inline, integrándose con el servicio de correo mediante registros MX, permitiendo la prevención de amenazas en tránsito antes de la entrega al usuario final.
- La solución deberá permitir el despliegue de la protección a nivel de dominio, aplicando controles de seguridad de manera centralizada sobre todos los usuarios.
- La solución deberá contar con una consola de administración centralizada que permita visualizar información detallada sobre incidentes de seguridad, reportes de amenazas y políticas aplicadas al tráfico de correo electrónico, proporcionando visibilidad completa para la gestión y monitoreo del servicio.
- La solución deberá permitir la definición y aplicación de políticas de control basadas en listas blancas y negras (whitelisting y blacklisting), utilizando parámetros como direcciones IP, dominios, remitentes, URLs y tipos de archivos, integradas dentro de un modelo de seguridad multicapa.
- La solución deberá permitir que los usuarios finales reporten de manera sencilla correos sospechosos o incorrectamente clasificados (falsos positivos o falsos negativos), integrando estos reportes en los procesos de análisis y respuesta de seguridad

- La solución deberá permitir el envío de notificaciones y resúmenes periódicos a los usuarios finales, incluyendo información sobre correos en cuarentena y acciones aplicadas, facilitando su visibilidad e interacción con los mensajes filtrados.

48. WAF - Seguridad para Aplicaciones Web (01 Unidades)

Modalidad del Servicio

- Tipo de Despliegue: La solución debe ser entregada bajo la modalidad de Software as a Service (SaaS) basado en la nube.
- Arquitectura: El servicio debe actuar como un proxy inverso en la nube, inspeccionando el tráfico antes de que este llegue a la infraestructura on-premise.
- Propósito: La solución debe proteger contra ataques en capa de aplicacion web en nube que soporte despliegues siempre activos, a través de modificación de DNS y que no requieran modificación alguna de Hardware o Sofware del lado de los servidores a proteger.

Licenciamiento

- Capacidad de Tráfico: El licenciamiento debe cubrir un ancho de banda (Throughput) de inspección adecuado para la demanda de las aplicaciones publicadas.
- Protección de Aplicaciones: Debe proteger un total de 10 aplicaciones con ancho de banda máximo de 100 Mbps.
- El servicio de Cloud WAAP debe soportar un modelo de integración basado en API que no requiera cambios de DNS o BGP para proteger las aplicaciones y que cuente tenga las siguientes características:
  - En la arquitectura basada en API no se requiere compartir el certificado digital.
  - En la arquitectura basada en API los requerimientos van directamente a la aplicación.

Capacidades de Seguridad

- La solución debe contar con un mecanismo que permita el bloqueo automático y temporal de direcciones IP de origen (source-blocking), basado en el análisis de los ataques realizados por un mismo actor a las diferentes aplicaciones protegidas. Este mecanismo debe ser automático, basado en ML, y permitir definir la sensibilidad de la activación.
- La solución debe contar con un mecanismo que permita visualizar los subdominios y/o URLs que invocan los scripts de java (JS) desde el navegador de los usuarios que consumen las aplicaciones, así como el nivel de amenaza de los mismos y si es que estos cuentan o no con certificados de seguridad.
- El servicio de Cloud WAAP debe proveer una protección basada en firmas que proteja la aplicación contra vulnerabilidades conocidas.
- El servicio debe proveer una protección contra comandos de SQL, comandos de shell y ataques de cross-site scripting, usando un algoritmo de reducción para detectar posibles segmentos de código en los parámetros. La protección debe cubrir al menos las siguientes amenazas: Cross Site Scripting (XSS), SQL Injections, Injection Flaws, Command Execution, Database Sabotage, Stealth Commanding, Backdoor.
- La solución deberá permitir al administrador, crear firmas custom (Custom Signatures). Mediante este mecanismo el administrador podra incorporar a las protecciones incluidas en la solución patrones especificos que desee tratar como eventos de seguridad.
- Gestión de Botnet: El servicio debe incluir protección contra ataques de tipo BOT (ataques automatizados) basado en firmas, siendo capaz de mitigar como minimo, bots de GEN 1 y GEN 2 (scripts y headless browsers)
- El servicio debe detectar y bloquear tráfico de bots en donde existan las siguientes anomalías de User-Agent:

- User-Agents invalidos.
- Headless Chrome.
- Navegadores Antiguos.

- El portal permitirá automatizar la creación de Certificados Digitales para las aplicaciones que así lo requieran. Este servicio no deberá representar costos adicionales para el cliente y permitira como minimo la creación de un certificado por aplicacion protegida
- Políticas de Seguridad Positiva y Negativa: Las políticas de seguridad debe implementar filtros de seguridad que soporten modelos de seguridad positivos y negativos.
- El portal debe contar con un servicio de Inteligencia reputacional, que permita a los operadores visualizar insights sobre las direcciones IP consultadas.
- El servicio debe garantizar la disponibilidad mínima de la infraestructura de red del servicio debe ser de 99.999% con un PoP de mitigación local.
- El servicio de Cloud WAAP debe ser un servicio de seguridad administrado por el fabricante con disponibilidad 7x24x365.

Gestión y Visibilidad

- El portal de servicios debe permitir visualizar los eventos de seguridad por aplicación. La información mínima que deben tener estos logs:
  - Acción tomada por el servicio
  - Dirección IP origen
  - País de Origen
  - Aplicación
  - Fecha y hora del evento
  - Severidad
  - Tipo de ataque
  - Clasificación del ataque de acuerdo al OWASP Top 10 2021
  - Entregar el detalle del encabezado del request de HTTP del ataque

49. SIEM (01 solución)

- La solución deberá realizar monitoreo, correlación y análisis de eventos de seguridad (SIEM), formando parte de una plataforma unificada de operaciones de seguridad que integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.
- La solución deberá permitir la ingesta, normalización y correlación automatizada de eventos en tiempo cercano a real, generando alertas consolidadas y permitiendo la ejecución de acciones de respuesta desde una única consola.
- La solución debe operar en modalidad SaaS (basada en la nube), permitiendo el uso de componentes locales (máquinas virtuales o agentes) únicamente para la recolección e integración de fuentes de datos internas, sin requerir infraestructura on-premise para el procesamiento, almacenamiento o correlación de eventos.
- La plataforma deberá estar basada en nube, con el objetivo de no tener limitaciones de hardware para el procesamiento de los algoritmos de Inteligencia Artificial (IA) en las fases de detección, investigación y respuesta ante amenazas.
- La nube desde donde se brinde el servicio deberá contar con las siguientes características para garantizar la confidencialidad, integridad y disponibilidad de los datos de la entidad:
  - Contar con la certificación SOC2 Plus de AICPA y CSA START Nivel 2 (Cloud Security Alliance)
  - Contar con certificaciones ISO 27001, ISO 27017, ISO 27018 e ISO 27701
  - Contar con doble factor de autenticación para el login proporcionado de manera nativa por la plataforma.
- Para el cifrado de los datos alojados en el tenant, la plataforma deberá soportar el mecanismo de BYOK (Bring Your Own Keys), permitiendo a la Entidad generar, importar y gestionar sus propias claves de cifrado, mediante un servicio de administración de claves, manteniendo control y auditabilidad sobre el acceso y el cifrado de los datos y apoyando cumplimiento regulatorio.

- La integración entre los distintos componentes deberá ser nativa, sin requerir desarrollos personalizados, procesos complejos de parsing o integraciones externas para la correlación de eventos.
- Debe soportar al menos 4,000 eventos por segundo y 50 dispositivos, o soportar ingesta de 350 GB por día.
- Debe permitir crecimiento de capacidad a demanda sin límites y únicamente adquiriendo licenciamiento adicional en caso la Entidad lo requiera a futuro.
- Deberá soportar múltiples mecanismos de ingesta/colección de logs, con conectores nativos para cientos de plataformas y la capacidad de integrar cualquier otra fuente donde no exista un conector nativo mediante mecanismos genéricos. Como mínimo, deberá soportar:
    - Syslog, en formato CEF, LEEF, RAW
    - API Polling/Pull: la solución extrae los logs de una plataforma externa.
    - API Receiver (HTTP Collector): la solución recibe logs enviados desde una plataforma externa.
    - Webhook
    - Netflow Collector
    - Windows Event Collector (WEC): colección de logs de Servidores Windows sin necesidad de desplegar agentes.
    - File Share Collector: colección de archivos de logs en formatos RAW, JSON, CEF, LEEF, CSV, TSV, almacenados en carpetas compartidas
    - FTP Server Collector: colección de archivos de logs en formatos RAW, JSON, CEF, LEEF, CSV, TSV, almacenados en servidores FTP/FTPS/SFTP.
    - Database Collector: colección de logs almacenados en tablas de bases de datos MySQL, MSSQL, Oracle, PostgreSQL.
    - Agentes de Colección: agentes
    - livianos para colectar logs de Auditoria, IIS, DNS, DHCP, entre otros, en servidores Windows y Linux.
- Todos los eventos, logs y telemetría recolectada deberán ser almacenados de manera normalizada y estructurada en tablas, datasets o índice de datos. El presente documento usará el término "tablas" para estandarizar el concepto.
- Deberá ser capaz de recolectar y almacenar centralizadamente logs y telemetría de endpoints provenientes de agentes EDR/XDR, ya sean del mismo fabricante o de terceros. El Postor deberá incluir el licenciamiento necesario para habilitar esta capacidad. Se entiende por telemetría no solo las alertas generadas por el EDR/XDR, sino también la actividad detallada del endpoint, incluyendo como mínimo: procesos (creación/árbol/command-line), archivos (creación/modificación/lectura), registro (Windows Registry), sesiones e identidad (logon/logoff), actividad de red (conexiones/DNS), y otros eventos relevantes de seguridad
- Deberá tener conectores nativos para más de 1000 plataformas de terceros y ser capaz de normalizar los eventos de manera nativa, sin necesidad de escribir reglas de correlación
- Debe ser capaz de monitorear en tiempo real el estado de salud de las fuentes de eventos y generar una alerta de manera automática ante estas ocurrencias. Por cada alerta deberá mostrar las causas del problema o posibles causas (tales como errores de conexión por API y otro), y debe tener la capacidad de ejecutar un playbook automatizado para el tratamiento de estos problemas.
- Deberá calcular automáticamente una línea base (baseline) de recepción de logs por cada fuente y generar alertas ante desviaciones significativas respecto a dicha línea base.
- Debe realizar la colección de eventos de los dispositivos en las premisas mediante la implementación de una máquina virtual (colector) o hardware appliance.
- Los colectores deberán tener la capacidad de ser desplegados en Alta Disponibilidad para tener resiliencia en la recolección de eventos.
- Deberá estar licenciado para almacenar todos los logs por al menos 30 días en formato de Hot Storage (almacenamiento en caliente para acceder a la data de manera constante) y 180 días en formato Cold Storage (almacenamiento en frio, que no requiere acceso constante a la data). Esta capacidad deberá ser granular, permitiendo elegir sobre que fuentes se requiere mayor periodo de retención.

- Debe ser capaz de almacenar la telemetría de los EDR/XDR integrados por al menos 30 días en formato Hot Storage (almacenamiento en caliente para acceder a la data de manera constante
- El método principal de detección deberá estar basado en inteligencia artificial. Es decir, la inteligencia artificial de la plataforma deberá ser capaz de procesar todos los logs y telemetría recolectada de las distintas fuentes para generar casos de uso de detección y alertar posibles incidentes.
- Cada alerta de seguridad debe ser enriquecida con atributos asociados a Tácticas y Técnicas de Ataque, Tipo de Amenaza, Severidad, Categoría.
- Los perfiles de comportamiento deberán de ser generados mediante el uso de perfiles estadísticos y algoritmos de machine learning.
- El motor de analítica debe procesar los eventos (red, autenticación, endpoint, cloud, etc.) para construir una línea base de actividad y generar alertas cuando identifique anomalías.
- Cada detector debe trabajar con intervalos de tiempo definidos: un periodo de activación/perfilado (tiempo de "calibración") para reunir datos suficientes y reducir falsos positivos; un periodo de evaluación para comparar la actividad reciente contra la línea base; y un periodo de entrenamiento (línea base) como histórico para calcular y ajustar continuamente y de manera automática los umbrales por cada activo.
- Debe contar con al menos 500 casos de uso de detección de amenazas. Todos estos casos de uso deberán estar activados de manera automática, sin necesidad de construir una regla de correlación o afinamiento manual.
- Deberá permitir la creación de reglas de correlación que permitan configurar casos de uso utilizando los eventos recolectados de las diversas fuentes.
- Las reglas de correlación deberán poder construirse en base a umbrales, filtros, rangos de tiempo y otros parámetros.
- Las reglas de correlación deberán poder construirse con más de una tabla (dataset o índice de eventos), es decir, una regla de correlación deberá poder usar distintas fuentes de logs.
- Un incidente deberá contener uno o varias alertas de seguridad, la plataforma deberá ser capaz de contextualizar y correlacionar automáticamente alertas de múltiples fuentes (cross-correlation) que formen parte de un mismo incidente.
- Las alertas de seguridad deberán tener un periodo de almacenamiento mínimo de 180 días.
- La solución deberá contar con un lenguaje de consulta especializado, diseñado para hacer consultas (querys) de forma directa a todos los eventos de seguridad recolectados desde fuentes externas integradas y de la Telemetría del Endpoint.
- El lenguaje deberá incluir operadores avanzados que permitan manipular, transformar y sintetizar la información, facilitando el análisis eficiente de grandes volúmenes de eventos.
- Deberá contar con capacidades de IA generativa que permitan asistir la construcción de consultas (queries) a partir de prompts en lenguaje natural, generando consultas en el lenguaje especializado de la plataforma, esto con la finalidad de facilitar el trabajo del analista.
- Debe tener más de 200 integraciones nativas con plataformas de inteligencia de amenazas, de los cuales se permita recolectar Feeds de manera automática, tales como: AbuseIPDB, Virus Total, Alienvault, Censys, Cyren, Domain Tools, Feedly, IP-API, IPQS, IPInfo, MISP, MITRE ATT&CK Feeds, MXtoolbox, Pwned, Shodan, Azure Feed.
- Con el objetivo de facilitar las labores de triage, la plataforma deberá ser capaz de correlacionar alertas provenientes de distintos mecanismos de detección y agruparlas automáticamente en un incidente unificado, de acuerdo a la naturaleza y similitudes de las alertas. Asimismo, deberá permitir la agrupación manual de alertas e incidentes cuando sea requerido por el analista.
- Debe permitir crear alertas e incidentes de manera manual, donde se pueda definir el nombre del evento, severidad, categoría, TTPs acorde a MITRE ATT&CK, y un playbook de respuesta.
- Por cada incidente se deberá mostrar las técnicas y tácticas de MITRE ATT&CK que fueron detectadas en ese incidente.
- La solución deberá contar con un módulo de reglas de puntaje de riesgo (risk scoring), que permita asignar un nivel de severidad cuantitativo (por ejemplo, en una escala de 0

a 100) a las amenazas detectadas, considerando la criticidad de los activos afectados y el tipo de amenaza.
- Debe tener un dashboard para monitorear el MTTR (mean time to response) en la gestión de incidentes.
- Debe tener un dashboard que permita dar seguimiento a los incidentes abiertos
- El soporte del fabricante deberá incluir un servicio que permita a la Entidad a optimizar la plataforma adquirida, para ello deberá tener como mínimo los siguientes alcances:
  - Verificar el estado de los componentes de la solución
  - Asistir en la configuración y corrección de parsing rules
  - Proveer recomendaciones para adoptar las configuraciones alineadas a las buenas prácticas
  - Proveer workshops y demostraciones del producto sobre nuevas capacidades que se publiquen a lo largo del servicio
  - Asistir a la Entidad con el afinamiento de las alertas e incidentes
  - Asistir a la Entidad a optimizar los playbooks de automatización
  - Proveer workshops a medida acorde a los objetivos de la Entidad
  - Realizar health checks completos de la plataforma al menos con una periodicidad anual

50. Plataforma de Detección y Respuesta de Amenazas Externas e Internas (01 solución)
- La solución deberá proporcionar capacidades de detección y análisis de amenazas externas mediante la identificación y evaluación de la superficie de ataque expuesta.
- La solución deberá formar parte de una plataforma unificada de operaciones de seguridad que permita complementar estas capacidades con la detección y respuesta de amenazas internas, mediante la integración y correlación de telemetría proveniente de diferentes fuentes de seguridad.
- La solución deberá permitir la correlación de riesgos externos con eventos internos, proporcionando una visión integral del riesgo de seguridad y facilitando la priorización de acciones de mitigación.
- La gestión deberá realizarse desde una plataforma centralizada, permitiendo la visibilidad unificada de amenazas, exposiciones y eventos de seguridad.
- La solución deberá descubrir de forma continua la superficie de ataque externa, atribuyendo activos públicos a la organización (incluyendo activos conocidos y no conocidos) mediante análisis de registros IP, dominios (WHOIS), Número de Sistema Autónomo (ASN), certificados y datos de escaneo, sin requerir agentes ni instalaciones adicionales.
- Deberá descubrir servicios cloud expuestos a Internet que no estén gestionados y/o no sean conocidos por la Entidad.
- Deberá permitir cargar activos al inventario mediante la interfaz (por ejemplo, importando un archivo CSV).
- Deberá soportar como mínimo la carga de dominios, subdominios y rangos IP.
- Deberá tener al menos 600 políticas predefinidas para detectar amenazas sobre activos expuestos.
- Deberá permitir evaluar rápidamente el nivel de exposición frente a amenazas emergentes tipo zero-day, identificando y priorizando los activos potencialmente afectados.
- Deberá inventariar certificados digitales usados para comunicaciones cifradas, registrando sus principales metadatos (emisor, clave pública/algoritmo, subject, organización y país/estado) y ejecutar clasificaciones básicas de "salud criptográfica" (por ejemplo, auto-firmado, wildcard, validación de control de dominio, expiración, tamaño de clave y algoritmo de firma).
- Deberá inventariar dominios externos atribuidos a la Entidad, indicando si tienen resolución reciente.
- Deberá recolectar información de dominios y DNS mediante técnicas globales de recolección activa y pasiva, incluyendo escaneos que permitan identificar servidores DNS.
- Deberá mantener un inventario de servicios expuestos a Internet atribuidos a la Entidad, y que respondan a escaneos sobre Internet público.

- Deberá clasificar cada servicio según el análisis basado en fingerprinting (software, tecnologías y comportamientos), indicando si cada clasificación está activa o inactiva según observaciones recientes.
- Deberá recolectar y presentar información adicional del servicio descubierto (por ejemplo, banner, respuestas y encabezados) para enriquecer el análisis y la priorización.
- Deberá escanear sitios web expuestos a Internet para identificar sitios inseguros, componentes y tecnologías usadas, manteniendo un inventario actualizado.
- Por cada sitio web, deberá detectar el uso de tecnologías/librerías de terceros, configuraciones inseguras, tecnologías vulnerables, incumplimiento de buenas prácticas, fechas de primera y última observación, host, tipo de HTTP, direcciones IP, estado de actividad, puerto, categoría del sitio.
- Deberá diferenciar dominios, servicios externos y sitios web, reflejando su relación (un dominio puede no tener sitio; un sitio puede depender de uno o más servicios HTTP).
- Por cada sitio web, deberá mostrar una captura de pantalla reciente y un enlace directo para facilitar la investigación.
- Deberá permitir agregar o retirar activos del inventario de forma manual desde la consola.
- Debe permitir adoptar medidas de contención rápida cuando se incumpla una política de seguridad, por ejemplo, restringiendo acceso al puerto no autorizado.
- Deberá validar la remediación de alertas de ASM mediante un escaneo de confirmación que verifique que el riesgo ya no es observable.
- Deberá descubrir vulnerabilidades y malas configuraciones en activos expuestos a Internet mediante pruebas controladas diarias, reduciendo la verificación manual.
- Deberá realizar escaneos únicamente a servicios externos accesibles públicamente y seleccionados para evaluación, ejecutando cada prueba solo donde aplique según el tipo de servicio del activo expuesto.
- Deberá ser capaz de detectar credenciales por defecto de los servicios expuestos
- Debe permitir seleccionar el nivel de intrusión al momento de realizar un escaneo, considerando al menos 4 niveles:
    - No intrusivo
    - Mínima intrusión
    - Impacto medio
    - Alto impacto
- Deberá permitir administrar los test de escaneo, permitiendo habilitar o deshabilitar los test. Por cada test deberá mostrar información como software afectado, identificadores de vulnerabilidad (CVE/CWE), score de severidad (CVSS), probabilidad de explotación (EPSS), referencias, guía de remediación, estado de habilitación y cantidad de servicios confirmados como vulnerables.
- Deberá ofrecer una vista centralizada de vulnerabilidades emergentes/zero-days para identificar rápidamente los eventos que puedan impactar a la organización, mostrando métricas clave (por ejemplo, CVSS y EPSS).
- Deberá brindar contexto detallado por cada evento, tales como, resumen, posibles impactos, evidencia de explotación. Asimismo, debe permitir evaluar el impacto en la superficie externa, incluyendo servicios/softwares afectados.
- Deberá incluir guía para remediación ante las vulnerabilidades emergentes.
- Deberá permitir consultar información global sobre Direcciones IP, dominios y certificados, enriqueciendo los resultados con información contextual (registro, geolocalización, certificados relacionados, servicios observados, ASNs y DNS pasivo), incluso si la consulta corresponde a otros valores no asociados a las alertas de superficie de ataque.
- Deberá tener capacidades de protección digital de marca, considerando al menos las siguientes funcionalidades:
- Detectar dominios de riesgo asociados a suplantación de marca y reportarlos para reducir riesgos como phishing, fraude, propagación de malware y robo de información.
- Identificar credenciales filtradas reportadas externamente y priorizar las ocurridas en una ventana reciente (por ejemplo, últimos seis meses).

51. SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta (01 solución)

- La solución deberá contar con capacidades de orquestación y automatización de la respuesta ante incidentes de seguridad (SOAR), formando parte de una plataforma unificada de operaciones de seguridad que integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.
- La solución deberá contar con un catálogo de al menos 800 playbooks predefinidos, orientados a automatizar la respuesta ante incidentes de seguridad. Dichos playbooks deberán poder personalizarse según las necesidades de la Entidad.
- La plataforma deberá permitir la creación y edición de playbooks, sin establecer un límite en la cantidad de playbooks que puedan ser definidos.
- Deberá permitir la construcción de playbook de manera amigable, usando mecanismos como drag-and-drop de las tareas/scripts y otros playbooks.
- La plataforma deberá soportar la reutilización de automatizaciones, permitiendo que un playbook pueda ser contenido dentro de otro, con el fin de estandarizar y optimizar los procesos de respuesta.
- La solución deberá permitir crear bucles dentro de un playbook principal mediante sub-playbooks, donde cada iteración calcule sus valores usando los datos del sub-playbook.
- La solución deberá permitir controlar el comportamiento del bucle (por ejemplo, máximo de iteraciones y tiempos de espera) para evitar impactos de rendimiento, y deberá iterar automáticamente cuando la entrada a una tarea del playbook sea un campo tipo arreglo (array), sin requerir configurar un bucle manual.
- La solución deberá contar con capacidades de filtrado, que permitan extraer información relevante desde estructuras complejas, utilizando criterios definidos por el analista y reutilizando los resultados en tareas posteriores.
- La solución deberá incluir funciones de transformación de datos, orientadas a normalizar, formatear y adaptar la información para su análisis, toma de decisiones o ejecución de acciones automatizadas.
- Deberá ser posible encadenar múltiples transformaciones, definiendo el orden de ejecución, y utilizar los resultados como inputs dinámicos dentro del playbook.
- Los playbook deberán ser capaces de manejar flujos de errores, de tal forma que si una tarea falla, la siguiente acción del playbook sea trasladado a un flujo que pueda gestionar este error.
- Permitir el uso de tareas estándar para ejecutar acciones automáticas o semiautomáticas, tales como enriquecimiento de indicadores, interacción con integraciones externas, ejecución de scripts, apertura de tickets, entre otros.
- Soportar tareas condicionales, que permitan evaluar resultados, atributos o respuestas previas y dirigir la ejecución del playbook mediante lógica de decisión y ramificación del flujo.
- Deberá soportar "sondeo" (espera activa) en playbooks para pausar la ejecución hasta que una acción remota en un producto externo finalice (por ejemplo, detonación/análisis de archivos o URLs, o consultas de larga duración), consultando periódicamente el estado y reanudando automáticamente cuando el proceso termine.
- Deberá permitir tareas de recolección de datos, orientadas a capturar input de usuarios o analistas, almacenando dicha información como contexto del incidente para su uso en pasos posteriores.
- Las tareas de captura de input del usuario deben permitir el envío de notificaciones (correo electrónico y/u otros canales) y soportar distintos tipos de respuesta (selección de alternativas, texto libre, numérico, fecha y carga de adjuntos), de modo que el playbook pueda continuar su ejecución automáticamente una vez recibido el input.
- Debe permitir que el formulario donde el usuario deba acceder para colocar el input, soporte mecanismos de acceso con y sin autenticación.
- Deberá permitir gestionar temporizadores a tareas específicas del playbook, con el objetivo de controlar el cumplimiento del SLA por etapa (por ejemplo, asignación y remediación)
- La solución deberá incorporar tareas basadas en inteligencia artificial, que permitan procesar prompts en lenguaje natural y generar salidas dinámicas, tales como análisis, resúmenes, reportes o comunicaciones automatizadas.

- La plataforma deberá permitir organizar los playbooks en secciones lógicas, facilitando la gestión, navegación y mantenimiento de flujos complejos.
- Debe tener la capacidad de ejecutar playbooks en modo debug, de tal forma que permita observar la ejecución paso a paso del mismo y resolver cualquier inconveniente de ser necesario
- Debe permitir crear scripts personalizados, para lo cual la solución deberá estar en la capacidad de consumir las API de las plataformas externas a integrar.
- El módulo SOAR deberá tener un IDE de desarrollo embebido para poder desarrollar los scripts personalizados. Este IDE deberá soportar al menos el lenguaje Python, JavaScript y Powershell.
- Los playbooks deben poder ser ejecutados como tareas programadas, es decir, sin necesidad de que exista una alerta o incidente de seguridad un playbook puede ejecutarse de manera periódica (permitiendo especificar la periodicidad) para automatizar alguna tarea.
- La solución deberá permitir crear reglas de automatización, donde se detalle bajo qué condiciones de una alerta de seguridad se gatillará la ejecución automática de un playbook.
- La solución debe sugerir automáticamente que playbook puede ser asociado a una alerta de seguridad, ante aquellas alertas que no tengan un playbook de respuesta asignado.
- La respuesta deberá tener cobertura a nivel de los endpoints para proteger contra amenazas altamente avanzadas, esto incluye:
  - Capacidad de poder colocar los malware en una carpeta de cuarentena
  - Capacidad de extraer el malware o archivo sospechoso del endpoint hacia la consola, para poder ser analizado por el investigador
  - Debe ser posible aislar el endpoint de la red para que no tenga comunicación con ningún dispositivo de la red interna o externa.
  - Deberá ser posible realizar una conexión remota a cada endpoint que forme parte de una investigación para ejecutar las siguientes acciones:
    - Listar procesos y archivos
    - Ejecutar instrucciones por línea de comandos (CMD y Powershell para el caso de Windows; Bash para el caso de Linux y MacOS).
    - Ejecutar scripts basados en Python
  - Capacidad de ejecutar scripts remotamente a múltiples endpoints de manera concurrentes.
  - Capacidad de tareas remotas a múltiples endpoints, como mínimo cerrar procesos, eliminar archivos, eliminar y/o modificar claves de registro.
- La solución deberá integrar capacidades avanzadas de inteligencia artificial para optimizar las operaciones de seguridad, permitiendo investigación asistida y ejecución de acciones automatizadas sobre la infraestructura.
- La plataforma deberá ofrecer una interfaz unificada para interactuar con agentes de IA predefinidos y personalizados, capaces de planificar y ejecutar flujos de trabajo de múltiples pasos.
- Debe permitir la creación de agentes de IA personalizados para investigación y respuesta, capaz de crear y ejecutar planes compuestos por acciones (playbooks, scripts, comandos y prompts).
- Debe proveer un módulo de administración para gestionar agentes y acciones, tales como, habilitar/deshabilitar, asignar acciones, crear acciones personalizadas.
- Deberá incorporar controles de seguridad en los prompts, validando automáticamente permisos y contexto antes de ejecutar cualquier acción, bloqueando solicitudes ambiguas, potencialmente maliciosas.
- Debe permitir marcar acciones sensibles que requieran aprobación explícita antes de ejecutarse, y ofrecer búsqueda/filtrado y trazabilidad para la gestión operativa de los agentes.
- Deberá garantizar la privacidad de las conversaciones del asistente, manteniendo al mismo tiempo trazabilidad completa mediante registros de auditoría que documenten de forma detallada quién inició una acción, qué acción se ejecutó y cuándo.
- Deberá permitir interacción conversacional con IA, utilizando el contexto del caso para investigar amenazas y ejecutar acciones como comandos, playbooks o scripts.
- Deberá permitir el uso de lenguaje natural para crear, ajustar y desplegar scripts de automatización, facilitando la interacción del analista.

- Deberá soportar integraciones con herramientas y fuentes externas, mediante protocolos estandarizados, para acceder a datos y ejecutar acciones en plataformas terceras.
- Deberá permitir la inclusión de tareas de inteligencia artificial generativa dentro de playbooks, como pasos independientes para análisis o generación de contenido.
- Deberá ser capaz de generar automáticamente resúmenes técnicos de incidentes, consolidando telemetría y datos de impacto para acelerar el triage y la comunicación.
- El asistente deberá organizar y gestionar el historial de conversaciones por periodos de tiempo, permitiendo revisar, retomar, renombrar o eliminar investigaciones previas de forma sencilla.
- Deberá garantizar la protección y cifrado de datos sensibles, con separación estricta entre clientes y control de acceso basado en identidades.
- Deberá asegurar que los datos procesados por la IA se utilicen exclusivamente para la respuesta inmediata, sin ser almacenados para entrenamiento ni compartidos con terceros.
- Debe integrarse con sistemas externos mediante MCP, permitiendo que los agentes consulten datos y ejecuten acciones en herramientas de terceros (ejm. Jira, GitHub).
- Debe permitir configurar múltiples instancias por integración, probar conectividad y mantener el estado habilitado/deshabilitado desde la consola.

52. ADC (application Delivery Controller) (02 Unidades)

Arquitectura y Capacidad de Hardware

- Procesamiento: Debe contar con una arquitectura multi-core optimizada, incluyendo un procesador de al menos 12 núcleos.
- Almacenamiento y Memoria: Debe incluir una unidad de estado sólido (SSD) de al menos 0.5 TB para logs y sistema operativo.
- Fuentes de Poder: Para garantizar la alta disponibilidad, cada unidad debe contar con doble fuente de poder redundante.

Rendimiento y Licenciamiento

- La solución debe incluir un pool de licencia flexible de throughput de 1 Gbps como mínimo.
- La solución ofertada debe incluir licenciamiento para un pool de 8 instancias de ADC (application delivery controllers).
- La solución debe incluir 2 equipos físicos operando en alta disponiblidad.
- La solución debe permitir remover la capacidad instalada de una instancia específica para que esta sea liberada y pueda ser reasignada a otras instancias de balanceo, para cualquiera de los factores de formas.
- La solución debe incluir una consola gráfica que permita administrar el pool de licencias, teniendo como mínimo las siguientes funcionalidades:
  - Aprovisionamiento de las licencias de throughput y funcionalidades.
  - Modificar las licencias asignadas a una instancia específica.
  - Desinstalación de las licencias de las instancias.
  - Visualizar la asignación del pool de licencias adquirido.
- Capacidad de Sesiones: Debe soportar un mínimo de 46 millones de conexiones concurrentes en Capa 4.
- Transacciones por Segundo L7: Capacidad para procesar al menos 1.8 millones de peticiones por segundo (RPS).
- Transacciones por Segundo L4: Capacidad para procesar al menos 1 millon de conexiones por segundo (CPS).
- La solución debe estar configurada en alta disponibilidad y debe soportar Stateful Failover.
- La solución debe permitir sincronizar la configuración entre equipos de forma manual o automática.
- La solución debe soportar balanceo transparente a través de filtros, en donde se realice inspección del tráfico, clasificación y envío a uno o más grupos de balanceo, sin alterar el paquete original y sin necesidad de exponer una IP virtual.
- La solución debe incluir una métrica por proximidad que correlacione la latencia y el número de saltos hacia un origen determinado, para el balanceo de salida y desde un origen determinado para el balanceo entrante.

Virtualización y Escalabilidad

- Instancias Virtuales (vADC): La solución debe soportar la partición del hardware en instancias lógicas independientes. Se debe incluir licenciamiento para un mínimo de 8 instancias vADC activas desde el primer día.
- Aislamiento: Cada vADC debe tener recursos de CPU y memoria garantizados para asegurar que el tráfico de una aplicación no afecte a las demás.

Conectividad Física y Escalabilidad

- El appliance debe contar con una densidad de puertos que garantice la integración en arquitecturas de alta velocidad y baja latencia, cumpliendo con los siguientes requisitos mínimos:
- Puertos de Cobre: Al menos ocho (08) puertos 10/100/1000 Mbps Base-T (RJ45) para gestión y servicios auxiliares.
- Puertos de Fibra (Acceso/Agregación): Al menos ocho (08) puertos con soporte nativo para 10 GbE (SFP+).
- Puertos de Alta Velocidad (Core): Al menos cuatro (04) puertos con soporte nativo para 25 GbE (SFP28) para interconexión de alta velocidad.
- Consola: Puerto dedicado para administración local (RJ45/USB).

Gestión Centralizada y Visibilidad

- Analíticas: Debe proporcionar visibilidad en tiempo real y reportes históricos sobre el rendimiento de las aplicaciones y el estado de salud de los servicios.
- La solución debe proveer visibilidad SSL/TLS para ambos, el tráfico hacia el Datacenter y el tráfico saliente a Internet, permitiendo a la solución ser la responsable de la orquestación y distribución dinámica de tráfico entre dispositivos de seguridad.

53. Anti – DDoS (02 Unidades)

Arquitectura y Componentes de la Solución

- Provisión de Hardware: La solución debe contemplar la entrega de 02 appliances físicos de alto rendimiento en configuración redundante.
- La solución de mitigación de ataques DDoS debe tener la siguiente configuración de interfaces para su integración a la red.
  - Como mínimo, 4 Interfaces de Cobre GE de entrada.
  - Como mínimo, 4 Interfaces de Cobre GE de salida.
- La solución de mitigación de ataques DDoS se debe integrar a la red de forma transparente en capa 2.
- Mecanismo de Bypass: Los puertos de cobre deben contar con un mecanismo de derivación (bypass) físico incorporado para garantizar la continuidad del tráfico en caso de fallo del equipo.
- La solución de mitigación de ataques DDoS debe soportar un número ilimitado de sesiones concurrentes de ataque.
- La solución de mitigación de ataques DDoS debe incluir doble fuente de poder hot swappable

Rendimiento y Performance

- La solución de mitigación de ataques DDoS debe estar licenciada para un throughput de tráfico legítimo de al menos 2 Gbps por equipo.
- La solución de mitigación de ataques DDoS debe soportar crecimiento de throughput por licenciamiento sobre el mismo hardware de hasta 5 Gbps por equipo.
- La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 10 Gbps por equipo
- Tasa de Paquetes: Debe soportar una tasa de procesamiento de hasta 12 Millones de Paquetes por Segundo (Mpps) para inundaciones de red.
- Latencia Máxima: La inspección del tráfico debe mantener una latencia ultra-baja, no superior a los 60 microsegundos.

Capacidades de Detección y Mitigación

- La solución debe tener la capacidad de crear y aplicar firmas para ataques DDoS de Dia Cero (Zero-Day) en menos de 20 segundos.
- Análisis de Comportamiento: La solución debe contar con protección de ataques DDoS DNS basada en análisis de comportamiento para detectar anomalías de tráfico y prevenir ataques de día cero incluyendo al menos los siguientes tipos de inundaciones de Queries DNS: A, AAAA, HTTPS, MX, PTR, TXT, SOA, NAPTR, SRV, Other.
- Protección Multicapa (L3-L7): Mitigación contra ataques de inundación TCP (SYN, SYN-ACK, RST, FIN-ACK.
- Anti-Spoofing: La solución debe identificar y filtrar los queries falsificados (spoofed) y prevenir contra ataques de Inundación DNS, Ataques de amplificación, fuerza bruta y DNS water torture.
- La protección contra ataques HTTPS debe soportar las siguientes versiones del protocolo SSL usando hardware dedicado interno sin requerir soluciones externas: TLS1.0, TLS 1.1, TLS 1.2 y TLS 1.3
- La solución debe ser capaz de detectar y mitigar ataques de randomización de encabezados y métodos HTTPS, a partir de los fingerprinting de TLS utilizados por la aplicación.
- La protección contra ataques HTTPS flood debe contar con al menos dos métodos de autenticación: 302 Redirect, Java Script.

Licenciamiento y Servicios Críticos

- Licencia de Capacidad: Deberá habilitar un rendimiento total de 10 Gbps del hardware sin restricciones lógicas.
- Servicio de Reputación (IP Reputation): Suscripción activa por 12 meses.

Gestión, Reportes y Monitoreo

- La solución debe incluir un elemento de gestión y control centralizado el cual soporte la administración y monitoreo de todos los mitigadores que hacen parte de la propuesta.
- Analítica Forense: La solución debe proporcionar una visualización completa de los detalles del ataque para los eventos de detección que lo ameriten, incluyendo ID del ataque, objeto protegido, hora de inicio, duración, nombre del ataque, firmas asociadas y atributos contextuales como IPs de origen/destino, puertos y protocolos.
- Métricas en Tiempo Real: La análitica de red debe incluir como mínimo la siguiente información para cada activo protegido.
  - Gráficos de Tráfico.
  - TOP IP Origen.
  - TOP IP Destino.
  - TOP Aplicaciones.
  - TOP Protocolos.
  - TOP Países
  - Tendencias de la última semana.

54. MFA - Administración de Identidad y Acceso (01 solución)

- La solución propuesta deberá ofrecerse como servicio (SaaS) y al menos tener las certificaciones SOC 2 Type 2, SOC 3, ISO27001, ISO 27017, ISO 27018 entre otras.
- La solución deberá proporcionar capacidades de autenticación multifactor (MFA) como parte de una plataforma de administración de identidad y acceso (IAM), permitiendo el control seguro de acceso a aplicaciones y recursos.
- La solución debe estar licenciada para 300 usuarios y deberá proveer 10 token mobiles, que se deberán integrar a la solución de gestión de identidad.
- La solución se debe basar en algoritmos de aprendizaje de máquina (machine learning) no supervisados. Es decir, los modelos estadísticos con los casos de uso ya deben estar listos y calibrados.
- La solución debe medir el riesgo de la autenticación verificando el comportamiento histórico de la identidad a través del conjunto de los siguientes atributos: - GeoVelocidad;

Geolocalizacion; Dia de la semana; Horario de acceso; Sistema operativo; Fallas de login consecutivas

- La solución debe permitirles a los administradores personalizar los rangos de puntuación (0 a 100) para las categorías:
  - Sin riesgo
  - Riesgo bajo
  - Riesgo medio
  - Riesgo alto
- El riesgo calculado durante la autenticación por el motor de análisis del comportamiento de los usuarios debe compartirse con los módulos (SSO y MFA) que realizan el login, para los casos de uso citados en este documento, y utilizarlo como contexto para:
  - Solicitar autenticación de múltiples factores de forma dinámica
  - Permitir el login sin el uso de múltiples factores
  - Negar la autenticación
- Debe brindarles a los administradores de la solución la capacidad de explorar los datos históricos a través de dashboards, filtros y gráficos configurables, verificar las alertas y los factores que los influenciaron y explorar los eventos capturados y sus atributos.
- Debe proveer gráficos de línea de tiempo, donuts, mapas con la geolocalización de los eventos, gráficos de barras, tablas analíticas y mapas de relación. Sus dimensiones y categorías deben ser personalizables.
- Debe brindarles a los administradores de la solución la capacidad de explorar los datos históricos a través de dashboards, filtros y gráficos configurables, verificar las alertas y los factores que los influenciaron y explorar los eventos capturados y sus atributos.
- Debe proveer gráficos de línea de tiempo, donuts, mapas con la geolocalización de los eventos, gráficos de barras, tablas analíticas y mapas de relación. Sus dimensiones y categorías deben ser personalizables.
- Debe ser capaz de exportar los datos de alertas, riesgos calculados y eventos a PDF y CSV y, además, grabar las visualizaciones en la solución para consultas posteriores.
- Debe estar integrada a fuentes de inteligencia cibernética de terceros reconocidas en el mercado como, por ejemplo, Palo Alto Cloud.
- Debe poseer interfaz para el envío de alertas de forma automatizada. Debe soportar, como mínimo:
  - Correo electrónico con contenido de alerta
  - Webhooks como, por ejemplo, envío de mensaje a un canal de Microsoft Teams o Slack
- Poseer dashboards configurados previamente con informaciones y gráficos con las siguientes características:
  - Utilización de motor de análisis del comportamiento de los usuarios
  - Comportamiento de los usuarios en la utilización de las aplicaciones
  - Visión sobre la seguridad de las aplicaciones
  - Mapa con la geolocalización de las autenticaciones
  - Visión sobre el comportamiento de los Endpoints (móviles y computadoras)
  - Visión sobre el comportamiento de las identidades
- La solución debe permitir configurar dashboards personalizados.
- Debe permitir compartir los dashboards con otros usuarios.
- La solución debe proveer un catálogo de aplicaciones web con modelos de configuración de SSO que contenga al menos 1000 ítems, incluidas las aplicaciones más conocidas del mercado, para facilitar la configuración de estas integraciones.
- La solución debe permitir configurar el SSO para aplicaciones web, como mínimo, a través de los siguientes protocolos y métodos:
  - OpenID connect
  - SAML 2.0
  - WS-Federation
  - Oauth 2.0 modo client
  - Oauth 2.0 modo server
  - NTLM
  - HTTP Basic
  - Extensión en el navegador para capturar aplicaciones web que utilicen formulario con usuario y contraseña, y completar automáticamente el login y la

contraseña. Está información se debe guardar de forma segura en la solución, para completar automáticamente futuros login en estas aplicaciones.

- La solución debe ofrecer un componente/software para intermediar el SSO en aplicaciones web que se encuentren en el centro de procesamiento de datos de la entidad, sin necesidad de exponer a estas aplicaciones al uso de internet o de VPN.
- La solución debe proveer una extensión de navegador avanzada solamente para los administradores de la solución para realizar el mapeo de los campos de los formularios (en general, login y contraseña) y después incluirlos como una aplicación web para SSO en el catálogo general. Este recurso ayudará en el SSO de aplicaciones que no soportan protocolos más modernos de federación, como SAML Oauth, y con diferentes contraseñas.
- Soporte para SSO mediante IWA (Integrated Windows Authentication), que reutiliza el login de red para autenticación en las aplicaciones web sin necesidad de ingresar con usuario y contraseña nuevamente.
- Ofrecer soporte para personalizar las respuestas SAML (SAML Response) como, por ejemplo, mapear atributos de los directorios para atributos SAML, tener la capacidad de incluir lógicas complejas para manipular las respuestas SAML y, en lo posible, visualizar la respuesta SAML configurada antes de su implantación.
- La solución debe proveer un portal web para el usuario final con las siguientes características:
    - Después de efectuar el login, debe presentar las aplicaciones web disponibles para realizar el SSO a través de un conjunto de íconos, donde cada uno represente una aplicación en la que el usuario tiene derecho a efectuar el SSO.
    - Que permita realizar cambios en los atributos de identidad, como teléfono celular, correo electrónico y foto.
    - Que verifique las actividades de su identidad a través de dashboard con la siguiente información:
        - Geolocalización de sus login
        - Verificación de la geolocalización actual de sus dispositivos registrados
        - Login totales.
        - Fallas de login totales.
        - Utilización de las aplicaciones.
        - Historial de eventos importantes, como adición de nueva aplicación en su portal de SSO o fallas de login, entre otros
- La solución debe poseer un servicio de directorio para almacenar identidades en la nube de la solución, sin depender de la sincronización con otros servicios de directorio locales (on-premises) o en la nube de terceros.
- El servicio de directorio de la solución debe ser capaz de realizar la extensión de su esquema a través de la configuración de atributos personalizados, para responder a requisitos de negocios complejos.
- El servicio de directorio de la solución debe ser autoescalable, para soportar millones de identidades y miles de autenticaciones simultaneas.
- Debe ser capaz de forzar la complejidad de las contraseñas, como mínimo, a través de los siguientes requisitos:
    - Exigir tamaño mínimo
    - Exigir tamaño máximo
    - Exigir cantidad mínima de números
    - Exigir letras mayúsculas y minúsculas
    - Exigir caracteres especiales (símbolos)
    - Limitar caracteres consecutivos
    - Forzar la expiración de contraseñas dependiendo de su antigüedad
    - Guardar el historial de contraseñas para evitar su reutilización
- Notificar sobre la expiración de la contraseña por correo electrónico.
- Registrar fallas de login repetidas para bloqueo de usuario.
- Al mismo tiempo, la solución debe soportar la integración con servicios de directorio locales (on-premises) y en la nube. Como mínimo, los siguientes:
    - Microsoft Active Directory
    - Microsoft Azure AD
    - Google Directory
    - Directorios LDAP

- Las integraciones realizadas con directorios de terceros no deben realizar sincronismo con estas bases, es decir, cargar todo el directorio configurado a la nube. La solución debe actuar como un intermediario ("broker") entre los servicios de directorio de terceros y la solución.
- La solución debe poseer integración con proveedores de identidades sociales, para delegar la autenticación a tales proveedores y responder ante posibles requisitos de negocio. Debe soportar, como mínimo, los siguientes proveedores:
  - Facebook
  - Google
  - LinkedIn
  - Microsoft
- La solución debe ser capaz de configurar IDPs (Identity Providers) de socios de negocio de la entidad, para permitir el acceso de las identidades federadas a nuestras aplicaciones de negocio sin la necesidad de crear una nueva identidad en nuestra infraestructura. Esta federación se debe realizar a través del protocolo SAML.
- El portal SSO (inicio de sesión único) debe permitir a los usuarios administrar usuarios y contraseñas para aplicaciones que no están integradas con SSO pero que les gustaría almacenar estos usuarios y contraseñas para otras aplicaciones web de forma segura, agregando una experiencia de SSO después de guardar estas credenciales.
- La solución debe permitir a los usuarios compartir estas credenciales y el flujo de SSO con otros usuarios sin depender del administrador de la solución. Cuando se comparte, debe elegir:
  - Compartir sin necesidad de ver credenciales
  - Compartir con visualización de las credenciales.
  - Compartir siendo posible editar las credenciales.
- También debería ser posible que el administrador de la solución defina las credenciales y los flujos de SSO para las aplicaciones web que están disponibles para los usuarios finales en función de sus perfiles de acceso en la solución.
- Estas credenciales (nombre de usuario y contraseñas) se pueden almacenar de forma segura en la nube de la solución o en la solución de bóveda de contraseñas local del mismo proveedor.
- La solución debe tener la capacidad de crear perfiles dinámicos basados en atributos de la identidad, por ejemplo, su departamento. Estos perfiles se pueden utilizar para autorizar o solicitar diferentes métodos de MFA al acceder a una aplicación web integrada en la plataforma.
- Debería ofrecer widgets personalizados para MFA y pantalla de inicio de sesión para la integración con las aplicaciones web de la empresa. Generar un código HTML para ser incrustado en la página de inicio de sesión de estas aplicaciones web.
- La solución debe ser capaz de cumplir mínimamente los siguientes casos de uso para solicitar uno y más factores de autenticación:
  - Aplicaciones web integradas en la autenticación simplificada - funciones SSO.
  - En las pantallas de inicio de sesión y desbloqueo de los sistemas operativos Windows
  - Autenticación multifactor para soluciones VPN a través de RADIUS o SAML.
  - Cualquier dispositivo o sistema operativo que admita RADIUS.
  - Complemento para ADFS (IDP, proveedor de identidad), servicios de federación de Active Directory.
  - A petición mediante el protocolo Oauth y las API de REST.
  - Para realizar el restablecimiento de contraseña de servicio automático o desbloqueo de usuario.
- La solución debe ser capaz de ofrecer mínimamente los siguientes métodos para múltiples factores de autenticación: Usuario y contraseña de los directorios admitidos en la solución:
  - A través de la aplicación móvil iOS y Android, que ofrece soporte para:
  - Biometría FaceID.
  - Biometría a través del lector digital.
  - Inserción de smartphone (Notificación para aprobar o rechazar una autenticación).
  - Geolocalización a través de GPS coordenadas e IDatabase.
  - Soporte tokens OATH OTP.

  - Autenticación en la pantalla de inicio de sesión a través de QRcode (Passwordless) sin necesidad de introducir el usuario y la contraseña, con la opción de forzar la biometría en el dispositivo móvil.
- Llamada telefónica para solicitar un PIN previamente configurado.
- Mensaje de texto vía SMS que ofrezca el código para entrada manual y también una URL única, que permita aprobar o rechazar la autenticación sin necesidad de digitar el código manualmente.
- Confirmación de código vía correo electrónico que ofrezca el código para entrada manual y también una URL única, que permita aprobar o rechazar la autenticación sin necesidad de digitar el código manualmente.
- Clientes de tipo OATH OTP.
- Autenticadores que soporten FIDO2/U2F. Como mínimo, debe soportar:
  - MacOS TouchID
  - Yubikey
  - Google Titan Key
- Preguntas y respuestas configuradas previamente.
- Permitir que los usuarios realicen el autoservicio de restablecimiento de contraseña y desbloqueo de usuario, utilizando los métodos citados en el ítem 8.2 y sus subítems, para la verificación positiva a través del portal web de la solución.
- Para cada caso de uso o conjunto de casos de uso citados en el ítem 8.2 y sus subítems, la solución debe ser capaz de identificar los atributos de contexto de cada autenticación, para proporcionar los mejores métodos definidos para la autenticación. Como mínimo, debe soportar:
  - Dirección IP.
  - Día de la semana.
  - Fechas específicas.
  - Intervalos de tiempo entre dos fechas.
  - Intervalos de tiempo entre horarios (ejemplo: horario comercial).
  - Tipo de sistema operativo.
  - Tipo de navegador (browser).
  - Perfiles configurados en la solución.
  - País desde el que se accede.
  - Si se trata de un dispositivo gestionado.
  - Autenticación vía certificado.
  - Nivel de riesgo de la autenticación medido por un motor de análisis de comportamiento de los usuarios (UBA, User Behavior Analytics)
- La solución debe ser capaz de detectar casos de uso o perfiles de autenticación ya validados por el usuario y no solicitar nuevamente la autenticación durante un período de tiempo configurado por el administrador de la solución, para evitar repetidas validaciones en un corto período de tiempo.
- Los factores de autenticación que fueron proporcionados durante el acceso deben basarse en las reglas especificadas y separarse de la siguiente manera:
  - Conjunto de aplicaciones.
  - Una única aplicación.
  - Reglas para realizar el autoservicio de restablecimiento de contraseña o desbloqueo de usuario
  - Portal del Administrador.
  - Portal del Usuario.
- La solución debe proveer un portal web para el usuario final con las siguientes características:
  - Permitir que el usuario realice el registro de sus propios factores de autenticación, como preguntas y respuestas, FIDO2 tokens, OATH OTP, definir PIN para llamada telefónica, TouchID, FaceID, entre otros.
  - Permitir que el usuario redireccione la autenticación de múltiples factores a otros usuarios (si está permitido), por ejemplo, para su gerente.
  - Permitir que los usuarios gestionen sus dispositivos registrados, como mínimo:
  - Smartphones Android y IOS.
  - Sistemas operativos Windows y MacOS.
  - Para cada dispositivo registrado, los usuarios deberán tener las siguientes capacidades de gestión:

  - Deshabilitar el SSO remotamente.
  - Habilitar el SSO remotamente.
  - Registrar nuevos dispositivos móviles.
- La solución debe proveer una aplicación móvil para Android y IOS con las siguientes características:
  - Después de efectuar el login, debe presentar las aplicaciones web disponibles para realizar el SSO a través de un conjunto de íconos, donde cada uno represente una aplicación en la que el usuario tenga derecho a efectuar el SSO ya integrado con los navegadores instalados en los dispositivos móviles.
  - Que permita el login a través del escaneo de código QR en el portal web, para permitir SSO sin identificación de usuario y contraseña.
  - Que permita configurar OATH OTP adicionales provenientes de otras soluciones.
  - Que permita configurar OATH OTP para autenticación de múltiples factores en los sistemas operativos Windows y MacOS (pantalla de login y bloqueo) sin conexión a Internet.
  - Que verifique los dispositivos registrados (dispositivos móviles y sistemas operativos).
  - Que cuente con integración nativa con FaceID, TouchID, lector biométrico de los dispositivos móviles e impulse su uso para la autenticación biométrica durante el login en las aplicaciones.
  - Que reporte coordenadas GPS a los sistemas que utilizan geolocalización.
  - Que detecte ROOT en dispositivos Android y Jailbreak en dispositivos IOS, para detectar actividades maliciosas y, como consecuencia, deshabilitar el uso de la aplicación.
- La aplicación móvil (IOS y Android) debe soportar la autenticación de tipo push, en que el usuario puede elegir si aceptar o rechazar el desafío. Esta notificación debe contener, como mínimo, la siguiente información:
  - Fecha y hora.
  - Ciudad/geolocalización de acceso.
  - Aplicación a la que se accede.
- Durante la creación de un perfil de autenticación con sus métodos multifactor, la solución debe indicar en qué nivel de confianza de autenticación el administrador de la solución configura dicho perfil de autenticación, según la publicación especial de NIST SP 800-63-3, sobre el guía de identidad digital que clasifica una autenticación en 3 niveles, AAL1, AAL2, AAL3 (Authenticator Assurance Level). Siendo 1 el menos seguro y 3 el más seguro posible con los métodos actuales de autenticación multifactor.

55. PAM - Administración de Acceso Privilegiado (01 solución)

- La solución propuesta deberá ofrecerse como servicio (SaaS) y al menos tener las certificaciones SOC 2 Type 2, SOC 3, ISO27001, ISO 27017, ISO 27018 entre otras.
- La solución debe estar licenciada para 50 usuarios privilegiados.
- La solución propuesta deberá tener un repositorio seguro o boveda digital, el cual debe estar patentado por el fabricante, esto quiere decir que no deberá tener software de bases de datos comerciales para resguardar la informacion.
- La solución ofertada deberá contar con una boveda (vault) segregado, con cifrado y hardening propietario certificado (FIPS/NIST), no dependiente de OS estándar.
- La solución propuesta debe tener una boveda patentada que debe estar certificada por el Common Criteria y tener un nivel de certificacion minima de Evaluation Assurance Level (EAL) 2+.
- La solución ofertada no debe requerir establecer enlaces VPNs IPSec o Direct Connect con la nube de la solución SaaS.
- La solución propuesta no debe de tener limites en cuanto a conexiones concurrentes por usuarios, estas deben ser ilimitadas.
- La solución propuesta, no debe tener limite en cuanto a la cantidad de dispositivos, integraciones o cuentas a proteger.
- La comunicación a internet necesaria por la solución debe ser solo de salida (outbound)
- La solución propuesta deberá tener la capacidad de cifrar, en reposo y en tránsito todos los datos que utilice. Incluyendo contraseñas, reportes almacenados, grabaciones y

registros de usuarios. Lo anterior utilizando algoritmos que cumplan con los estándares en FIPS 140-2, como AES-256 y RSA-2048.

- La solución debe ayudar a la organización a administrar y monitorear los accessos privilegiados y el uso de las credenciales privilegiadas, utilizadas por identidades humanas y no humanas, asociadas a infraestructura en ambientes híbridos; incluyendo servidores, bases de datos, dispositivos de comunicaciones, soluciones de seguridad y apliaciones en un centro de datos, así como en ambientes de nube pública
- Deberá tener la capacidad de ejecutar operaciones de forma masiva (bulk operations) sobre las cuentas privilegiadas, como altas y modificaciones.
- La solución de Seguridad de Cuentas Privilegiadas deberá tener la capacidad de administrar la plataforma de forma centralizada a través de un portal web y capacidad para restringir accesos a través de zonas de red confiables.
- El SLA del servicio debe ser mínimo de 99.9%
- La solución ofertada al ser SaaS, deberá contar con mecanismos de alta disponibilida entre regiones, sin incurrir en costos adicionales.
- La solución ofertada al ser SaaS, deberá de estar disponible minimo en 8 zonas de disponibilidad.
- La solución debe tener la capacidad de soportar el uso de aplicaciones y servicios que se ejecuten en un sistema hibrido, esto quiere decir en entornos nube y en la premisa.
- La solución propuesta deberá tener la capacidad de proporcionar un esquema Bring-your-own key (BYOK), de tal manera que le permita al cliente retirar la llave que descifra la informacion de la boveda cuando lo vea conveniente.
- La solución propuesta deberá tener la capacidad de permitir al cliente definir su propia llave de cifrado y reemplazar la llave de cifrado predeterminada de la plataforma cuando crea conveniente. Esto le permite a la solución ofertada acceder a su llave de cifrado y que la solución la utilice para cifrar sus datos.
- La solución deberá tener la capacidad de descubrir cuentas privilegiadas humanas y no-humanas, sin la necesidad de agentes.
- La solución deberá tener la capacidad de descubrir cuentas de servicio que tengan dependencias con aplicaciones o servicios ejecutados en la organizacion (ej: tareas programadas, archivos de sistema, servicios de windows, entre otros).
- La solución deberá tener la capacidad de descubrir usuarios y llaves SSH sobre sistemas Unix y Linux.
- La solución deberá tener la capacidad de descubrir usuarios o cuentas privilegiadas en Windows y MACoS
- La solución deberá tener la capacidad de descubrir usuarios o cuentas privilegiadas en bases de datos, minimo MS SQL Server, Oracle y PostgresSQL.
- La solución ofertada deberá tener la capacidad de descubrir credenciales en ambientes de nube publica, obteniendo el contexto no solo de cuentas sino tambien de roles y grupos que puedan tener privilegios.
- La solución ofertada deberá proporcionar capacidades de escaneos de una sola vez o de manera recurrente para el proceso de descubrimiento.
- La solución ofertada deberá tener la capacidad de programar los escaneos.
- La solución ofertada deberá tener la capacidad de crear politicas para que las cuentas que se descubran sean protegidas en un esquema automático.
- La solución ofertada debe permitir importación y exportación de conjuntos de reglas de descubrimiento y proteccion permitiendo a los administradores reutilizar las reglas en diferentes entornos de forma eficiente.
- La solución ofertada deberá tener componentes de IA que utilicen las capacidades basadas en la experiencia operativa y los conocimientos que el fabricante ha acumulado durante muchos años en la gestión de sistemas de seguridad de identidad, sin costo adicional.
- La solución ofertada deberá tener un asistente conversacional basado en IA que le permita interactuar con los servicios de la solución a través del lenguaje natural para generar consultas, obtener información importante sobre el sistema, ejecutar comandos, configuraciones y mantener fácilmente su sistema, sin costo adicional.
- La solución ofertada deberá tener componentes de IA que trabajen de forma integrada en las funciones claves para proteger la identidad y el acceso de los usuarios. Esto incluye la detección de cuentas y recomendaciones para la baja de cuentas. Estas

funciones le ayudan a encontrar rápidamente cuentas importantes o a eliminar las que ya no necesita, sin costo adicional.

- La solución propuesta deberá tener mecanismos de detección y alerta cuando se detecta una desviación en el patrón de comportamiento de un usuario humano al recuperar/obtener un secreto de la boveda digital o de la plataforma. Esta detección puede indicar un abuso de la plataforma de identidades y la vulnerabilidad o brecha de la identidad del usuario.
- La solución ofertada deberá incorporar mecanismos de Inteligencia Artificial (IA) y/o Machine Learning que permitan procesar y analizar las sesiones privilegiadas de los usuarios. Dichos mecanismos deberán:
    - Generar un veredicto automático sobre la sesión (ej. categorización como normal, riesgosa o anómala).
    - Detectar comportamientos atípicos o desviaciones respecto a patrones de uso establecidos.
    - Proveer un informe resumido y auditable del veredicto, con trazabilidad y evidencia que sustente la clasificación realizada.
    - Permitir la integración con sistemas de monitoreo y alertamiento para la gestión de incidentes de seguridad.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de los siguientes Sistemas Operativos: Windows, Unix, Linux, IBM iSeries, Z/OS, HP Tandem, MAC OS, ESX/ESXi, XenServers, Linux RedHat, etc. Detallar todos los Sistemas Operativos que son soportados por la solución.
- La solución propuesta debe permitir que los administradores de la solución no tengan acceso a las contraseñas almacenadas si así se define por el negocio.
- La solución propuesta deberá tener la capacidad de permitir que ciertos administradores no puedan visualizar las contraseñas que son controladas por otros departamentos de la compañía, como por ejemplo que los administradores de Windows Server no puedan visualizar las contraseñas ni accesos a instancias de bases de datos SQL Server. Esto es para garantizar la separación de roles lo más posible para evitar el uso indebido de las cuentas privilegiadas protegidas por la solución.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de las siguientes Bases de datos: Oracle, MSSQL, DB2, Postgresql, mongoDB, Teradata, etc. Detallar todos los motores de base de datos SQL y NOSQL que son soportados por la solución.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas basadas en los siguientes servicios de directorio: Microsoft AD, Azure AD, Google. Detallar todos los servicios de directorio que son soportado por la solución.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de dispositivos de red (Firewalls, Routers, Switches, APs, etc). Detallar un listado completo con todos los diferentes dispositivos de Red que son soportados por la solución.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de Aplicaciones Cloud como Facebook, Google G Suite, Google Gmail, GitHub, Docker, Puppet,Cloudflare, Aqua, IBM Cloud, LinkedIn,instagram, Twitter, Amazon, Azure, VMware, Office 365,Paloalto, RedHat Ansible/OpenShift, salesforce. Detallar para que servicios SAS que son soportados por la solución "out of the box"
- En el caso que la cuenta privilegiada de una plataforma SaaS (ejemplo consola Cloud) posea un doble factor de autenticación en el inicio de sesion, en este escenario la solución debe poder permitir que el usuario agregue el factor necesario a lo menos en cuentas AWS y Azure. Detallar
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de aplicaciones de Nube/DevOps y controlar el acceso de herramientas a consolas de nube que utilicen mecanismos modernos de integracion tales como SAML, OpenID y WS-Federation, entregando una experiencia nativa, sin utilizar el jumpserver.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de redes sociales: Facebook, Instagram, Whatsapp, Linkedin, etc. Sin pasar por el jumpserver y garantizando los mecanismos de control, proteccion y grabacion de sesion.
- La solución propuesta deberá ser capaz de soportar cualquier dispositivo de red mediante conexión SSH.
- La solución propuesta deberá ser capaz de soportar cualquier repositorio de datos mediante conexión ODBC

- La solución propuesta deberá ser capaz de permitir a través de un administrador definir y agregar cuentas privilegiadas.
- La solución propuesta deberá ser capaz de soportar Conecciones de tipo Ad Hoc.
- La solución propuesta deberá permitir busquedas dentro de los videos de auditoria.
- La solución propuesta deberá ser capaz de detectar automáticamente nuevos dispositivos Laptops o PCs Windows, Servicios Windows(Windows Services), Scheduled Tasks, IIS Service Accounts, etc. para su administración en la solución. Detallar como se realiza este proceso.
- Integración con SIEM (Security Información and Event Management). Detallar un listado de las soluciones que se integra "out of the box"
- Integración con HSM (Hardware Security Module). Detallar un listado con las marcas soportadas.
- Integración con soluciones 2FA. Detallar un listado con las marcar que se integran "out of the box".
- Integración con soluciones de análisis de vulnerabilidades.
- La solución debe disponer de un servicio REST API (Application Programming Interface) vía WebServices para administrar y aprovisionamiento de la solución, que permita entre otras cosas automatizar procesos.
- La solución debe tener la capacidad de entregar un acceso remoto seguro (externo a la red corporativa) a los usuarios sin necesidad de instalación de clientes VPN en los dispositivos de usuarios remotos y garantizando un acceso seguro con MFA sin necesidad de modificar los recursos de autenticación corporativos como el AD,
- Debe supervisar las sesiones privilegiadas, grabar, detectar, correlacionar y mitigar comportamientos anormales, en todas las sesiones soportadas por PAM, entre ellos servidores Linux/Unix, Windows, controladores de dominio de Microsoft Active Directory, estaciones de trabajo Windows, diversos activos de red y de Seguridad, así como aplicaciones Cliente servidor/Web y servicios en Nube ya sean IaaS, SaaS o PaaS.
- Debe proveer un motor de UBA, que ademas de supervisar y adaptase segun el comportamiento, debe tambien tener la capacidad de detectar acciones en sesiones privilegiadas, con al menos soporte para SSH, Windows, SQL, Entradas de Teclado y SCP.
- La Solución debe entregar sesiones administrativas a las que se acceda y monitoree en tiempo real, con el uso compartido de pantalla y el control de periféricos, como el teclado y el ratón (asistencia remota), y mediante la grabación de comandos y vídeos de los mismos, en formato estándar de ejecución no propietaria de la solución, permitiendo que los comandos y vídeos generados se puedan indexar para futuras búsquedas, permitiendo el filtro de comandos y acciones realizadas a lo largo de la sesión grabada , lo que le permite buscar acciones específicas en la sesión grabada;
- La solución debe ser capaz de detectar comportamientos que tipifican abusos, comportamientos anormales y fuera de los estándares aprendidos/asignados, aplicando acciones atenuantes automáticas como la re-autenticación, suspensión y terminación de sesiones y rotación de credenciales privilegiadas en caso de actividad sospechosa de alto riesgo, detectando al menos los siguientes casos: 1- Durante horarios irregulares (cuando un usuario recupera una contraseña de cuenta con privilegios en un momento irregular según su perfil de comportamiento); Durante días irregulares (cuando un usuario recupera una contraseña de cuenta con privilegios en un día irregular de acuerdo con su perfil de comportamiento); A través de IP irregular y desconocida (cuando un usuario accede a cuen-tas con privilegios de una dirección IP o subred inusual, de acuerdo con su perfil de comportamiento); (cuando se realiza una conexión a un equipo con una cuenta con privilegios que no se administra en la solución).
- La solución propuesta deberá ser en formato SaaS, pero que incluya a lo menos los componentes de Proxy (Jump Server) y procesos de cambio de contrasena, en ambientes on-prem, cercano a los usuarios y aplicaciones, con el fin de optimizar el trafico, y seguridad junto con interrupciones de microcorte que no afecte las sesiones locales.
- La solución de Seguridad de Cuentas Privilegiadas debe ser una solución basada en software y debe estar disponible como SaaS o en modelo de suscripción para implementación en ambientes de Nube (AWS, Azure y Google Cloud) y/o instalable sobre entorno físico o virtualizado con infraestructura (servidores / software en entorno virtualizado, S.O., capa de balanceo de tráfico / redirección, etc.

- La solución debe ser modular y escalable para adaptarse a crecimientos de utilización o expansión de funcionalidades e incluso esquemas de Alta Disponibilidad de roles y/o componentes. Es decir, debe poder crecer por cada rol de forma independiente según sea requerido, sin incurrir en licenciamiento adicional
- La solución propuesta deberá contar con la capacidad de integrarse con el modulo SIEM de la Plaforma de Operaciones de Ciberseguridad.
- La solución propuesta deberá tener la capacidad de integrarse a directorios terceros de nube de forma nativa (sin la necesidad de utilizar agentes o maquinas intermediarias), tales como Entra-ID, Google Directory, entre otros.
- La solución propuesta deberá tener la capacidad de integrarse con directorios LDAP/AD y LDAPS, asi como con sistemas Radius.
- La solución propuesta deberá tener la capacidad de integrarse a sistemas de Ticketing/HelDesk/Change Management y permitir la validación de tickets antes de establecer la sesión.
- La solución propuesta deberá tener la capacidad de mostrar en un quick view todas las actividades relativas a una cuenta privilegiada, como el release de un password o sesiones de administración utilizando dicha cuenta
- La solución propuesta deberá tener la capacidad de generar todos los reportes de forma periódica, bajo demanda o en forma programada
- La solución propuesta deberá tener la capacidad de generar reportes detallados y programados con la siguiente información:
    - Entitlements Reports
    - Actividad de usuarios
    - Inventario de cuentas privilegiadas
    - Inventario de aplicaciones
    - Reportes de Cumplimiento
- La solución propuesta deberá tener la capacidad de auditar y generar reportes de todos los cambios administrativos realizados en el sistema
- La solución propuesta deberá cumplir con las siguientes normativas:
    - Ley 25.326 de Protección de Datos Personales
    - GDPR
    - ISO27001
    - PCI-DSS
    - NIST 800-53
- La solución propuesta deberá proporcionar la rotación de contraseñas y llaves en entornos complejos (Mainframe, AS/400, dispositivos OT, aplicaciones legacy) con soporte probado y certificado.
- La solución propuesta deberá tener la capacidad de cambiar passwords cada X días, meses, años
- La solución propuesta deberá tener la capacidad de cambiar múltiples passwords en una sola vez para un solo sistema o sistemas agrupados bajo un solo criterio
- La solución propuesta deberá tener la capacidad de cambiar un password o un grupo de passwords:
    - De acuerdo a una política (cada x días u 'on-demand')
    - Cambios manuales efectuados por un usuario
    - Automáticamente, cuando un password no ha sido sincronizado (falla en verificación)
- La solución propuesta deberá tener la capacidad de asignar passwords a un valor random
- La solución propuesta deberá tener la capacidad de cambiar manualmente un password por un administrador en cualquier momento
- La solución propuesta deberá tener la capacidad de cambiar automáticamente el valor de un password después de un tiempo especificado de un "chek out" del password
- La solución propuesta deberá tener la capacidad de cambiar automáticamente el password de una cuenta que acaba de ser definida en el sistema
- La solución propuesta deberá tener la capacidad de verificación automática del valor de un password en el sistema correspondiente
- La solución propuesta deberá tener la capacidad de automáticamente reconciliar passwords que se hayan detectado como "out of sync" o que se hayan perdido, sin utilizar herramientas externas de restauración

- La solución propuesta deberá tener la capacidad de configurar una longitud mínima de contraseña y complejidad para cuentas de súper-usuarios de todos los sistemas
- La solución propuesta deberá tener la capacidad de mantener el historial de contraseñas, ej. Las últimas tres contraseñas o por periodo de tiempo y proveer fácil acceso a ellas a través de la interfaz web del producto
- La solución propuesta deberá tener la capacidad de administrar cuentas de súper-usuario que han sido renombradas de su nombre por default
- La solución ofertada deberá proporcionar mecanismos de acceso privilegiado seguro a aplicaciones web empresariales sin requerir el uso de un jump server tradicional. Dicho acceso deberá:
    - Ofrecer una experiencia nativa de usuario (el usuario ingresa directamente a la aplicación sin interfaces intermedias forzadas).
    - Establecer sesiones seguras mediante protocolos estándar (ej. HTTPS/TLS) con aislamiento de credenciales, de forma que éstas nunca sean expuestas al usuario.
    - Soportar Single Sign-On (SSO) y federación de identidades (SAML, OIDC, Kerberos, etc.) para un acceso simplificado y seguro.
    - Incorporar registro y monitoreo de la sesión en segundo plano para garantizar auditoría y trazabilidad completas.
    - Permitir integración con MFA/biometría como paso adicional de seguridad antes de conceder privilegios.
- La solución propuesta deberá tener la capacidad de soportar conexiones transparentes a un dispositivo target, sin la necesidad de ver o teclear la contraseña como parte de la conexión. Detallar los requerimientos para realizar esta funcionalidad.
- La solución propuesta deberá tener la capacidad de soportar conexión directa a dispositivos UNIX/LINUX de administración (SSH) pudiendo grabar la sesion, con una experiencia de conexion nativa, esto quiere decir utilizando los clientes o herramientas instaladas en la estacion de trabajo y sin la necesidad de acceder al portal de la plataforma de gestion de accesos privilegiados.
- La solución debe permitir establecer sesiones de bases de datos de manera nativa, tales como SQL Server, PostgresSQL, Oracle, MySQL, Snowflake y MongoDB utilizando el cliente nativo correspondiente al que el usuario y/o administrador utiliza en su estacion de trabajo (SQL Server Management Studio, PGAdmin, PL/SQL Developer, entre otros), sin mostrar la contraseña.
- La solución debe permitir establecer sesiones de RDP, SSH y SCP de manera nativa ejecutando el cliente correspondiente instalado (MSTSC, Putty Manager, Moba Xterm, entre otros.) en la estación de trabajo del usuario y/o administrador, sin mostrar la contraseña.
- La solución debe permitir establecer sesiones a ambientes de Kubernetes de manera nativa, ejecutando el cliente correspondiente instalado (Kubectl) en la estación de trabajo del usuario y/o administrador, sin mostrar la contraseña.
- La solución propuesta debe permitir conexiones VPN-less de manera nativa, esto quiere decir que permita conexiones remotas hacia equipos destino sin la necesidad del uso de conexiones IPSec o de agentes VPN instalados.
- La solución propuesta deberá contar con mecanismos de MFA-Caching de tal manera que agilite el acceso privilegiado dentro de las multiples sesiones diarias que puede generar un usuario.
- La solución ofertada debe proporcionar un de acceso basado en el privilegio minimo y con experiencia nativa.
- La solución ofertada deberá soportar diferentes principios de acceso privilegiado de tal manera que pueda robustecer los accesos en ambientes estaticos y dinamicos, asi como disminuir el riesgo e impacto en el acceso otorgado.
- La solución ofertada debe proporcionar un esquema de acceso privilegiado "permanente", en cual se tienen capacidades como almacenamiento de cuentas en boveda digital, rotacion, aislamiento, monitoreo y grabacion de sesion.
- La solución ofertada debe proporcionar un esquema de acceso privilegiado "JIT (Just-In-Time)", en el cual el acceso privilegiado puede ser dado al momento, pero a intervalos limitados de tiempo con procesos de elevacion o aprobacion de acceso.
- La solución ofertada debe proporcionar un acceso privilegiado "Temporal", en el cual se controle el acceso y el privilegio, de esta forma se va a proporcionar el privilegio al

momento de generar la sesion de acceso privilegiado mediante un rol y/o cuenta privilegiada de manera temporal, dentro de un intervalo de tiempo especifico y basado en el minimo privilegio.
- La plataforma ofertada deberá tener la granuralidad para definir politicas de acceso basados en atributos o características propias de la nube, tales como VPC, Subnets, Segmentos y tags.
- La solución propuesta deberá tener la capacidad de grabar sesiones privilegiadas en: Windows, Virtual Servers, Linux, equipos de comunicaciones, Bases de Datos, Aplicaciones Web. Detallar cuales son los requerimientos para realizar esta capacidad.
- La solución propuesta deberá tener la capacidad de hacer búsquedas de comandos privilegiados dentro de las grabaciones de video. Detallar los requerimientos para realizar esta operacion.
- La solución propuesta deberá tener la capacidad de grabar las sesiones privilegiadas sin necesidad de un agente instalado en los targets o en los origenes del sistema operativo desde donde se genera la sesion.
- La solución propuesta deberá almacenar los videos de grabacion de manera cifrada, utilizando algoritmos de cifrado robustos, tales como aes-256.
- La solución propuesta deberá contar con la funcionalidad de terminar la sesion cuando el auditor o administrador lo requiera, de tal manera de poder generar un mecanismo de accion inmediato ante algun incidente presentado.
- La solución propuesta deberá contar con la funcionalidad de monitorear la sesion en tiempo real, sin requerir el control remoto de la sesion establecida de tal manera que se respete el principio de no-repudio y se mantenga la integridad de la sesion generada.
- La solución propuesta deberá tener la capacidad de mantener la grabacion de sesiones como minimo 2 años, y contará con almacenamiento ilimitado durante ese tiempo.
- La solución propuesta deberá tener la capacidad de contar con un método para detectar llaves SSH pares, llaves huérfanas y relaciones de confianza en la organización
- La solución propuesta deberá tener la capacidad de almacenar de forma segura y controla el acceso a las llaves privadas SSH
- La solución propuesta deberá tener la capacidad de permitir la automatización de rotación de llaves.

56. NDR (Network Detection and Response) – 01 solución

- La solución debe consistir en una plataforma capaz de detectar amenazas que se propagan por la red, así como comportamientos anómalos asociados a un ciberataque. Debiendo integrarse o formar parte de una plataforma unificada de operaciones de seguridad que integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.
- Deberá integrarse a un dispositivo de tipo hardware conectado a la red interna de la Entidad y extraer información del tráfico para la detección de amenazas.
- El dispositivo deberá tener una capacidad de inspección de 28 Gbps de tráfico, e incluir 02 interfaces de Fibra de 1G/10G (formato SF/SFP+) y 04 interfaces de Cobre 1G RJ45.
- Se deberá incluir 02 transceiver SFP+ 10Gbps MMF.
- El sensor debe ser capaz de recolectar y enviar automáticamente la siguiente telemetría de red:
    - Logs avanzados o telemetría detallada, es decir eventos que incluyan contenido de la aplicación de red en capa 7, cabecera HTTP, querys de DNS, información del tráfico DHCP y otros datos de la telemetría de red.
    - Eventos del tráfico mostrando: IP y puerto origen y destino, nombre de la aplicación en capa 7, país origen y destino, IP NAT de origen y destino, usuario de dominio, Bytes enviados y recibidos, Paquetes enviados y recibidos, DNS Querys, información sobre tráfico DHCP.
    - Nombre, serial number, nombre de la política y/o regla de seguridad de los Firewalls.
    - Nombre, tipo, categoría y severidad de la amenaza identificada.
    - Nombre del archivo transferido a través del tráfico de red.

  - Logs de tráfico URL, detallando URL accedida, categoría, severidad, hora, IP origen/destino, usuario, país de la URL, User-Agent de los paquetes HTTP.
  - Atributos de los dispositivos de red, tales como tipo de dispositivo, categoría, marca, sistema operativo, fabricante del dispositivo.

- La solución deberá ser una plataforma de autoaprendizaje con enfoque adaptativo, que utilice inteligencia artificial validada para modelar el comportamiento normal del entorno, permitiendo detectar, analizar y responder a desviaciones anómalas de la actividad esperada.
- La plataforma deberá ser capaz de identificar comportamientos anómalos en el entorno, resaltándolos de forma clara y contextualizada para su análisis e investigación por parte del equipo de seguridad.
- La solución deberá emplear algoritmos avanzados de inteligencia artificial y aprendizaje automático, incluyendo como mínimo Machine Learning supervisado, no supervisado y técnicas de Deep Learning, orientados a la detección de amenazas conocidas y desconocidas.
- La plataforma deberá asociar automáticamente cada alerta o incidente de seguridad con las tácticas y técnicas del framework MITRE ATT&CK, facilitando el análisis, priorización y entendimiento del ataque.
- La solución deberá contar con al menos 80 casos de uso predefinidos para la detección de anomalías en la red, orientados a identificar comportamientos sospechosos y patrones de ataque.
  - Accesos recurrentes a IP sospechosas
  - Sesiones SMB sospechosas hacia un host remoto
  - Uso de aplicaciones de red inusuales
  - Llamada EFSRPC sospechosa al domain controller
  - Subida masiva de información a sitios de storage
  - Escaneo de red y puertos
  - Sesiones SMTP anómalas
  - Subida de información anómala y excesiva por HTTPS, FTP u otro puerto no estándar.
  - Recurrente acceso a un Dominio y/o IP inusual
  - Acceso no-web a un sitio como Pastebin o similar
  - Proceso no-web accediendo a un website
  - Transferencias de archivos sospechosas vía protocolo SMB
  - Conexión inusual de túnel de red
  - Múltiples conexiones fallidas de DNS que puedan representar C&C
  - DNS Tunneling
  - Paquetes ICMP sospechoso con posible ataque de tunneling de protocolo
  - Posible cryptominer en un host
  - Fuzzing de subdominios
- La solución deberá contar con un módulo de monitoreo, descubrimiento, identificación y clasificación de dispositivos como teléfonos IP, cámaras de vigilancia, consolas de videojuegos, impresoras, dispositivos médicos, equipos industriales, entre otros.
- Por cada dispositivo identificado deberá mostrar la marca del fabricante, tipo de dispositivo, serial number, sistema operativo, dirección IP, dirección MAC, tipo de conexión (cableada o wireless), nombre del SSID o Puerto del switch al cual está conectado, según corresponda. Deberá ser capaz de crear grupos basados en el tipo de dispositivo.

57. Sandboxing (01 solución)

- La plataforma sandbox deberá proporcionar capacidades de análisis dinámico de amenazas (sandboxing) como un componente centralizado, orientado a la detección de malware avanzado y amenazas desconocidas.
- Esta plataforma deberá operar de forma integrada y transversal con los diferentes componentes de la arquitectura de seguridad propuesta, incluyendo como mínimo: los equipos NGFW, la solución XDR, la solución NDR, la solución SIEM, la solución SOAR y automatización (SOAR).
- La plataforma de Sandbox podrá ser ofrecido en Nube (Cloud), On-premise o ambos.
- Deberá ser capaz de emular el potencial malware en entornos Windows, Linux y MacOS.

- Los firewalls deberán ser capaces de de enviar 5000 archivos por hora al sandbox.
- El sandbox deberá ser capaz de analizar 5000 archivos por hora realizando análisis dinámico del archivo (entiéndase por análisis dinámico aquel que no está basado en firmas, ni prefiltros, sino en emulación completa del potencial malware).
- También se aceptará soluciones sandbox terceras de otro fabricante distinto al NGFW.
- En caso de tratarse de una plataforma de Sandbox Cloud, deberá cumplir con los siguientes requerimientos:
    - Deberá tener una disponibilidad de al menos 99.9% contabilizados mensualmente.
    - Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II Plus de AICPA, ISO 27001, ISO 27017 e ISO 27018.
- En caso de tratarse de una plataforma de Sandbox On-premise, deberá cumplir con los siguientes requerimientos:
    - Deberá soportar un throughput de 8 Gbps por cada equipo.
    - Deberá ser desplegado en Alta Disponibilidad (Activo-Pasivo) en cada sede, con el objetivo de mantener los controles de seguridad en caso de contingencia.
    - Debe proveer información forense sobre las acciones realizadas por el malware, tales como resumen del comportamiento visto, actividad sobre los archivos, peticiones DNS, conexiones de red, actividad de los archivos, procesos y registros. Esta información deberá poder se extraída en un reporte PDF.
    - Deberá ser capaz de analizar archivos sospechosos que se transfieran por los protocolos SMTP, POP3, IMAP, SMB, FTP, HTTP y HTTPS.
    - Debe ser capaz de identificar amenazas de tipo Fileless.
- Deberá contar con al menos 20 técnicas patentadas para realizar el análisis del malware.
- El sandbox debe identificar los ataques de phishing al momento de emular los potenciales archivos maliciosos: swf, html, lnk y js.
- Luego del análisis realizado por el sandbox, éste deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. Las firmas deben estar basadas en patrones del malware y no únicamente hashes, de tal forma que sea capaz de bloquear el malware polimórfico con una única firma.
- Debe permitir al administrador la descarga del archivo original analizado por el sandbox.
- Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.
- Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico.
- Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
- La solución debe incorporar un motor avanzado de prevención de malware para la inspección de tráfico en tiempo real. Dicho motor deberá estar potenciado por inteligencia artificial (Inline Malware Prevention) y/o aprendizaje automático (Inline machine learning) para la detección proactiva de amenazas, incluyendo las de día cero.

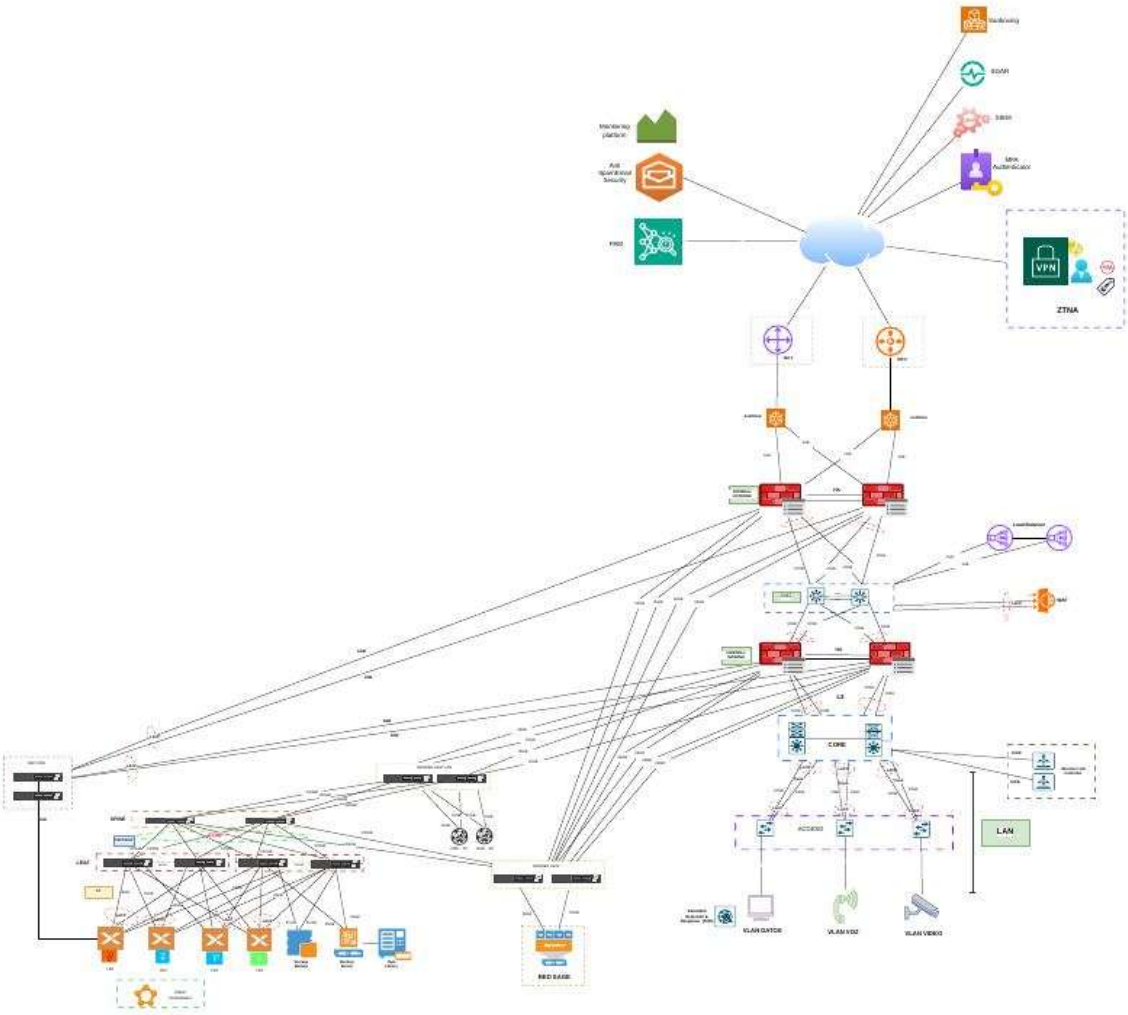
58. Solución de Análisis de Tráfico de Red - (01 Solución)

- La solución podrá ser provista en appliance físico del mismo fabricante, virtual appliance o bajo modelo SaaS (Cloud).
- El postor deberá incluir el hardware o los requerimientos necesarios para el montaje y operación de la instancia.
- No se aceptará que algún componente de la solución sea freeware, trial u open-source sin soporte del fabricante.
- Debe poder monitorear al menos 100 dispositivos, servidores o nodos de red.
- Debe contar con una vista de alto nivel del estado de la infraestructura que permita agrupar y explorar dinámicamente nodos, identificando de inmediato los puntos conflictivos.
- Debe ofrecer opciones de agrupamiento por grupo de instancia, etiqueta, tipo de dispositivo o sitio.

- Debe permitir la navegación jerárquica a través de los distintos niveles de la topología conservando filtros y modalidades de agrupamiento.
- Debe posibilitar la creación de vistas guardadas, capturando configuración de filtros y agrupamientos para acceso rápido.
- Debe exponer en una sola página la disponibilidad, rendimiento, incidentes y configuración de monitoreo de la instancia
- Debe disponer de un panel de acciones rápidas para agregar mantenimiento, aplicar plantillas.
- Debe permitir la creación de nuevos paneles de control definiendo propiedades como nivel de acceso y disponibilidad pública mediante URL.
- Debe permitir monitorear servidores y servicios accesibles públicamente utilizando una red de sondas distribuidas o colectores locales.
- Debe permitir el uso de un colector local para lograr monitoreo en profundidad y alcanzar de forma segura dispositivos detrás del firewall.
- Debe permitir el monitoreo de métricas clave de salud del sistema operativo y rendimiento de aplicaciones mediante protocolos estándar o agentes.
- Debe permitir agregar monitoreo a un servidor o dispositivo manualmente, seleccionando los servicios o aplicaciones y configurando las métricas.
- Debe monitorear para asegurar que las aplicaciones y servicios estén disponibles, funcionales y cumplan con las expectativas en tiempo real.
- Debe permitir recolectar información detallada sobre la calidad de la red de enlaces activos y de respaldo.
- Debe presentar el rendimiento a nivel de dispositivo y a nivel de puerto/interfaz mediante gráficos de línea y estadísticas de entrada/salida.
- Debe soportar la recepción de traps SNMP, permitiendo configurar alertas basadas en OID y severidad.
- Las notificaciones deben poder enviarse a través de canales directos e integraciones con herramientas de terceros.

ANEXO 2 – DIAGRAMA TOPOLOGICO

Se adjunta el diagrama topológico de la red LAN para la Central 911


VPN
ZTNA
CORE
LAN

"Año de la Esperanza y el Fortalecimiento de la Democracia"

ANEXO 3 – GARANTÍA Y SOPORTE DE LOS BIENES

La garantía y soporte será de 12 meses 24x7 on-site, con cuatro (04) horas de tiempo de respuesta, por el periodo con actualizaciones permanentes y condiciones indicado en el siguiente cuadro:

Cuadro Nro. 01

Nro	Bien	Cantidad	Características de la garantía y soporte.
1	Computadora de Escritorio Tipo 1	210	12 meses onsite por el proveedor
2	Computadora de Escritorio Tipo 2	71	12 meses onsite por el proveedor
3	Monitor para Computadoras	696	12 meses onsite por el proveedor
4	Teclado y Mouse	281	12 meses onsite por el proveedor
5	Soporte de Monitores Computadoras de Escritorio Tipo 1	210	12 meses onsite por el proveedor
6	Equipo Portátil	9	12 meses onsite por el proveedor
7	Auricular Monoaural	210	12 meses onsite por el proveedor
8	Micrófono	115	12 meses onsite por el proveedor
9	Altavoces	115	12 meses onsite por el proveedor
10	PPT de pie	210	12 meses onsite por el proveedor
11	Cámara Web	281	12 meses onsite por el proveedor
12	Teléfonos IP Tipo 1	201	12 meses onsite por el proveedor
13	Teléfonos IP Tipo 2	62	12 meses onsite por el proveedor
14	Teléfonos IP Tipo 3	16	12 meses onsite por el proveedor
15	Teléfonos IP Tipo 4	4	12 meses onsite por el proveedor
16	Botonera para teléfono IP 4	1	12 meses onsite por el proveedor
17	Pantalla para Monitoreo	2	12 meses onsite por el proveedor
18	Videoconferencia	4	12 meses onsite por el proveedor
19	Impresora tipo personal	13	12 meses onsite por el proveedor
20	Impresora tipo mediano volumen	5	12 meses onsite por el proveedor
21	Proyector Multimedia	4	12 meses onsite por el proveedor
22	Tabletas Rugerizadas	37	12 meses onsite por el proveedor
23	Switches Spine Data Center	2	12 meses onsite por el proveedor
24	Switches Leaf Data Center	8	12 meses onsite por el proveedor
25	Solución de Orquestador DC	1	12 meses onsite por el proveedor
26	Switch Core LAN Campus	2	12 meses onsite por el proveedor
27	Switch de acceso 48 puertos PoE	23	12 meses onsite por el proveedor
28	Switch de acceso 24 puertos PoE	4	12 meses onsite por el proveedor
29	Switch DMZ	2	12 meses onsite por el proveedor
30	Switch de Gestión Fuera de Banda	2	12 meses onsite por el proveedor
31	Controlador inalámbrico	2	12 meses onsite por el proveedor
32	Access Point	47	12 meses onsite por el proveedor
33	Solución de Administración y Gestión Campus	1	12 meses onsite por el proveedor
34	Solución de Control de Acceso	1	12 meses onsite por el proveedor
35	Hardware de Hiperconvergencia	4	12 meses onsite por el proveedor
36	Software Hiperconvergencia	1	12 meses onsite por el proveedor
37	Servidor para backup	1	12 meses onsite por el proveedor
38	Servidor de inmutabilidad	1	12 meses onsite por el proveedor
39	Almacenamiento para backup	1	12 meses onsite por el proveedor
40	Librería de backup	1	12 meses onsite por el proveedor
41	Software de backup	1	12 meses onsite por el proveedor
42	Firewall NGFW Perimetral	2	12 meses onsite por el proveedor

43	Firewall Interno	2	12 meses onsite por el proveedor
44	Consola de analítica y reportes	1	12 meses onsite por el proveedor
45	XDR (Extended Detection & Response)	1	12 meses onsite por el proveedor
46	ZTNA (Zero Trust Network Access)	1	12 meses onsite por el proveedor
47	Seguridad para correo electronico	1	12 meses onsite por el proveedor
48	WAF - Seguridad para Aplicaciones Web	1	12 meses onsite por el proveedor
49	SIEM	1	12 meses onsite por el proveedor
50	Plataforma de detección y re spuesta de amenazas externas e internas	1	12 meses onsite por el proveedor
51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	1	12 meses onsite por el proveedor
52	ADC (application Delivery Controller)	2	12 meses onsite por el proveedor
53	Anti-DDos	2	12 meses onsite por el proveedor
54	MFA - Administración de identidad y acceso	1	12 meses onsite por el proveedor
55	PAM - Administración de acceso privilegiado	1	12 meses onsite por el proveedor
56	NDR (Network Detection and Response)	1	12 meses onsite por el proveedor
57	Sandboxing	1	12 meses onsite por el proveedor
58	Solución de Análisis de Tráfico de Red	1	12 meses onsite por el proveedor

Deberá presentar en su propuesta la carta por cada fabricante y/o declaración jurada del proveedor indicando el cumplimiento de la garantía y soporte exigido.

"Año de la Esperanza y el Fortalecimiento de la Democracia"

ANEXO 4 – ACCESORIOS / CONSUMIBLES

1. **Accesorios y consumibles en sitio**
   Corresponde a elementos destinados a reposición por falla, desgaste, mantenimiento preventivo/correctivo o continuidad del servicio.

   Con la finalidad de garantizar la continuidad operativa de las soluciones tecnológicas en el presente requerimiento, el Proveedor deberá entregar los siguientes accesorios adicionales de solo los equipos detallados en el presente anexo, para cambios inmediatos ante fallas:

Componente Tecnológico - Data Center (Spine – Leaf)	Cantidad
Transceivers 100GE-SR4	04
Transceivers 25GE-SR	04
Transceivers 10GE-SR	02
Transceivers 1000Base-T	02

Componente Tecnológico - Campus (Core – Acceso)	Cantidad
Transceivers 25GE-SR	02
Transceivers 10GE-LR	04
Transceivers 10GE-SR	02
Transceivers 1000Base-T	02

Componente Tecnológico - NAC	Cantidad
Transceivers 10GE-SR	02

Componente Tecnológico - Wireless Controller	Cantidad
Transceivers 10GE-SR	02

Componente Tecnológico - DMZ	Cantidad
Transceivers 10GE-SR	02
Transceivers 1000Base-T	02

Componente Tecnológico - Firewall Externo	Cantidad
Transceivers SFP+ 10GE	02
Transceivers SFP28 25GE	02

Componente Tecnológico - Firewall Interno	Cantidad
Transceivers SFP+ 10GE	02
Transceivers SFP28 25GE	02

Componente Tecnológico - Impresoras	Cantidad
Fusor para impresora de tipo personal	01
Fusor para impresora de tipo mediano volumen	02

Asimismo, se deberá proveer los siguientes consumibles para impresoras:

Componente Tecnológico - Impresoras	Cantidad
Toner+Tambor integrado para impresora de tipo personal	26
Toner para impresora de tipo mediano volumen	26
Tambor para impresora de tipo mediano volumen	26

Nota: Durante el periodo de garantía y soporte, estos repuestos y consumibles se ubicarán en el almacen de TI del Edificio de la Central 911, y administrado por el Proveedor durante el periodo indicado para su atención oportuna a través de la mesa de servicio, bajo la Supervisión de la Entidad.

PARTE 3. Contrato

Sección VIII. Condiciones Generales del Contrato

Índice

1. Margen de preferencia (IAL 33) 258

2. Documentos del Contrato 259

3. Fraude y Corrupción 259

4. Interpretación 259

5. Idioma 261

6. Asociación en Participación, Consorcio o Asociación 261

7. Elegibilidad 261

8. Notificaciones 262

9. Ley aplicable 262

10. Solución de controversias 262

11. Inspecciones y auditorías a cargo del Banco 263

12. Alcance de los suministros 263

13. Entrega y documentos 263

14. Responsabilidades del Proveedor 263

15. Precio del Contrato 265

16. Condiciones de Pago 265

17. Impuestos y derecho 265

18. Garantía de Cumplimiento 266

19. Derechos de Autor 266

20. Confidencialidad de la información 267

21. Subcontratación 268

22. Especificaciones y normas 268

23. Embalaje y documentos 268

24. Seguros 269

25. Transporte y servicios conexos 269

26. Inspecciones y pruebas 270

27. Liquidación por daños y perjuicios 271

28. Garantía de los Bienes 271

29. Patentes y exención de responsabilidad 272

30. Limitación de responsabilidad 273

31. Cambio en las leyes y regulaciones 274

32. Fuerza Mayor 274

33. Órdenes de cambio y enmiendas al Contrato 275

34. Prórroga de los plazos 276

35. Resolución 277

36. Cesión 278

37. Restricciones a la exportación 278

Sección VIII. Condiciones Generales del Contrato

1. Definiciones

1.1 Las siguientes palabras y expresiones tendrán los significados que aquí se les asigna:

(a) Por "Banco" se entiende el Banco Mundial y se refiere al Banco Internacional de Reconstrucción y Fomento (BIRF) o a la Asociación Internacional de Fomento (IDA).

(b) Por "Contrato" se entiende el Convenio de Contrato celebrado entre el Comprador y el Proveedor, junto con los Documentos del Contrato allí referidos, incluyendo todos los anexos y apéndices, y todos los documentos incorporados allí por referencia.

(c) Por "Documentos del Contrato" se entiende los documentos enumerados en el Convenio de Contrato, incluyendo cualquier enmienda.

(d) Por "Precio del Contrato" se entiende el precio pagadero al Proveedor según se especifica en el Convenio de Contrato, sujeto a las condiciones y ajustes allí estipulados o deducciones propuestas, según corresponda en virtud del Contrato.

(e) Por "día" se entiende día calendario.

(f) Por "cumplimiento" se entiende la prestación de los Servicios Conexos por parte del Proveedor de acuerdo con los términos y condiciones establecidas en el Contrato.

(g) Por "CGC" se entiende las Condiciones Generales del Contrato.

(h) Por "Bienes" se entiende todos los productos, materia prima, maquinaria y equipos, y otros materiales que el Proveedor deba proporcionar al Comprador en virtud del Contrato.

(i) El "País del Comprador" es el país especificado en las **Condiciones Especiales del Contrato (CEC)**.

(j) Por "Comprador" se entiende la entidad que compra los Bienes y Servicios Conexos, según **se indica en las CEC**.

(k) Por "Servicios Conexos" se entiende los servicios incidentales relativos a la provisión de los bienes, tales como seguro, instalación, capacitación y mantenimiento

inicial y otras obligaciones similares del Proveedor en virtud del Contrato.

(l) Por "CEC" se entiende las Condiciones Especiales del Contrato.

(m) Por "Subcontratista" se entiende cualquier persona física, entidad privada o pública, o una combinación de estas, a las cuales el Proveedor ha subcontratado para que suministren parte de los Bienes o presten parte de los Servicios Conexos.

(n) Por "Proveedor" se entiende la persona física o entidad privada o pública, o una combinación de estas, cuya oferta para ejecutar el Contrato ha sido aceptada por el Comprador y es denominada como tal en el Convenio de Contrato.

(o) Por "emplazamiento del Proyecto", donde corresponde, se entiende el lugar citado en las **CEC**.

2. Documentos del Contrato

2.1 Con sujeción al orden de precedencia establecido en el Convenio de Contrato, se entiende que todos los documentos que forman parte integral del Contrato (y todos sus componentes allí incluidos) son correlativos, complementarios y recíprocamente aclaratorios. El Convenio de Contrato deberá leerse de manera integral.

3. Fraude y Corrupción

3.1 El Banco requiere el cumplimiento de sus Directrices Contra el Fraude y la Corrupción y de sus políticas y procedimientos de sanciones vigentes incluidos en el Marco de Sanciones del Grupo Banco Mundial, conforme a lo estipulado en el Apéndice 1 de las CGC.

3.2 El Comprador exige al Proveedor que divulgue aquellas comisiones u honorarios que pudieran haber sido pagados o que hayan de ser pagados a los agentes o cualquier otra parte con relación al proceso de Licitación o ejecución del Contrato. La información divulgada deberá incluir al menos el nombre y domicilio del agente o de la otra parte, el monto y la moneda, y el propósito de la comisión, gratificación u honorario.

4. Interpretación

4.1 Si el contexto así lo requiere, el singular significa el plural, y viceversa.

4.2 Incoterms

(a) El significado de cualquier término comercial, así como los derechos y obligaciones de las partes serán los prescritos en los Incoterms, **conforme se especifica en las CEC**, a menos que sea incongruente con alguna disposición del Contrato.

(b) El uso de los términos EXW, CIP, FCA, CFR y otros similares se regirá por las normas establecidas en la edición vigente de los Incoterms especificada en las **CEC** y publicada por la Cámara de Comercio Internacional en París, Francia.

4.3 Totalidad del acuerdo

El Contrato constituye la totalidad de lo acordado entre el Comprador y el Proveedor y sustituye todas las comunicaciones, negociaciones y acuerdos (escritos o verbales) realizados entre las partes con anterioridad a la fecha de la celebración del Contrato.

4.4 Enmienda

Ninguna enmienda u otra variación al Contrato será válida, a menos que sea hecha por escrito, esté fechada, se refiera expresamente al Contrato y esté firmada por un representante de cada una de las partes debidamente autorizado.

4.5 Limitación de dispensas

(a) Con sujeción a lo indicado en la Subcláusula 4.5 (b) siguiente de las CGC, ninguna dilación, tolerancia, demora o aprobación por cualquiera de las partes al hacer cumplir algún término y condición del Contrato, así como tampoco el otorgamiento de prórrogas por una de las partes a la otra, perjudicará, afectará o limitará los derechos de esa parte en virtud del Contrato. Asimismo, ninguna dispensa concedida por cualquiera de las partes por incumplimiento del Contrato servirá de dispensa para incumplimientos posteriores o continuos del Contrato.

(b) Toda dispensa de los derechos, facultades o remedios de una de las partes en virtud del Contrato deberá otorgarse por escrito, llevar la fecha y estar firmada por un representante autorizado de la parte que la otorga, y deberá especificar la obligación que está dispensando y el alcance de la dispensa.

4.6 Divisibilidad

Si cualquier disposición o condición del Contrato fuese prohibida o resultase inválida o inejecutable, dicha prohibición, invalidez o falta de ejecución no afectará la validez o el cumplimiento de las otras disposiciones o condiciones del Contrato.

5. Idioma

5.1 El Contrato, así como toda la correspondencia y documentos relativos al Contrato intercambiados entre el Proveedor y el Comprador, deberán ser escritos en el idioma especificado en las **CEC**. Los documentos de respaldo y el material impreso que formen parte del Contrato pueden estar en otro idioma, siempre que vayan acompañados de una traducción fidedigna de las partes pertinentes al idioma especificado, en cuyo caso dicha traducción prevalecerá para a los efectos de la interpretación del Contrato.

5.2 El Proveedor será responsable de todos los costos que implique traducir al idioma principal los documentos que proporcione, así como de todos los riesgos derivados de las posibles imprecisiones de dicha traducción.

6. Asociación en Participación, Consorcio o Asociación

6.1 Si el Proveedor es una Asociación en Participación, Consorcio o Asociación ("APCA"), un consorcio o una asociación, todas las partes que lo conforman serán solidariamente responsables frente al Comprador por el cumplimiento de las disposiciones del Contrato y deberán designar a una de ellas para que actúe como representante con facultades para obligar jurídicamente a la APCA, el consorcio o la asociación. La composición o constitución de la APCA no podrá modificarse sin el previo consentimiento del Comprador.

7. Elegibilidad

7.1 El Proveedor y sus Subcontratistas deberán tener la nacionalidad de un país elegible. Se considera que un Proveedor o Subcontratista tiene la nacionalidad de un país si es un ciudadano o está constituido o inscripto en él y opera de conformidad con sus normas y leyes.

7.2 Todos los Bienes y Servicios Conexos que hayan de suministrarse en el marco del Contrato con financiamiento del Banco deberán tener su origen en países elegibles. Por "origen" se entiende, a los fines de esta instrucción, el país donde los bienes han sido extraídos, cosechados, cultivados, producidos, fabricados o procesados, o donde, como resultado de la manufactura, el procesamiento o el ensamblaje, se genera otro artículo reconocido comercialmente que difiere en gran medida de las características básicas de sus componentes.

8. Notificaciones

8.1 Todas las notificaciones entre las partes en virtud de este Contrato deberán cursarse por escrito a la dirección indicada en las **CEC**. El término "por escrito" se refiere a toda comunicación en forma escrita con prueba de recibo.

8.2 Las notificaciones serán efectivas en la fecha de entrega y en la fecha de la notificación, la que sea posterior.

9. Ley aplicable

9.1 El Contrato se regirá por las leyes del País del Comprador, y se interpretará conforme a dichas leyes, a menos que en las **CEC** se indique otra cosa.

9.2 Durante la ejecución del Contrato, el Proveedor deberá cumplir con las prohibiciones relativas a la importación de bienes y servicios del País del Comprador cuando:

(a) como consecuencia de las leyes o regulaciones oficiales, el país del Prestatario prohibiera las relaciones comerciales con dicho país;

(b) por un acto realizado en cumplimiento de una decisión del Consejo de Seguridad de las Naciones Unidas adoptada conforme al Capítulo VII de la Carta de las Naciones Unidas, el país del Prestatario prohíba cualquier importación de bienes de aquel país, o pagos a cualquier país, persona o entidad de aquel país.

10. Solución de controversias

10.1 El Comprador y el Proveedor harán todo lo posible para resolver amigablemente, mediante negociaciones directas informales, cualquier desacuerdo o controversia que se haya suscitado entre ellos en relación con el Contrato.

10.2 Si, transcurridos 28 (veintiocho) días, las partes no han podido resolver la controversia o diferencia mediante dichas consultas mutuas, el Comprador o el Proveedor podrá notificar a la otra parte sobre sus intenciones de iniciar un proceso de arbitraje con respecto al asunto en disputa, conforme a las disposiciones que se indican a continuación, y no podrá iniciarse un proceso de arbitraje con respecto a dicho asunto, a menos que se haya cursado dicha notificación. Cualquier controversia o diferencia respecto de la cual se haya notificado la intención de iniciar un proceso de arbitraje de conformidad con esta cláusula se resolverá definitivamente mediante arbitraje. El proceso de arbitraje podrá comenzar antes o después de la entrega de los Bienes en virtud del Contrato. El arbitraje se llevará a cabo según el reglamento de procedimientos **estipulado en las CEC.**

10.3 Sin perjuicio de las referencias al arbitraje que figuran en este documento,

(a) ambas partes deben continuar cumpliendo con sus respectivas obligaciones derivadas del Contrato, a menos que acuerden otra cosa;

(b) el Comprador pagará al Proveedor el dinero que le adeude.

11. Inspecciones y auditorías a cargo del Banco

11.1 El Proveedor deberá mantener, y realizar todos los esfuerzos razonables para que sus Subcontratistas mantengan, cuentas exactas y sistematizadas, así como registros contables relativos a los Bienes de forma tal que permitan identificar los tiempos de cambios pertinentes y los costos.

11.2 De conformidad con el párrafo 2.2 (e). del Apéndice 1 de las Condiciones Generales, el Proveedor permitirá, y procurará que sus agentes (hayan sido declarados o no), subcontratistas subconsultores, prestadores de servicios, proveedores y personal permitan, que el Banco o las personas designadas por el Banco inspeccionen las instalaciones y/o las cuentas, los registros y otros documentos relacionados con los procesos de calificación, selección y/o la ejecución del Contrato, y dispongan que dichas cuentas, registros y otros documentos sean auditados por medio de auditores designados por el Banco. El Proveedor y sus Subcontratistas y subconsultores deberán prestar atención a lo estipulado en la Cláusula 3.1 (Fraude y Corrupción), que establece, *inter alia*, que las acciones encaminadas a impedir sustancialmente el ejercicio de los derechos del Banco de realizar auditorías e inspecciones constituyen una práctica prohibida sujeta a la resolución del contrato (además de la determinación de inelegibilidad con arreglo a los procedimientos de sanciones vigentes del Banco).

12. Alcance de los suministros

12.1 Los Bienes y Servicios Conexos se suministrarán según lo estipulado en los Requisitos de los Bienes y Servicios Conexos.

13. Entrega y documentos

13.1 Con sujeción a lo dispuesto en la Subcláusula 33.1 de las CGC, la entrega de los Bienes y la Finalización de los Servicios Conexos se realizará de acuerdo con el Cronograma de Entregas y de Cumplimiento indicado en los Requisitos de los Bienes y Servicios Conexos. Los detalles de los documentos de embarque y otros que deberá suministrar el Proveedor se especifican en las **CEC**.

14. Responsabilidades del Proveedor

14.1 El Proveedor deberá proporcionar todos los Bienes y Servicios Conexos incluidos en el alcance de suministros de conformidad con la Cláusula 12 de las CGC, el Cronograma de Entregas

y de Finalización, de conformidad con la Cláusula 13 de las CGC.

14.2 El Proveedor, incluidos sus Subcontratistas, no empleará ni contratará trabajo forzoso o personas sujetas a trata, como se describe en las Subcláusulas 14.3 y 14.4 de las CGC.

14.3 El trabajo forzoso consiste en cualquier trabajo o servicio, no realizado voluntariamente, que se exige a un individuo bajo amenaza de fuerza o sanción, e incluye cualquier tipo de trabajo involuntario u obligatorio, como trabajo en régimen de servidumbre o acuerdos laborales similares.

14.4 La trata de personas se define como el reclutamiento, transporte, traslado, albergue o recepción de personas mediante la amenaza o el uso de la fuerza u otras formas de coerción, secuestro, fraude, engaño, abuso de poder o de una posición de vulnerabilidad o de dar o recibir pagos o beneficios para lograr el consentimiento de una persona que tiene control sobre otra, con fines de explotación.

14.5 El Proveedor, incluidos sus Subcontratistas, no empleará ni contratará a un niño menor de 14 años a menos que la ley nacional especifique una edad superior (la edad mínima).

14.6 14.6 El Proveedor, incluidos sus Subcontratistas, no deberá emplear ni contratar a un niño entre la edad mínima y la edad de 18 años de una manera que pueda ser peligrosa, o que interfiera con la educación del niño, o que sea dañina para el niño. salud o desarrollo físico, mental, espiritual, moral o social.

14.7 14.7 El trabajo considerado peligroso para los niños es aquel que, por su naturaleza o las circunstancias en las que se lleva a cabo, puede poner en peligro la salud, la seguridad o la moralidad de los niños. Tales actividades laborales prohibidas para los niños incluyen el trabajo:

(a) con exposición a abuso físico, psicológico o sexual;

(b) bajo tierra, bajo el agua, trabajando en alturas o en espacios reducidos;

(c) con maquinaria, equipo o herramientas peligrosos, o que impliquen manipulación o transporte de cargas pesadas;

(d) en entornos insalubres que expongan a los niños a sustancias, agentes o procesos peligrosos, o a temperaturas, ruidos o vibraciones perjudiciales para la salud; o

(e) en condiciones difíciles, como el trabajo durante muchas horas, durante la noche o en confinamiento en las instalaciones del contratante.

14.8 El Proveedor cumplirá y exigirá a sus Subcontratistas, si los hubiere, que cumplan con todas las reglamentaciones, leyes, directrices y cualquier otro requisito de salud y seguridad que se establezca en las Especificaciones Técnicas.

14.9 El Proveedor deberá cumplir con las obligaciones adicionales que se especifican en las **CEC**.

15. Precio del Contrato

15.1 Los precios que cobre el Proveedor por los Bienes proporcionados y los Servicios Conexos prestados en virtud del Contrato no podrán ser diferentes de los cotizados por el Proveedor en su Oferta, salvo que se trate de un ajuste de precios autorizado en las **CEC**.

16. Condiciones de Pago

16.1 El Precio del Contrato, incluyendo cualquier pago por anticipo, si corresponde, se pagará según se establece en las **CEC**.

16.2 La solicitud de pago del Proveedor al Comprador deberá formularse por escrito e ir acompañada de recibos que describan, según corresponda, los Bienes entregados y los Servicios Conexos prestados, y de los documentos presentados de conformidad con la Cláusula 13 de las CGC y en cumplimiento de las obligaciones estipuladas en el Contrato.

16.3 El Comprador efectuará los pagos prontamente, pero en ningún caso podrá hacerlo una vez transcurridos 60 (sesenta) días de la fecha en que el Proveedor haya presentado una factura o una solicitud de pago, y el Comprador la haya aceptado.

16.4 Las monedas en las que se pagará al Proveedor en virtud de este Contrato serán aquellas que el Proveedor hubiese especificado en su Oferta.

16.5 Si el Comprador no efectuara cualquiera de los pagos al Proveedor en las fechas de vencimiento correspondientes o dentro del plazo establecido en las **CEC**, el Comprador le pagará intereses sobre los montos de los pagos en mora a la tasa establecida en las **CEC**, por el período de la demora y hasta que se haya efectuado el pago completo, ya sea antes o después de cualquier sentencia judicial o laudo arbitral.

17. Impuestos y derechos

17.1 En el caso de bienes fabricados fuera del País del Comprador, el Proveedor será totalmente responsable por todos los

impuestos, timbres, comisiones por licencias y otros cargos similares impuestos fuera de dicho país.

17.2 En el caso de bienes fabricados en el País del Comprador, el Proveedor será totalmente responsable por todos los impuestos, gravámenes, comisiones por licencias y otros cargos similares que se abonen hasta la entrega de los Bienes contratados al Comprador.

17.3 El Comprador arbitrará todos los medios necesarios para que el Proveedor se beneficie con el mayor alcance posible de cualquier exención impositiva, concesión o privilegio legal que pudiese serle aplicable en el País del Comprador.

18. Garantía de Cumplimiento

18.1 Si así se estipula en las **CEC**, el Proveedor, dentro de los 28 (veintiocho) días posteriores a la notificación de la adjudicación del Contrato, deberá suministrar la Garantía de Cumplimiento del Contrato por el monto establecido en las **CEC**.

18.2 Los recursos de la Garantía de Cumplimiento serán pagaderos al Comprador como indemnización por cualquier pérdida que pudiera ocasionarle el incumplimiento de las obligaciones del Proveedor en virtud del Contrato.

18.3 Como se establece en las CEC, la Garantía de Cumplimiento, en caso de ser requerida, deberá estar denominada en la(s) misma(s) moneda(s) del Contrato o en una moneda de libre convertibilidad aceptable para el Comprador, y deberá presentarse en uno de los formatos estipulados por el Comprador en las CEC o en otro formato que este considere aceptable.

18.4 A menos que se indique otra cosa en las **CEC**, la Garantía de Cumplimiento será liberada por el Comprador y devuelta al Proveedor a más tardar 28 (veintiocho) días contados a partir de la fecha de Cumplimiento de las obligaciones del Proveedor en virtud del Contrato, incluyendo cualquier obligación relativa a la garantía de los bienes.

19. Derechos de Autor

19.1 Los derechos de autor respecto de todos los planos, documentos y otros materiales que contengan datos e información proporcionados por el Proveedor al Comprador seguirán siendo de propiedad del Proveedor. Si esta información fue suministrada al Comprador directamente o a través del Proveedor por un tercero, incluyendo proveedores de materiales, el derecho de autor de dichos materiales seguirá siendo de propiedad de dichos terceros.

20. Confidencialidad de la información

20.1 El Comprador y el Proveedor deberán mantener bajo estricta confidencialidad y en ningún momento divulgarán a terceros, sin el consentimiento de la otra parte, documentos, datos u otra información que hubiera sido directa o indirectamente proporcionada por la otra parte en relación con el Contrato antes, durante o después de su ejecución. Sin perjuicio de ello, el Proveedor podrá proporcionar a sus Subcontratistas los documentos, datos e información recibidos del Comprador a fin de que estos puedan llevar a cabo su trabajo en el marco del Contrato. En tal caso, el Proveedor obtendrá de dichos Subcontratistas un compromiso de confidencialidad similar al que debe asumir el Proveedor en virtud de la Cláusula 20 de las CGC.

20.2 El Comprador no utilizará dichos documentos, datos u otra información recibidos del Proveedor para ningún fin que no esté relacionado con el Contrato. Asimismo, el Proveedor no utilizará los documentos, datos u otra información recibidos del Comprador para ningún otro fin que el de la ejecución del Contrato.

20.3 No obstante, la obligación de las partes derivada de las Subcláusulas 20.1 y 20.2 de las CGC no se aplicará a información que:

(a) el Comprador o el Proveedor deba compartir con el Banco u otras instituciones que participan en el financiamiento del Contrato;

(b) actualmente o en el futuro pase a ser de dominio público sin culpa de la parte en cuestión;

(c) pueda comprobarse que estaba en poder de dicha parte al momento de ser divulgada y que no fue obtenida previamente, de manera ni indirecta, de la otra parte, o

(d) que un tercero que no tenía obligación de confidencialidad puso a disposición de esa parte.

20.4 Las disposiciones precedentes de esta Cláusula 20 de las CGC no modificarán de modo alguno ningún compromiso de confidencialidad asumido por cualquiera de las partes de este instrumento antes de la fecha del Contrato con respecto a los Suministros o a cualquier parte de ellos.

20.5 Las disposiciones de la Cláusula 20 de las CGC seguirán siendo válidas luego del cumplimiento o la extinción del Contrato, sea cual fuere el motivo.

21. Subcontratación

21.1 El Proveedor informará al Comprador por escrito acerca de todos los subcontratos que adjudique en virtud del Contrato, siempre que no los hubiera especificado en su Oferta. La Notificación del Proveedor para agregar cualquier subcontratista que no haya sido designado en el Contrato deberá estar acompañada de la declaración del Subcontratista de conformidad con el Apéndice 2 de las CGC - Declaración de Desempeño en materia de Explotación y Abuso Sexual (EAS) y/o Acoso Sexual (ASx). Dicha notificación, en la Oferta original u Ofertas posteriores, no eximirá al Proveedor de las obligaciones, deberes y compromisos o responsabilidades contraídas en virtud del Contrato.

21.2 Todos los subcontratos deberán cumplir con las disposiciones de las Cláusulas 3 y 7 de las CGC.

22. Especificaciones y normas

22.1 Especificaciones técnicas y planos

(a) Los Bienes y Servicios Conexos proporcionados en el marco de este Contrato deberán ajustarse a las especificaciones técnicas y a las normas estipuladas en la Sección VI, "Requisitos de los Bienes y Servicios Conexos", y, cuando no se haga referencia a una norma aplicable, la norma será equivalente o superior a las normas oficiales cuya aplicación sea apropiada en el país de origen de los Bienes.

(b) El Proveedor tendrá derecho a deslindar su responsabilidad por cualquier diseño, dato, plano, especificación u otro documento, o por cualquier modificación de estos, proporcionado o diseñado por el Comprador o en nombre de él, notificando a este último de dicho deslinde.

(c) Cuando en el Contrato se haga referencia a códigos y normas conforme a los cuales este deberá ejecutarse, la edición o versión revisada de dichos códigos y normas será la especificada en los Requisitos de los Bienes y Servicios Conexos. Cualquier cambio de dichos códigos o normas durante la ejecución del Contrato se aplicará solamente con la aprobación previa del Comprador y dicho cambio estará regido por la Cláusula 33 de las CGC.

23. Embalaje y documentos

23.1 El Proveedor embalará los Bienes en la forma necesaria para impedir que se dañen o deterioren durante el transporte al lugar de destino final indicado en el Contrato. El embalaje deberá ser adecuado para resistir, entre otras cosas, la manipulación descuidada, la exposición a temperaturas extremas, la sal y las precipitaciones, y el almacenamiento en espacios abiertos. En el tamaño y peso de los embalajes se tendrá en cuenta,

cuando corresponda, la lejanía del lugar de destino final de los bienes y la carencia de equipos para la carga y descarga de materiales pesados en todos los puntos en que los bienes deban transbordarse.

23.2 El embalaje, las identificaciones y los documentos que se coloquen dentro y fuera de los bultos deberán cumplir estrictamente con los requisitos especiales que se hayan estipulado expresamente en el Contrato, y cualquier otro requisito, si lo hubiere, especificado en las CEC y en cualquier otra instrucción dispuesta por el Comprador.

24. Seguros

24.1 A menos que se disponga otra cosa en las **CEC**, los Bienes suministrados en el marco del Contrato deberán estar completamente asegurados, en una moneda de libre convertibilidad de un país elegible, contra riesgo de extravío o daños incidentales ocurridos durante la fabricación, adquisición, transporte, almacenamiento y entrega, de conformidad con los Incoterms aplicables o según se disponga en las **CEC**.

25. Transporte y servicios conexos

25.1 A menos que se disponga otra cosa en las **CEC**, la responsabilidad por los arreglos de transporte de los Bienes se regirá por los Incoterms indicados.

25.2 Podrá exigirse al Proveedor que suministre alguno o la totalidad de los siguientes servicios, además de los servicios adicionales, si los hubiere, especificados en las CEC:

(a) funcionamiento o supervisión *in situ* del ensamblaje o puesta en marcha de los Bienes suministrados;

(b) provisión de herramientas de ensamblaje o mantenimiento de los Bienes suministrados;

(c) provisión de un manual detallado de operaciones y de mantenimiento apropiado para cada una de las unidades de los Bienes suministrados;

(d) funcionamiento o supervisión o mantenimiento o reparación de los Bienes suministrados, por un período de tiempo acordado entre las partes, entendiéndose que este servicio no exime al Proveedor de ninguna de las garantías de funcionamiento derivadas de este Contrato; y

(e) capacitación del personal del Comprador, en la planta del Proveedor o en el sitio de entrega, en relación con el ensamblaje, el inicio, la operación, el mantenimiento o la reparación de los Bienes suministrados.

25.3 Los precios que cobre el Proveedor por los servicios conexos, si no estuvieran incluidos en el Precio Contractual de los Bienes, serán acordados por las partes con antelación y no excederán las tarifas que el Proveedor normalmente cobre a otras partes por servicios similares.

26. Inspecciones y pruebas

26.1 El Proveedor realizará, por su cuenta y sin costo alguno para el Comprador, todas las pruebas o inspecciones de los Bienes y Servicios Conexos según se dispone en las **CEC**.

26.2 Las inspecciones y pruebas podrán realizarse en las instalaciones del Proveedor o de su Subcontratista, en el lugar de entrega o en el lugar de destino final de los Bienes o en otro lugar en el País del Comprador establecido en las **CEC**. De conformidad con la Subcláusula 26.3 de las CGC, cuando dichas inspecciones o pruebas se realicen en establecimientos del Proveedor o de sus Subcontratistas, se proporcionará a los inspectores todas las facilidades y asistencia razonables, incluido el acceso a los planos y datos sobre producción, sin cargo alguno para el Comprador.

26.3 El Comprador o su representante designado tendrá derecho a presenciar las pruebas o inspecciones mencionadas en la Subcláusula 26.2 de las CGC, siempre y cuando asuma todos los costos y gastos que ocasione su participación, incluidos, entre otros, gastos de viaje, alojamiento y alimentación.

26.4 Cuando el Proveedor esté listo para realizar dichas pruebas e inspecciones, notificará oportunamente al Comprador indicándole el lugar y la hora. El Proveedor obtendrá del tercer o del fabricante que corresponda el permiso o consentimiento necesario para permitir al Comprador o a su representante designado presenciar las pruebas o inspecciones.

26.5 El Comprador podrá exigir al Proveedor que realice algunas pruebas o inspecciones que no estén contempladas en el Contrato, pero que considere necesarias para verificar que las características y el funcionamiento de los Bienes cumplan con los códigos de las especificaciones técnicas y normas establecidas en el Contrato. Los costos y gastos adicionales razonables que sufrague el Proveedor por dichas pruebas e inspecciones se sumarán al Precio del Contrato. Asimismo, si dichas pruebas o inspecciones impidieran el avance de la fabricación o el cumplimiento de otras obligaciones del Proveedor derivadas del Contrato, deberán realizarse los ajustes correspondientes a las fechas de entrega y de finalización y a las otras obligaciones afectadas.

26.6 El Proveedor presentará al Comprador un informe de los resultados de dichas pruebas o inspecciones.

26.7 El Comprador podrá rechazar cualquiera de los Bienes o cualquier componente de estos que no pase las pruebas o inspecciones o que no se ajuste a las especificaciones. El Proveedor deberá rectificar o reemplazar dichos Bienes o componentes rechazados o hacer las modificaciones necesarias para cumplir con las especificaciones, sin costo alguno para el Comprador. Asimismo, deberá repetir las pruebas o inspecciones, sin costo alguno para el Comprador, una vez que notifique al Comprador de conformidad con la Subcláusula 26.4 de las CGC.

26.8 El Proveedor está de acuerdo en que ni la realización de pruebas o inspecciones de los Bienes o de parte de ellos, ni la presencia del Comprador o de su representante, ni la emisión de informes con arreglo a la Subcláusula 26.6 de las CGC lo eximirán de las garantías u otras obligaciones derivadas del Contrato.

27. Liquidación por daños y perjuicios

27.1 Con excepción de lo dispuesto en la Cláusula 32 de las CGC, si el Proveedor no cumple con la entrega de la totalidad o parte de los Bienes en la(s) fecha(s) establecida(s) o con la prestación de los Servicios Conexos dentro del período especificado en el Contrato, el Comprador, sin perjuicio de los demás recursos de que disponga en virtud del Contrato, podrá deducir del Precio del Contrato, por concepto de liquidación por daños y perjuicios, una suma equivalente al porcentaje del precio de entrega de los Bienes atrasados o de los Servicios no prestados establecido en las **CEC** por cada semana o parte de la semana de retraso hasta alcanzar el máximo del porcentaje especificado en dichas **CEC**. Una vez alcanzado el máximo establecido, el Comprador podrá dar por rescindido el Contrato de conformidad con la Cláusula 35 de las CGC.

28. Garantía de los Bienes

28.1 El Proveedor garantiza que todos los Bienes suministrados en virtud del Contrato son nuevos, no tienen uso previo y corresponden al modelo más reciente o actual, y que incorporan todas las mejoras recientes en cuanto a diseño y materiales, a menos que el Contrato disponga otra cosa.

28.2 De conformidad con la Subcláusula 22.1 (b) de las CGC, el Proveedor garantiza que todos los Bienes suministrados estarán libres de defectos derivados de sus actos y omisiones, o derivados del diseño, los materiales o la manufactura, durante el uso normal en las condiciones que imperen en el país de destino final.

28.3 Salvo que en las **CEC** se indique otra cosa, la garantía seguirá vigente durante 12 (doce) meses a partir de la fecha en que los Bienes, o cualquier parte de ellos, según el caso, hayan sido entregados y aceptados en el punto final de destino indicado en las **CEC**, o 18 (dieciocho) meses a partir de la fecha de embarque en el puerto o lugar de carga en el país de origen, si dicho período concluye primero.

28.4 El Comprador notificará al Proveedor consignando la naturaleza de los defectos y proporcionará toda la evidencia disponible inmediatamente después de haberlos descubierto. El Comprador otorgará al Proveedor una oportunidad razonable para inspeccionar tales defectos.

28.5 Al recibir dicha notificación, el Proveedor deberá reparar o reemplazar, dentro del plazo establecido en las **CEC**, los Bienes defectuosos o sus partes, sin costo alguno para el Comprador.

28.6 Si el Proveedor, tras haber sido notificado, no corrige los defectos dentro del plazo establecido en las **CEC**, el Comprador, dentro de un tiempo razonable, podrá proceder a tomar las medidas necesarias para remediar la situación, por cuenta y riesgo del Proveedor y sin perjuicio de otros derechos que el Comprador pueda tener contra el Proveedor en el marco del Contrato.

29. Patentes y exención de responsabilidad

29.1 El Proveedor eximirá al Comprador, siempre que este cumpla con lo establecido en la Subcláusula 29.2 de las CGC, así como a sus empleados y funcionarios, de toda responsabilidad derivada de litigios, acciones legales o procedimientos administrativos, reclamos, demandas, pérdidas, daños, costos y gastos de cualquier naturaleza, incluyendo gastos y honorarios por representación legal, que deba sufragar como resultado de la transgresión o la supuesta transgresión de derechos de patente, uso de modelo, diseño registrado, marca registrada, derecho de autor u otro derecho de propiedad intelectual registrado o ya existente en la fecha del Contrato debido a:

(a) la instalación de los Bienes por el Proveedor o el uso de los Bienes en el país donde se encuentra emplazado el proyecto; y

(b) la venta, en cualquier país, de los productos generados por los Bienes.

Dicha exención de responsabilidad no procederá si los Bienes o una parte de ellos fuesen utilizados para fines no previstos en el Contrato o que no pudieran inferirse razonablemente de este. Tampoco abarcará ninguna transgresión que resultará del uso

de los Bienes o parte de ellos, o de cualquier producto generado en asociación o combinación con otro equipo, planta o materiales no suministrados por el Proveedor en virtud del Contrato.

29.2 Si se entablara un proceso o una demanda contra el Comprador como resultado de alguna de las situaciones indicadas en la Subcláusula 29.1 de las CGC, este notificará sin demora al Proveedor y este último, por su propia cuenta y en nombre del Comprador, llevará adelante dicho proceso o reclamo, y realizará las negociaciones necesarias para llegar a un acuerdo respecto de dicho proceso o reclamo.

29.3 Si dentro de los 28 (veintiocho) días posteriores a la fecha en que recibió dicha comunicación el Proveedor no notifica al Comprador de su intención de llevar adelante dicho proceso o reclamo, el Comprador tendrá derecho a iniciar dichas acciones en su propio nombre.

29.4 El Comprador se compromete a prestar al Proveedor, cuando este se lo solicite, toda la asistencia posible para que pueda llevar adelante dicho proceso o reclamo, y el Proveedor le reembolsará todos los gastos razonables que hubiera realizado al hacerlo.

29.5 El Comprador eximirá de toda responsabilidad al Proveedor, así como a sus empleados, funcionarios y Subcontratistas, por cualquier litigio, acción legal o procedimiento administrativo, reclamo, demanda, pérdida, daño, costo y gasto de cualquier naturaleza, incluyendo honorarios y gastos de abogados, que pudieran afectarlo como resultado de cualquier transgresión o supuesta transgresión de derechos de patentes, modelo de utilidad, diseño registrado, marca registrada, derecho de autor u otro derecho de propiedad intelectual registrado o ya existente a la fecha del Contrato que pudiera derivarse de cualquier diseño, dato, plano, especificación, u otros documentos o materiales que hubieran sido suministrados o diseñados por el Comprador o a su nombre.

30. Limitación de responsabilidad

30.1 Excepto en casos de negligencia grave o conducta dolosa,

(a) el Proveedor no tendrá ninguna responsabilidad contractual, extracontractual o de otra índole frente al Comprador por pérdidas o daños indirectos o eventuales, pérdidas de uso, pérdidas de producción, o pérdidas de ganancias o por costo de intereses; esta exclusión no se aplicará a ninguna de las obligaciones del Proveedor de pagar al Comprador los daños y perjuicios previstos en el Contrato; y

(b) la responsabilidad total del Proveedor frente al Comprador, ya sea contractual, extracontractual o de otra índole, no podrá exceder el Precio del Contrato; tal limitación de responsabilidad no se aplicará a los costos provenientes de la reparación o reemplazo de equipos defectuosos ni afecta la obligación del Proveedor de eximir de responsabilidad al Comprador por transgresiones de derechos de patentes.

31. Cambio en las leyes y regulaciones

31.1 A menos que se indique otra cosa en el Contrato, si después de 28 días antes de la fecha de presentación de Ofertas, cualquier ley, reglamento, decreto, ordenanza o estatuto con carácter de ley entrase en vigencia, se promulgase, se derogase o se modificase en el lugar del País del Comprador donde está ubicado el Emplazamiento del Proyecto (incluyendo cualquier cambio en la interpretación o aplicación por parte de las autoridades competentes) que afecte posteriormente la Fecha de Entrega o el Precio del Contrato, dicha Fecha de Entrega o Precio del Contrato se incrementarán o reducirán según corresponda, en la medida en que el Proveedor se haya visto afectado por estos cambios en el cumplimiento de obligaciones derivadas del Contrato. Sin perjuicio de ello, dicho incremento o disminución del costo no se pagará separadamente ni se acreditará si ya se ha tenido en cuenta en las disposiciones de ajuste de precio cuando corresponda, de conformidad con la Cláusula 15 de las CGC.

32. Fuerza Mayor

32.1 El Proveedor no estará sujeto a la ejecución de su Garantía de Cumplimiento, liquidación por daños y perjuicios o terminación por incumplimiento en la medida en que la demora o el incumplimiento de sus obligaciones en virtud del Contrato sea el resultado de un evento de Fuerza Mayor.

32.2 A los fines de esta cláusula, por "Fuerza Mayor" se entiende un evento o situación fuera del control del Proveedor que es imprevisible, inevitable y no se origina por descuido o negligencia del Proveedor. Tales eventos pueden incluir, entre otros, actos del Comprador en su capacidad soberana, guerras o revoluciones, incendios, inundaciones, epidemias, restricciones de cuarentena y embargos de cargamentos.

32.3 Si se produce un hecho de Fuerza Mayor, el Proveedor notificará al Comprador, por escrito y sin demora, de dicha situación y de su causa. A menos que el Comprador disponga otra cosa por escrito, el Proveedor seguirá cumpliendo con las obligaciones que le impone el Contrato en la medida en que sea razonablemente práctico, y buscará todos los medios alternativos de cumplimiento que no estuviesen afectados por la situación de Fuerza Mayor existente.

33. Órdenes de cambio y enmiendas al Contrato

33.1 El Comprador podrá, en cualquier momento, ordenar al Proveedor, mediante notificación conforme a lo dispuesto en la Cláusula 8 de las CGC, que realice cambios dentro del alcance general del Contrato en uno o más de los siguientes aspectos:

(a) planos, diseños o especificaciones, cuando los Bienes que deban suministrarse en virtud al Contrato hayan de fabricarse específicamente para el Comprador;

(b) la forma de embarque o de embalaje;

(c) el lugar de entrega; y

(d) los Servicios Conexos que deba brindar el Proveedor.

33.2 Si cualquiera de estos cambios causara un aumento o disminución en el costo o en el tiempo necesario para que el Proveedor cumpla cualquiera de las disposiciones del Contrato, se realizará un ajuste equitativo al Precio del Contrato o al Cronograma de Entregas y de Cumplimiento, o a ambas cosas, y el Contrato se modificará según corresponda. El Proveedor deberá presentar la solicitud de ajuste conforme a lo establecido en esta cláusula dentro de los 28 (veintiocho) días contados a partir de la fecha en que reciba la solicitud de la orden de cambio del Comprador.

33.3 Los precios que cobrará el Proveedor por Servicios Conexos que pudieran ser necesarios, pero que no fueron incluidos en el Contrato, deberán convenirse previamente entre las partes y no excederán los precios que el Proveedor cobra habitualmente a terceros por servicios similares.

33.4 **Ingeniería de valor:** El Proveedor podrá preparar una propuesta de ingeniería de valor en cualquier momento durante la ejecución del Contrato, y correrá con los gastos realizados en tal preparación. La propuesta de ingeniería de valor deberá incluir, como mínimo, lo siguiente:

(a) los cambios propuestos y una descripción de la diferencia respecto de los requisitos contractuales existentes;

(b) un análisis exhaustivo de costos/beneficios de los cambios propuestos, incluidas una descripción y una estimación de los costos (entre ellos, los correspondientes al ciclo de vida útil) que el Comprador pueda sufragar durante la implementación de la propuesta de ingeniería de valor; y

(c) una descripción de los efectos del cambio en el rendimiento y la funcionalidad.

El Comprador podrá aceptar la propuesta de ingeniería de valor si en esta se demuestran beneficios que permitan:

(a) acelerar el período de entrega;

(b) reducir el Precio del Contrato o los costos del ciclo de vida útil para el Comprador;

(c) mejorar la calidad, eficiencia o sostenibilidad de los Bienes; o

(d) aportar cualquier otro beneficio al Comprador, sin poner en riesgo las funciones necesarias de las Instalaciones.

Si el Comprador aprueba la propuesta de ingeniería de valor y su implementación genera:

(a) una reducción en el Precio del Contrato; el monto que se ha de pagar al Proveedor será equivalente al porcentaje indicado **en las CEC** de la reducción del Precio del Contrato; o

(b) un aumento en el Precio del Contrato, pero conlleva una reducción de los costos de la vida útil debido a cualquiera de los beneficios descritos en los incisos (a) a (d) anteriores, el monto que se ha de pagar al Proveedor será equivalente al aumento total en el Precio del Contrato.

33.5 Con sujeción a lo anterior, no se introducirá ningún cambio o modificación al Contrato excepto mediante enmienda por escrito firmada por ambas partes.

34. Prórroga de los plazos

34.1 Si en cualquier momento durante la ejecución del Contrato el Proveedor o sus Subcontratistas encontrasen condiciones que impidiesen la entrega oportuna de los Bienes o la finalización de los Servicios Conexos de conformidad con la Cláusula 13 de las CGC, el Proveedor informará de inmediato y por escrito al Comprador sobre la demora, la posible duración y la causa. Tan pronto como sea posible después de recibir la comunicación del Proveedor, el Comprador evaluará la situación y, a su discreción, podrá prorrogar el plazo de cumplimiento del Proveedor. En tal caso, ambas Partes ratificarán la prórroga mediante una enmienda al Contrato.

34.2 Excepto en caso de Fuerza Mayor, como se dispone en la Cláusula 32 de las CGC, cualquier retraso en el cumplimiento de sus obligaciones de Entrega y Finalización expondrá al Proveedor a la imposición de liquidación por daños y perjuicios de conformidad con la Cláusula 26 de las CGC, a menos que se acuerde una prórroga en virtud de la Subcláusula 34.1 de las CGC.

35. Resolución

35.1 Resolución por incumplimiento

(a) El Comprador, sin perjuicio de otros recursos previstos para casos de incumplimiento del Contrato, podrá resolver el Contrato en su totalidad o en parte enviando una notificación de incumplimiento por escrito al Proveedor:

(i) si el Proveedor no entrega alguno o ninguno de los Bienes dentro del período establecido en el Contrato, o dentro de alguna prórroga otorgada por el Comprador conforme a lo establecido en la Cláusula 34 de las CGC;

(ii) si el Proveedor no cumple con cualquier otra obligación derivada del Contrato; o

(iii) si el Proveedor, a juicio del Comprador, durante el proceso de Licitación o de ejecución del Contrato, ha participado en actos de fraude y corrupción, según se define en el párrafo 2.2 (a) del Apéndice 1 de las CGC.

(b) En caso de que el Comprador rescinda el Contrato en su totalidad o en parte, de conformidad con lo dispuesto en la Cláusula 35.1 (a) de las CGC, podrá adquirir, en los términos y condiciones que considere apropiados, Bienes o Servicios Conexos similares a los no suministrados o no prestados, y el Proveedor deberá pagar al Comprador los costos adicionales resultantes de dicha adquisición. Sin embargo, el Proveedor seguirá cumpliendo las obligaciones derivadas de la parte del Contrato que no se hubiese rescindido.

35.2 Resolución por insolvencia.

(a) El Comprador podrá resolver el Contrato notificando de ello por escrito al Proveedor si este se declarase en quiebra o en estado de insolvencia. En tal caso, la resolución no conllevará indemnización alguna para el Proveedor, siempre que no perjudique ni afecte algún derecho de

acción o recurso que tenga o pudiera llegar a tener posteriormente hacia el Comprador.

35.3 Resolución por conveniencia.

(a) El Comprador, mediante comunicación enviada al Proveedor, podrá resolver el Contrato total o parcialmente, en cualquier momento, por razones de conveniencia. La comunicación de resolución deberá indicar que esta se debe a la conveniencia del Comprador, el alcance de la extinción de las responsabilidades del Proveedor en virtud del Contrato y la fecha de entrada en vigencia de dicha resolución.

(b) Los Bienes que ya estén fabricados y listos para embarcar dentro de los 28 (veintiocho) días siguientes a la fecha en que el Proveedor reciba la notificación de resolución del Comprador deberán ser aceptados por el Comprador de acuerdo con los términos y precios establecidos en el Contrato. En cuanto al resto de los Bienes, el Comprador podrá elegir entre las siguientes opciones:

(iv) que se complete alguna porción y se entregue de acuerdo con las condiciones y precios del Contrato; y/o

(v) que se cancele el resto y se pague al Proveedor una suma convenida por aquellos Bienes o Servicios Conexos que se hubiesen completados parcialmente y por los materiales y repuestos adquiridos previamente por el Proveedor.

36. Cesión

36.1 El Comprador y Proveedor se abstendrán de ceder total o parcialmente las obligaciones que hubiesen contraído en virtud del Contrato, salvo que cuenten con el consentimiento previo por escrito de la otra parte.

37. Restricciones a la exportación

37.1 No obstante cualquier obligación incluida en el Contrato de cumplir con todas las formalidades de exportación, cualquier restricción de exportación atribuible al Comprador, al País del Comprador o al uso de los productos/bienes, sistemas o servicios que se proveerán, que provenga de regulaciones comerciales de un país proveedor de los productos/bienes, sistemas o servicios, y que impida que el Proveedor cumpla con sus obligaciones contractuales, liberará al Proveedor de la obligación de proveer bienes o servicios. Lo anterior tendrá efecto siempre y cuando el Proveedor pueda demostrar, a satisfacción del Banco y el Comprador, que ha cumplido puntualmente con todas las

formalidades, tales como la solicitud de permisos, autorizaciones y licencias necesarias para la exportación de los productos/bienes, sistemas o servicios de acuerdo con los términos del Contrato. El Contrato se resolverá sobre esta base para conveniencia del Comprador conforme a lo estipulado en la Subcláusula 35.3.

APÉNDICE 1

Fraude y Corrupción

(El texto de este anexo no deberá modificarse)

1. Propósito

1.1 Las Directrices del Banco de Lucha Contra la Corrupción y este anexo se aplicarán a las adquisiciones en el marco de las operaciones de Financiamiento para Proyectos de Inversión del Banco.

2. Requisitos

2.1 El Banco exige que los Prestatarios (incluidos los beneficiarios del financiamiento del Banco), licitantes (postulantes / proponentes), consultores, contratistas y proveedores, todo subcontratista, subconsultor, prestadores de servicios o proveedores, todo agente (haya sido declarado o no), y todo miembro de su personal, observen las más elevadas normas éticas durante el proceso de adquisición, la selección y la ejecución de contratos financiados por el Banco, y se abstengan de prácticas fraudulentas y corruptas.

2.2 Con ese fin, el Banco:

a. Define de la siguiente manera, a los efectos de esta disposición, las expresiones que se indican a continuación:

i. Por “práctica corrupta” se entiende el ofrecimiento, entrega, aceptación o solicitud directa o indirecta de cualquier cosa de valor con el fin de influir indebidamente en el accionar de otra parte.

ii. Por “práctica fraudulenta” se entiende cualquier acto u omisión, incluida la tergiversación de información, con el que se engañe o se intente engañar en forma deliberada o imprudente a una parte con el fin de obtener un beneficio financiero o de otra índole, o para evadir una obligación.

iii. Por “práctica colusoria” se entiende todo arreglo entre dos o más partes realizado con la intención de alcanzar un propósito ilícito, como el de influir de forma indebida en el accionar de otra parte.

iv. Por “práctica coercitiva” se entiende el perjuicio o daño o la amenaza de causar perjuicio o daño directa o indirectamente a cualquiera de las partes o a sus bienes para influir de forma indebida en su accionar.

v. Por “práctica de obstrucción” se entiende:

(a) la destrucción, falsificación, alteración u ocultamiento deliberado de pruebas materiales referidas a una investigación o el acto de dar falsos testimonios a los investigadores para impedir materialmente que el Banco investigue denuncias de prácticas corruptas, fraudulentas, coercitivas o colusorias, o la amenaza, persecución o intimidación de otra parte para evitar que revele lo que conoce

sobre asuntos relacionados con una investigación o lleve a cabo la investigación, o

(b) los actos destinados a impedir materialmente que el Banco ejerza sus derechos de inspección y auditoría establecidos en el párrafo 2.2 e, que figura a continuación.

b. Rechazará toda propuesta de adjudicación si determina que la empresa o persona recomendada para la adjudicación, los miembros de su personal, sus agentes, subconsultores, subcontratistas, prestadores de servicios, proveedores o empleados han participado, directa o indirectamente, en prácticas corruptas, fraudulentas, colusorias, coercitivas u obstructivas para competir por el contrato en cuestión.

c. Además de utilizar los recursos legales establecidos en el convenio legal pertinente, podrá adoptar otras medidas adecuadas, entre ellas declarar que las adquisiciones están viciadas, si determina en cualquier momento que los representantes del prestatario o de un receptor de una parte de los fondos del préstamo participaron en prácticas corruptas, fraudulentas, colusorias, coercitivas u obstructivas durante el proceso de adquisición, o la selección o ejecución del contrato en cuestión, y que el prestatario no tomó medidas oportunas y adecuadas, satisfactorias para el Banco, para abordar dichas prácticas cuando estas ocurrieron, como informar en tiempo y forma a este último al tomar conocimiento de los hechos.

d. Podrá sancionar, conforme a lo establecido en las Directrices del Banco de Lucha Contra la Corrupción y a sus políticas y procedimientos de sanciones vigentes, a cualquier empresa o persona en forma indefinida o durante un período determinado, lo que incluye declarar a dicha empresa o persona inelegibles públicamente para: (i) obtener la adjudicación o recibir cualquier beneficio, ya sea financiero o de otra índole, de un contrato financiado por el Banco[1]; (ii) ser nominada[2]como subcontratista, consultor, fabricante o proveedor, o prestador de servicios de una firma que de lo contrario sería elegible a la cual se le haya adjudicado un contrato financiado por el Banco, y (iii) recibir los fondos de un préstamo del Banco o participar más activamente en la preparación o la ejecución de cualquier proyecto financiado por el Banco.

e. Exigirá que en los documentos de solicitud de ofertas/propuestas y en los contratos financiados con préstamos del Banco se incluya una cláusula en la que se exija que los licitantes (postulantes /proponentes), consultores, contratistas y proveedores, así como sus respectivos subcontratistas, subconsultores, prestadores de servicios,

[1] A fin de disipar toda duda al respecto, la inelegibilidad de una parte sancionada en relación con la adjudicación de un contrato implica, entre otras cosas, que la empresa o persona no podrá: (i) presentar una solicitud de precalificación, expresar interés en una consultoría, y participar en una licitación, ya sea directamente o en calidad de subcontratista nominado, consultor nominado, fabricante o proveedor nominado, o prestador de servicios nominado, con respecto a dicho contrato, ni (ii) firmar una enmienda mediante la cual se introduzca una modificación sustancial en cualquier contrato existente.

[2] Un subcontratista nominado, consultor nominado, fabricante o proveedor nominado, o prestador de servicios nominado (se utilizan diferentes nombres según el documento de licitación del que se trate) es aquel que: (i) ha sido incluido por el licitante en su solicitud de precalificación u oferta por aportar experiencia y conocimientos técnicos específicos y esenciales que le permiten al licitante cumplir con los requisitos de calificación para la oferta particular; o (ii) ha sido designado por el Prestatario.

proveedores, agentes y personal, permitan al Banco inspeccionar[3]todas las cuentas, registros y otros documentos referidos a la presentación de ofertas y la ejecución de contratos, y someterlos a la auditoría de profesionales nombrados por este.

[3] Las inspecciones que se llevan a cabo en este contexto suelen ser de carácter investigativo (es decir, forense). Consisten en actividades de constatación realizadas por el Banco o por personas nombradas por este para abordar asuntos específicos relativos a las investigaciones/auditorías, como determinar la veracidad de una denuncia de fraude y corrupción a través de los mecanismos adecuados. Dicha actividad incluye, entre otras cosas, acceder a la información y los registros financieros de una empresa o persona, examinarlos y hacer las copias que corresponda; acceder a cualquier otro tipo de documentos, datos o información (ya sea en formato impreso o electrónico) que se considere pertinente para la investigación/auditoría, examinarlos y hacer las copias que corresponda; entrevistar al personal y otras personas; realizar inspecciones físicas y visitas al emplazamiento, y someter la información a la verificación de terceros.

APÉNDICE 2

Declaración de Desempeño en materia de Explotación y Abuso Sexual (EAS) y/o Acoso Sexual (ASx) de los Subcontratistas

[La siguiente Tabla debe ser completada por cada Subcontratista propuesto por el Proveedor que no haya sido designado en el Contrato]

Nombre del Subcontratista: *[indicar el nombre completo]*
Fecha: *[insertar día, mes, año]*
No. y nombre del Contrato: *[insertar la referencia número y nombre]*
Página *[insertar número de página] de [insertar número total] páginas*

Declaración EAS y /o ASx
Nosotros: ☐ (a) no hemos sido objeto de descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS / ASx. ☐ (b) no estamos sujetos a descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS / ASx ☐ (c) hemos sido descalificados por el Banco por incumplimiento de las obligaciones sobre EAS/ASx, pero fuimos excluidos de las empresas descalificadas. Se ha dictado un laudo arbitral en el caso de descalificación a nuestro favor.
[Si (c) anterior es aplicable, adjunte evidencia de un laudo arbitral que revierta las conclusiones sobre los problemas subyacentes a la descalificación.]

Nombre del Subcontratista

Nombre de la persona debidamente autorizada para firmar a nombre del Subcontratista____

Cargo de la Persona que firma a nombre del Subcontratista_____

Firma de la persona designada arriba

Fecha de la firma _____ día de_____, _____

Firma del representante autorizado del Proveedor:

Firma: _____

Fecha de la firma _____ día de _____, _____

Sección IX. Condiciones Especiales del Contrato

Las siguientes Condiciones Especiales del Contrato (CEC) complementarán o enmendarán las Condiciones Generales del Contrato (CGC) y, en caso de conflicto, prevalecerán sobre ellas.

CGC 1.1 (i)	El País del Comprador es: Peru.
CGC 1.1 (j)	El comprador es: Programa Nacional de Telecomunicaciones - PRONATEL.
CGC 1.1 (o)	El destino final del emplazamiento del Proyecto es: Las instalaciones del Edificio de la Central 911, ubicado en la Avenida El Sol S/N, distrito de Chorrillos, provincia y departamento de Lima, donde se ejecutará de manera presencial el servicio objeto del Contrato. Para la implementación del Proyecto, la entrega de los equipos y accesorios previa a su instalación se realizará en el almacén que implemente el Proveedor dentro de las instalaciones de la Central 911, el cual deberá contar con las condiciones físicas, ambientales y de seguridad requeridas, previa coordinación con el Gerente de Proyecto asignados para el Contrato.
CGC 1.1 (p)	El término EAS/ASx se usa en el Contrato con el siguiente significado: • "**Explotación y Abuso Sexual**" **"(EAS)"** significa lo siguiente: La **Explotación Sexual** se define como cualquier abuso o intento de abuso a una posición vulnerable, abuso de poder o de confianza con fines sexuales, que incluyen, entre otros, el aprovechamiento monetario, social o político mediante la explotación sexual de otra persona. El **Abuso Sexual** se define como la amenaza o la intrusión física real de naturaleza sexual, ya sea por la fuerza o bajo condiciones desiguales o coercitivas; • **"Acoso Sexual" "ASx"** se define como avances sexuales indeseables, demanda de favores sexuales, y otras conducta física o verbal de una naturaleza sexual por el Personal del Proveedor con otros miembros del personal del Proveedor, subcontratistas o del personal del Comprador.
CGC 4.2 (a)	El significado de los términos comerciales será el establecido en los Incoterms.
CGC 4.2 (b)	La versión de la edición de los Incoterms será*:* 2020.
CGC 5.1	El idioma será: Español.

CGC 8.1	Para **notificaciones**, la dirección del Comprador será: Atención: UE 1720: Programa Nacional de Telecomunicaciones - PRONATEL. Atención: Gerente de Proyecto asignado al Contrato - (Proyecto 911). Domicilio postal: Av. Paseo de la República Nº 1645 - La Victoria - Lima - Perú. Piso/oficina: 17 Ciudad: Lima Código postal: 15034 País: Peru. Dirección de correo electrónico: crep911@pronatel.gob.pe
CEC 9.1	El derecho aplicable será el de: República del Perú.
CGC 10.2	Las controversias que surjan entre las Partes en relación con este Contrato, incluidas aquellas referidas a su interpretación, ejecución, incumplimiento, resolución, nulidad o validez, serán resueltas definitivamente mediante arbitraje, de conformidad con las siguientes disposiciones: (a) Contrato con Proveedor extranjero: Toda controversia, discrepancia o reclamación derivada de este Contrato o relacionada con él, incluyendo cualquier cuestión relativa a su existencia, validez, interpretación, ejecución, incumplimiento, resolución o terminación, será resuelta mediante arbitraje internacional administrado por el Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú (PUCP). El arbitraje se desarrollará de acuerdo con el Reglamento de Arbitraje de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) vigente a la fecha de inicio del arbitraje, complementado por las normas administrativas del Centro de Arbitraje antes señalado. 1. **Selección de árbitros** a) Cuando las Partes acuerden que la controversia versa principalmente sobre aspectos técnicos, podrán designar de común acuerdo un árbitro único. Si no alcanzan acuerdo dentro de los treinta (30) días calendario siguientes a la solicitud de arbitraje, cualquiera de las Partes podrá solicitar al Centro de Análisis y Resolución de Conflictos de la PUCP la designación del árbitro único.

	b) Cuando las Partes no acuerden que la controversia es de naturaleza técnica o cuando la complejidad del caso así lo requiera, el tribunal arbitral estará conformado por tres (3) árbitros. Cada Parte designará un árbitro y los dos árbitros así designados nombrarán al presidente del tribunal arbitral. Si cualquiera de las designaciones no se realiza dentro de los treinta (30) días calendario correspondientes, o si los árbitros designados no acuerdan el nombramiento del presidente dentro del plazo señalado, la designación pendiente será efectuada por el Centro de Análisis y Resolución de Conflictos de la PUCP. 2. **Reglas de procedimiento** Sin perjuicio de lo establecido en esta cláusula, el procedimiento arbitral se regirá por el Reglamento de Arbitraje CNUDMI vigente a la fecha de inicio del arbitraje y, de manera supletoria, por el Reglamento del Centro de Análisis y Resolución de Conflictos de la PUCP. 3. **Sustitución de árbitros** Si un árbitro renuncia, fallece, es recusado o se encuentra imposibilitado de ejercer sus funciones, será sustituido conforme al mismo procedimiento utilizado para su designación original. 4. **Sede, idioma y ley aplicable** La sede del arbitraje será la ciudad de Lima, Perú. El idioma del arbitraje será el español. El tribunal arbitral decidirá la controversia conforme a la ley sustantiva aplicable al Contrato. 5. **Carácter definitivo** El laudo arbitral será definitivo, vinculante para las Partes y ejecutable conforme a la legislación aplicable. (b) Contrato con Proveedor ciudadano del país del Comprador: Si el Proveedor es ciudadano del país del Comprador, toda controversia derivada o relacionada con este Contrato será resuelta mediante arbitraje institucional administrado por el Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú (PUCP), de conformidad con su Reglamento vigente al momento de la presentación de la solicitud de arbitraje. El tribunal arbitral estará integrado por un árbitro único o por tres árbitros, según corresponda de acuerdo con el Reglamento del Centro de Arbitraje. La sede del arbitraje será Lima, Perú, el idioma será el español y el laudo arbitral será definitivo y vinculante para las Partes.

CGC 13.1	Detalle de los documentos de embarque y otros documentos que deben ser proporcionados por el Proveedor, según corresponda al medio de transporte utilizado, los siguientes documentos: 1. **Factura comercial original** del Proveedor que describa los Bienes, cantidades, precio unitario y valor total del contrato. 2. **Lista de empaque (Packing List)** que identifique el contenido de cada bulto, peso bruto, peso neto y dimensiones. 3. **Documento de transporte**, según corresponda. 4. **Certificado de origen** de los Bienes emitido por la autoridad competente del país de origen, cuando sea aplicable. 5. **Documentos de despacho aduanero de importación**, incluyendo la declaración aduanera y evidencia del pago de derechos, impuestos y demás gravámenes aplicables, de conformidad con el Incoterm DDP, cuando sea aplicable. 6. **Certificados de calidad o conformidad del fabricante**, cuando sea aplicable. 7. **Manual de operación, mantenimiento y documentación técnica**, cuando sea aplicable. 8. **Certificado de garantía del fabricante o proveedor**. 9. **Acta o constancia de entrega en el lugar de destino**, firmada por el representante del Comprador o la entidad receptora.
CGC 14.10	**<u>Se agrega:</u>** El Proveedor deberá contar con normas de conducta aplicables a su personal y garantizar la sensibilización y capacitación correspondiente, a fin de que el personal encargado de la ejecución de los Servicios Relacionados, incluyendo cuando corresponda las actividades de **instalación, operación y/o mantenimiento del equipamiento ofimático y de redes LAN**, mantenga un ambiente de trabajo seguro, respetuoso y libre de cualquier forma de explotación, abuso o acoso sexual. En tal sentido, el personal del Proveedor deberá abstenerse de participar en las siguientes conductas: (i) **Cualquier forma de acoso sexual**, incluyendo insinuaciones sexuales no deseadas, solicitudes de favores sexuales, comentarios, gestos, conductas verbales o físicas de naturaleza sexual dirigidas al personal del Comprador, del Proveedor o de terceros vinculados con la ejecución del Contrato; (ii) **Cualquier forma de explotación sexual**, entendida como el abuso real o intento de abuso de una situación de vulnerabilidad, una relación de poder o una posición de confianza con fines sexuales, incluyendo, entre otros, la

	obtención de beneficios económicos, sociales o políticos derivados de la explotación sexual de otra persona; (iii) **Cualquier forma de abuso sexual**, entendido como la intrusión física real o amenaza de intrusión de naturaleza sexual, ya sea mediante el uso de la fuerza, coerción o bajo condiciones de desigualdad o vulnerabilidad; y (iv) **Cualquier actividad sexual con personas menores de dieciocho (18) años**, salvo cuando exista un matrimonio legalmente reconocido previo conforme a la normativa aplicable. **CGC 14.10.2** El Comprador podrá solicitar al Proveedor el retiro inmediato del sitio de ejecución del Contrato, o de cualquier otro lugar donde se desarrollen los Servicios Relacionados de **instalación, operación y/o mantenimiento del equipamiento ofimático y de redes LAN**, de cualquier miembro de su personal que incurra en conductas contrarias a las normas de conducta establecidas en la CGC 14.10.1. Ante dicha solicitud, y sin perjuicio de cualquier obligación adicional de reemplazo que establezca el Comprador, el Proveedor deberá retirar o disponer el retiro inmediato de dicha persona del lugar de ejecución de los Servicios Relacionados. En todos los casos, cuando corresponda, el Proveedor deberá designar oportunamente un reemplazo idóneo que cuente con competencias, experiencia y calificaciones equivalentes, garantizando la continuidad adecuada de la prestación de los Servicios Relacionados.
CGC 15.1	Los precios de los Bienes suministrados y los Servicios Conexos prestados no serán ajustables.
CGC 16.1	La forma y las condiciones de pago al Proveedor en virtud del Contrato serán las siguientes: El Proveedor deberá presentar la solicitud de pago acompañada del certificado de conformidad correspondiente emitido por el Comprador, que acredite que los bienes han sido recibidos y/o que los servicios contratados han sido prestados de conformidad con las condiciones del Contrato, a través de la Mesa de Partes de la UE 1720: Programa Nacional de Telecomunicaciones – PRONATEL, adjuntando obligatoriamente la documentación requerida. El pago se realizará dentro de los treinta (30) días siguientes a la presentación de la solicitud de pago acompañada de la totalidad de la documentación requerida. El incumplimiento o la presentación incompleta de la documentación suspenderá el trámite de pago hasta su total subsanación.

	El pago se realizará en la moneda de la oferta, de la siguiente manera: **(i)Al recibir los bienes:** El ochenta por ciento (80 %) del valor ofertado de los bienes efectivamente entregados y conformados en el lugar de destino final, contra la presentación de los documentos especificados en la Cláusula 13.1 de las CGC. Podrán efectuarse pagos parciales en función de las entregas efectivamente realizadas y conformadas, calculados proporcionalmente sobre el valor ofertado de los bienes correspondientes a cada entrega. En conjunto, dichos pagos no podrán exceder el ochenta por ciento (80 %) del valor total ofertado de los bienes. **(ii) Contra Aceptación Operativa de la solución:** El veinte por ciento (20 %) restante del valor total ofertado de los bienes será pagado una vez culminadas satisfactoriamente las actividades de instalación, configuración, integración, pruebas y comisionamiento, previa suscripción del Acta de Aceptación Operativa y emisión de la conformidad correspondiente por parte del Comprador. **(iii) Servicios conexos:** El cien por ciento (100 %) del valor ofertado de cada Servicio Conexo, conforme a la Lista de Precios que forma parte del Contrato, será pagado mediante cuatro (4) pagos trimestrales, cada uno equivalente al veinticinco por ciento (25 %) del valor ofertado del respectivo servicio, previa conformidad del Comprador respecto de las prestaciones ejecutadas durante cada trimestre. El período de doce (12) meses de prestación de los Servicios Conexos se computará a partir de la fecha establecida en el Acta de Aceptación Operativa.
CGC 16.5	El plazo de pago después del cual el Comprador deberá pagar intereses al Proveedor es de 30 días. La tasa de interés que se aplicará es la publicada en el Banco Central de Reserva del Perú.
CGC 18.1	Si se requiere una Garantía de Cumplimiento, esta deberá presentarse en la forma de una Garantía Bancaria. El monto de la Garantía Bancaria deberá ser equivalente al 10% del monto total del Contrato y deberá mantenerse vigente hasta la entrega y conformidad de los bienes suministrados, incluida su instalación. Una vez emitida la aceptación operativa de los bienes e iniciada la prestación de los servicios conexos, el monto de la Garantía de Cumplimiento se reducirá al 5% del valor del Contrato, manteniéndose vigente hasta el cumplimiento satisfactorio de dichos servicios.

CGC 18.3	Si se requiere una Garantía de Cumplimiento, esta deberá presentarse en la forma de: **Garantía Bancaria** en **la moneda del monto del contrato.** Esta garantía tendrá carácter irrevocable, solidaria, incondicional, sin beneficio de excusión, de realización automática y será emitida por un banco que se encuentre bajo la supervisión de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.
CGC 18.4	La liberación de la Garantía de Cumplimiento será previa solicitud por escrito, al cumplimiento de la entrega total de los bienes y servicios conexos materia del contrato.
CGC 23.2	El Proveedor será responsable de que el embalaje, rotulado, identificación y documentación de los Bienes sean adecuados y suficientes para garantizar su protección, conservación, manipulación, transporte, almacenamiento, identificación y entrega en el Lugar de Destino Final indicado en el Contrato. El embalaje deberá ser nuevo y apropiado para equipos de tecnologías de la información (TI), de conformidad con las buenas prácticas comerciales y las recomendaciones del fabricante, a fin de evitar daños, deterioro o pérdida durante el transporte y almacenamiento hasta su recepción final. Todos los bultos deberán estar debidamente rotulados e identificados de manera clara, legible e indeleble. El rotulado deberá incluir, como mínimo, la siguiente información: a) Nombre o razón social del Proveedor; b) Descripción de los Bienes; c) Cantidad contenida en cada bulto; d) Número de serie, cuando corresponda; e) Número del Contrato; f) Referencia al Proyecto 911; y g) Cualquier otra información necesaria para la correcta identificación y control de los Bienes. Asimismo, cada entrega deberá estar acompañada de la documentación correspondiente, incluyendo, según resulte aplicable, guía de remisión, lista de empaque (packing list), relación de números de serie, certificados, garantías,

	manuales y cualquier otro documento exigido en las Especificaciones Técnicas o en el Contrato. La Entidad Contratante verificará el cumplimiento de las presentes disposiciones durante la recepción de los Bienes. En caso de detectarse deficiencias en el embalaje, rotulado, identificación o documentación, la Entidad podrá formular las observaciones correspondientes y requerir al Proveedor su subsanación, sin costo adicional para la Entidad y sin perjuicio de las demás obligaciones y responsabilidades previstas en el Contrato.
CGC 24.1	La cobertura de seguro se ajustará a lo establecido en los Incoterms.
CGC 24.2	Se agrega: El Proveedor será responsable por la custodia, conservación y protección de los Bienes desde su entrega y hasta la emisión del Informe de Conformidad Final por parte del Comprador, asumiendo los riesgos de pérdida, daño o deterioro durante el transporte, almacenamiento, instalación, configuración, integración, pruebas y puesta en operación de la solución. El Proveedor deberá contar con los seguros que resulten necesarios para cubrir dichos riesgos durante la ejecución contractual, manteniéndolos vigentes hasta la emisión del Informe de Conformidad Final. Las primas, deducibles y demás costos asociados serán asumidos íntegramente por el Proveedor. Asimismo, el personal que participe en las actividades de instalación, configuración, integración y pruebas deberá contar con los seguros laborales exigibles conforme a la normativa aplicable.
CGC 25.1	La responsabilidad por el transporte de los Bienes se ajustará a lo establecido en los Incoterms.
CGC 25.2	Los servicios incidentales que deberá suministrar el Proveedor, incluidos en el precio del Contrato, comprenden como mínimo: a) La instalación, configuración, parametrización e implementación integral del equipamiento y servicios conexos objeto del Contrato. b) El suministro de toda herramienta, utilidad, licencia temporal o recurso técnico necesario para la correcta instalación, configuración, pruebas y operación inicial de la solución. c) La entrega de manuales técnicos y funcionales actualizados, en idioma español, incluyendo como mínimo: • Manual de instalación. • Manual de administración. • Manual de operación. • Manual de mantenimiento y soporte.

	• Documentación técnica de configuración y parametrización. d) La prestación de servicios de soporte técnico durante el período de garantía establecido en el Contrato, incluyendo mantenimiento correctivo, atención de incidencias y asistencia remota o presencial cuando sea requerida. e) La capacitación del personal designado por el Comprador en la administración, operación, mantenimiento funcional y uso del software implementado, tanto en las instalaciones del Comprador como mediante sesiones virtuales cuando corresponda. f) La asistencia técnica durante las pruebas de aceptación, puesta en producción y estabilización de la solución. Todos los costos asociados a los servicios incidentales descritos precedentemente se consideran incluidos en el precio total del Contrato y no generarán pagos adicionales para el Comprador.
CGC 26.1	Las inspecciones y pruebas del equipamiento y servicios conexos se realizarán por cuenta y costo del Proveedor e incluirán, como mínimo, las siguientes actividades: a. Revisión de la documentación técnica y funcional entregada por el Proveedor. b. Verificación de la correcta instalación, configuración e integración del equipamiento con la infraestructura tecnológica existente de la Central de Emergencia 911. c. Pruebas funcionales para verificar el cumplimiento de todos los requisitos técnicos y funcionales establecidos en las Especificaciones Técnicas. d. Pruebas de rendimiento, estabilidad y disponibilidad del sistema. e. Pruebas de seguridad y control de acceso, cuando correspondan. f. Pruebas de integración con sistemas internos y externos definidos en el alcance del proyecto. g. Pruebas de puesta en producción y estabilización operativa. El Proveedor deberá notificar al Comprador con una anticipación mínima de cinco (5) días hábiles respecto de la fecha programada para la ejecución de cualquier prueba formal de aceptación. El Proveedor presentará informes documentados de resultados de cada fase de pruebas, incluyendo incidencias detectadas, acciones correctivas implementadas y evidencias de cumplimiento.

	La aceptación final de la solución estará condicionada a la aprobación satisfactoria de todas las pruebas establecidas y a la subsanación de cualquier observación formulada por el Comprador.
CGC 26.2	Las inspecciones y pruebas se realizarán en: a) Las instalaciones de la Central de Emergencia 911, ubicadas en Av. El Sol S/N, distrito de Chorrillos, Lima, Perú. b) Las instalaciones del Proveedor, cuando se trate de pruebas preliminares, pruebas de fábrica o validaciones previas a la instalación, pudiendo el Comprador participar presencial o remotamente.
CGC 27.1	El valor de la liquidación por daños y perjuicios será: El valor de la liquidación por daños y perjuicios será de cero comas cinco por ciento (0,5 %) por cada semana o fracción de semana de retraso, calculado sobre el precio de los bienes no entregados o de los servicios conexos no prestados oportunamente, conforme al Contrato.
CGC 28.3	**a) <u>Período de validez de la Garantía</u>:** El período de validez de la Garantía será de **365 (trescientos sesenta y cinco) días calendario**, equivalentes a **doce (12) meses**, contados a partir de la **fecha establecida en el Acta firmada en la Aceptación Operativa** de la totalidad de los bienes, sistemas y componentes por parte del Comprador. Para fines de la Garantía, el (los) lugar(es) de destino final(es) será(n): **Las instalaciones de la Central de Emergencia 911, ubicadas en Av. El Sol S/N, distrito de Chorrillos, Lima, Perú**, donde los bienes serán instalados, integrados, probados y puestos en operación. **b) <u>Alcance de la garantía</u>:** El Proveedor garantiza que los bienes suministrados cumplirán con todas las especificaciones técnicas, funcionales, de desempeño, interoperabilidad y disponibilidad establecidas en el Contrato durante todo el período de garantía. **c) <u>Obligaciones del Proveedor</u>:** Si durante el período de garantía los bienes o cualquier parte de ellos no cumplen con las condiciones de funcionamiento, desempeño o calidad establecidas en el Contrato, el Proveedor deberá, a elección del Comprador: **(i) <u>Corrección sin costo</u>** Realizar, sin costo adicional para el Comprador, todas las reparaciones, ajustes, modificaciones o reemplazos necesarios para restablecer el cumplimiento de las garantías contractuales, incluyendo la repetición de pruebas conforme a la Cláusula 26.7 de las CGC.

	(ii) <u>Daños liquidados por incumplimiento de garantía</u> En caso de incumplimiento reiterado o imposibilidad de corrección dentro de un plazo razonable, el Proveedor deberá pagar daños liquidados al Comprador por incumplimiento de la garantía contractual. La cuantía de dichos daños liquidados será la conforme a la Cláusula 27.1 de las CGC y a lo previsto en los Documentos de Licitación. **(iii) <u>Alcance adicional:</u>** El Proveedor deberá cumplir con todas las garantías adicionales de funcionamiento, disponibilidad, compatibilidad e integración establecidas en el Contrato, las cuales se considerarán complementarias a la presente garantía. El incumplimiento de dichas garantías no exime al Proveedor de sus demás obligaciones contractuales ni limita la aplicación de las Cláusulas 27 y 35 de las CGC.
CGC 28.5, CGC 28.6	El plazo para reparar o reemplazar los bienes defectuosos será de cinco (5) días calendario contados a partir de la notificación efectuada por el Comprador. Durante el período de garantía, el Proveedor deberá cumplir con las condiciones de garantía y soporte establecidas en las Especificaciones Técnicas, incluyendo la prestación de soporte técnico 24 horas al día, 7 días a la semana (24x7) en sitio (on-site) y un tiempo máximo de respuesta de cuatro (4) horas. La reparación o reemplazo de los bienes defectuosos deberá realizarse sin costo alguno para el Comprador, incluyendo mano de obra, repuestos, licencias, transporte, instalación, configuración, pruebas y cualquier otro gasto necesario para restablecer las condiciones de funcionamiento previstas en el Contrato. Cuando la reparación definitiva no pueda completarse dentro del plazo establecido, el Proveedor deberá proporcionar temporalmente, sin costo adicional para el Comprador, equipos, componentes o soluciones de reemplazo de características técnicas iguales o superiores que permitan mantener la continuidad operativa de la Central de Emergencia 911 hasta la solución definitiva. Si el Proveedor no corrige los defectos o no reemplaza los bienes dentro del plazo señalado, el Comprador podrá adoptar las medidas necesarias para remediar la situación, directamente o mediante terceros, por cuenta y riesgo del Proveedor y sin perjuicio de cualquier otro derecho o recurso previsto en el Contrato.

CGC 33.4	**Ingeniería de valor** Si el Comprador aprueba la propuesta de ingeniería del valor, el monto que se pagará al Proveedor será equivalente al setenta por ciento (70 %) de la reducción en el precio del Contrato resultante de la implementación de dicha propuesta.

Sección X. Formularios del Contrato

Esta Sección contiene formularios que, una vez completados, formarán parte del Contrato. Los formularios para la Garantía de Cumplimiento y para la Garantía por Pago de Anticipo, cuando sean requeridas, deberán ser completados solamente por el Licitante seleccionado luego de la adjudicación del Contrato.

Índice de Formularios

Carta de Aceptación……..…….…….298
Convenio de Contrato…….……299
Garantía de Cumplimiento…….……301
Garantía Bancaria por Pago de Anticipo Garantía a demanda…….……303

Carta de Aceptación

[utilice papel con membrete del Comprador]

[Fecha]

Para:*[nombre y dirección del Proveedor]*

Asunto: ***Notificación de la Adjudicación del Contrato n.º:***

Por medio de la presente le hacemos saber que nuestra Agencia ha decidido aceptar su Oferta de fecha ***[indique fecha]*** para la ejecución de ***[indique el nombre del Contrato y el número de identificación, según se indica en las CEC]***, por el Precio del Contrato aceptado de ***[indique el precio del Contrato en números y letras y la moneda]***, con las correcciones y modificaciones realizadas según las Instrucciones a los Licitantes.

Se le solicita que presente (i) la Garantía de Cumplimiento dentro de un plazo de 28 días, de acuerdo con las Condiciones del Contrato; para ello, deberá utilizar el formulario de Garantía de Cumplimiento.

Firma de la persona autorizada:
Nombre y cargo del firmante:
Nombre de la Agencia:

Adjunto: Convenio de Contrato.

Convenio de Contrato

[El Licitante seleccionado completará este formulario de acuerdo con las instrucciones indicadas].

ESTE CONVENIO DE CONTRATO se celebra

el día *[indique **número**]* de *[indique **mes**]* de *[indique **año**]*

ENTRE

(1) *[Indique nombre completo del Comprador], [indique la descripción de la entidad jurídica, por ejemplo, agencia del Ministerio de ... del Gobierno de {indique el nombre del País del Comprador}, o sociedad constituida al amparo de las leyes de {indique el nombre del País del Comprador}]*, con sede principal en *[indique la dirección del Comprador]* (en adelante, el "Comprador"), y

(2) *[Indique el nombre del Proveedor]*, sociedad constituida al amparo de las leyes de *[indique el nombre del país del Proveedor]* con sede principal en *[indique la dirección del Proveedor]* (en adelante, el "Proveedor").

POR CUANTO el Comprador ha llamado a licitación respecto de ciertos Bienes y Servicios Conexos, a saber, *[indique una breve descripción de los Bienes y Servicios]*, y ha aceptado una Oferta del Proveedor para el suministro de dichos Bienes y Servicios.

El Comprador y el Proveedor acuerdan lo siguiente:

1. En este Convenio las palabras y expresiones tendrán el mismo significado que se les asigne en los respectivos documentos del Contrato a que se refieran.

2. Los siguientes documentos constituyen el Contrato entre el Comprador y el Proveedor, y serán leídos e interpretados como parte integral del Contrato. Este Convenio prevalecerá sobre los demás documentos del Contrato.

   (a) la Carta de Aceptación;

   (b) la Carta de la Oferta;

   (c) las enmiendas n.° _____ (si las hubiera);

   (d) las Condiciones Especiales del Contrato;

   (e) las Condiciones Generales del Contrato;

   (f) los requerimientos técnicos (incluyendo los Requisitos de los Bienes y Servicios Conexos y las Especificaciones Técnicas);

   (g) las listas completas (incluyendo las Listas de Precios);

(h) cualquier otro documento enumerado en las CGC como parte integrante del Contrato.

3. Como contraprestación por los pagos que el Comprador hará al Proveedor conforme a lo estipulado en este Contrato, el Proveedor se compromete a suministrar los Bienes y Servicios al Comprador y a subsanar los defectos de estos en total consonancia con las disposiciones del Contrato.

4. El Comprador se compromete a pagar al Proveedor, como contraprestación por el suministro de los Bienes y Servicios Conexos y la subsanación de sus defectos, el Precio del Contrato o las sumas que resulten pagaderas de conformidad con lo dispuesto en el Contrato en el plazo y en la forma prescriptos en este.

EN PRUEBA DE CONFORMIDAD, las Partes han suscripto el presente Convenio, de conformidad con el derecho vigente de *[indique el nombre de la ley del país que gobierna el Contrato]* en el día, mes y año antes indicados.

En representación del Comprador

Firma: *[firma]*
en calidad de *[indique el cargo u otra designación apropiada]*
en presencia de *[indique la identificación del testigo]*

En representación del Proveedor

Firma: *[firmas de los representantes autorizados del Proveedor]*
en calidad de *[indique el cargo u otra designación apropiada]*
en presencia de *[indique la identificación del testigo]*

Garantía de Cumplimiento

Opción 1: (Garantía bancaria)

[El banco, a solicitud del Licitante seleccionado, completará este formulario de acuerdo con las instrucciones indicadas].

[Membrete del Garante o código de identificación SWIFT].

Beneficiario: *[Indique el nombre y la dirección del Comprador].*

Fecha: *[Indique la fecha de la emisión].*

GARANTÍA DE CUMPLIMIENTO N.°: *[Indique número de referencia de la Garantía].*

Garante: *[Indique el nombre y la dirección del emisor de la garantía, a menos que esté indicado en el membrete].*

Se nos ha informado que *[indique el nombre del Proveedor, que, en el caso de APCA, será el de la APCA]* (en adelante, el "Solicitante") ha celebrado el Contrato n.° *[indique número de referencia del Contrato]*, de fecha *[indique fecha]*, con el Beneficiario, para el suministro de *[indique nombre del contrato y breve descripción de los Bienes y Servicios Conexos]* (en adelante, el "Contrato").

Además, entendemos que, de acuerdo con las condiciones del Contrato, se requiere una Garantía de Cumplimiento.

A solicitud del Solicitante, nosotros, en calidad de Garantes, por medio de la presente Garantía nos obligamos irrevocablemente a pagar al Beneficiario una suma (o sumas) que no exceda *[indique la(s) suma(s) en cifras y en letras]* (_____)[1]. Dichas sumas se pagarán en los tipos y las proporciones de monedas en las que se debe pagar el Precio del Contrato, cuando recibamos la demanda del Beneficiario, respaldada por la declaración del Beneficiario, ya sea en la misma demanda o en un documento aparte firmado para acompañar o identificar la demanda, en la que se indique que el Solicitante incumplió las obligaciones contraídas en el marco del Contrato, sin necesidad de que el Beneficiario tenga que probar o aducir causa o razón alguna de su demanda o la suma especificada en ella.

10*[indique el número]* de *[indique el mes]* de *[indique el año]*[2], y cualquier reclamación de pago al amparo de ella deberá ser recibida por nosotros en la oficina mencionada arriba a más tardar en esa fecha.

---

[1] *El Garante deberá especificar una suma que represente el porcentaje del monto aceptado del Contrato que se detalla en la Carta de Aceptación y que esté denominada ya sea en la(s) moneda(s) del Contrato o en una moneda de libre convertibilidad aceptable al Beneficiario.*

11Cámara de Comercio Internacional (CCI) relativas a las garantías contra primera solicitud, revisión de 2010, publicación n.° 758 de la CCI; queda excluida de la presente la declaración de respaldo del inciso (a) del artículo 15 de dichas reglas.

_____

[firma(s)]

Nota: El texto en cursiva (incluidas las notas de pie de página) se incluye al solo efecto de preparar el presente formulario y deberá eliminarse en la versión definitiva.

---

[2] *Consigne una fecha 28 días posteriores a la fecha prevista para la finalización, como se describe en la Cláusula 18.4 de las CGC. El Comprador deberá advertir que, en caso de prórroga del plazo para cumplimiento del Contrato, el Comprador deberá solicitar al Garante una extensión de esta Garantía. Dicha solicitud deberá formularse por escrito y presentarse antes de la fecha de vencimiento establecida en la Garantía. Al preparar esta Garantía, el Comprador podría considerar la posibilidad de agregar el siguiente texto al final del penúltimo párrafo del Formulario: "El Garante acepta una sola extensión de esta Garantía por un plazo no superior a [seis meses] [un año], en respuesta a una solicitud por escrito de dicha extensión formulada por el Beneficiario, la que nos será presentada antes del vencimiento de la Garantía".*

Garantía Bancaria por Pago de Anticipo
Garantía a demanda

[Membrete del Garante o código de identificación SWIFT].

Beneficiario: *[Indique el nombre y la dirección del Comprador].*

Fecha: *[Indique la fecha de la emisión].*

GARANTÍA POR PAGO DE ANTICIPO N.°: *[Indique número de referencia de la Garantía].*

Garante: *[Indique el nombre y la dirección del emisor de la garantía, a menos que esté indicado en el membrete].*

Se nos ha informado que *[indique el nombre del Proveedor, que, en el caso de APCA, será el de la APCA]* (en adelante, el "Solicitante") ha celebrado el Contrato n.° *[indique número de referencia del Contrato]*, de fecha *[indique fecha]* con el Beneficiario, para el suministro de *[indique nombre del contrato y breve descripción de los Bienes y Servicios Conexos]* (en adelante, el "Contrato").

Asimismo, entendemos que, de acuerdo con las condiciones del Contrato, se hará un anticipo por la suma de *[indique el monto en cifras]* (____) *[indique el monto en palabras]* contra una garantía por pago de anticipo.

A solicitud del Solicitante, nosotros, en calidad de Garantes, por medio de la presente Garantía nos obligamos irrevocablemente a pagar al Beneficiario una suma (o sumas) que no exceda *[indique la(s) suma(s) en cifras y en letras]* (_____)[1] al recibo en nuestras oficinas de la demanda conforme a los requisitos del Beneficiario, respaldada por una declaración del Beneficiario, ya sea en la demanda propiamente dicha o en un documento aparte firmado que acompañe o identifique la demanda, donde conste que el Solicitante:

(d) 12para la provisión de los Bienes, o

[1] *El Garante deberá especificar una suma que represente el monto del pago por anticipado que esté denominada ya sea en la(s) moneda(s) del pago por anticipado que se indica(n) en el Contrato o en una moneda de libre convertibilidad aceptable al Comprador.*

(e) no ha cumplido con el reembolso del pago por anticipo de acuerdo con las condiciones del Contrato, especificando el monto que el Solicitante no ha reembolsado.

En virtud de esta Garantía se podrá presentar un reclamo a partir del momento en que el Garante presente un certificado del banco del Beneficiario en el que se indique que el pago mencionado arriba se ha acreditado en la cuenta número *[indique número]* que el Solicitante mantiene en *[indique el nombre y la dirección del banco del Solicitante]*.

El monto máximo de esta garantía se reducirá gradualmente en la misma cantidad de reembolsos de pagos anticipados que realice el Solicitante conforme se indica en las copias de los estados o certificados de pago provisionales que se nos deberán presentar. Esta garantía vencerá, a más tardar, en el momento en que recibamos una copia del certificado provisional de pago en el que se indique que se ha certificado para pago el 90 % (noventa por ciento) del monto aceptado del Contrato, o bien el día _____ de _____, 20___ (lo que ocurra primero). En consecuencia, cualquier reclamo de pago realizado en virtud de esta garantía deberá recibirse en nuestra oficina a más tardar en la fecha señalada.

Esta garantía está sujeta a las Reglas Uniformes de la Cámara de Comercio Internacional relativas a las garantías contra primera solicitud, revisión de 2010, publicación n.° 758 de la CCI; queda excluida de la presente la declaración de respaldo del inciso (a) del artículo 15 de dichas reglas.

_____

[firma(s)]

Nota: El texto en cursiva (incluidas las notas de pie de página) se incluye al solo efecto de preparar el presente formulario y deberá eliminarse en la versión final.

DOCUMENTO ESTÁNDAR DE ADQUISICIONES

Solicitud de Ofertas
Bienes
(Proceso de Licitación de sobre único)

BANCO MUNDIAL
BIRF • AIF

Firmado digitalmente por:
SOLORZANO LEON JACHELINE FIR 45366553 hard
Motivo: Soy el autor del documento
Fecha: 25/08/2026 16:59:05-0500

Firmado digitalmente por TOMY BALTAZAR MARCO ANTONIO
Motivo: Soy el autor del documento
Fecha: 25.08.2026 17:02:50 -05:00

Firmado digitalmente por:
GONZALES SEGOVIA WILFREDO FIR 40215020 hard
Motivo: En señal de conformidad
Fecha: 25/08/2026 16:55:32-0500

Solicitud de Ofertas
Bienes
(Proceso de Licitación de sobre único)

“Adquisición de Equipamiento Ofimático y de Redes LAN para la Central 911 en el marco del Proyecto Creación de un Sistema de Atención de Emergencias, Urgencias e Información mediante un Número Único en Lima Metropolitana y el Callao - Proyecto 911”

SDO Nº: PE-PRONATEL-569321-GO-RFB

Proyecto: “Creación de un Sistema de atención de emergencias, urgencias e información mediante un número único 911 en Lima Metropolitana y el Callao” - Proyecto 911.

Comprador: Programa Nacional de Telecomunicaciones - PRONATEL

País: Perú

Emitido el día: **25 de agosto 2026**

Documento Estándar de Adquisiciones

Índice general

PARTE 1. Procedimientos de la Licitación 2

Sección I. Instrucciones a los Licitantes 3
Sección II. Datos de la Licitación (DDL) 37
Sección III. Criterios de Evaluación y Calificación.....48
Sección IV. Formularios de la Oferta ……..54
Sección V. Países Elegibles……...…….……109
Sección VI. Fraude y Corrupción……..111

PARTE 2. Requisitos de los Bienes y Servicios Conexos…….……114

Sección VII. Requisitos de los Bienes y Servicios Conexos…….……115

PARTE 3. Contrato……255

Sección VIII. Condiciones Generales del Contrato……...258
Sección IX. Condiciones Especiales del Contrato…….284
Sección X. Formularios del Contrato…….297

PARTE 1. Procedimientos de la Licitación

Sección I. Instrucciones a los Licitantes

Índice

A. Disposiciones Generales 5
1. Alcance de la Licitación 5
2. Fuente de Financiamiento 5
3. Fraude y Corrupción 6
4. Licitantes Elegibles 6
5. Elegibilidad de los Bienes y Servicios Conexos 10

B. Contenido del Documento de Solicitud de Ofertas 10
6. Secciones del Documento de Licitación 10
7. Aclaración del Documento de Licitación 11
8. Enmienda del Documento de Licitación 12

C. Preparación de las Ofertas 12
9. Costo de la Oferta 12
10. Idioma de la Oferta 12
11. Documentos que componen la Oferta 12
12. Carta de la Oferta y Lista de Precios 14
13. Ofertas Alternativas 14
14. Precios de la Oferta y Descuentos 14
15. Monedas de la Oferta y de Pago 17
16. Documentos que Establecen la Elegibilidad y Conformidad de los Bienes y Servicios Conexos 17
17. Documentos que Establecen la Elegibilidad y las Calificaciones del Licitante 18
18. Período de Validez de las Ofertas 19
19. Garantía de Mantenimiento de Oferta 19
20. Formato y Firma de la Oferta 22

D. Presentación y Apertura de las Ofertas 23
21. Presentación, Cierre e Identificación de las Ofertas 23
22. Plazo para Presentar las Ofertas 24
23. Ofertas Tardías 24
24. Retiro, Sustitución y Modificación de las Ofertas 24
25. Apertura de las Ofertas 25

E. Evaluación y Comparación de las Ofertas 27
26. Confidencialidad 27
27. Aclaración de las Ofertas 27
28. Desviaciones, Reservas y Omisiones 27
29. Determinación del Cumplimiento de las Ofertas 28
30. Falta de Conformidad, Errores y Omisiones 29

31. Corrección de Errores Aritméticos 29
32. Conversión a una Sola Moneda 30
33. Margen de Preferencia 30
34. Evaluación de las Ofertas.....30
35. Comparación de las Ofertas 32
36. Ofertas Excesivamente Bajas.....32
37. Calificación del Licitante 33
38. Derecho del Comprador a Aceptar Cualquier Oferta y a Rechazar Cualquiera o Todas las Ofertas 33

F. Adjudicación del Contrato 34

39. Criterios de Adjudicación 34
40. Derecho del Comprador a Variar las Cantidades en el Momento de la Adjudicación 34
41. Notificación de Adjudicación del Contrato 34
42. Firma del Contrato 35
43. Garantía de Cumplimiento.....36

Sección I. Instrucciones a los Licitantes

A. Disposiciones Generales

1. Alcance de la Licitación

1.1 En relación con el Anuncio Específico de Adquisiciones: Solicitud de Ofertas (SDO), especificado **en los Datos de la Licitación (DDL)**, el Comprador, que se indica **en los DDL**, emite este documento de licitación para la adquisición de los Bienes y, si corresponde, de cualesquiera Servicios Conexos que puedan ser necesarios, conforme a lo especificado en la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos". El nombre, la identificación y la cantidad de lotes (contratos) de esta SDO **se especifican en los DDL**.

1.2 Para todos los efectos de este documento de licitación:

(a) Por el término "por escrito" se entiende comunicación en forma escrita (por ejemplo, por correo postal, correo electrónico, fax, incluso, si así **se especifica en los DDL**, aquella enviada o recibida a través del sistema electrónico de adquisiciones utilizado por el Comprador) con prueba de recibo.

(b) Si el contexto así lo requiere, "singular" significa "plural" y viceversa.

(c) Por "día" se entiende día calendario, salvo que se especifique lo contrario mediante la expresión "días hábiles". Son días hábiles todos los días laborables del Prestatario. Se excluyen los feriados oficiales del Prestatario.

2. Fuente de Financiamiento

2.1 El Prestatario o Beneficiario (en adelante, el "Prestatario") **indicado en los DDL** ha solicitado o recibido financiamiento (en adelante, "fondos") del Banco Internacional de Reconstrucción y Fomento (BIRF) o de la Asociación Internacional de Fomento (IDA) (en adelante denominados el "Banco Mundial" o el "Banco") por el monto **mencionado en los DDL**, para el proyecto especificado **en los DDL**. El Prestatario destinará una porción de dichos fondos para efectuar pagos elegibles en virtud del contrato para el cual se emite este documento de licitación.

2.2 El Banco efectuará pagos solamente a pedido del Prestatario y una vez que los haya aprobado de conformidad con los términos y las condiciones establecidos en el Convenio de Préstamo (u otro tipo de financiamiento). El Convenio de Préstamo (u otro tipo de financiamiento) prohíbe el retiro de fondos de la cuenta de Préstamo para pagos de cualquier naturaleza a personas o entidades, o para cualquier importación de bienes, si dicho pago o importación ha sido prohibido por decisión del Consejo de Seguridad de las Naciones Unidas en virtud del capítulo VII de la Carta de las Naciones Unidas. Ninguna otra parte más que el Prestatario podrá derivar derecho alguno del Préstamo (u otro tipo de financiamiento) o reclamar los fondos.

3. Fraude y Corrupción

3.1 El Banco requiere el cumplimiento de sus Directrices Contra el Fraude y la Corrupción y de sus políticas y procedimientos de sanciones vigentes incluidos en el Marco de Sanciones del Grupo del Banco Mundial, conforme se describe en la Sección VI, “Fraude y Corrupción”.

3.2 En virtud de esta política, los Licitantes deberán permitir al Banco —y requerir que lo permitan sus agentes (hayan sido declarados o no), subcontratistas, subconsultores, prestadores de servicios, proveedores y personal— inspeccionar todas las cuentas, registros y otros documentos relativos a cualquier procesos de selección inicial o precalificación, las presentaciones de ofertas o propuestas y la ejecución de contratos (en el caso de adjudicación), y disponer que sean auditados por auditores designados por el Banco.

4. Licitantes Elegibles

4.1 Un Licitante puede ser una firma que sea una entidad privada, una empresa o ente estatal de acuerdo con la Instrucción a los Licitantes (IAL) 4.6, o una combinación de ellas, bajo la forma de una Asociación en Participación, Consorcio o Asociación (“APCA”), a través de un convenio existente o con la presentación de una carta de intención que manifieste su voluntad de celebrar el convenio que formalice la conformación de dicha APCA. En el caso de una APCA, todos sus miembros serán solidariamente responsables por la ejecución de la totalidad del Contrato, de acuerdo con sus términos. La APCA deberá designar un Representante, que deberá estar facultado para llevar a cabo todos los

procedimientos y gestiones en nombre de cualquiera y todos los miembros de la APCA durante el proceso de la licitación y, en el caso de que la APCA fuera adjudicataria, durante la ejecución del Contrato. Salvo que se especifique **en los DDP**, no existe límite en el número de miembros de una APCA.

4.2 Ningún Licitante podrá tener conflictos de interés. Cualquier Licitante que se determine que tiene conflictos de interés será descalificado. A los fines de este proceso de Licitación, se considerará que un Licitante tiene conflictos de interés si:

(a) Controla de manera directa o indirecta a otro Licitante, es controlado de manera directa o indirecta por otro Licitante o es controlado junto a otro Licitante por una entidad en común;

(b) recibe o ha recibido subsidios directos o indirectos de otro Licitante;

(c) tiene el mismo representante legal que otro Licitante;

(d) tiene una relación con otro Licitante, directamente o a través de terceros en común, que lo coloca en una posición de influir en la oferta de otro Licitante, o de influir en las decisiones del Comprador en relación con este proceso de Licitación;

(e) cualquiera de sus filiales ha participado como consultora en la preparación del diseño o especificaciones técnicas de los bienes y servicios conexos que constituyen el objeto de la Oferta;

(f) cualquiera de sus filiales ha sido contratada (o se propone para ser contratada) por el Comprador o por el Prestatario para la ejecución del Contrato;

(g) proveerá bienes, obras o servicios distintos de los de consultoría que resulten o estén directamente relacionados con servicios de consultoría para la preparación o implementación del proyecto especificado en la IAL 2.1 de los DDL que fue provisto o fuera provisto por cualquier filial que directa o indirectamente controle, sea controlada por esa firma o esté bajo su control común, o

(h) posee una estrecha relación comercial o familiar con un algún profesional del Prestatario (o de la agencia

de implementación del proyecto, o del receptor de una parte del préstamo) que (i) esté directa o indirectamente relacionado con la preparación del documento de licitación o las especificaciones del Contrato, o el proceso de evaluación de la Oferta de ese Contrato, o (ii) pudiera estar relacionado con la ejecución o supervisión de ese Contrato, a menos que el conflicto derivado de tal relación haya sido resuelto de manera aceptable para el Banco durante el proceso de Licitación y la ejecución del Contrato.

4.3 Una firma que sea Licitante (ya sea en forma individual o como miembro de una Asociación en Participación, Consorcio o Asociación ("APCA") no podrá participar en más de una oferta, salvo en el caso de las ofertas alternativas permitidas. Esto incluye su participación en calidad de subcontratista. Tal participación redundará en la descalificación de todas las ofertas en las que haya estado involucrada la firma en cuestión. Por su parte, una firma que no sea Licitante ni tampoco parte de una APCA podrá participar en calidad de subcontratista en más de una Oferta.

4.4 Un Licitante podrá tener la nacionalidad de cualquier país, sujeto a las restricciones establecidas en la IAL 4.8. Se considerará que un Licitante tiene la nacionalidad de un país cuando esté constituido o inscripto en ese país y opere de conformidad con sus leyes, de lo cual deberán dar cuenta sus estatutos (o documentos de constitución o asociación equivalentes) o sus documentos de registro, en caso de corresponder. Estos criterios también se aplicarán para determinar la nacionalidad de los subcontratistas o subconsultores propuestos por cualquiera de las partes del Contrato, incluyendo los servicios conexos.

4.5 Un Licitante que haya sido sancionado conforme a las Directrices del Banco Contra el Fraude y la Corrupción y a sus políticas y procedimientos de sanciones vigentes incluidos en el Marco de Sanciones del Grupo del Banco Mundial, tal como se describe en el párrafo 2.2 (d) de la Sección VI, no podrá ser precalificado para la adjudicación de contratos financiados por el Banco, presentar ofertas a tales efectos ni recibir la adjudicación de dichos contratos, así como tampoco recibir cualquier beneficio, financiero o de otra índole, de un contrato financiado por el Banco durante el período determinado

por este. La lista de firmas inhabilitadas se encuentra disponible en la dirección electrónica que se indica en los DDL.

4.6 Los Licitantes que sean empresas o entes estatales del País del Comprador solamente podrán ser elegibles para competir y recibir la adjudicación de uno o más Contratos si pueden establecer, de forma aceptable para el Banco, que (i) tienen autonomía legal y financiera; (ii) operan conforme a las leyes comerciales, y (iii) no se encuentran bajo la supervisión del Comprador.

4.7 Un Licitante no debe estar suspendido por el Comprador para presentar ofertas como resultado del incumplimiento con una Declaración de Mantenimiento de la Oferta o de la Propuesta.

4.8 Las empresas y las personas podrán ser declaradas inelegibles si así se indica en la Sección V. "Países Elegibles", y (a) si las leyes o reglamentaciones del país del Prestatario prohíben las relaciones comerciales con el país de dichas empresas y personas, siempre y cuando se demuestre, de manera satisfactoria para el Banco, que la exclusión no impedirá la competencia efectiva con respecto al suministro de bienes o la contratación de obras o servicios requeridos, o (b) si, en cumplimiento de una decisión del Consejo de Seguridad de las Naciones Unidas adoptada en virtud del capítulo VII de la Carta de esa institución, el país del Prestatario prohíbela importación de bienes o la contratación de obras o servicios de ese país, o el pago a personas o entidades en ese país.

4.9 Los Licitantes deberán proporcionar al Comprador evidencia documental satisfactoria de su elegibilidad, cuando el Comprador la solicite de manera razonable.

4.10 Una firma a la cual el Prestatario haya impuesto una sanción de inhabilitación que impida que se le adjudique un contrato será elegible para participar en esta adquisición, salvo que el Banco corrobore, a pedido del Prestatario, que la inhabilitación:

(a) está relacionada con un caso de fraude o corrupción; y

(b) se llevó a cabo en cumplimiento de un procedimiento judicial o administrativo en virtud del cual la firma estuvo sujeta al debido proceso.

5. Elegibilidad de los Bienes y Servicios Conexos

5.1 Todos los Bienes y Servicios Conexos que hayan de suministrarse de conformidad con el Contrato y que sean financiados por el Banco podrán tener su origen en cualquier país, de acuerdo con la Sección V, "Países Elegibles".

5.2 A los fines de estas IAL, el término "bienes" incluye mercaderías, materias primas, maquinarias, equipos y plantas industriales; el término "servicios conexos" incluye servicios tales como seguros, instalaciones, capacitación y mantenimiento inicial.

5.3 Por el término "origen" se entiende el país donde los bienes han sido extraídos, cosechados, cultivados, producidos, fabricados o procesados, o, tras su procesamiento, manufactura o ensamblaje, dan como resultado otro artículo reconocido en el ámbito comercial que difiere sustancialmente de las características básicas de sus componentes.

B. Contenido del Documento de Solicitud de Ofertas

6. Secciones del Documento de Licitación

6.1 El documento de licitación está compuesto por las partes 1, 2, y 3, que incluyen todas las secciones que a continuación se indican y deben leerse junto con cualquier enmienda emitida en virtud de la IAL 8.

PARTE 1. Procedimientos de Licitación

- Sección I. Instrucciones a los Licitantes
- Sección II. Datos de la Licitación
- Sección III. Criterios de Evaluación y Calificación
- Sección IV. Formularios de la Oferta
- Sección V. Países Elegibles
- Sección VI. Fraude y Corrupción

PARTE 2. Requisitos de los Bienes y Servicios Conexos

- Sección VII. Requisitos de los Bienes y Servicios Conexos

PARTE 3. Contrato

- Sección VIII. Condiciones Generales del Contrato
- Sección IX. Condiciones Especiales del Contrato
- Sección X. Formularios del Contrato

6.2 El Anuncio Específico de Adquisiciones: Solicitud de Ofertas (SDO) emitido por el Comprador no forma parte de este documento de licitación.

6.3 Salvo que se hubieran obtenido directamente del Comprador, este no se responsabiliza por la integridad del documento, las respuestas a las solicitudes de aclaración, las actas de las reuniones previas a la presentación de Ofertas, si las hubiere, o las enmiendas a los documentos de licitación de acuerdo con la IAL 8. En caso de contradicción, prevalecerán los documentos obtenidos directamente del Comprador.

6.4 Es responsabilidad del Licitante examinar todas las instrucciones, los formularios, los términos y las especificaciones del documento de licitación y presentar toda la información o documentación de la Oferta requerida en dicho documento.

7. Aclaración del Documento de Licitación

7.1 Todo Licitante que requiera alguna aclaración sobre el documento de licitación deberá comunicarse con el Comprador por escrito a la dirección del Comprador que se suministra **en los DDL**. El Comprador responderá por escrito a todas las solicitudes de aclaración, siempre que dichas solicitudes sean recibidas antes del vencimiento del plazo para la presentación de ofertas dentro del período especificado **en los DDL**. El Comprador enviará copia de las respuestas a todos los Licitantes que hubiesen adquirido el documento de licitación de acuerdo con la IAL 6.3, incluyendo una descripción de las consultas realizadas, sin identificar su fuente. Si así estuviera especificado **en los DDL**, el Comprador también deberá publicar prontamente su respuesta en la

página web identificada **en los DDL**. Si como resultado de las aclaraciones surgieran cambios a elementos esenciales del documento de licitación, el Comprador podrá enmendar dicho documento siguiendo el procedimiento indicado en las IAL 8 y 22.2.

8. Enmienda del Documento de Licitación

8.1 El Comprador podrá, en cualquier momento antes del vencimiento del plazo para la presentación de ofertas, enmendar el documento de licitación mediante la emisión de una enmienda.

8.2 Toda enmienda emitida formará parte integral del documento de licitación y deberá ser comunicada por escrito a todos los que hayan obtenido el documento de licitación del Comprador, de acuerdo con la IAL 6.3. El Comprador deberá también publicar prontamente la enmienda en su página web de acuerdo con la IAL 7.1.

8.3 El Comprador podrá, a su discreción, prorrogar el plazo de presentación de ofertas a fin de dar a los posibles Licitantes un plazo razonable para que puedan tomar en cuenta las enmiendas en la preparación de sus Ofertas, de conformidad con la IAL 22.2.

C. Preparación de las Ofertas

9. Costo de la Oferta

9.1 El Licitante financiará todos los costos relacionados con la preparación y presentación de su Oferta, y el Comprador no será responsable en ningún caso por dichos costos, independientemente del desarrollo o del resultado del proceso de Licitación.

10. Idioma de la Oferta

10.1 La oferta, así como toda la correspondencia y los documentos relativos a la Oferta que intercambien el Licitante y el Comprador, deberán ser escritos en el idioma especificado **en los DDL**. Los documentos de respaldo y el material impreso que formen parte de la Oferta podrán estar escritos en otro idioma siempre y cuando vayan acompañados de una traducción fidedigna de las secciones pertinentes al idioma que se especifica **en los DDL**, en cuyo caso la traducción prevalecerá en lo que respecta a la interpretación de la Oferta.

11. Documentos que componen la Oferta

11.1 La Oferta deberá contener los siguientes documentos:

(a) **Carta de la Oferta**, preparada de acuerdo con la IAL 12;

(b) **Listas de Precios** completas, de acuerdo con las IAL 12 y 14;

(c) **Garantía de Mantenimiento de Oferta** o **Declaración de Mantenimiento de Oferta**, de conformidad con la IAL 19.1;

(d) **Oferta Alternativa**, si estas fueran permitidas, de acuerdo con la IAL 13;

(e) **Autorización** escrita que autorice al firmante de la Oferta a comprometer al Licitante, de conformidad con la IAL 20.3;

(f) **Calificaciones:** Prueba documental, de conformidad con la IAL 17, que establezca que el Licitante está calificado para ejecutar el Contrato en caso de que su oferta sea aceptada;

(g) **Elegibilidad del Licitante:** Prueba documental, de conformidad con la IAL 17, que establezca que el Licitante es elegible para presentar una oferta;

(h) **Elegibilidad de los Bienes y Servicios Conexos:** Prueba documental, de conformidad con la IAL 16, que demuestre la elegibilidad de los Bienes y Servicios Conexos que proporcionará el Licitante;

(i) **Cumplimiento de las disposiciones:** Prueba documental, de conformidad con las IAL 16 y 30, que establezca que los Bienes y Servicios Conexos cumplen con las disposiciones del documento de licitación;

(j) Cualquier otro documento requerido **en los DDL**.

11.2 Además de los requisitos estipulados en la IAL 11.1, las ofertas presentadas por una APCA deberán incluir una copia del Convenio de APCA celebrado por todos sus miembros. Alternativamente, se deberá presentar conjuntamente con la Oferta una carta de intención de suscribir un Convenio de APCA, firmada por todos sus miembros, en el caso de que la Oferta sea adjudicada, acompañada de una copia del Convenio propuesto.

11.3 El Licitante deberá suministrar información en la Carta de la Oferta sobre comisiones y gratificaciones, si hubiera, pagadas o por pagarse a agentes u a otra parte relacionada con esta Oferta.

12. Carta de la Oferta y Lista de Precios

12.1. El Licitante presentará la Carta de la Oferta y las Listas de Precios utilizando los formularios suministrados en la Sección IV, Formularios de la Oferta. Estos formularios deberán ser debidamente llenados sin alterar su forma y no se aceptarán sustitutos, excepto según lo dispuesto en la IAL 20.3. Todos los espacios en blanco deberán ser llenados con la información solicitada.

13. Ofertas Alternativas

13.1. A menos que se indique lo contrario **en los DDL**, no se considerarán Ofertas Alternativas.

14. Precios de la Oferta y Descuentos

14.1 Los precios y descuentos cotizados por el Licitante en la Carta de la Oferta y en la Lista de Precios deberán ajustarse a los requerimientos que se indican a continuación.

14.2 Todos los lotes y artículos deberán enumerarse y cotizarse por separado en las Listas de Precios.

14.3 El precio cotizado en la Carta de la Oferta de acuerdo con la IAL 12.1deberá ser el precio total de la Oferta, excluyendo cualquier descuento que se ofrezca.

14.4 El Licitante cotizará cualquier descuento e indicará su método de aplicación en la Carta de la Oferta, de acuerdo con la IAL 12.1.

14.5 Los precios cotizados por el Licitante serán fijos durante la ejecución del Contrato y no estarán sujetos a ninguna variación por ningún motivo, salvo indicación contraria **en los DDL**. Una oferta presentada con precios ajustables no responde a lo solicitado y, en consecuencia, será rechazada de conformidad con la IAL 29. Sin embargo, si, de acuerdo con lo indicado **en los DDL**, los precios cotizados por el Licitante pueden estar sujetos a ajustes durante la ejecución del Contrato, las ofertas que coticen precios fijos no serán rechazadas, y el ajuste de los precios se tratará como si fuera cero.

14.6 Si así se indica en la IAL 1.1, el Llamado a Licitación se hará por Ofertas para lotes individuales (contratos) o para combinación de lotes (grupo de contratos). A menos que se indique lo contrario **en los DDL**, los precios cotizados deberán corresponder al 100 % de los artículos indicados en cada lote y al 100 % de las cantidades indicadas para cada artículo de un lote. Los Licitantes que deseen ofrecer descuentos por la adjudicación de más de un Contrato deberán indicar en su Oferta los descuentos aplicables para cada grupo de contratos o,

alternativamente, para Contratos individuales en el grupo. Los descuentos deberán presentarse de conformidad con la IAL 14.4, siempre y cuando las ofertas por todos los lotes sean presentadas y abiertas al mismo tiempo.

14.7 Las expresiones "EXW", "CIP" y otros términos afines se regirán por las normas prescritas en la edición vigente de Incoterms, publicada por la Cámara de Comercio Internacional, según lo especificado **en los DDL**.

14.8 Los precios deberán cotizarse como se indica en cada lista de precios incluida en la Sección IV, "Formularios de la Oferta". El desglose de los componentes de los precios se requiere con el único propósito de facilitar al Comprador la comparación de las Ofertas. Esto no limitará de ninguna manera el derecho del Comprador de contratar en cualquiera de los términos ofrecidos. Al cotizar los precios, el Licitante podrá incluir costos de transporte cotizados por empresas transportadoras registradas en cualquier país elegible, de conformidad con la Sección V, "Países Elegibles". Asimismo, el Licitante podrá adquirir servicios de seguros de cualquier país elegible de conformidad con la Sección V, "Países Elegibles". Los precios deberán registrarse de la siguiente manera:

(a) Para Bienes fabricados en el País del Comprador:

(i) el precio de los Bienes cotizados EXW (taller, fábrica, bodega, sala de exhibición o en existencia, según corresponda), incluyendo todos los derechos de aduana y los impuestos a la venta o de otro tipo ya pagados o por pagar sobre los componentes y materia prima utilizada en la fabricación o ensamblaje de los Bienes;

(ii) todo impuesto a las ventas u otro tipo de impuesto que obligue el País del Comprador a pagar sobre los Bienes en caso de ser adjudicado el Contrato al Licitante;

(iii) el precio de transporte interno, seguros y otros servicios necesarios para hacer llegar los Bienes al destino final (emplazamiento del Proyecto) especificado **en los DDL**.

(b) Para Bienes fabricados fuera del País del Comprador y que serán importados:

(i) el precio de los Bienes, cotizados CIP lugar de destino convenido, en el País del Comprador, según se indica **en los DDL**;

(ii) el precio de transporte interno, seguros y otros servicios locales necesarios para hacer llegar los Bienes del lugar de destino convenido a su destino final (emplazamiento del Proyecto) indicado **en los DDL**.

(c) Para Bienes fabricados fuera del País del Comprador, e importados previamente:

(i) el precio de los Bienes, incluyendo el valor original de importación más cualquier margen (o descuento), más cualquier otro costo relacionado, derechos de aduana y otros impuestos de importación pagados o por pagar sobre los Bienes previamente importados;

(ii) los derechos de aduana y otros impuestos de importación pagados (deberán ser respaldados con prueba documental) o pagaderos sobre los Bienes previamente importados;

(iii) el precio de los Bienes obtenido de la diferencia entre (i) y (ii);

(iv) cualquier impuesto sobre la venta u otro impuesto pagadero en el País del Comprador sobre los Bienes si el Contrato es adjudicado al Licitante;

(v) el precio de transporte interno, seguro y otros servicios locales necesarios para hacer llegar los Bienes al lugar de destino final (emplazamiento del Proyecto) indicado **en los DDL**.

(d) Para los Servicios Conexos distintos del transporte interno y otros servicios necesarios para hacer llegar los Bienes a su destino final, cuando dichos Servicios Conexos estén especificados en la Lista de Requisitos de los Bienes y Servicios Conexos, el precio de cada artículo que comprende los

Servicios Conexos (incluido cualquier impuesto aplicable).

15. Monedas de la Oferta y de Pago

15.1 La(s) moneda(s) de la Oferta y la(s) moneda(s) de pago serán las mismas. El Licitante deberá cotizar en la moneda del País del Comprador la parte del Precio de la Oferta correspondiente a los gastos incurridos en la moneda del País del Comprador, salvo que se estipule lo contrario **en los DDL**.

15.2 El Licitante podrá expresar el Precio de su Oferta en cualquier moneda. Si el Licitante desea recibir el pago en una combinación de montos en diferentes monedas, podrá cotizar su precio en las monedas que correspondan. Sin embargo, no podrá incluir más de tres monedas extranjeras además de la del País del Comprador.

16. Documentos que Establecen la Elegibilidad y Conformidad de los Bienes y Servicios Conexos

16.1 Para establecer la elegibilidad de los Bienes y Servicios Conexos de conformidad con la IAL 5, los Licitantes deberán completar las declaraciones del país de origen en los Formularios de Lista de Precios, incluidos en la Sección IV, "Formularios de la Oferta".

16.2 Con el fin de establecer la conformidad de los Bienes y Servicios Conexos con el documento de licitación, los Licitantes deberán proporcionar, como parte de su Oferta, prueba documental que acredite que los Bienes cumplen con las especificaciones técnicas y los estándares especificados en la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos".

16.3 La prueba documental podrá consistir en material bibliográfico, planos o datos, y deberá incluir una descripción detallada de las características esenciales técnicas y de funcionamiento de cada artículo que demuestre conformidad sustancial de los Bienes y Servicios Conexos con las especificaciones técnicas, y, de ser procedente, una declaración de desviaciones y excepciones a las disposiciones de la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos".

16.4 Los Licitantes también deberán proporcionar una lista detallada que incluya disponibilidad y precios actuales de repuestos, herramientas especiales, etc., necesarios para el funcionamiento adecuado y continuo de los Bienes durante el período **indicado en los DDL**, a partir

del momento en que el Comprador comience a utilizar dichos Bienes.

16.5 Las normas de fabricación, procesamiento, material y equipos, así como las referencias a marcas o a números de catálogos que haya incluido el Comprador en la Lista de Requisitos de los Bienes y Servicios Conexos, son de carácter meramente descriptivo, y no restrictivo. Los Licitantes podrán ofrecer otras normas de calidad, marcas y/o números de catálogo, siempre y cuando demuestren, a satisfacción del Comprador, que las sustituciones son sustancialmente equivalentes o superiores a las especificadas en la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos".

17. Documentos que Establecen la Elegibilidad y las Calificaciones del Licitante

17.1 Para establecer su elegibilidad de conformidad con la IAL 4, los Licitantes deberán completar la Carta de la Oferta, incluida en la Sección IV, "Formularios de la Oferta".

17.2 La prueba documental de las calificaciones del Licitante para ejecutar el Contrato, si su Oferta es aceptada, deberá establecer, a completa satisfacción del Comprador, que:

(a) si se requiere **en los DDL**, el Licitante que no fabrica ni produce los Bienes que propone proveer deberá presentar una autorización del fabricante utilizando el formulario incluido en la Sección IV, "Formularios de la Oferta", para demostrar que ha sido debidamente autorizado por el fabricante o productor de los Bienes para suministrarlos en el País del Comprador;

(b) si se requiere **en los DDL**, en el caso de un Licitante que no esté establecido comercialmente en el País del Comprador, el Licitante está o estará (si se le adjudica el Contrato) representado por un agente en el País del Comprador equipado y con capacidad para cumplir con las obligaciones de mantenimiento, reparaciones y almacenamiento de repuestos del Proveedor estipuladas en las condiciones del Contrato y/o las especificaciones técnicas;

(c) el Licitante cumple con cada uno de los criterios de calificación estipulados en la Sección III, "Criterios de Evaluación y Calificación".

18. Período de Validez de las Ofertas

18.1. Las ofertas deberán mantener su validez hasta la fecha especificada **en los DDL** o cualquier fecha extendida si el Comprador la modifica de conformidad con la IAL 8. Una Oferta que no sea válida hasta la fecha especificada en **los DDL**, o cualquier fecha extendida por el Comprador de conformidad con la IAL 8, será rechazada por el Comprador por incumplimiento.

18.2. En circunstancias excepcionales, antes de la fecha de expiración de la validez de la Oferta, el Comprador podrá solicitar a los Licitantes que extiendan el período de la validez de sus Ofertas. Las solicitudes y las respuestas deberán hacerse por escrito. Si se hubiese solicitado una Garantía de Mantenimiento de Oferta, de acuerdo con la IAL 19, también esta deberá prorrogarse por el período correspondiente. Un Licitante puede rechazar tal solicitud sin que ello implique la pérdida de su Garantía de Mantenimiento de Oferta. Al Licitante que acepte la solicitud de prórroga no se le pedirá ni permitirá modificar su Oferta, salvo en los casos previstos en la IAL 18.3.

18.3. Si la adjudicación se retrasase por un período mayor a 56 (cincuenta y seis) días a partir del vencimiento de la validez inicial de la Oferta, el precio del Contrato será determinado de la siguiente forma:

(a) en el caso de contratos con precio fijo, el precio del Contrato será el precio de la Oferta ajustado según el factor especificado **en los DDL**;

(b) en el caso de contratos con precio ajustable, no se harán ajustes;

(c) en todos los casos, la evaluación de la Oferta deberá basarse en el precio cotizado sin tomar en cuenta la corrección aplicable que corresponda según los casos indicados arriba.

19. Garantía de Mantenimiento de Oferta

19.1. El Licitante deberá presentar, como parte de su Oferta, una Garantía de Mantenimiento de Oferta o una Declaración de Mantenimiento de Oferta, según lo especificado **en los DDL**, en formulario original, y, en el caso de una Garantía de Mantenimiento de Oferta, por el monto y en la moneda especificados **en los DDL**.

19.2. Para la Declaración de Mantenimiento de Oferta se utilizará el formulario incluido en la Sección IV, "Formularios de la Oferta".

19.3. Si, según lo especificado en la IAL 19.1, se debe presentar una Garantía de Mantenimiento de Oferta, esta deberá ser una garantía a primer requerimiento emitida por una institución de prestigio de un país elegible y deberá tener cualquiera de las siguientes formas, a opción del Licitante:

(a) una garantía incondicional emitida por un banco o una institución financiera no bancaria (como una compañía de seguros, fianzas o avales);

(b) una carta de crédito irrevocable;

(c) un cheque de gerencia o cheque certificado;

(d) otra garantía especificada **en los DDL**,

emitida por una institución de prestigio de un país elegible. Si una garantía incondicional es emitida por una institución financiera no bancaria localizada fuera del país del Comprador, la institución financiera no bancaria deberá tener una institución financiera corresponsal ubicada en el país del Comprador para hacer efectiva la garantía, salvo que el Comprador haya acordado por escrito, antes de la presentación de la Oferta, que la existencia de dicha institución financiera corresponsal no es obligatoria. En el caso de una garantía bancaria, la Garantía de Mantenimiento de Oferta deberá presentarse utilizando el Formulario de Garantía de Mantenimiento de Oferta incluido en la Sección IV, "Formularios de la Oferta", o en otro formato sustancialmente similar aprobado por el Comprador antes de la presentación de la Oferta. La Garantía de Mantenimiento de Oferta tendrá una validez de veintiocho (28) días a partir de la fecha original de expiración de la validez de la Oferta o de cualquier fecha extendida, si ésta se hubiera solicitado de conformidad con lo establecido en la IAL 18.2.

19.4. Si se exige una Garantía de Mantenimiento de Oferta de conformidad con la IAL 19.1, todas las Ofertas que no estén acompañadas de una Garantía de Mantenimiento de Oferta que se ajuste sustancialmente a los requisitos pertinentes serán rechazadas por el Comprador por incumplimiento.

19.5. Si en la IAL 19.1 se establece la obligación de presentar una Garantía de Mantenimiento de Oferta, las Garantías de Mantenimiento de Oferta de los Licitantes cuyas ofertas no fueron seleccionadas serán devueltas tan pronto como sea posible una vez que el Licitante seleccionado firme el Contrato y provea la Garantía de Cumplimiento, de conformidad con la IAL 46.

19.6. La Garantía de Mantenimiento de Oferta del Licitante seleccionado será devuelta tan pronto como sea posible una vez que el Licitante seleccionado suscriba el Contrato y proporcione la Garantía de Cumplimiento.

19.7. La Garantía de Mantenimiento de Oferta podrá hacerse efectiva o la Declaración de Mantenimiento de Oferta podrá ejecutarse si:

(a) un Licitante retira su Oferta antes de la fecha de expiración de la validez de la Oferta especificada por el Licitante en la Carta de la Oferta, o cualquier fecha extendida otorgada por el Licitante; o

(b) el Licitante seleccionado:

(i) no suscribe el Contrato de conformidad con lo dispuesto en la IAL 45, o

(ii) no suministra una Garantía de Cumplimiento de conformidad con lo dispuesto en la IAL 46.

19.8. La Garantía de Mantenimiento de Oferta o la Declaración de Mantenimiento de Oferta de una APCA se emitirán en nombre de la Asociación que presenta la Oferta. Si la APCA no se hubiera constituido formalmente como entidad jurídica al momento de presentar la Oferta, la Garantía de Mantenimiento de Oferta o la Declaración de Mantenimiento de Oferta se emitirán en nombre de todos los futuros miembros que figuren en la carta de intención mencionada en las IAL 4.1 y 11.2.

19.9. Si **en los DDL** no se exige una Garantía de Mantenimiento de Oferta según se estipula en la IAL 19.1, y si

(a) un Licitante retira su Oferta antes de la fecha de expiración de la validez de la Oferta estipulada por

el Licitante en la Carta de la Oferta o cualquier fecha extendida otorgada por el Licitante; o

(b) el Licitante seleccionado:

(i) no suscribe el Contrato con arreglo a lo dispuesto en la IAL 45; o

(ii) no proporciona una Garantía de Cumplimiento de conformidad con la IAL 46,

el Prestatario podrá, si así se dispone **en los DDL**, declarar al Licitante inelegible para ser adjudicatario de un contrato otorgado por el Comprador por el período que se especifique **en los DDL**.

20. Formato y Firma de la Oferta

20.1 El Licitante preparará un original de los documentos que comprenden la Oferta según se describe en la IAL 11 y lo marcará claramente como "ORIGINAL". Las Ofertas Alternativas, si son admitidas de acuerdo con la IAL 13, deberán estar claramente marcadas como "ALTERNATIVA". Además, el Licitante deberá presentar el número de copias de la Oferta **que se indica en los DDL** y marcar claramente cada ejemplar como "COPIA". En caso de discrepancia, el texto del original prevalecerá sobre el de las copias.

20.2 Los Licitantes deberán marcar como "CONFIDENCIAL" la información incluida en sus Ofertas que revista carácter confidencial para sus empresas. Esto puede incluir información reservada, secretos comerciales o información delicada de índole comercial o financiera.

20.3 El original y todas las copias de la Oferta deberán mecanografiarse o escribirse con tinta indeleble, y deberán estar firmadas por la persona debidamente autorizada para firmar en nombre del Licitante. Esta autorización consistirá en una confirmación escrita de acuerdo con lo especificado **en los DDL** y se adjuntará a la Oferta. El nombre y el cargo de cada persona que firme la autorización deberán mecanografiarse o escribirse en letra de imprenta bajo la firma. Todas las páginas de la Oferta que contengan anotaciones o enmiendas deberán estar firmadas o inicialadas por la persona que suscriba la Oferta.

20.4 En el caso de que el Licitante sea una APCA, la Oferta deberá estar firmada por un representante autorizado de la APCA en nombre de esta y en representación

legalmente vinculante para actuar en nombre de todos los miembros, formalizado por un poder firmado por sus representantes legales.

20.5 Los textos entre líneas, borraduras o palabras superpuestas serán válidos solamente si llevan la firma o las iniciales de la persona que firma la Oferta.

D. Presentación y Apertura de las Ofertas

21. Presentación, Cierre e Identificación de las Ofertas

21.1. El Licitante deberá presentar la Oferta en un único sobre cerrado (proceso de Licitación con mecanismo de sobre único), en cuyo interior deberá colocar los siguientes sobres cerrados:

(a) un sobre identificado como "ORIGINAL", que contendrá todos los documentos que componen la Oferta, como se describe en la IAL 11;

(b) un sobre identificado como "COPIAS", que contendrá las copias de la Oferta que se hubieran solicitado;

(c) si se permiten Ofertas alternativas según lo dispuesto en la IAL 13 y, si corresponde:

i un sobre identificado como "ORIGINAL: OFERTA ALTERNATIVA", donde se colocará la Oferta alternativa,

ii un sobre identificado como "COPIAS: OFERTA ALTERNATIVA", donde se colocarán todas las copias de la Oferta alternativa que se hubieran solicitado.

21.2. Los sobres interiores y exteriores deberán:

(a) llevar el nombre y la dirección del Licitante;

(b) estar dirigidos al Comprador de acuerdo con lo indicado en la IAL 22.1;

(c) llevar la identificación específica de este proceso de Licitación indicada en la IAL 1.1; y

(d) llevar la advertencia de no abrir antes de la hora y fecha de apertura de Ofertas.

21.3. Si los sobres no están cerrados e identificados como se requiere, el Comprador no se responsabilizará en caso de que la Oferta se extravíe o sea abierta prematuramente.

22. Plazo para Presentar las Ofertas

22.1. El Comprador deberá recibir las Ofertas en la dirección y, a más tardar, en la fecha y hora que se especifican **en los DDL**. Cuando así se especifique **en los DDL**, los Licitantes tendrán la opción de enviar sus Ofertas de forma electrónica. Los Licitantes que opten por esta modalidad, deberán ajustarse a los procedimientos de presentación electrónica de Ofertas establecidos **en los DDL**.

22.2. El Comprador podrá, a su discreción, extender el plazo para la presentación de Ofertas mediante una enmienda al documento de licitación, de conformidad con la IAL 8. En este caso, todos los derechos y las obligaciones del Comprador y de los Licitantes previamente sujetos al plazo original para presentar las ofertas quedarán sujetos al plazo prorrogado.

23. Ofertas Tardías

23.1. El Comprador no considerará ninguna Oferta que llegue con posterioridad al término del plazo para la presentación de Ofertas, de conformidad con lo dispuesto en la IAL 22. Toda Oferta que reciba el Comprador después del plazo para la presentación de las Ofertas será declarada tardía, rechazada y devuelta al Licitante sin abrir.

24. Retiro, Sustitución y Modificación de las Ofertas

24.1. Un Licitante podrá retirar, sustituir o modificar su Oferta después de presentada mediante el envío de una comunicación por escrito, debidamente firmada por un representante autorizado; que deberá incluir una copia de la autorización (poder) de acuerdo con lo estipulado en la IAL 20.3 (con excepción de la comunicación de retiro, que no requiere copias). La Oferta sustitutiva o la modificación deberán adjuntarse a la respectiva comunicación por escrito. Todas las comunicaciones deberán ser:

(a) preparadas y presentadas de conformidad con las IAL 20 y 21 (con excepción de la comunicación de retiro, que no requiere copias) y, además, los respectivos sobres deberán llevar claramente indicado "RETIRO", "SUSTITUCIÓN" o "MODIFICACIÓN"; y

(b) recibidas por el Comprador antes de que venza el plazo establecido para la presentación de las Ofertas, de conformidad con la IAL 22.

24.2. Las ofertas cuyo retiro fue solicitado de conformidad con la IAL 24.1 se devolverán sin abrir a los Licitantes.

24.3. Ninguna Oferta podrá retirarse, sustituirse ni modificarse durante el intervalo comprendido entre la fecha límite para la presentación de Ofertas y el vencimiento del período de Validez de la Oferta indicado por el Licitante en la Carta de Oferta o cualquier prórroga de ese período.

25. Apertura de las Ofertas

25.1. Salvo en los casos especificados en las IAL 23 y 24.2, el Comprador, en el acto de apertura de las Ofertas, abrirá públicamente y leerá en voz alta todas las Ofertas recibidas antes del vencimiento del plazo indicado, en la fecha, a la hora y en el lugar especificados **en los DDL**, en presencia de los representantes designados por los Licitantes y de cualquier persona que desee asistir. Los procedimientos específicos para la apertura de Ofertas presentadas en forma electrónica, si estuvieran permitidas en virtud de la IAL 22.1, se realizarán conforme a lo dispuesto **en los DDL**.

25.2. Primero se abrirán y leerán en voz alta los sobres marcados "RETIRO"; el sobre con la Oferta correspondiente se devolverá sin abrir al Licitante. Si el sobre del retiro no contiene una copia del "poder" que confirme que el firmante es una persona autorizada por el Licitante para firmar en representación de él, se procederá a abrir la Oferta. No se permitirá el retiro de ninguna Oferta a menos que la respectiva comunicación de retiro contenga la autorización válida para solicitarlo y se lea en voz alta en el acto de apertura de las Ofertas.

25.3. Seguidamente se abrirán los sobres marcados como "SUSTITUCIÓN", los cuales se leerán en voz alta y se intercambiarán con la Oferta correspondiente que se está reemplazando; la Oferta sustituida se devolverá sin abrir al Licitante. No se permitirá ninguna sustitución, a menos que la respectiva comunicación de sustitución contenga una autorización válida para solicitar la sustitución y se lea en voz alta en el acto de apertura de las Ofertas

25.4. A continuación, se abrirán y se leerán en voz alta los sobres marcados con el rótulo "MODIFICACIÓN" con la

Oferta correspondiente. No se permitirá ninguna modificación de Ofertas, a menos que la comunicación de sustitución correspondiente contenga una autorización válida para solicitar la modificación y sea leída en voz alta en el acto de apertura de las Ofertas.

25.5. Luego se abrirán de a uno los demás sobres y se leerá en voz alta la siguiente información: el nombre del Licitante y si se ha presentado alguna modificación; el Precio total de la Oferta, por lote (contrato), si corresponde, incluidos los descuentos u Ofertas alternativas que hubiese; la existencia o inexistencia de Garantía de Mantenimiento de Oferta, si se hubiese solicitado, y cualquier otro detalle que el Comprador juzgue pertinente.

25.6. En la evaluación solo se considerarán las Ofertas, las Ofertas Alternativas y los descuentos abiertos y leídos en voz alta. La Carta de la Oferta y las Listas de Precios deberán ser inicialados por los representantes del Comprador que asistan al acto de apertura de Ofertas, tal como se especifica **en los DDL**.

25.7. El Comprador no discutirá los méritos de las Ofertas ni rechazará ninguna (excepto las Ofertas tardías, según lo dispuesto en la IAL 23.1).

25.8. El Comprador preparará un acta del acto de apertura de las Ofertas que incluirá como mínimo:

(a) el nombre del Licitante y si hubo retiro, sustitución o modificación;

(b) el precio de la Oferta, por lote (contrato) si corresponde, incluyendo cualquier descuento;

(c) cualquier Oferta Alternativa;

(d) la existencia o no de Garantía de Mantenimiento de Oferta o de la Declaración de Mantenimiento de Oferta, de haberse requerido.

25.9. Se solicitará a los representantes de los Licitantes presentes que firmen el acta. La omisión de la firma de uno de los Licitantes en el acta no invalidará el contenido ni los efectos de esta. Se entregará una copia del acta a todos los Licitantes.

E. Evaluación y Comparación de las Ofertas

26. Confidencialidad

26.1 No se divulgará a los Licitantes ni a ninguna persona que no participe oficialmente en el proceso de Licitación, información relacionada con la evaluación de las Ofertas o con la recomendación de adjudicación del contrato hasta que la información sobre la adjudicación del Contrato se haya publicado, con arreglo a la IAL 41.

26.2 Cualquier intento por parte de un Licitante de influenciar al Comprador en las decisiones relacionadas con la evaluación de las Ofertas o en la adjudicación del Contrato podrá resultar en el rechazo de su Oferta.

26.3 No obstante, lo dispuesto en la IAL 26.2, si durante el plazo transcurrido entre el acto de apertura y la fecha de adjudicación del Contrato, un Licitante desea comunicarse con el Comprador sobre cualquier asunto relacionado con el proceso de Licitación, deberá hacerlo por escrito.

27. Aclaración de las Ofertas

27.1 Para facilitar el examen, la evaluación, comparación de las Ofertas y la calificación de los Licitantes, el Comprador podrá, a su discreción, solicitar a cualquier Licitante aclaraciones sobre su Oferta. No se considerarán aclaraciones presentadas por un Licitante cuando nos sean en respuesta a una solicitud del Comprador. La solicitud de aclaración del Comprador y la respuesta deberán constar por escrito. No se solicitará, ofrecerá ni permitirá ninguna modificación, incluidos aumentos o reducciones voluntarios, de los precios o de la sustancia de la Oferta, salvo para confirmar la corrección de errores aritméticos que el Comprador hubiera descubierto durante la evaluación de las Ofertas, de conformidad con lo dispuesto en la IAL 31.

27.2 Si un Licitante no provee las aclaraciones a su Oferta antes de la fecha y hora indicada por el Comprador en su solicitud de aclaraciones de la Oferta, su Oferta puede ser rechazada.

28. Desviaciones, Reservas y Omisiones

28.1 Durante la evaluación de las Ofertas, se aplicarán las siguientes definiciones:

(a) “desviación” es cualquier variación respecto de los requisitos especificados en el documento de licitación;

(b) "reserva" es la imposición de condiciones limitativas o la negativa a aceptar plenamente los requisitos especificados en el documento de licitación;

(c) "omisión" es la falta de presentación de parte o de la totalidad de la información o de la documentación requeridas en el documento de licitación.

29. Determinación del Cumplimiento de las Ofertas

29.1 Para determinar si la Oferta se ajusta sustancialmente al documento de licitación, el Comprador se basará en el contenido de la propia Oferta, según se define en la IAL 11.

29.2 Una Oferta que se ajusta sustancialmente al documento de licitación es aquella que satisface todos los términos, condiciones y especificaciones estipuladas en dicho documento sin desviaciones, reservas u omisiones significativas. Una desviación, reserva u omisión significativa es aquella que:

(a) en caso de ser aceptada:

(i) afectaría de una manera sustancial el alcance, la calidad o el funcionamiento de los Bienes y Servicios Conexos especificados en el contrato;

(ii) limitaría de modo sustancial, incongruente con el documento de licitación, los derechos del Comprador o las obligaciones del Licitante en virtud del Contrato, o

(b) en caso de ser rectificada, afectaría injustamente la posición competitiva de otros Licitantes que presenten Ofertas que se ajusten sustancialmente a lo estipulado.

29.3 El Comprador examinará los aspectos técnicos de la Oferta presentada de acuerdo con las IAL 16 y 17, en particular, para confirmar que se hayan cumplido todos los requisitos de la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos", sin ninguna desviación, reserva ni omisión significativa.

29.4 Si una Oferta no se ajusta sustancialmente al documento de licitación, será rechazada por el Comprador y el Licitante no podrá ajustarla posteriormente mediante la corrección de las desviaciones, reservas u omisiones significativas.

30. Falta de Conformidad, Errores y Omisiones

30.1 Siempre y cuando una Oferta se ajuste sustancialmente al documento de licitación, el Comprador podrá dispensar cualquier falta de conformidad.

30.2 Siempre y cuando una Oferta se ajuste sustancialmente al documento de licitación, el Comprador podrá solicitar al Licitante que, dentro de un plazo razonable, presente la información o la documentación necesarias para corregir las discrepancias u omisiones no significativas relacionadas con requisitos de documentación. Dichas omisiones no podrán estar relacionadas con ningún aspecto del precio de la Oferta. Si el Licitante no cumple con la solicitud, podrá rechazarse su Oferta.

30.3 Siempre y cuando una Oferta se ajuste sustancialmente al documento de licitación, el Comprador corregirá las discrepancias no significativas cuantificables relativas al Precio de la Oferta. A tal efecto, se ajustará el Precio de la Oferta únicamente a los efectos de la comparación, para reflejar el precio de una partida o un componente que falte o en el que se observen discrepancias, un ítem o un componente que falte o en el que se observen discrepancias, agregando el precio promedio del ítem o componente cotizado por los Licitantes que cumplieron sustancialmente. Si el precio del ítem o componente no se puede derivar del precio de otras Ofertas que cumplen sustancialmente, el Comprador deberá utilizar su mejor estimación.

31. Corrección de Errores Aritméticos

31.1 Siempre y cuando la Oferta se ajuste sustancialmente al documento de licitación, el Comprador corregirá los errores aritméticos de la siguiente manera:

(a) Si hay una discrepancia entre un precio unitario y el precio total que se ha obtenido multiplicando el precio unitario por la cantidad correspondientes, prevalecerá el precio unitario y se corregirá el precio total, a menos que, a juicio del Comprador, hubiera un error evidente en la expresión del punto decimal en el precio unitario, en cuyo caso prevalecerá el total cotizado para ese rubro y se corregirá el precio unitario.

(b) Si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán sobre el total y este último deberá ajustarse.

(c) Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras, a menos que este último corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras, de conformidad con los párrafos (a) y (b) precedentes.

31.2 Se pedirá a los Licitantes que acepten la corrección de los errores aritméticos. Si no aceptan la corrección realizada con arreglo a lo dispuesto en la IAL 31.1, su Oferta será rechazada.

32. Conversión a una Sola Moneda

32.1 A los fines de evaluación y comparación, la moneda o las monedas de la Oferta serán convertidas a una sola moneda, tal como se especifica **en los DDL**.

33. Margen de Preferencia

33.1 Salvo que se indique lo contrario **en los DDL**, no se aplicará ningún margen de preferencia.

34. Evaluación de las Ofertas

34.1 El Comprador empleará los criterios y las metodologías enumerados en estas IAL y en la Sección III, "Criterios de Evaluación y Calificación". No se aceptará ningún otro criterio ni metodología de evaluación. Mediante la aplicación de dichos criterios y metodologías, el Comprador determinará cuál es la Oferta más Conveniente, que será la oferta presentada por un Licitante que reúna los criterios de calificación y respecto de la cual se haya determinado que:

(a) se ajusta sustancialmente al documento de licitación; y

(b) tiene el costo evaluado más bajo.

34.2 Al evaluar una Oferta, el Comprador considerará lo siguiente:

(a) la evaluación se hará por artículos o lotes (contratos) de la manera especificada **en los DDL**; el Precio de la Oferta se cotizará conforme a lo establecido en la IAL 14;

(b) el ajuste de precios por corrección de errores aritméticos, conforme a lo establecido en la IAL 31.1;

(c) el ajuste de precios por descuentos ofrecidos, conforme a lo establecido en la IAL 14.4;

(d) la conversión a una moneda única del monto resultante de la aplicación de los apartados (a) a (c) precedentes, si procede, de conformidad con la IAL 32;

(e) el ajuste de precios por falta de conformidad cuantificables, conforme a lo establecido en la IAL 30.3; y

(f) los factores de evaluación adicionales especificados en la Sección III, "Criterios de Evaluación y Calificación".

34.3 En la evaluación de las Ofertas no se tendrá en cuenta el efecto estimado de las disposiciones sobre ajuste de precios que se hayan establecido en las Condiciones Contractuales, aplicadas durante el período de ejecución de este Contrato.

34.4 Si este documento de licitación permite que los Licitantes coticen precios separados para diferentes lotes (contratos), la metodología para determinar el costo evaluado más bajo de las combinaciones de lotes (contratos), incluidos los descuentos ofrecidos en la Carta de la Oferta, se especificará en la Sección III, "Criterios de Evaluación y Calificación".

34.5 Al evaluar una Oferta, el Comprador excluirá y no tendrá en cuenta:

(a) en el caso de Bienes producidos en el País del Comprador, los impuestos sobre las ventas y otros impuestos similares pagaderos sobre los bienes si el Licitante resulta adjudicatario del Contrato;

(b) en el caso de Bienes no producidos en el País del Comprador, previamente importados o que se importarán, los derechos de aduana y otros impuestos a la importación, los impuestos sobre las ventas y otros impuestos similares pagaderos sobre los Bienes si el Licitante resulta adjudicatario del Contrato;

(c) cualquier disposición relativa al ajuste de precios durante el período de ejecución del Contrato, en el caso de que figure en la Oferta.

34.6 La evaluación de una Oferta puede requerir que el Comprador considere otros factores, además del precio

cotizado de conformidad con la IAL 14. Estos factores podrán estar relacionados con las características, el rendimiento, los términos y las condiciones de compra de los Bienes y Servicios Conexos. El efecto de los factores seleccionados, si los hubiere, se expresará en términos monetarios para facilitar la comparación de las Ofertas, a menos que se indique lo contrario en la Sección III, "Criterios de Evaluación y Calificación" **de los DDL**. Se aplicarán los criterios y las metodologías especificados en la IAL 34.2 (f).

35. Comparación de las Ofertas

35.1 El Comprador comparará, conforme a lo establecido en la IAL 34.2, los costos evaluados de todas las Ofertas que se ajusten sustancialmente al documento de licitación, para determinar cuál es la Oferta con el costo evaluado más bajo. La comparación se hará sobre la base de precios CIP (lugar de destino final) en el caso de los bienes importados y precios EXW más el costo de transporte interno y seguro hasta el lugar de destino en el caso de los bienes fabricados dentro del País del Comprador, junto con los precios de cualquier instalación, capacitación, comisiones y otros servicios requeridos. En la evaluación de precios no deberán tenerse en cuenta los impuestos de aduanas y otros impuestos recaudados sobre bienes importados cotizados CIP ni impuestos a las ventas o similares en relación con la venta o distribución de bienes.

36. Ofertas Excesivamente Bajas

36.1 Una Oferta excesivamente baja es aquella cuyo precio, en combinación con otros elementos constitutivos de la Oferta, parece ser tan bajo que despierta serias dudas en el Comprador sobre la capacidad del Licitante para ejecutar el Contrato al precio cotizado.

36.2 En caso de detectar lo que podría constituir una Oferta excesivamente baja, el Comprador pedirá al Licitante que brinde aclaraciones por escrito, y en especial, que presente análisis pormenorizados del Precio de la Oferta en relación con el objeto del contrato, el alcance, la metodología propuesta, el cronograma, la distribución de riesgos y responsabilidades y cualquier otro requisito establecido en el documento de licitación.

36.3 Tras evaluar los análisis de precios, si determina que el Licitante no demostrado su capacidad para ejecutar el Contrato al precio cotizado, el Comprador rechazará la Oferta.

37. Calificación del Licitante

37.1 El Comprador determinará, a su entera satisfacción, si el Licitante elegible seleccionado por haber presentado la Oferta que tiene el costo evaluado más bajo y que se ajusta sustancialmente al documento de licitación, reúne los requisitos de calificación especificados en la Sección III, "Criterios de Evaluación y Calificación".

37.2 La determinación se basará en el examen de las pruebas documentales presentadas por el Licitante para respaldar sus calificaciones, de conformidad con la IAL 17. No se tendrán en cuenta las calificaciones de otras empresas, como las subsidiarias, la casa matriz, las filiales y los subcontratistas (excepto los Subcontratistas Especializados permitidos por el documento de licitación) del Licitante, ni de ninguna otra empresa distinta de este.

37.3 Antes de la adjudicación del Contrato, el Comprador verificará que el Licitante seleccionado (incluyendo cada uno de los miembros de la APCA o JV) no esté descalificado por el Banco como consecuencia del incumplimiento de las obligaciones contractuales de EAS /ASx, El Comprador hará la misma verificación para cada uno de los subcontratistas propuestos por el Licitante seleccionado. Si alguno de los subcontratistas propuestos no cumple con el requisito, el Comprador exigirá que el Licitante proponga un subcontratista sustituto.

37.4 El Comprador determinará, a su entera satisfacción, si el Licitante elegible seleccionado por haber presentado la Oferta que tiene el costo evaluado más bajo y que se ajusta sustancialmente al documento de licitación, reúne los requisitos de calificación especificados en la Sección III, "Criterios de Evaluación y Calificación".

38. Derecho del Comprador a Aceptar Cualquier Oferta y a Rechazar Cualquiera o Todas las Ofertas

38.1 El Comprador se reserva el derecho de aceptar o rechazar cualquier Oferta, de anular el proceso de Licitación y de rechazar todas las Ofertas en cualquier momento antes de la adjudicación del Contrato, sin que por ello adquiera responsabilidad alguna frente a los Licitantes. En caso de anularse el proceso, el Comprador devolverá prontamente a los Licitantes todas las Ofertas y, específicamente, las Garantías de Mantenimiento de Oferta que hubiera recibido.

F. Adjudicación del Contrato

39. Criterios de Adjudicación

39.1 Con sujeción a lo dispuesto en la IAL 38, el Comprador adjudicará el Contrato al Licitante que ofrezca la Oferta más Conveniente, es decir, aquella que ha sido presentada por un Licitante que cumple con los criterios de calificación y que, además:

(a) se ajusta sustancialmente al documento de licitación; y

(b) tiene el costo evaluado más bajo.

40. Derecho del Comprador a Variar las Cantidades en el Momento de la Adjudicación

40.1 Al momento de adjudicar el Contrato, el Comprador se reserva el derecho de aumentar o disminuir la cantidad de los Bienes y Servicios Conexos especificados originalmente en la Sección VII, "Lista de Requisitos de los Bienes y Servicios Conexos", siempre y cuando esta variación no exceda los porcentajes indicados **en los DDL**, ni altere los precios unitarios u otros términos y condiciones de la Oferta y del documento de licitación.

41. Notificación de Adjudicación del Contrato

41.1 Antes de la fecha de expiración de la Validez de la Oferta o de cualquier prórroga otorgada, si la hubiera, el Comprador notificará al Licitante seleccionado, por escrito, que su Oferta ha sido aceptada. En la notificación de adjudicación (denominada adelante y en los Formularios del Contrato, la "Carta de Aceptación") se especificará el monto que pagará al Proveedor por la ejecución del Contrato (denominado en lo sucesivo, así como en las Condiciones Contractuales y en los Formularios del Contrato, el "Precio del Contrato").

41.2 Dentro de los diez (10) días hábiles posteriores a la fecha de transmisión de la Carta de Aceptación, el Comprador publicará la Notificación de la Adjudicación del Contrato, que contendrá, como mínimo, la siguiente información:

(a) el nombre y la dirección del Comprador;

(b) el nombre y el número de referencia del contrato que se está adjudicando y método de selección utilizado;

(c) los nombres de todos los Licitantes que hubieran presentado Ofertas, con sus respectivos precios tal como se leyeron en voz alta y tal como se evaluaron;

(d) los nombres de los Licitantes cuyas Ofertas fueron rechazadas (ya sea por no responder a los requisitos o por no cumplir con los criterios de calificación) o no fueron evaluadas, con los motivos correspondientes;

(e) el nombre del Licitante ganador, el precio final total del Contrato, su duración y un resumen de su alcance; y

41.3 La Notificación de la Adjudicación del Contrato se publicará en el sitio web de acceso gratuito del Comprador, si se encontrara disponible, o en al menos un periódico de circulación nacional del País del Comprador o en el boletín oficial. El Comprador también deberá incluir dicha notificación en el sitio web de la publicación de las Naciones Unidas *Development Business*.

41.4 Hasta que se prepare y perfeccione el Contrato formal, la Carta de Aceptación constituirá un Contrato vinculante.

41.5 El Comprador responderá por escrito prontamente a cualquier Licitante no seleccionado que, luego de la notificación de la adjudicación de acuerdo con las Subcláusulas 41.1 y 41.2 de las IAL, solicite por escrito los motivos por los cuales su oferta no fue seleccionada.

42. Firma del Contrato

42.1 El Comprador enviará al Licitante seleccionado la Carta de Aceptación, incluido el Convenio

42.2 El Licitante seleccionado tendrá un plazo de veintiocho (28) días después de la fecha de recibo del formulario del Convenio de Contrato para firmarlo, fecharlo y devolverlo al Comprador.

42.3 No obstante, lo establecido en la IAL 42.2 precedente, en caso de que la firma del Convenio de Contrato se vea impedida por alguna restricción de importación atribuible al Comprador, al País del Comprador o al uso de los productos/bienes, sistemas o servicios que han de proveerse y que dichas restricciones de importación

provengan de regulaciones comerciales de un país proveedor de los productos/bienes, sistemas o servicios, el Licitante no será obligado por su Oferta. Lo anterior tendrá efecto siempre y cuando el Licitante pueda demostrar, a satisfacción del Banco y el Comprador, que la firma del Convenio de Contrato no se ha visto impedida por la falta de diligencia de parte del Licitante en el cumplimiento de las formalidades tales como las solicitudes para permisos, autorizaciones y licencias necesarias para la exportación de los productos/bienes, sistemas o servicios de acuerdo con los términos del Contrato.

43. Garantía de Cumplimiento

43.1 Dentro de los veintiocho (28) días posteriores a la fecha en que reciba la Carta de Aceptación enviada por el Comprador, el Licitante seleccionado deberá presentar la Garantía de Cumplimiento del Contrato, de conformidad con la Cláusula 18 de las CGC, utilizando para ello el formulario de Garantía de Cumplimiento incluido en la Sección X, "Formularios del Contrato", u otro formulario aceptable para el Comprador. Si el Licitante seleccionado presenta la Garantía de Cumplimiento del Contrato en forma de fianza, deberá cerciorarse de que esta haya sido emitida por una empresa de fianzas o seguros que resulte aceptable para el Comprador. Toda institución extranjera que proporcione una fianza deberá tener una institución financiera corresponsal domiciliada en el País del Comprador, salvo que este haya acordado por escrito que la existencia de dicha institución financiera corresponsal no es obligatoria.

43.2 El incumplimiento, por parte del Licitante seleccionado, de su obligación de presentar la Garantía de Cumplimiento antes mencionada o de firmar el Convenio constituirá causa suficiente para la anulación de la adjudicación y la pérdida de la Garantía de Mantenimiento de Oferta. En tal caso, el Comprador podrá adjudicar el Contrato al Licitante que haya presentado la segunda Oferta más Conveniente.

Sección II. Datos de la Licitación (DDL)

Los datos específicos que se presentan a continuación sobre los bienes que hayan de adquirirse complementarán, suplementarán o enmendarán las disposiciones de las Instrucciones a los Licitantes (IAL). En caso de conflicto, las disposiciones contenidas aquí prevalecerán sobre las disposiciones de las IAL.

<table>
<tr><th>Referencia en las IAL</th><th>A. Disposiciones generales</th></tr>
<tr><td>IAL 1.1</td><td>
El número de referencia de la Solicitud de Ofertas (SDO) es: PE-PRONATEL-569321-GO-RFB.

El Comprador es: Programa Nacional de Telecomunicaciones - PRONATEL.

El nombre de la SDO es:

“Adquisición de equipamiento ofimático y de redes LAN para la Central 911 en el marco del Proyecto Creación de un Sistema de Atención de Emergencias, Urgencias e Información mediante un Número Único en Lima Metropolitana y el Callao - Proyecto 911”.

La adquisición comprende un (01) <u>Único Lote</u> y comprende los siguientes ítems:
<table>
<tr><th>Item</th><th>Denominacion de Equipos</th><th>Cantidades expresadas en unidades</th></tr>
<tr><td>1</td><td>Computadora de Escritorio Tipo 1</td><td>210</td></tr>
<tr><td>2</td><td>Computadora de Escritorio Tipo 2</td><td>71</td></tr>
<tr><td>3</td><td>Monitor para Computadoras</td><td>696</td></tr>
<tr><td>4</td><td>Teclado y Mouse</td><td>281</td></tr>
<tr><td>5</td><td>Soporte para 03 Monitores Computadoras de Escritorio Tipo 1</td><td>210</td></tr>
<tr><td>6</td><td>Equipo Portátil</td><td>9</td></tr>
<tr><td>7</td><td>Auricular Monoaural</td><td>210</td></tr>
<tr><td>8</td><td>Micrófono</td><td>115</td></tr>
<tr><td>9</td><td>Altavoces</td><td>115</td></tr>
<tr><td>10</td><td>PPT de pie</td><td>210</td></tr>
<tr><td>11</td><td>Cámara Web</td><td>281</td></tr>
<tr><td>12</td><td>Teléfonos IP Tipo 1</td><td>201</td></tr>
<tr><td>13</td><td>Teléfonos IP Tipo 2</td><td>62</td></tr>
<tr><td>14</td><td>Teléfonos IP Tipo 3</td><td>16</td></tr>
<tr><td>15</td><td>Teléfonos IP Tipo 4</td><td>4</td></tr>
<tr><td>16</td><td>Botonera para teléfono IP 4</td><td>1</td></tr>
<tr><td>17</td><td>Pantalla para Monitoreo</td><td>2</td></tr>
<tr><td>18</td><td>Videoconferencia</td><td>4</td></tr>
<tr><td>19</td><td>Impresora tipo personal</td><td>13</td></tr>
<tr><td>20</td><td>Impresora tipo mediano volumen</td><td>5</td></tr>
<tr><td>21</td><td>Proyector Multimedia</td><td>4</td></tr>
<tr><td>22</td><td>Tabletas Rugerizadas</td><td>37</td></tr>
</table>
</td></tr>
</table>

	23	Switches Spine Data Center	2
	24	Switches Leaf Data Center	8
	25	Solución de Orquestador DC	1
	26	Switch Core LAN Campus	2
	27	Switch de acceso 48 puertos PoE	23
	28	Switch de acceso 24 puertos PoE	4
	29	Switch DMZ	2
	30	Switch de Gestión Fuera de Banda	2
	31	Controlador inalámbrico	2
	32	Access Point	47
	33	Solución de Administración y Gestión Campus	1
	34	Solución de Control de Acceso	1
	35	Hardware de Hiperconvergencia	4
	36	Software Hiperconvergencia	1
	37	Servidor para backup	1
	38	Servidor de inmutabilidad	1
	39	Almacenamiento para backup	1
	40	Librería de backup	1
	41	Software de backup	1
	42	Firewall NGFW (Perimetral)	2
	43	Firewall Interno	2
	44	Consola de analítica y reportes	1
	45	XDR (Extended Detection & Response)	1
	46	ZTNA (Zero Trust Network Access)	1
	47	Seguridad para correo electronico	1
	48	WAF - Seguridad para Aplicaciones Web	1
	49	SIEM	1
	50	Plataforma de detección y respuesta de amenazas externas e internas	1
	51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	1
	52	ADC (application Delivery Controller)	2
	53	Anti - DDos	2
	54	MFA - Administración de identidad y acceso	1
	55	PAM - Administración de acceso privilegiado	1
	56	NDR (Network Detection and Response)	1
	57	Sandboxing	1
	58	Solución de Análisis de Tráfico de Red	1
	59	Servicios conexos	1

Nota Importante:

Es requisito indispensable que la oferta debe incluir la totalidad de los ítems especificados, **no admitiéndose ofertas parciales**.

IAL 1.2 (a)	**Sistema electrónico de adquisiciones:** No Aplica.
IAL 2.1	El nombre del Prestatario es: **República del Perú**. Nombre del Proyecto: **Creación de un Sistema de Atención de Emergencias, Urgencias e Información mediante un Número Único en Lima Metropolitana y el Callao – Proyecto 911.** Número del Proyecto: **P170658**.

	Contrato de Préstamo: **N.° 9039-PE**. Monto del Convenio de Préstamo o Financiamiento: **USD 36'324,000 (Treinta y seis Millones Trescientos Veinticuatro Mil Dólares).** Organismo ejecutor/Comprador: **Programa Nacional de Telecomunicaciones - PRONATEL**.
IAL 4.1	El número máximo de miembros de la APCA será: Tres (03).
IAL 4.5	La lista de firmas y personas inhabilitadas para participar en proyectos del Banco Mundial se puede consultar en el sitio web externo del Banco: http://www.worldbank.org/debarr.
B. Contenido del Documento de Licitación	
IAL 7.1	Para **aclaraciones del proceso de Licitación** solamente, la dirección del Comprador es: Atención: Presidente de Comité de Evaluacion Dirección: Av. Paseo de la República Nº 1645 - La Victoria - Lima – Peru. Piso/oficina: Piso 17 Ciudad: Lima Código postal: 15034 País: Perú. Número de fax: N/A Dirección de correo electrónico: crep911@pronatel.gob.pe. **El Comprador no recibirá solicitudes de aclaraciones luego de catorce (14) días útiles, contabilizados a partir del día siguiente de publicado el Anuncio Específico de Adquisiciones.** Pagina Web: https://www.gob.pe/pronatel **Importante:** ▪ El Licitante puede hacer uso del correo electrónico para la presentación de aclaraciones y/o consultas referidas al proceso de selección. ▪ Los Licitantes podrán formular consultas relacionadas con el proceso de licitación, incluyendo aspectos técnicos, administrativos y condiciones de entrega bajo el Incoterm DDP (Delivered Duty Paid) conforme a Incoterms 2020. ▪ Para la presentación de solicitudes de aclaración y/o consultas, se adjunta el formato correspondiente en la **Sección IV - Formularios de la Oferta**.

	▪ Cuando las solicitudes de aclaración y/o consultas sean presentadas por medios electrónicos, se recomienda que el tamaño de cada correo electrónico no exceda de **25 MB**. Será responsabilidad del Licitante verificar la correcta remisión de sus comunicaciones. El Comprador realizará el correspondiente **acuse de recibo** al correo electrónico del Licitante que haya remitido la solicitud.
C. Preparación de las Ofertas	
IAL 10.1	El idioma en que se presentará la Oferta es el **español**. Todo intercambio de correspondencia se hará en el idioma **español.** El idioma para la traducción de la documentación de apoyo y material impreso es el **español**.
IAL 11.1 (i)	Se agrega: **(i) Documentación que acredita la conformidad técnica de los Bienes y Servicios Conexos:** El Licitante deberá presentar documentación técnica suficiente y verificable que permita acreditar la conformidad de los Bienes y Servicios Conexos ofertados con los requisitos establecidos en la Sección VII - Requisitos de los Bienes y Servicios Conexos. Para tal efecto, deberá identificar, según corresponda, el fabricante, marca, modelo, código, SKU o Part Number de los bienes ofertados, el cual se completará con el Anexo 1. Para la evaluación técnica, deberá evidenciar de manera fehaciente con documentación pública del fabricante los establecido en el Anexo 02 de la Sección IV, el no cumplimiento descalifica al Licitante. La documentación presentada deberá permitir al Comprador establecer de manera objetiva la conformidad de la Oferta con las especificaciones técnicas aprobadas, sin modificar, sustituir o complementar los requisitos establecidos en la Sección VII. Los requisitos específicos relativos a EOL/EOS, servicios posteriores a la venta y demás condiciones particulares se acreditarán exclusivamente conforme a los numerales correspondientes de los DDL y la Sección VII, según corresponda.

IAL 11.1 (j)	Los Licitantes deberán presentar los siguientes documentos adicionales con su Oferta: **<u>Documentos de presentación general:</u>** ✓ Índice del contenido de la Oferta. La Oferta deberá presentarse foliada. **<u>Documentos Legales y Financieros:</u>** ✓ Copia simple de constitución social de la empresa vigente e inscrita en los Registros Públicos o su equivalente en el país de origen del Licitante. La legalización de este requisito podrá ser exigible al(os) Licitante(s) que resulte(n) adjudicado(s). ✓ Poder del Representante Legal de la empresa Licitante, con atribuciones para presentar Ofertas y suscribir contratos. ✓ Declaración Jurada firmada por el Representante Legal de no estar impedido de contratar con el Estado Peruano; en el caso de APCA, cada integrante presentará esta declaración. ✓ De ser el caso, Convenio de APCA o carta de intención de suscribir un Convenio de APCA, de conformidad con la IAL 11.2. ✓ Estados financieros correspondientes a los tres (03) últimos ejercicios fiscales cerrados, anteriores a la fecha límite de presentación de Ofertas, preparados conforme a las NIIF o a las normas contables vigentes en el país del Licitante, auditados cuando corresponda conforme a la normativa aplicable, incluyendo como mínimo el Balance General, el Estado de Resultados y las notas a los estados financieros. Para los Licitantes constituidos en el Perú, podrá adjuntarse la constancia de presentación de declaraciones ante la SUNAT u otro documento equivalente que permita verificar la información financiera declarada. Para los Licitantes extranjeros, se aceptará documentación equivalente emitida por la autoridad competente de su país de origen. **<u>Documentos técnicos:</u>** ✓ **Anexo N.° 01 – Hoja de presentación de los bienes ofertados y sustento de cumplimiento de las características técnicas.** El Licitante deberá identificar claramente, según corresponda, el fabricante, marca, modelo, código de producto, SKU o número de parte (Part Number) de los bienes ofertados, así como la documentación técnica que permita verificar los requisitos establecidos en el Anexo 01.

	✓ **Anexo N.° 02 - Características Técnicas a Sustentar.** El Licitante deberá adjuntar las fichas técnicas, hojas de datos, catálogos, manuales, certificados, documentación oficial del fabricante que permita verificar el cumplimiento de las características técnicas establecidas en la Sección en el Anexo 02. La documentación presentada deberá permitir identificar de manera clara y trazable el requisito que se acredita y el documento, página, sección o referencia técnica donde se encuentra sustentado. ✓ **Anexo N.° 03 – Declaración Jurada de Compromiso de Garantía de los Equipos y sus Componentes**, conforme a las condiciones establecidas en la Sección VII – Requisitos de los Bienes y Servicios Conexos. **<u>Disposición general sobre la documentación técnica:</u>** o La documentación técnica presentada deberá corresponder a los Bienes efectivamente ofertados y deberá ser clara, consistente, verificable y trazable. o Cuando el Documento de Licitación requiera expresamente documentación emitida por el fabricante, dicha condición deberá acreditarse mediante el documento correspondiente, conforme al numeral específico que regule dicho requisito. o Los requisitos relativos a EOL/EOS, servicios posteriores a la venta y demás condiciones específicas se acreditarán conforme a las IAL y a la Sección VII que los regulan, sin que resulte necesario reproducir dichos requisitos en el presente numeral.
IAL 13.1	No se considerarán ofertas alternativas.
IAL 14.5	Los precios cotizados por el Licitante serán **fijos durante la ejecución del Contrato y no estarán sujetos a ajustes**.
IAL 14.6	Los precios cotizados para el Lote (Contrato) deberán cubrir el **100 % de los ítems especificados en el Lote Único**, incluyendo, cuando corresponda, los Servicios Conexos asociados. Asimismo, los precios cotizados para cada ítem deberán corresponder al **100 % de las cantidades especificadas** para dicho ítem. En consecuencia, **no se aceptarán Ofertas parciales** respecto de los ítems ni de las cantidades requeridas en el Lote Único.

IAL 14.7	La edición de Incoterms aplicable será **Incoterms® 2020**. Para efectos de la presente Licitación, los Bienes serán cotizados bajo el término **DDP (Delivered Duty Paid)**, conforme a Incoterms® 2020.
IAL 14.8 (b) (i) y (c) (v)	Lugar de destino: De acuerdo a lo señalado en el apartado "Plazo y Lugar de Entrega" de las Especificaciones Técnica de la Sección VII.
IAL 14.8 (a) (iii); (b) (ii) y (c) (v)	Destino final (emplazamiento del Proyecto): **Av. El Sol S/N, distrito de Chorrillos, provincia y departamento de Lima, Perú.**
IAL 15.1	El Licitante no está obligado a cotizar en la moneda del País del Comprador la porción del precio de la Oferta que corresponde a gastos en que se incurra en esa moneda.
IAL 16.4	El período para el cual el Licitante deberá proporcionar información sobre la disponibilidad de repuestos, herramientas especiales y demás elementos necesarios para el funcionamiento adecuado y continuo de los Bienes será de cinco (05) años, conforme a las condiciones establecidas en la Sección VII - Requisitos de los Bienes y Servicios Conexos. Los Bienes ofertados no deberán encontrarse ni ingresar en condición de End of Life (EOL) o End of Support (EOS) durante los cinco (05) años siguientes a la fecha límite de presentación de las Ofertas. Esta condición deberá acreditarse mediante documentación oficial emitida por el fabricante, conforme a lo requerido en la Sección VII. Este requisito no será aplicable a los accesorios y periféricos, cconforme a lo establecido en la Sección VII.
IAL 17.2 (a)	**No se requiere Autorización del Fabricante.** Para acreditar su capacidad para suministrar los bienes ofertados, el Licitante podrá acreditar su condición de distribuidor, representante comercial, integrador, revendedor autorizado o proveedor habitual, conforme a los requisitos establecidos en la Sección III.
IAL 17.2 (b)	Se requieren servicios posteriores a la venta, de conformidad con lo establecido en el **Anexo 3 - "Garantía y Soporte de los Bienes" de las Especificaciones Técnicas**, contenido en la **Sección VII – Requisitos de los Bienes y Servicios Conexos**.
IAL 18.1	La Oferta deberá ser válida hasta: **23 de diciembre de 2026**.

IAL 18.3 (a)	El precio del contrato no estará sujeto a reajuste durante la ejecución. Sin embargo, en caso de que la adjudicación se retrase más de 56 días después de la expiración de la validez inicial de la oferta, la porción en moneda nacional será ajustada mediante el Índice de Precios al Consumidor (IPC) publicado por [INEI], correspondiente al período de prórroga. La porción en moneda extranjera del precio del Contrato se ajustará mediante la aplicación de un factor que refleje la inflación internacional, utilizando el Índice de Precios al Consumidor (CPI) del país correspondiente a la moneda extranjera ofertada, durante el período de prórroga
IAL 19.1	La Oferta deberá incluir una "Declaración de Mantenimiento de Oferta", utilizando el formulario incluido en la Sección IV. Formularios de la Oferta.
IAL 19.3 (d)	Otro tipo de garantías aceptables: **No aplica**.
IAL 19.9	Si el Licitante incurre en alguna de las acciones previstas en las IAL 19.9(a) o 19.9(b), el Prestatario podrá declarar al Licitante inelegible para ser adjudicatario de un contrato por un período de **dos (02) años**, cconforme a lo establecido en la Declaración de Mantenimiento de Oferta.
IAL 20.1	Además de la oferta original, el número de copias es: ✓ **Una (01) copia en archivo digital**, copia fiel de la Oferta original, debidamente encriptada y presentada en un medio de almacenamiento digital (USB, CD u otro similar), que deberá entregarse conjuntamente con la Oferta original como parte del mismo acto de presentación. ✓ De presentarse diferencias entre el ejemplar original y la información del archivo digital, prevalece la información del ejemplar original de la Oferta.
IAL 20.3	La confirmación escrita de la autorización para firmar en nombre del Licitante comprenderá: i. Copia simple de la vigencia de poder o documento equivalente que acredite las facultades del representante autorizado para presentar y suscribir la Oferta y, cuando corresponda, suscribir el Contrato. ii. Para los Licitantes extranjeros se aceptará el documento equivalente emitido conforme a la legislación de su país de origen.

	iii. Copia del documento de identidad o documento equivalente del país de origen del representante autorizado.
D. Presentación y apertura de las Ofertas	
IAL 22.1	Para fines de **presentación de la Oferta**, la dirección del Comprador es: Atención: Comité de Evaluación Dirección: Av. Paseo de la República Nº 1645 - La Victoria - Lima - Peru. Piso/oficina: Piso 01 Ciudad: Lima. Código postal: 15034 País: Perú **La fecha límite para presentar las ofertas es:** Fecha: **24 de setiembre de 2026**. Hora: 15:00 horas (Hora local) Los Licitantes no tendrán la opción de presentar sus Ofertas electrónicamente.
IAL 25.1	La apertura de las Ofertas tendrá lugar en: Dirección: Av. Paseo de la República Nº 1645 - La Victoria - Lima - Peru. Piso/oficina: Piso 01 Ciudad: Lima País: Perú Fecha: **24 de setiembre de 2026**. Hora: 15:30 horas (Hora local) **Los Licitantes no tendrán la opción de presentar sus Ofertas electrónicamente.**
IAL 25.6	Durante el acto público de apertura de las Ofertas, el Notario Público que certifique el acto procederá a rubricar la **Carta de la Oferta y las Listas de Precios** presentadas por los Licitantes.

	Dichos documentos también serán rubricados por los **tres (03) representantes del Comprador** que participen en el acto de apertura de las Ofertas.
E. Evaluación y Comparación de las Ofertas	
IAL 32.1	La moneda que se utilizará a fin de evaluar y comparar las Ofertas para convertir en una sola moneda, al tipo de cambio vendedor, todoslos precios de las Ofertas expresados en diversas monedas es: Soles (S/). La fuente del tipo de cambio será la **tasa de cambio tipo venta publicada por la Superintendencia de Banca, Seguros y AFP del Perú (SBS)**. La fecha del tipo de cambio será: siete (07) días calendario antes a la fecha de presentación de las Ofertas.
IAL 33.1	No se aplicará un margen de preferencia nacional.
IAL 34.2 (a)	La evaluación se hará por: **Lote único.** Las Ofertas serán evaluadas considerando el precio total ofertado para todos los artículos que integran el lote, bajo la condición de entrega Delivered Duty Paid (DDP) en el lugar de destino final indicado por el Comprador, conforme a Incoterms 2020. La evaluación y comparación de las Ofertas se realizará aplicando exclusivamente los criterios y metodologías establecidos en las IAL y en la Sección III - Criterios de Evaluación y Calificación. <u>Importante:</u> Los licitantes deberán cotizar la totalidad de los artículos incluidos en el lote; de lo contrario, la Oferta podrá ser considerada **<u>no</u>** sustancialmente conforme.
IAL 34.6	Los ajustes se determinarán utilizando los siguientes criterios de entre los enumerados en la Sección III, "Criterios de Evaluación y Calificación": (a) Desviación en el Cronograma de Entregas: **No aplica.** (b) Desviación en el plan de pagos: **No aplica.** (c) Costo de reemplazo de componentes importantes, repuestos obligatorios y servicio **No aplica.** (d) Disponibilidad en el País del Comprador de repuestos y servicios posteriores a la venta para los equipos ofrecidos en la Oferta: **No Aplica.**

	(e) Costos durante la vida útil: Los costos en que se incurra durante la vida útil de los bienes o los equipos **No aplica.** (f) El rendimiento y la productividad de los equipos ofrecidos: **No aplica.**
F. Adjudicación del Contrato	
IAL 42	Las cantidades podrán aumentarse, como máximo, en un 15%. Las cantidades podrán reducirse, como máximo, en un 15%

Sección III. Criterios de Evaluación y Calificación

Esta Sección contiene los criterios que el Comprador utilizará para evaluar una Oferta y determinar si los Licitantes cumplen con las calificaciones requeridas. No se utilizará ningún otro factor, método ni criterio que no sean los que se especifican en este documento de licitación.

Índice

1. Margen de preferencia (IAL 33)..... 49

2. Evaluación (IAL 34)..... 49

3. Calificación (IAL 37) 49

1. Margen de preferencia (IAL 33)

"No Aplica"

2. Evaluación (IAL 34)

2.1. Criterios de evaluación (IAL 34.6)

"No Aplica"

2.2. Contratos múltiples (IAL 34.4)

"No Aplica"

2.3. Ofertas Alternativas (IAL 13.1)

"No Aplica"

3. Calificación (IAL 37)

3.1. Criterios de calificación (IAL 37.1)

Luego de determinar entre las Ofertas que cumplen sustancialmente con los requisitos la que presenta el costo evaluado más bajo de acuerdo con la IAL 34, y, si corresponde, de evaluar cualquier Oferta Excesivamente Baja de acuerdo con la IAL 36, el Comprador efectuará la calificación posterior del Licitante de acuerdo con la IAL 37, empleando únicamente los requisitos estipulados en la presente Sección.

Los requisitos que no estén incluidos en el siguiente texto no podrán utilizarse para evaluar las calificaciones del Licitante.

Todos los criterios establecidos en los numerales 3.1.1 a 3.1.7 son requisitos mínimos habilitantes y serán evaluados exclusivamente bajo la modalidad **CUMPLE / NO CUMPLE**, sin asignación de puntaje, bonificación, preferencia o ventaja comparativa por superar los mínimos establecidos.

3.1.1 CAPACIDAD FINANCIERA

El Licitante deberá demostrar que cuenta con capacidad financiera suficiente para financiar la ejecución del Contrato sin depender exclusivamente de los pagos del Comprador.

a) **Solidez financiera.** El Licitante deberá presentar estados financieros correspondientes a los tres (3) últimos ejercicios fiscales cerrados anteriores a la fecha límite de presentación de Ofertas, auditados cuando corresponda conforme a la legislación aplicable.

El patrimonio neto correspondiente al último ejercicio fiscal cerrado deberá ser positivo y el capital de trabajo, entendido como la diferencia entre activo corriente

y pasivo corriente, correspondiente al último ejercicio fiscal cerrado deberá ser positivo.

b) **Asociación en Participación, Consorcio o Asociación (APCA)**. En caso de APCA, todos sus integrantes deberán presentar la información financiera correspondiente a los tres (3) últimos ejercicios fiscales cerrados y acreditar patrimonio neto positivo en el último ejercicio.

3.1.2 EXPERIENCIA ESPECÍFICA DEL LICITANTE

El Licitante deberá acreditar la ejecución satisfactoria, durante los diez (10) años anteriores a la fecha límite de presentación de Ofertas, de al menos dos (2) contratos que hayan comprendido el suministro e implementación de soluciones de tecnologías de información, infraestructura de centro de datos, redes LAN/campus, equipamiento informático y/o soluciones de ciberseguridad de naturaleza y complejidad comparables con la presente contratación.

Cada contrato deberá acreditar un monto ejecutado mínimo equivalente a USD 5 000 000 (cinco millones de dólares de los Estados Unidos de América).

Para uno (1) de los dos (2) contratos requeridos se permitirá acumular hasta dos (2) contratos ejecutados por el mismo Licitante o por el mismo integrante de la APCA, siempre que el monto acumulado sea igual o superior a USD 5 000 000.

Para ser considerado similar, el contrato deberá incluir como mínimo el suministro e implementación y, adicionalmente, al menos dos (2) de los siguientes grupos:

a) Networking/red LAN o data center;
b) Servidores, almacenamiento, hiperconvergencia o backup;
c) Equipamiento informático/ofimático; y
d) Seguridad de red o ciberseguridad.

Al menos uno (01) de los contratos acreditados deberá incluir componentes de networking/red LAN, data center o ciberseguridad.

La experiencia deberá acreditarse mediante copia del contrato u orden de compra y, adicionalmente, acta de conformidad, certificado de recepción, constancia de prestación satisfactoria, comprobante de pago cancelado u otro documento equivalente que permita verificar de manera fehaciente el objeto, monto ejecutado, período y culminación satisfactoria del contrato.

Cuando el documento se encuentre expresado en una moneda distinta del dólar estadounidense, se aplicará el tipo de cambio previsto en los DDL para fines de comparación.

En caso de APCA, la experiencia podrá acreditarse conjuntamente. El integrante líder deberá acreditar por sí mismo al menos uno (01) de los contratos requeridos.

Los contratos aportados deberán corresponder al integrante que efectivamente los ejecutó.

No se sumarán contratos ejecutados por distintos integrantes para alcanzar el monto mínimo exigido para un contrato. La acumulación excepcional de hasta dos (2) contratos prevista en este numeral únicamente podrá efectuarse respecto de contratos ejecutados por un mismo integrante.

Para determinar el cumplimiento del número mínimo de contratos, se considerará el total de contratos válidamente acreditados por los integrantes de la APCA, de conformidad con las reglas establecidas en el presente numeral.

3.1.3 CONFORMIDAD TÉCNICA Y TRAZABILIDAD DOCUMENTAL

El Licitante deberá acreditar el cumplimiento de las características técnicas identificadas para sustento documental en los Anexos de la Sección IV.

Para cada bien o solución ofertada deberá identificar, según corresponda, fabricante, marca, modelo, versión, SKU y/o Part Number, de modo que el bien o solución ofertada quede inequívocamente individualizado.

El sustento deberá realizarse mediante documentación técnica pública oficial del fabricante, tal como ficha técnica, data sheet, catálogo, manual, certificado, u otra documentación pública del fabricante.

El Licitante deberá señalar, para cada requisito que requiera sustento documental del **Anexo 02**, el documento, página, sección o enlace/referencia técnica exacta donde pueda verificarse su cumplimiento.

Una declaración genérica del Licitante no sustituirá la evidencia técnica del fabricante cuando el requisito exija expresamente documentación oficial del fabricante.

3.1.4 VIGENCIA TECNOLÓGICA

Para los bienes respecto de los cuales la Sección VII o los DDL exijan respaldo del fabricante, no se requerirá acreditar experiencia comercial mínima del fabricante en la fabricación o provisión de la familia de productos ofertada.

La evaluación se centrará en la vigencia tecnológica de los bienes ofertados, a fin de garantizar su disponibilidad de soporte y continuidad tecnológica durante el período requerido.

a) **Vigencia tecnológica**. Cuando corresponda, de conformidad con la IAL 16.4 y la Sección VII, los bienes ofertados no deberán encontrarse ni ingresar en condición de End of Life (EOL) o End of Support (EOS) durante los cinco (5) años siguientes a la fecha límite de presentación de

Ofertas. Esta condición deberá acreditarse mediante documentación oficial del fabricante.

b) **Correspondencia documental**. La documentación presentada deberá corresponder exactamente a la marca, familia, modelo o versión ofertada y deberá ser verificable por el Comprador.

3.1.5 CAPACIDAD PARA IMPLEMENTAR SOLUCIONES DE CIBERSEGURIDAD

Dada la criticidad operativa de la Central 911 y la inclusión de soluciones de seguridad previstas en la Sección VII, el Licitante deberá demostrar capacidad para implementar o integrar componentes de seguridad de red y/o ciberseguridad.

Este requisito se considerará cumplido cuando dicha capacidad se encuentre acreditada en al menos uno (1) de los contratos válidos presentados para acreditar la experiencia específica prevista en el numeral 3.1.2, o mediante un contrato adicional ejecutado satisfactoriamente de naturaleza equivalente.

La experiencia contractual no podrá ser sustituida por una certificación del fabricante.

Las certificaciones técnicas, cuando sean exigidas por la Sección VII para personal o soluciones específicas, acreditarán competencia técnica, pero no reemplazarán la experiencia contractual del Licitante exigida en el presente numeral.

3.1.6 ACREDITACIÓN DEL LICITANTE

El Licitante que no sea fabricante deberá acreditar su condición de distribuidor, representante comercial, integrador, revendedor autorizado o proveedor habitual de los bienes ofertados, según corresponda.

La acreditación podrá realizarse mediante certificados de distribución autorizada, cartas emitidas por el fabricante, acuerdos comerciales vigentes, registros de socios comerciales, contratos de suministro, órdenes de compra ejecutadas u otra documentación equivalente aceptable para el Comprador, que permita verificar razonablemente la capacidad del Licitante para suministrar los bienes ofertados.

3.1.7 CAPACIDAD DE SOPORTE TÉCNICO, GARANTÍA Y SERVICIO POSTVENTA

El Licitante deberá acreditar que cuenta con capacidad para brindar soporte técnico, atención de garantías, mantenimiento y reposición de componentes durante el período de garantía establecido en los Documentos de Licitación.

La acreditación podrá realizarse mediante la presentación de certificados de soporte autorizado, cartas de respaldo del fabricante, relación de centros de servicio autorizados, personal técnico certificado, contratos de soporte o documentación equivalente.

3.1.8 PERSONAL CLAVE

El Licitante deberá demostrar que cuenta con el personal requerido para ocupar las posiciones claves, debidamente calificado y en cantidad suficiente, conforme a lo establecido en los numerales 4.2, 4.3, 4.4 y 4.5 de las Especificaciones Técnicas de la Sección VII.

El Licitante deberá proporcionar la información del personal propuesto para la ejecución del Contrato, incluyendo sus calificaciones académicas, experiencia laboral y demás información requerida en los formularios correspondientes. Para tal efecto, el Licitante deberá completar y presentar los formularios establecidos en la Sección IV, Formularios de Licitación, correspondientes al Personal Clave.

La evaluación verificará que la Oferta no contenga reservas, exclusiones, limitaciones o condiciones que reduzcan los niveles de servicio exigidos en el Documento de Licitación.

Únicamente las Ofertas que cumplan sustancialmente con los requisitos del Documento de Licitación y cuyos Licitantes cumplan los criterios de calificación establecidos en los numerales 3.1.1 a 3.1.8 podrán continuar a la comparación del costo evaluado y, de corresponder, a la determinación de la Oferta con el costo evaluado más bajo, de conformidad con las IAL aplicables.

Sección IV. Formularios de la Oferta

Índice de Formularios

Carta de la Oferta 55

Formulario de Información sobre el Licitante 58

Formulario de información sobre los miembros de la APCA 60

Formulario de la Oferta Lista de Precios de los Bienes (1) 61

Formulario para Solicitud de Aclaración 103

Declaración de Desempeño sobre Explotación y Abuso Sexual (EAS) y/o Acoso Sexual (ASx) 104

Formulario de Declaración de Mantenimiento de Oferta 105

Autorización del Fabricante 107

Carta de la Oferta

INSTRUCCIONES A LOS LICITANTES: ELIMINE ESTE RECUADRO UNA VEZ QUE HAYA COMPLETADO EL DOCUMENTO

El Licitante deberá preparar esta Carta de la Oferta en papel con membrete que indique claramente el nombre completo del Licitante y su dirección comercial.

Nota: El texto en cursiva se incluye para ayudar a los Licitantes en la preparación de este formulario.

Fecha de presentación de esta Oferta: *[Indique día, mes y año de la presentación de la Oferta]*.
SDO n.°: *[Indique el número del proceso de la SDO]*.
Solicitud de Oferta n.°: *[Indique identificación]*.

Para: ***[Indique el nombre del Comprador]***.

(a) **Sin reservas:** Hemos examinado el documento de licitación, incluidas las enmiendas emitidas de conformidad con la IAL 8, y no tenemos reserva alguna al respecto.

(b) **Elegibilidad:** Cumplimos los requisitos de elegibilidad y no tenemos conflictos de intereses, de acuerdo con la IAL 4.

(c) **Declaración de Mantenimiento de Oferta/Propuesta:** No hemos sido suspendidos ni declarados inelegibles por el Comprador sobre la base de la suscripción de una Declaración de Mantenimiento de Oferta/Propuesta en el País del Comprador de acuerdo con la IAL 4.7.

(d) **Explotación y Abuso Sexual (EAS) y/o Acoso Sexual (ASx):** [*seleccione la opción apropiada de (i) a (iii) a continuación y elimine las demás. En caso de los miembros de una APCA y/o subcontratistas, indicar la situación de descalificación por parte del Banco de cada miembro de la APCA y/o subcontratista.]*

Nosotros, incluyendo todos nuestros subcontratistas:

(i) [no hemos sido objeto de descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS/ASx.]

(ii) [estamos sujetos a descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS/ASx]

(iii) [habíamos sido descalificados por el Banco por incumplimiento de las obligaciones sobre EAS/ASx. Se ha dictado un laudo arbitral en el caso de descalificación a nuestro favor.]

(e) **Conformidad:** Ofrecemos proveer los siguientes bienes de conformidad con el documento de licitación y de acuerdo con el Cronograma de Entregas establecido en los

Requisitos de los Bienes y Servicios Conexos: *[proporcione una descripción breve de los Bienes y Servicios Conexos]*.

(f) **Precio de la Oferta:** El precio total de nuestra Oferta, excluyendo cualquier descuento ofrecido en el artículo (f) a continuación es:

el precio total es *[indique el precio total de la Oferta en letras y en cifras, indicando los diferentes montos y las respectivas monedas]*.

(g) **Descuentos:** Los descuentos ofrecidos y la metodología para su aplicación son los siguientes:

(i) Los descuentos ofrecidos son: *[especifique cada descuento ofrecido]*.

(ii) El método de cálculo exacto para determinar el precio neto luego de aplicados los descuentos se detalla a continuación: *[detalle la metodología que se usará para aplicar los descuentos]*.

(h) **Validez de la Oferta:** Nuestra Oferta será válida hasta *[ingresar el día, mes y año de conformidad con la IAL 18.1]*, y seguirá teniendo carácter vinculante para nosotros y podrá ser aceptada en cualquier momento antes del vencimiento de dicho período.

(i) **Garantía de Cumplimiento:** Si nuestra oferta es aceptada, nos comprometemos a obtener una Garantía de Cumplimiento del Contrato de conformidad con el documento de licitación.

(j) **Una Oferta por Licitante:** No estamos presentando ninguna otra Oferta como Licitantes individuales, y no estamos participando en ninguna otra Oferta ni como miembros de una APCA ni como subcontratistas, y cumplimos con los requisitos de la IAL 4.3, sin considerar las Ofertas Alternativas presentadas de acuerdo con la IAL 13.

(k) **Suspensión e inhabilitación:** Nosotros, junto con todos nuestros subcontratistas, proveedores, consultores, fabricantes o prestadores de servicios requeridos para ejecutar cualquier parte del contrato, no dependemos de ninguna entidad o persona, ni somos controlados por ninguna entidad o persona, que esté sujeta a una suspensión o inhabilitación temporal impuesta por el Grupo Banco Mundial ni a una inhabilitación impuesta por el Grupo Banco Mundial de conformidad con el Acuerdo de Aplicación Mutua de las Decisiones de Inhabilitación, suscrito por el Banco Mundial y otros bancos de fomento. Asimismo, no somos inelegibles en virtud de las leyes o regulaciones oficiales del País del Comprador ni en virtud de una decisión del Consejo de Seguridad de las Naciones Unidas.

(l) **Empresa o ente de propiedad estatal:** *[Seleccione la opción correspondiente y elimine la otra]*. *[No somos una empresa o ente de propiedad estatal]*/*[Somos una empresa o ente de propiedad estatal, pero cumplimos con los requisitos de la IAL 4.6]*.

(m) **Comisiones, gratificaciones, honorarios:** Hemos pagado o pagaremos los siguientes honorarios, comisiones o gratificaciones en relación con el Proceso de Licitación o la ejecución del Contrato: *[proporcione el nombre completo de cada receptor, su dirección*

completa, la razón por la cual se pagó cada comisión o gratificación, y la cantidad y moneda de cada comisión o gratificación a la que se haga referencia].

Nombre del receptor	Dirección	Concepto	Monto

(Si no ha efectuado o no se efectuará pago alguno, escriba "ninguno").

(n) **Contrato vinculante:** Entendemos que esta Oferta, junto con su debida aceptación por escrito incluida en su Carta de Aceptación, constituirá una obligación contractual entre nosotros hasta que las partes hayan preparado y perfeccionado un contrato formal.

(o) **Comprador no obligado a aceptar:** Entendemos que ustedes no están obligados a aceptar la Oferta con el costo evaluado más bajo, la Oferta más Conveniente ni ninguna otra Oferta que reciban.

(p) **Fraude y Corrupción:** Por el presente, certificamos que hemos tomado las medidas necesarias para garantizar que ninguna persona que actúe en nuestro nombre o representación incurra en prácticas fraudulentas o corruptas.

Nombre del Licitante*: *[proporcione el nombre completo del Licitante]*.

Nombre de la persona debidamente autorizada para firmar la Oferta en nombre del Licitante:** *[proporcione el nombre completo de la persona debidamente autorizada a firmar el Formulario de la Oferta]*.

Cargo de la persona firmante del Formulario de la Oferta: *[indique el cargo de la persona que firma el Formulario de la Oferta]*

Firma de la persona nombrada anteriormente: *[indique la firma de la persona cuyo nombre y capacidad se indican en los párrafos anteriores]*.

Fecha de la firma: El día *[indique la fecha de la firma]* **del mes** *[indique mes]* **del año** *[indique año]*.

***** En el caso de las Ofertas presentadas por una APCA, especifique el nombre de la APCA que actúa como Licitante.

** La persona que firme la Oferta deberá contar con el poder otorgado por el Licitante. El poder deberá adjuntarse a los Formularios de la Oferta.

Formulario de Información sobre el Licitante

[El Licitante deberá completar este formulario de acuerdo con las instrucciones indicadas a continuación. No se aceptará ninguna alteración a este formulario ni se aceptarán substitutos].

Fecha: *[indique día, mes y año de la presentación de la Oferta]*.
SDO n.°: *[Indique el número del proceso de la SDO]*.
Alternativa n.°: *[indique el n.° de identificación, si esta es una oferta por una alternativa]*.

Página _____ de _____ páginas

1. Nombre del Licitante: *[indique el nombre jurídico del Licitante]*.
2. Si se trata de una APCA, nombre jurídico de cada miembro: *[indique el nombre jurídico de cada miembro de la APCA]*.
3. País donde está registrado el Licitante en la actualidad o país donde intenta registrarse: *[indique el país donde está registrado el Licitante en la actualidad o país donde intenta registrarse]*.
4. Año de registro del Licitante: *[indique el año de registro del Licitante]*.
5. Dirección del Licitante en el país donde está registrado: *[indique el domicilio legal del Licitante en el país donde está registrado]*.
6. Información del representante autorizado del Licitante: Nombre: *[indique el nombre del representante autorizado]*. Dirección: *[indique la dirección del representante autorizado]*. Números de teléfono y fax*: [indique los números de teléfono y fax del representante autorizado]*. Dirección de correo electrónico: *[indique la dirección de correo electrónico del representante autorizado]*.
7. Se adjuntan copias de los siguientes documentos originales: *[marque las casillas que correspondan]* ☐ Estatutos de la Sociedad (o documentos equivalentes de constitución o asociación), o documentos de registro de la persona jurídica antes mencionada, y de conformidad con la IAL 4.4. ☐ Si se trata de una APCA, carta de intención de formar la APCA, o el Convenio de APCA, de conformidad con la IAL 4.1. ☐ Si se trata de una empresa o ente de propiedad estatal, de conformidad con la IAL 4.6, documentación que acredite: • su autonomía jurídica y financiera, • su operación conforme al Derecho comercial, • que el Licitante no se encuentra bajo la supervisión del Comprador.

8. Se incluye el organigrama, la lista de los miembros del Directorio y la propiedad efectiva.

Formulario de información sobre los miembros de la APCA

[El Licitante deberá completar este formulario de acuerdo con las instrucciones indicadas a continuación. El siguiente cuadro deberá ser completado por el Licitante y por cada uno de los miembros de la APCA].

Fecha: *[indique día, mes y año de la presentación de la Oferta]*.
SDO n.°: *[indique el número del proceso de Licitación]*.
Alternativa n.°: *[indique el n.° de identificación, si esta es una oferta por una alternativa]*.

Página ____ de ____ páginas

1. Nombre del Licitante *[indique el nombre jurídico del Licitante]*.
2. Nombre jurídico del miembro de la APCA *[indique el nombre jurídico del miembro de la APCA]*.
3. Nombre del país de registro del miembro de la APCA *[indique el nombre del país de registro del miembro de la APCA]*.
4. Año de registro del miembro de la APCA: *[indique el año de registro del miembro de la APCA]*.
5. Dirección del miembro de la APCA en el país donde está registrado: *[domicilio legal del miembro de la APCA en el país donde está registrado]*.
6. Información sobre el representante autorizado del miembro de la APCA: Nombre: *[indique el nombre del representante autorizado del miembro de la APCA]*. Dirección: *[indique la dirección del representante autorizado del miembro de la APCA]*. Números de teléfono y fax: *[indique los números de teléfono y fax del representante autorizado del miembro de la APCA]*. Dirección de correo electrónico: *[indique la dirección de correo electrónico del representante autorizado del miembro de la APCA]*.
7. Se adjuntan copias de los siguientes documentos originales: *[marque las casillas que correspondan]*. ☐ Estatutos de la Sociedad (o documentos equivalentes de constitución o asociación) o documentos de registro de la persona jurídica antes mencionada, y de conformidad con la IAL 4.4. ☐ Si se trata de una empresa o ente de propiedad estatal, documentación que acredite su autonomía jurídica y financiera, su operación de conformidad con el Derecho comercial y que no se encuentra bajo la supervisión del Comprador, de conformidad con la IAL 4.6. 8. Se incluye el organigrama, la lista de los miembros del Directorio y la propiedad efectiva.

Formulario de la Oferta
Lista de Precios de los Bienes (1)
(Lote Unico)

(El Licitante deberá completar el presente formulario de conformidad con las instrucciones establecidas en el Documento de Licitación. La identificación, descripción y numeración de los artículos deberán corresponder exactamente a las establecidas por el Comprador en la Sección VII – Lista de Requisitos de los Bienes y Servicios Conexos).

Señores
COMITÉ DE EVALUACION
PROCESO SDO Nº PE-PRONATEL-561608-GO-RFB

Lote Nº	**Artículo Nº**	**DESCRIPCIÓN**	**UNIDAD DE MEDIDA**	**CANTIDAD**	**PRECIO UNITARIO DDP** (incluye IGV y demás tributos aplicables) *(indicar moneda)*	**PRECIO TOTAL** (incluye IGV y demás tributos aplicables) *(indicar moneda)*
Único	1	Computadora de Escritorio Tipo 1	Und.	210		
	2	Computadora de Escritorio Tipo 2	Und.	71		
	3	Monitor para Computadoras	Und.	696		
	4	Teclado y Mouse	Und.	281		
	5	Soporte para 03 Monitores Computadoras de Escritorio Tipo 1	Und.	210		
	6	Equipo Portátil	Und.	9		
	7	Auricular Monoaural	Und.	210		
	8	Micrófono	Und.	115		
	9	Altavoces	Und.	115		
	10	PPT de pie	Und.	210		
	11	Cámara Web	Und.	281		
	12	Teléfonos IP Tipo 1	Und.	201		
	13	Teléfonos IP Tipo 2	Und.	62		
	14	Teléfonos IP Tipo 3	Und.	16		
	15	Teléfonos IP Tipo 4	Und.	4		
	16	Botonera para teléfono IP 4	Und.	1		
	17	Pantalla para Monitoreo	Und.	2		
	18	Videoconferencia	Und.	4		
	19	Impresora tipo personal	Und.	13		
	20	Impresora tipo mediano volumen	Und.	5		
	21	Proyector Multimedia	Und.	4		
	22	Tabletas Rugerizadas	Und.	37		
	23	Switches Spine Data Center	Und.	2		
	24	Switches Leaf Data Center	Und.	8		
	25	Solución de Orquestador DC	Und.	1		

	26	Switch Core LAN Campus	Und.	2		
	27	Switch de acceso 48 puertos PoE	Und.	23		
	28	Switch de acceso 24 puertos PoE	Und.	4		
	29	Switch DMZ	Und.	2		
	30	Switch de Gestión Fuera de Banda	Und.	2		
	31	Controlador inalámbrico	Und.	2		
	32	Access Point	Und.	47		
	33	Solución de Administración y Gestión Campus	Und.	1		
	34	Solución de Control de Acceso	Und.	1		
	35	Hardware de Hiperconvergencia	Und.	4		
	36	Software Hiperconvergencia	Und.	1		
	37	Servidor para backup	Und.	1		
	38	Servidor de inmutabilidad	Und.	1		
	39	Almacenamiento para backup	Und.	1		
	40	Librería de backup	Und.	1		
	41	Software de backup	Und.	1		
	42	Firewall NGFW (Perimetral)	Und.	2		
	43	Firewall Interno	Und.	2		
	44	Consola de analítica y reportes	Und.	1		
	45	XDR (Extended Detection & Response)	Und.	1		
	46	ZTNA (Zero Trust Network Access)	Und.	1		
	47	Seguridad para correo electronico	Und.	1		
	48	WAF - Seguridad para Aplicaciones Web	Und.	1		
	49	SIEM	Und.	1		
	50	Plataforma de detección y respuesta de amenazas externas e internas	Und.	1		
	51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	Und.	1		
	52	ADC (application Delivery Controller)	Und.	2		
	53	Anti - DDos	Und.	2		
	54	MFA - Administración de identidad y acceso	Und.	1		
	55	PAM - Administración de acceso privilegiado	Und.	1		
	56	NDR (Network Detection and Response)	Und.	1		
	57	Sandboxing	Und.	1		
	58	Solución de Análisis de Tráfico de Red	Und.	1		
Total						

Condiciones de Cotización:

Los bienes deberán cotizarse bajo la condición **DDP (Delivered Duty Paid – Entregado Derechos Pagados)**. El precio ofertado deberá incluir todos los costos necesarios para suministrar y entregar los bienes en el lugar de destino final indicado por el Comprador, incluyendo el valor de los bienes, embalaje, transporte internacional, seguros, derechos e impuestos de importación, nacionalización, manipuleo, transporte interno, descarga, entrega en destino y todos los tributos, tasas y demás gastos aplicables hasta la recepción conforme de los bienes.

Los precios consignados en el presente formulario corresponden exclusivamente al suministro de los bienes. Los **Servicios Conexos** requeridos en las Especificaciones Técnicas deberán ser cotizados en el **Formulario N.° 02 – Precio y Cronograma de Cumplimiento de los Servicios Conexos**, formando parte de la oferta económica integral.

Lugar y Plazo de Entrega:

Lugar de entrega: _____

Tiempo de entrega máximo requerido[1]: _____

Tiempo de Entrega ofrecido: _____
[De acuerdo a la subcláusula 13.9 de la Sección I, las ofertas que presenten un plazo de entrega mayor al máximo requerido serán rechazadas.]

Datos del Licitante:

Razón Social: _____

RUC: _____

Dirección: _____

Teléfono: _____

Correo electrónico: _____

Lugar y Fecha: _____

Firma del Representante Legal y sello de la Empresa

[1] *Las ofertas que excedan el plazo máximo requerido serán rechazadas conforme a lo establecido en el Documento de Licitación.*

Precio y cronograma de cumplimiento: Servicios conexos[2]

(El Licitante deberá completar el presente formulario de conformidad con las instrucciones establecidas en el Documento de Licitación. Los servicios conexos ofertados deberán corresponder a los requeridos en la Sección VII – Lista de Requisitos de los Bienes y Servicios Conexos y en las Especificaciones Técnicas.)

Monedas de conformidad con la IAL 15					**Fecha:_____ _____ SDO n.º _____ Página n.º _____ de _____**	
1	2	3	4	5	6	7
Servicio n.º	**Plazo de prestación del servicio**	**Plazo de prestación del servicio**	**Unidad de medida**	**Cantidad**	**Precio unitario (incluye todos los tributos aplicables)**	**Precio total por servicio (Col. 5 x 6 o un estimado) (incluye todos los tributos aplicables)**
[Indique número del servicio].	*[Indique el nombre de los servicios].*	*[Indique la fecha de entrega al lugar de destino final por servicio].*			*[Indique el precio unitario por servicio].*	*[Indique el precio total por servicio].*
1	Servicio de implementación (instalación, configuración, pruebas y comisionamiento)	90 días	Servicio	1		
2	Mesa de Servicio	12 meses	Meses	12		
3	Centro de Operaciones de Seguridad	12 meses	Meses	12		

[2] *Este formulario corresponde al Lote Único y está destinado exclusivamente a la valorización de los Servicios Conexos. La unidad de contratación se establece como "Servicio" y la cantidad como "1", debido a que cada prestación corresponde a un servicio integral con un alcance y plazo definido en las Especificaciones Técnicas. Los bienes serán valorizados separadamente en el Formulario de Lista de Precios de los Bienes bajo condición DDP.*

4	Garantía y Soporte de los Bienes	12 meses	Meses	12		
			Precio total Servicios Conexos de la oferta			

Declaración del Licitante:

Los precios ofertados en el presente formulario corresponden exclusivamente a los **Servicios Conexos** requeridos por el Comprador y comprenden todos los costos necesarios para su ejecución integral, incluyendo personal especializado, herramientas, equipos, materiales, licencias, gestión operativa, gastos administrativos, tributos aplicables y cualquier otro costo relacionado con la prestación de los servicios.

Los precios consignados incluyen todos los costos directos e indirectos necesarios para la correcta ejecución de los Servicios Conexos durante el plazo establecido en las Especificaciones Técnicas.

Cronograma de Cumplimiento de los Servicios Conexos

Servicio Conexos	Fecha de Inicio	Fecha de Culminación
Servicio de implementación (instalación, configuración, pruebas y comisionamiento)		
Mesa de Servicio		
Centro de Operaciones de Seguridad (SOC)		
Garantía y Soporte de los Bienes		

Firmada: [firma del representante autorizado]. En capacidad de [indique el cargo]

Nombre: [indique el nombre en letra de molde o mecanografiado]

Debidamente autorizado para firmar la Oferta por y en nombre de: [indique el nombre la entidad que autoriza]

Fechada el [indique el día] día de [indique el mes] de [indique el año]

ANEXO N° 01

Declaración Jurada / Hoja de Presentación Equipos sobre Cumplimiento de las Características Técnicas de las Especificaciones Técnicas.

Señores
COMITÉ DE EVALUACION
PROCESO SDO Nº PE-PRONATEL-569321-GO-RFB

Presente. -

En calidad de postor, luego de haber examinado los documentos del procedimiento de selección SOLICITUD DE OFERTA SDO Nº PE-PRONATEL-569321-GO-RFB, conociendo todas las condiciones existentes, el suscrito adjunta declaración Jurada sobre el Cumplimiento de acuerdo con los Requerimientos Técnicos Mínimos y demás condiciones que se indican en la sección VII de las especificaciones técnicas de las Bases.

DECLARACION JURADA DE CUMPLIMIENTO DE LAS CARACTERISTICAS TÉCNICAS DE LAS ESPECIFICACIONES TECNICAS
NOMBRE O RAZÓN SOCIAL DEL LICITANTE Y/O APCA:
REPRESENTANTE LEGAL:
FECHA:

RESUMEN DE LOS BIENES OFERTADOS

Ítem	**Descripción del bien**	**Cantidad**	**Marca**	**Modelo**	**País de origen**	**Año de fabricación**	**Cumple (Sí/No)**
1							
2							
3							
…							
7…							

DETALLE DEL CUMPLIMIENTO POR ÍTEM

Ítem N.° ___
Descripción del bien:

N.°	**Requerimiento técnico mínimo EETT**	**Datos del equipo ofertado**	**Cumple (Si/No)**	**Sustento de corresponder (Folio Nº)**
1		• Marca: • Modelo: • Fabricante: • País de origen: • Año de fabricación:		

2				
3				
…				

(Repetir la misma estructura para cada uno de los ítems del lote).

En ese sentido, declaro que toda la información consignada es veraz y que los bienes ofertados cumplen con las especificaciones técnicas establecidas en la Sección VII de la Solicitud de Ofertas, que forman parte integral de las Bases del procedimiento de selección, y de resultar adjudicatario me comprometo a entregar los bienes y servicios conexos según las características técnicas requerido y en las condiciones señaladas, en la forma y detalles especificados.

Ciudad, ……..de …….de……..

_____

Firma y Sello del Representante Legal
Sello del postor/ Razón Social del Proveedor

ANEXO N° 02

Sustento de Cumplimiento obligatorio de las Características Técnicas de las Especificaciones Técnicas.

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Switch Spine Data Center (02 Unidades)			
Debe contar con 32 puertos QSFP28 (con capacidad de conectar transceivers a 40 o 100 Gbps).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 16GB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 64GB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer no menor a 32MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de conmutación no menor a 6.4 Tbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío de paquetes no menor a 2 Bpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 90K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 130K y rutas IPv6 de 30K	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
EEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1p y DSCP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN dinámica mediante BGP-EVPN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
BFD y ECMP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
DCBx, PFC, ETS, ECN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VRF.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch Leaf Data Center (08 Unidades)			
Debe contar con 48 puertos SFP28 (con capacidad de conectar transceiver a 1, 10 ó 25 Gbps) y 6 puertos QSFP28 (con capacidad de conectar transceiver a 40 ó 100 Gbps	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 32GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 64GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer no menor a 32MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Capacidad de conmutación no menor a 3.6 Tbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío de paquetes no menor a 2 Bpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 98K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 130K y rutas IPv6 de 30K	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN dinámica mediante BGP-EVPN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
BFD y ECMP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
DCBx, PFC, ETS, ECN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VRF.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Solución de Orquestador DC (01 Unidad)			
La solución deberá contar con la capacidad de orquestar los switches de Data Center spine y leaf ofertados como un único fabric, simplificando las operaciones y la resolución de problemas en infraestructura de red de Centros de Datos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Debe permitir la automatización de las configuraciones VXLAN entre varias sedes	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Debe permitir la creación de políticas basadas en etiquetas de vSphere o nombres de MV.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch Core LAN Campus (02 Unidades)			
Debe contar con 32 puertos SFP28 (con capacidad de conectar transceiver a 1, 10 ó 25 Gbps) y 4 puertos QSFP28 (con capacidad de conectar transceiver a 40 ó 100 Gbps).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer no menor a 32MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de conmutación no menor a 2.4 Tbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío de paquetes no menor a 1.7 Bpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 80K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 130K y rutas IPv6 de 30K	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1p y DSCP	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN dinámica mediante BGP-EVPN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
BFD y ECMP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
DCBx, PFC, ETS, ECN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VRF.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch de acceso 48 puertos PoE (22 Unidades + 01 unidad en spare)			
El switch debe contar con 48 puertos RJ45 10/100/1000 Base-T con soporte de PoE 802.3at Clase 4 y 04 puertos de uplink SFP+ (con capacidad de conectar transceivers a 1 o 10 Gbps).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 8 GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 8 GB.	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
	documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío no menor a 130 Mpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de switching no menor a 176 Gbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer mínimo de 6 MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 32K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1p y DSCP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN estática	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por RADIUS, para los usuarios de	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
la red que se autentican vía 802.1x.	documentación técnica pública y oficial del fabricante.		
RADIUS y RADIUS CoA.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch de acceso 24 puertos PoE (04 Unidades)			
El switch debe contar con 24 puertos RJ45 10/100/1000 Base-T con soporte de PoE 802.3at Clase 4 y 04 puertos de uplink SFP+ (con capacidad de conectar transceivers a 1 o 10 Gbps).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 8 GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 8 GB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío no menor a 95 Mpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de switching no menor a 128 Gbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer mínimo de 6 MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 32K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
	documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN estática	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por RADIUS, para los usuarios de la red que se autentican vía 802.1x.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
RADIUS y RADIUS CoA.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch DMZ (02 Unidades)			
Debe contar con 24 puertos SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps) y 04 puertos SFP56 (con capacidad de conectar transceivers a 1, 10, 25 ó 50 Gbps	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 8 GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 32 GB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío no menor a 654 Mpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de switching no menor a 880 Gbps.	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
	documentación técnica pública y oficial del fabricante.		
Buffer mínimo de 8 MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 32K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 32K y rutas IPv6 de 16K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1p y DSCP	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN estática	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VRF	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Switch de Gestión Fuera de Banda (02 Unidades)			

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
El switch debe contar con 48 puertos RJ-45 10/100/1000 Base T con y 04 puertos SFP+ (con capacidad de conectar transceivers a 1 o 10 Gbps).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria RAM: Mínimo 8 GB	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Memoria Flash o SSD: Mínimo 8 GB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de reenvío no menor a 130 Mpps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de switching no menor a 176 Gbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Buffer mínimo de 6 MB.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de tabla de direcciones MAC no menor a 32K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Spanning Tree (802.1w, 802.1s y 802.1d).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
IEEE 802.1ab LLDP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping.	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
	documentación técnica pública y oficial del fabricante.		
IEEE 802.1p y DSCP.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
VXLAN estática	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Controlador Inalámbrico (02 Unidades)			
Características de controlador en formato appliance hardware: • Mínimo cuatro (04) puertos SFP+ (con capacidad de conectar transceivers a 1 o 10 Gbps). Se deberá incluir dos (02) transceivers 10GE-SR por cada equipo ofertado.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
• Un (01) puerto consola RJ45 o similar.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
• Fuente redundante de energía.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
• Capacidad de poder registrar/controlar al menos 3000 dispositivos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
• Capacidad de mantener conectados al menos 9000 clientes/endpoints simultáneos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
▪ Capacidad de manejar 30,000 túneles	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
• Throughput no menor de 10 Gbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Access Point (43 Unidades + 04 Unidades en Spare			

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Antenas omnidireccionales integradas para MIMO 2x2	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Access point para interiores de tres radios: 2.4Ghz, 5Ghz y 6Ghz	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Ganancia de antena mínimo de 4 dBi en 2.4GHz, 7 dBi en 5GHz y 6 dBi en 6Ghz.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
ACC (Advanced Cellular Coexistence)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
MRC (Maximum Ratio Combining)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
CDD/CSD (Cyclic Delay/Shift Diversity)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
STBC (Space-Time Block Coding)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
LDPC (Low-Density Parity Check)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
TxBF (transmit beam-forming)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
TWT (Target Wait Time)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
FTM (Fine Timing Measurement	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
A-MPDU, A-MSDU	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Dos interfaces 100/1000/2500 BASE-T Ethernet (RJ-45)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
Radio BLE (Bluetooth Low Energy) y Zigbee (802.15.4	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Solución de Administración y Gestión de Campus			
En el caso de una solución en premisa, deberá incluir alta disponibilidad de todos sus servicios. Cada appliance físico deberá tener: Dos (02) interfaces de 10Gbps Fuente de poder redundante Altura no mayor a dos (02) Rack Units (RUs) Kit para poder ser instalado en rack de 19”	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
En el caso de una solución en nube, se deberá presentar documentación o carta del fabricante que indique un SLA no menor a 99.95%. No se aceptarán soluciones basadas en VMs que obliguen a la institución a gestionar o contratar un Tenant de nube pública.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Debe realizar el aprovisionamiento de los dispositivos de red por medio de PnP (Plug and Play) o ZTP (Zero Touch Provisioning)	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
La solución debe mostrar el mapa topológico de la red.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Debe incluir integración por medio de APIs.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Solución de Control de Acceso (01 Unidad)			
- La solución debe centralizar el control de acceso de usuarios administradores a dispositivos de red de la entidad vía TACACS+ para autenticación, autorización y accounting.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
- La solución debe basarse en un esquema AAA (autenticación, autorización y accounting).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
- La solución debe soportar y tener habilitados los siguientes	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
métodos de autenticación como mínimo: ▪ PAP ▪ OAuth2	documentación técnica pública y oficial del fabricante.		
▪ CHAP			
▪ EAP-MSCHAPv2			
▪ EAP-MD5			
▪ PEAP			
▪ EAP-TLS			
▪ EAP-GTC			
▪ MAC Authentication			
▪ WEB Authentication			
▪ EAP-FAST			
▪ EAP-PWD			
▪ SAML			
- Identificación y clasificación (profiling) basada en datos contextuales tales como: ▪ MAC OUIs	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
▪ Nmap Scan			
▪ DHCP fingerprints			
▪ TCP fingerprints			
▪ HTTP user agent			
▪ SNMP traps			
▪ LLDP			
▪ Netflow / IPFIX			
▪ WMI			
▪ Span Port			
Plataforma de la solución en formato appliance, mínimo de dos (02) nodos (appliances físicos) redundantes, con capacidad de soportar cada uno al menos 60,000 dispositivos endpoints autenticados simultáneamente.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Cada nodo deberá tener dos (02) conexiones 10GE-SR para conectarse con la red.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Deberá soportar Microsoft Active Directory Deberá soportar base de datos internas.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Deberá soportar Kerberos	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Deberá soportar LDAP	Esta capacidad deberá sustentarse mediante		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita	Sustento (Folio Nº)
	documentación técnica pública y oficial del fabricante.		
Deberá soportar SQL server compatible con ODBC	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Deberá soportar listas estáticas	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		
Deberá soportar listas estáticas	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.		

HIPERCONVERGENCIA

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Hardware de Hiperconvergencia		
La solución hiperconvergente por definición es cómputo, virtualización y storage totalmente definido por software. Los nodos HCI deben encontrarse en la matriz de compatibilidad e interoperabilidad del fabricante del software. Los nodos HCI deben estar identificado en el portal del fabricante del hardware como appliance o sistema hiperconvergente.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de que el hardware sea certificado por el software hiperconvergente. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Dos (02) procesadores x86 de la última generación, con fecha de lanzamiento 2025 como mínimo, de 12 cores como mínimo, de al menos 2.2GHz de frecuencia base y mínimo 48MB de cache L3. Debe soportar la tecnología Hyper-Threading o Multithreading	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de que los procesadores sean de última generación. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Cada servidor o nodo HCI deberá contar con discos SSD NVMe intercambiables en caliente, deberá incluir al menos 10 bahías para discos SSD NVMe. La solución hiperconvergente (HCI) debe ser configurada para permitir la tolerancia de fallos ante la caída de un (01) servidor o nodo (N+1) La capacidad efectiva o usable total de almacenamiento de la solución HCI deberá ser de al menos 50TiB SSD NVMe en RF2 o RAID 1 o mirror, sin considerar factores de eficiencia como compresión y de duplicación.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de las capacidades. No se aceptarán cartas de fabricante para dicho cumplimiento.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
El dimensionamiento deberá ser sobre arquitectura de acceso directo a la capa de almacenamiento NVMe. La solución debe realizar réplicas de datos almacenados a través de los nodos de clúster.		
Cuatro (04) puertos Ethernet de 25Gb SFP28, deben incluir sus respectivos transceivers SR SFP28 y cables de fibra LC-LC MM OM3 de mínimo 3 metros. los cuales se utilizarán para garantizar redundancia de conectividad LAN y para la interconexión de la solución hiperconvergente.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de la cantidad de puertos y velocidades. No se aceptarán cartas de fabricante para dicho cumplimiento.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Software Hiperconvergencia		
El licenciamiento del software debe ser por suscripción, del tipo OPEN, de forma que no esté vinculado a un solo fabricante de hardware.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	
La solución deberá ser agnóstica al hipervisor y debe soportar distintos hipervisores como: VMware ESXi y basados en Linux KVM.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Deberá soportar el crecimiento scale-out en nodos heterogéneos, o diferentes modelos para maximizar recursos de procesamiento, memoria o almacenamiento según requiera.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Servidor para backup		
Un (01) procesador x86 de la última generación, con fecha de lanzamiento 2025 como mínimo, cada procesador de 12 cores como mínimo, de al menos 2.2 GHz de frecuencia base y mínimo 48 MB de cache L3.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
El servidor debe soportar el crecimiento hasta dos (02) procesadores.	de fabricante para dicho cumplimiento.	
Dos (02) puertos Ethernet de 25Gb SFP28, deben incluir sus respectivos transceivers SR SFP28 y cables de fibra LC-LC MM OM3 de mínimo 5 metros.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de la cantidad de puertos y velocidades. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Dos (02) discos SSD de 3.84TB como mínimo configurados en RAID 1. Los discos deben poder ser intercambiables en caliente. Deberá incluir el backplane con soporte de al menos ocho (08) discos.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento de la capacidad solicitada y de la cantidad de puertos, así como también las velocidades. No se aceptarán cartas de fabricante para dicho cumplimiento.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Almacenamiento para backup		
Deberá estar diseñado para una disponibilidad de 99.9999%, deberá poder ser verificado en la documentación pública del fabricante del sistema de almacenamiento.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Dos controladoras en configuración activo-activo con balanceo de carga automático.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Dos (02) puertos iSCSI de 10/25 Gb, deben incluir sus respectivos transceivers.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Librería de backup		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
La librería deberá incluir cuarenta (40) slots para cartuchos de cinta magnética LTO en su máxima configuración.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	
Cada tape drive LTO9 debe incluir como mínimo un (01) puerto en fibra canal (FC) para conectarse al servidor de backup solicitado, cada uno de estos puertos debe ser de 8 Gbps como mínimo.	El postor deberá presentar documentación pública del fabricante o brochure que sustente el cumplimiento. No se aceptarán cartas de fabricante para dicho cumplimiento.	

CIBERSEGURIDAD

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Firewall NGFW Perimetral (02 Unidades)		
Deberá tener un rendimiento de Prevención de Amenazas de 28 Gbps cuando opera en simultáneo: Application Control, firewall, IPS, Antivirus/Anti-Bot/Antispyware o 14 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7) teniendo las siguientes funcionalidades habilitadas de manera simultánea: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. La solución debe operar bajo una arquitectura de procesamiento único donde todas las funciones de seguridad se apliquen simultáneamente sobre el mismo flujo de tráfico.	El postor deberá presentar documentación pública del fabricante que sustente el cumplimiento del performance y condiciones de medición requeridas. No se aceptarán cartas de fabricante como sustentos para el cumplimiento del performance y condiciones de medición solicitadas.	
El equipo debe soportar como mínimo 20 millones de sesiones concurrentes medidas con transacciones TCP o 2.5 millones medidas con transacciones HTTP. El equipo debe soportar 800 mil nuevas sesiones por segundo medidas con transacciones TCP o 200 mil nuevas sesiones por segundo medidas con transacciones HTTP.	El postor deberá presentar documentación pública que sustente expresamente la metodología de medición de sesiones concurrentes y sesiones por segundo utilizada por el fabricante, precisando si corresponde a transacciones TCP (L4) o HTTP (L7). No se aceptarán equivalencias sustentadas mediante cartas de fabricante.	
Debe incluir mínimo 12 interfaces de 1G/2.5G/5G/10G RJ-45, 10 interfaces de	Las interfaces requeridas deberán encontrarse activas, soportadas y	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
10Gbps SFP/ SFP+, 4 interfaces de 25Gbps SFP28 y 2 interfaces de 40G/100GGbps QSFP28.	documentadas públicamente por el fabricante. No se aceptarán habilitaciones futuras, roadmap de producto ni cartas de compromiso.	
Capacidad de inspeccionar el contenido en túneles GRE, opcionalmente GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.	Esto deberá encontrarse expresamente documentado en información pública del fabricante	
Debe incluir capacidades de identificación y perfilado de dispositivos conectados a la red (incluyendo dispositivos IoT/OT), permitiendo su clasificación, evaluación de riesgo y aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, sin requerir la instalación de agentes adicionales	Las capacidades de identificación y perfilado de dispositivos IoT, asi como la aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, deberán sustentarse con documentación públicamente del fabricante, no se aceptará integración con otros componentes ni carta de fabricante para sustentar lo solicitado.	
Firewall Interno (02 Unidades)		
- Deberá tener un rendimiento de Prevención de Amenazas de 110 Gbps cuando opera en simultáneo: Application Control, firewall, IPS, Antivirus/Anti-Bot/Antispyware o 48 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7) teniendo las siguientes funcionalidades habilitadas de manera simultánea: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. La solución debe operar bajo una arquitectura de procesamiento único donde todas las funciones de seguridad se apliquen simultaneamente sobre el mismo flujo de tráfico.	El postor deberá presentar documentación pública del fabricante que sustente el cumplimiento del performance y condiciones de medición requeridas. No se aceptarán cartas de fabricante como sustentos para el cumplimiento del performance y condiciones de medición solicitadas.	
El equipo debe soportar como mínimo 80 millones de sesiones concurrentes medidas con transacciones TCP o 7 millones medidas con transacciones HTTP. El equipo debe soportar 1.2 millones de nuevas sesiones por segundo medidas con transacciones TCP o 370 mil nuevas sesiones por segundo medidas con transacciones HTTP.	El postor deberá presentar documentación pública que sustente expresamente la metodología de medición de sesiones concurrentes y sesiones por segundo utilizada por el fabricante, precisando si corresponde a transacciones TCP (L4) o HTTP (L7). No se aceptarán equivalencias sustentadas mediante cartas de fabricante.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Debe incluir mínimo 8 interfaces de 1G/2.5G/5G/10G RJ-45, 12 interfaces de 1G/10G SFP/ SFP+, 4 interfaces de 25Gbps SFP28 y 4 interfaces de 40G/100GGbps QSFP28.	Las interfaces requeridas deberán encontrarse activas, soportadas y documentadas públicamente por el fabricante. No se aceptarán habilitaciones futuras, roadmap de producto ni cartas de compromiso.	
Capacidad de inspeccionar el contenido en túneles GRE, opcionalmente GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.	Esto deberá encontrarse expresamente documentada en información pública del fabricante.	
Debe incluir capacidades de identificación y perfilado de dispositivos conectados a la red (incluyendo dispositivos IoT/OT), permitiendo su clasificación, evaluación de riesgo y aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, sin requerir la instalación de agentes adicionales.	Las capacidades de identificación y perfilado de dispositivos IoT, así como la aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, deberán sustentarse con documentación públicamente del fabricante, no se aceptará integración con otros componentes ni carta de fabricante para sustentar lo solicitado	
Consola de analítica y reportes		
La solución deberá contar con una plataforma de almacenamiento centralizado de logs de seguridad, que permita la ingesta continua de telemetría sin restricciones por volumen de datos y que incluya una capacidad de retención de logs de al menos un (01) año.	La capacidad de retención de logs requerida deberá estar expresamente sustentada mediante documentación pública y oficial del fabricante, incluyendo las condiciones de licenciamiento y operación correspondientes. No se aceptarán declaraciones comerciales ni cartas de fabricante como sustento único	
Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red.	Las capacidades de evaluación automática de buenas prácticas, gráficas de adopción de los módulos de seguridad y el módulo de filtrado y depuración de reglas deberán ser expresamente sustentadas con información pública y oficial del fabricante	
XDR (Extended Detection & Response) – 1 solución		
La solución deberá ser de tipo XDR (Extended Detection & Response) y permitir la operación centralizada de capacidades de detección, análisis y respuesta para endpoints, formando parte de una plataforma unificada de operaciones de seguridad que integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la	Estas capacidades deberán encontrarse expresamente documentadas en información pública y oficial del fabricante, no se aceptará integración con otros componentes ni carta de fabricante para sustentar lo solicitado	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.		
La solución XDR deberá permitir la integración con la solución SIEM propuesta o formar parte de la misma plataforma, habilitando el envío y consumo de telemetría de seguridad, de forma nativa y estructurada, sin requerir desarrollos personalizados o procesos complejos de normalización, garantizando su uso para correlación, análisis y respuesta automatizada	La capacidad de integración nativa, intercambio estructurado de telemetría y correlación y respuesta automatizada entre la solución XDR y la solución SIEM deberá encontrarse expresamente documentada mediante documentación pública y oficial del fabricante.	
El mismo agente de Endpoint Protectión deberá ser capaz de colectar la siguiente telemetría para equipos MacOS y Linux: • Logs de eventos de autenticación • Actividades de creación, escritura, renombre, eliminación, modificación de archivos. • Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma digital. • Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP). • Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.	Las capacidades de recolección de telemetría continua, almacenamiento estructurado y disponibilidad de telemetría para analítica y threat hunting deberán sustentarse expresamente mediante información pública y oficial del fabricante. No se aceptarán cartas de fabricante, declaraciones juradas ni documentos emitidos específicamente para el presente proceso.	
Con base en el comportamiento aprendido, el módulo de UEBA deberá ser capaz de detectar y alertar actividades inusuales o desviaciones significativas respecto al perfil base establecido. Deberá tener al menos 150 casos de uso nativos, generados por machine learning, incluyendo los siguientes: • Comandos anómalos ejecutados en el endpoint • Múltiples procesos LOLBINs ejecutados • Procesos raros ejecutados sobre el endpoint	Toda capacidad asociada a aprendizaje automático no supervisado, perfiles base, UEBA, modelos analíticos, generación automática de comportamientos y casos de uso nativos deberá sustentarse expresamente mediante documentación pública y oficial del fabricante, en caso no pueda ser verificada bajo dicho criterio, será considerada como no sustentada para fines de evaluación técnica.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
• Eventos de Pass the ticket • Proceso conectándose a un sitio externo inusual • Comandos de powershell inusuales • Cifrado de datos sospechoso en el endpoint • Carga de driver inusual • Conexión anómala usando WMI • Servicio detenido de manera inusual • Tráfico LDAP generado desde un proceso inusual • Transferencia inusual de archivos por SMB		
ZTNA (Zero Trust Network Access) – 01 Solución		
Las políticas de validación de postura del endpoint deberán poder ser aplicadas a un grupo de usuarios o direcciones IP.	Las capacidades de validación de postura de seguridad del endpoint deberán sustentarse mediante documentación pública oficial del fabricante.	
La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada, de manera manual y automática. Los equipos en cuarentena no deberán tener conexión con ningún recurso de red protegido por la solución. Esta capacidad deberá tener cobertura dentro de la red interna, sin necesidad de hacer túneles VPN	Deberá sustentarse mediante documentación pública oficial del fabricante, no se aceptará cartas de fabricante.	
Este navegador web debe permitir el acceso seguro desde dispositivos no gestionados o de terceros, garantizando el aislamiento de la sesión y la protección de la información accedida.	La capacidad de acceso seguro mediante navegador web sin instalación de agentes (agentless), así como los mecanismos de aislamiento y control de acceso asociados, deberán encontrarse debidamente sustentados mediante documentación pública y oficial del fabricante.	
Seguridad para correo electrónico – 01 solución		
El servicio de correo electrónico es Zimbra, por lo que la solución deberá integrarse mediante protocolos SMTP, operando como gateway de correo electrónico a través de registros MX, permitiendo la inspección completa del tráfico entrante y saliente antes de su entrega.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
La solución deberá contar con mecanismos avanzados de protección de URLs que permitan analizar los enlaces contenidos en los correos electrónicos mediante técnicas como reescritura de URLs, evaluación de reputación en tiempo	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
real y análisis dinámico en el momento de interacción del usuario (time-of-click), con el fin de identificar y bloquear enlaces maliciosos antes y después de su entrega al usuario final.		
La solución deberá contar con capacidades de análisis avanzado de archivos adjuntos mediante tecnología de sandboxing, integrada dentro de un modelo de protección multicapa que combine técnicas de análisis estático, reputación, machine learning y análisis dinámico selectivo, permitiendo la detección de amenazas conocidas y desconocidas en archivos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
La solución deberá garantizar que los procesos de análisis de archivos adjuntos se realicen sin alterar su estructura ni contenido original, utilizando mecanismos de análisis seguros como entornos aislados (sandbox) y técnicas de inspección que operen sobre copias del archivo, manteniendo la integridad del contenido original	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
La solución deberá operar mediante un modelo Secure Email Gateway (SEG) en modo inline, integrándose con el servicio de correo mediante registros MX, permitiendo la prevención de amenazas en tránsito antes de la entrega al usuario final.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
WAF - Seguridad para Aplicaciones Web		
Modalidad del Servicio		
Tipo de Despliegue: La solución debe ser entregada bajo la modalidad de Software as a Service (SaaS) basado en la nube.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Licenciamiento		
Mitigación de DDoS en Capa 7: Debe incluir protección nativa contra ataques de denegación de servicio distribuidos dirigidos específicamente a la capa de aplicación (HTTP/HTTPS).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Capacidades de Seguridad		
Protección contra Top 10 de OWASP: Debe mitigar de forma automática amenazas como Inyección SQL, Cross-Site Scripting (XSS), rotura de autenticación, entre otros.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Políticas de Seguridad Positiva y Negativa: Capacidad de combinar firmas de ataque conocidas con modelos de comportamiento para detectar amenazas "Zero-day".	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
SIEM (01 Solución)		
La solución deberá realizar monitoreo, correlación y análisis de eventos de seguridad (SIEM), formando parte de una plataforma unificada de operaciones de seguridad que	Esto deberá sustentarse expresamente mediante documentación pública y oficial del fabricante	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.		
Deberá ser capaz de recolectar y almacenar centralizadamente logs y telemetría de endpoints provenientes de agentes EDR/XDR, ya sean del mismo fabricante o de terceros. El Postor deberá incluir el licenciamiento necesario para habilitar esta capacidad. Se entiende por telemetría no solo las alertas generadas por el EDR/XDR, sino también la actividad detallada del endpoint, incluyendo como mínimo: procesos (creación/árbol/command-line), archivos (creación/modificación/lectura), registro (Windows Registry), sesiones e identidad (logon/logoff), actividad de red (conexiones/DNS), y otros eventos relevantes de seguridad	La capacidad de recolección de telemetría detallada de endpoint y compatibilidad con EDR/XDR de terceros deberá ser sustentada mediante documentación pública oficial del fabricante.	
Deberá tener conectores nativos para más de 1000 plataformas de terceros y ser capaz de normalizar los eventos de manera nativa, sin necesidad de escribir reglas de correlación	Debe sustentarse expresamente mediante documentación pública y oficial del fabricante, no se aceptarán como sustento cartas de fabricante, declaraciones juradas ni documentos emitidos específicamente para el presente proceso.	
Debe contar con al menos 500 casos de uso de detección de amenazas. Todos estos casos de uso deberán estar activados de manera automática, sin necesidad de construir una regla de correlación o afinamiento manual.	La capacidad de analítica para la construcción de línea base, generación de alertas de anomalías y detección de amenazas deberá ser sustentada mediante documentación pública oficial del fabricante.	
Plataforma de Detección y Respuesta de Amenazas Externas e Internas (01 Solución)		
La solución deberá formar parte de una plataforma unificada de operaciones de seguridad que permita complementar estas capacidades con la detección y respuesta de amenazas internas, mediante la integración y correlación de telemetría proveniente de diferentes fuentes de seguridad	Esto deberá sustentarse expresamente mediante documentación pública y oficial del fabricante, no se aceptarán como sustento cartas de fabricante, declaraciones juradas ni documentos emitidos específicamente para el presente proceso.	
Deberá descubrir servicios cloud expuestos a Internet que no estén gestionados y/o no sean conocidos por la Entidad.	Las técnicas de descubrimiento requeridas deberán encontrarse expresamente documentados	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
	mediante información pública oficial del fabricante.	
Deberá permitir administrar los test de escaneo, permitiendo habilitar o deshabilitar los test. Por cada test deberá mostrar información como software afectado, identificadores de vulnerabilidad (CVE/CWE), score de severidad (CVSS), probabilidad de explotación (EPSS), referencias, guía de remediación, estado de habilitación y cantidad de servicios confirmados como vulnerables.	Las capacidades de escaneo solicitadas deberán ser sustentadas mediante mediante documentación pública oficial del fabricante.	
SOAR – Solución de Orquestación de Seguridad, Automatización y Respuesta (01 Solución)		
La solución deberá contar con un catálogo de al menos 800 playbooks predefinidos, orientados a automatizar la respuesta ante incidentes de seguridad. Dichos playbooks deberán poder personalizarse según las necesidades de la Entidad.	La cantidad mínima de playbooks predefinidos y las capacidades de personalización deberán sustentarse mediante información pública y oficial del fabricante. No se aceptarán cartas de fabricante como sustento.	
La solución deberá permitir crear bucles dentro de un playbook principal mediante sub-playbooks, donde cada iteración calcule sus valores usando los datos del sub-playbook	Esto deberá sustentarse expresamente mediante documentación pública y oficial del fabricante, no se aceptarán como sustento cartas de fabricante, declaraciones juradas ni documentos emitidos específicamente para el presente proceso.	
Los playbooks deben poder ser ejecutados como tareas programadas, es decir, sin necesidad de que exista una alerta o incidente de seguridad un playbook puede ejecutarse de manera periódica (permitiendo especificar la periodicidad) para automatizar alguna tarea.	Esto deberá sustentarse expresamente mediante documentación pública y oficial del fabricante, no se aceptarán como sustento cartas de fabricante, declaraciones juradas ni documentos emitidos específicamente para el presente proceso.	
La plataforma deberá ofrecer una interfaz unificada para interactuar con agentes de IA predefinidos y personalizados, capaces de planificar y ejecutar flujos de trabajo de múltiples pasos	Esto deberá sustentarse expresamente mediante documentación pública y oficial del fabricante.	
ADC (application Delivery Controller) (02 Unidades)		
Arquitectura y Capacidad de Hardware		
Chasis Físico: El equipo debe ser un appliance de propósito específico (Hardware-based) con una capacidad física de cómputo (throughput) de hasta 40 Gbps.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Procesamiento: Debe contar con una arquitectura multi-core optimizada, incluyendo un procesador de al menos 12 núcleos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
Rendimiento y Licenciamiento		
Capacidad de Sesiones: Debe soportar un mínimo de 46 millones de conexiones concurrentes en Capa 4.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Transacciones por Segundo: Capacidad para procesar al menos 1.8 millones de peticiones por segundo (RPS) en Capa 7.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Conectividad Física y Escalabilidad		
Puertos de Cobre: Al menos ocho (08) puertos 10/100/1000 Mbps Base-T (RJ45) para gestión y servicios auxiliares.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Puertos de Fibra (Acceso/Agregación): Al menos ocho (08) puertos con soporte nativo para 10 GbE (SFP+).	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Puertos de Alta Velocidad (Core): Al menos cuatro (04) puertos con soporte nativo para 25 GbE (SFP28) para interconexión de alta velocidad.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Anti – DDoS (02 Unidades)		
Arquitectura y Componentes de la Solución		
Mecanismo de Bypass: Los puertos de cobre deben contar con un mecanismo de derivación (bypass) físico incorporado para garantizar la continuidad del tráfico en caso de fallo del equipo.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Rendimiento y Performance		
Rendimiento de Mitigación: La solución debe admitir un rendimiento total de inspección y mitigación de hasta 10 Gbps al 100% de la carga.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Latencia Máxima: La inspección del tráfico debe mantener una latencia ultra-baja, no superior a los 70 microsegundos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Capacidades de Detección y Mitigación		
Firmas en Tiempo Real: Capacidad de generar firmas automáticas (Real-Time Signatures) para ataques de día cero en un tiempo inferior a los 15 segundos sin intervención humana.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Licenciamiento y Servicios Críticos		
Cloud Signaling: El licenciamiento debe permitir la comunicación automática entre el equipo on-premise y el centro de inteligencia del fabricante.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Solución de Análisis de Tráfico de Red - (01 Solución)		
Debe contar con una vista de alto nivel del estado de la infraestructura que permita agrupar y explorar dinámicamente nodos, identificando de inmediato los puntos conflictivos.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Debe permitir el monitoreo de métricas clave de salud del sistema operativo y rendimiento de	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
aplicaciones mediante protocolos estándar o agentes.		
Debe presentar el rendimiento a nivel de dispositivo y a nivel de puerto/interfaz mediante gráficos de línea y estadísticas de entrada/salida.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
MFA – Administración de Identidad y Acceso (01 Solución)		
La solución se debe basar en algoritmos de aprendizaje de máquina (machine learning) no supervisados. Es decir, los modelos estadísticos con los casos de uso ya deben estar listos y calibrados.	Esta capacidad deberá sustentarse expresamente mediante documentación pública y oficial del fabricante.	
La solución debe ofrecer un componente/software para intermediar el SSO en aplicaciones web que se encuentren en el centro de procesamiento de datos de la entidad, sin necesidad de exponer a estas aplicaciones al uso de internet o de VPN.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Soporte para SSO mediante IWA (Integrated Windows Authentication), que reutiliza el login de red para autenticación en las aplicaciones web sin necesidad de ingresar con usuario y contraseña nuevamente	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante, no se aceptarán cartas de fabricante como sustento.	
PAM – Administración de Acceso Privilegiado (01 Solución)		
La solución propuesta deberá tener la capacidad de cifrar, en reposo y en tránsito todos los datos que utilice. Incluyendo contraseñas, reportes almacenados, grabaciones y registros de usuarios. Lo anterior utilizando algoritmos que cumplan con los estándares en FIPS 140-2, como AES-256 y RSA-2048.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
La solución propuesta deberá tener mecanismos de detección y alerta cuando se detecta una desviación en el patrón de comportamiento de un usuario humano al recuperar/obtener un secreto de la bóveda digital o de la plataforma. Esta detección puede indicar un abuso de la plataforma de identidades y la vulnerabilidad o brecha de la identidad del usuario.	La arquitectura de la bóveda digital, incluidas sus capacidades, deberán sustentarse mediante documentación técnica pública y oficial del fabricante.	
La solución debe tener la capacidad de entregar un acceso remoto seguro (externo a la red corporativa) a los usuarios sin necesidad de instalación de clientes VPN en los dispositivos de usuarios remotos y garantizando un acceso seguro con MFA sin necesidad de modificar los recursos de autenticación corporativos como el AD.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
NDR (Network Detection and Response) (01 Solución)		

Característica Técnicas a sustentar de las EETT	Acreditación documental requerida	Documento Sustento que lo acredita / Sustento (Folio Nº)
El sensor debe ser capaz de recolectar y enviar automáticamente la siguiente telemetría de red: o Logs avanzados o telemetría detallada, es decir eventos que incluyan contenido de la aplicación de red en capa 7, cabecera HTTP, querys de DNS, información del tráfico DHCP y otros datos de la telemetría de red. o Eventos del tráfico mostrando: IP y puerto origen y destino, nombre de la aplicación en capa 7, país origen y destino, IP NAT de origen y destino, usuario de dominio, Bytes enviados y recibidos, Paquetes enviados y recibidos, DNS Querys, información sobre tráfico DHCP. o Nombre, serial number, nombre de la política y/o regla de seguridad de los Firewalls. o Nombre, tipo, categoría y severidad de la amenaza identificada. o Nombre del archivo transferido a través del tráfico de red. o Logs de tráfico URL, detallando URL accedida, categoría, severidad, hora, IP origen/destino, usuario, país de la URL, User-Agent de los paquetes HTTP. o Atributos de los dispositivos de red, tales como tipo de dispositivo, categoría, marca, sistema operativo, fabricante del dispositivo.	Las capacidades de extracción de telemetría, análisis de tráfico y mecanismos utilizados para la obtención de información de red deberán sustentarse mediante información pública oficial del fabricante	
La solución deberá emplear algoritmos avanzados de inteligencia artificial y aprendizaje automático, incluyendo como mínimo Machine Learning supervisado, no supervisado y técnicas de Deep Learning, orientados a la detección de amenazas conocidas y desconocidas	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Sandboxing (01 Solución)		

Característica Técnicas a sustentar de las EETT	**Acreditación documental requerida**	**Documento Sustento que lo acredita / Sustento (Folio Nº)**
Los firewalls deberán ser capaces de enviar 5000 archivos por hora al sandbox.	Esto deberá sustentarse mediante documentación técnica pública y oficial del fabricante, no se aceptará carta de fabricante para el sustento.	
Deberá contar con al menos 20 técnicas patentadas para realizar el análisis del malware.	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante.	
Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico	Esta capacidad deberá sustentarse mediante documentación técnica pública y oficial del fabricante	

En ese sentido, me comprometo a entregar el bien con las características, en la forma y detalles especificados.

Ciudad, ……..de …….de……..

_____

Firma y Sello del Representante Legal
Sello del postor/ Razón Social del Proveedor

Nota: *Consignar el número de folio del sustento de la característica técnicas, deberá presentar un formato por cada bien y/o equipo ofertado.*

ANEXO N° 03

Declaración Jurada de Compromiso de Garantía, Soporte y Mantenimiento de los Bienes y Licencias Ofertados

Señores
COMITÉ DE EVALUACIÓN
PROCESO SDO Nº PE-PRONATEL-569321-GO-RFB

Presente. -

El que suscribe, _____, identificado con DNI Nº _____, en calidad de Representante Legal de _____, con RUC Nº _____, declaro bajo juramento que, de resultar adjudicado, mi representada se compromete a otorgar la garantía, soporte y mantenimiento de los bienes, licencias y servicios asociados ofertados, conforme a las condiciones establecidas en las Especificaciones Técnicas de la presente contratación.

La garantía comprenderá la atención de fallas, defectos de fabricación, reemplazo o reparación de componentes, actualización de versiones, parches de seguridad y demás prestaciones requeridas para asegurar la continuidad operativa de la solución implementada durante el período de garantía establecido.

Nº	BIENES / SOLUCIONES	GARANTÍA Y SOPORTE MÍNIMO	ACREDITACIÓN
1	Todos los bienes, equipos, software y soluciones comprendidos en el Lote Único, según corresponda.	Doce (12) meses, 24x7 on-site, con tiempo de respuesta de cuatro (04) horas, más las condiciones particulares establecidas en el Anexo 3 de las EETT.	Declaración Jurada de Compromiso y respaldo del fabricante/canal autorizado cuando corresponda.

Asimismo, declaro que mi representada garantizará:

- La disponibilidad de soporte técnico durante el período establecido en las Especificaciones Técnicas, incluyendo atención bajo modalidad **24x7**, generación de tickets y tiempos de respuesta conforme a los niveles de servicio requeridos.
- La atención de incidencias, mantenimiento preventivo y correctivo, así como la aplicación de actualizaciones y parches de seguridad proporcionados por los fabricantes.
- La continuidad operativa de la solución implementada durante el período de garantía, incluyendo los bienes, licencias, configuraciones e integraciones realizadas como parte del contrato.

La vigencia de la garantía y servicios asociados iniciará a partir de la suscripción del Acta de Aceptación Operativa, cconforme a lo establecido en las Especificaciones Técnicas.

La presente declaración será respaldada, de corresponder, mediante las cartas de garantía, soporte y respaldo emitidas por los fabricantes de los bienes ofertados, conforme a los requisitos establecidos en los Documentos de Licitación.
En señal de conformidad, suscribo la presente declaración.

Nombre del Licitante*:

Nombre de la persona debidamente autorizada para firmar la Oferta en nombre del Licitante**: _____

Cargo de la persona firmante del Formulario de la Oferta: _____

Firma de la persona nombrada anteriormente: _____

Fecha de la firma: El día _____ del mes _____ del año _____.

***** En el caso de las Ofertas presentadas por una APCA, especifique el nombre de la APCA que actúa como Licitante.

** La persona que firme la Oferta deberá contar con el poder otorgado por el Licitante. El poder deberá adjuntarse a los Formularios de la Oferta.

[Nota: En caso de que se trate de una APCA, la Declaración de Mantenimiento de Oferta deberá emitirse en nombre de todos los miembros de la APCA que presenta la Oferta].

Formulario PER – 1
Personal Clave propuesto
Formulario

Los Licitantes deberán suministrar los nombres y otros detalles de las personas clave debidamente calificadas para cumplir con el Contrato. La información sobre su experiencia se deberá consignar utilizando el Formulario PER-2 de los que aparecen más abajo para cada candidato.

Personal Clave

1.	**Título de la posición:** *[insertar título]*	
	Nombre del candidato:	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*
	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*
2.	**Título de la posición:** *[insertar título]*	
	Nombre del candidato:	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*
	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*
3.	**Título de la posición:** *[insertar título]*	
	Nombre del candidato:	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*
	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*
4.	**Título de la posición:** *[insertar título]*	
	Nombre del candidato:	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*

	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*
5	**Título de la posición:** *[insertar título]* *[**Cuando los riesgos EAS de un Proyecto sean sustanciales o altos, el Personal clave debe incluir un especialista** en Explotación Sexual, Abuso y Acoso Sexual **con experiencia pertinente en tratar casos de** en explotación sexual, abuso y acoso sexual]*	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*
	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*
6.	**Título de la posición:** *[insertar título]*	
	Nombre del candidato:	
	Duración del nombramiento:	*[insertar la duración (fechas de inicio y terminación) para la cual esta posición será retenida]*
	Tiempo destinado a esta posición:	*[insertar el número de días/semanas/meses planeados para esta posición]*
	Calendario planeado para esta posición:	*[insertar el calendario esperado para esta posición (por ejemplo, adjuntar el gráfico Gantt de primer nivel)]*

Formulario PER – 2:
Currículum Vítae del Personal Propuesto

Nombre del Licitante

Cargo ***[#1] [título del puesto según Formulario PER-1]***		
Información personal	**Nombre***	**Fecha de nacimiento**
	Dirección:	**Correo electrónico:**
	Calificaciones profesionales	
	Calificaciones académicas:	
	Conocimiento de idiomas: ***(idiomas y nivel de conversación, lectura y escritura)***	
Detalles		
	Dirección del empleador	
	Teléfono	**Persona de contacto (gerente / funcionario de personal)**
	Fax	
	Denominación del cargo	**Años con el empleador actual**

Resuma la experiencia profesional en orden cronológico inverso. Indique la experiencia particular, técnica y gerencial pertinente para este proyecto.

Proyecto	**Posición**	**Duración**	**Experiencia pertinente**
[principales características del proyecto]	*[posición y responsabilidades en el proyecto]*	*[tiempo en la posición]*	*[describir la experiencia pertinente de esta posición]*

Declaración

Yo, en mi calidad de miembro del personal clave abajo firmante, certifico que, a mi leal saber y entender, la información contenida en este Formulario PER-2 me describe correctamente, así como a mis calificaciones y a mi experiencia.

Confirmo que estoy disponible como certifico en la siguiente tabla y en todo el calendario previsto para esta posición, según lo dispuesto en la Oferta:

Compromiso	**Detalles**
Compromiso con la duración del contrato:	*[Indicar el período (fechas de inicio y de finalización) para el cual este personal clave está disponible para trabajar en este contrato]*
Compromiso de tiempo:	*[Inserte el número de días / semana / meses / que este personal clave será contratado]*

Entiendo que cualquier declaración falsa u omisión en este Formulario puede:

(a) que se tome en consideración durante la evaluación de la Oferta;

(b) causar mi descalificación para participar en la Oferta;

(c) causar mi despido del contrato.

Nombre del personal clave: ***[insertar nombre]***

Firma: _____

Fecha: (día/ mes/ año): _____

Firma del representante autorizado del Licitante:

Firma: _____

Fecha: (día/ mes/ año): _____

ANEXO N° 04

Formulario para Solicitud de Aclaración

SDO Nº PE-PRONATEL-569321-GO-RFB

“Adquisición de Equipamiento Ofimático y de Redes Lan para la Central 911 en el Marco del Proyecto Creación de un Sistema de Atención de Emergencias, Urgencias e Información Mediante un Número Único en Lima Metropolitana y El Callao - Proyecto 911”

LICITANTE:
……

CONSULTA N° 1
Referente a las bases: Sección: Numeral: Página: Consulta:

(i) Puede adicionar más bloques de filas según lo requiera.

Firmada: [firma del representante autorizado]. En capacidad de [indique el cargo]

Nombre: [indique el nombre en letra de molde o mecanografiado]

Debidamente autorizado para firmar la Oferta por y en nombre de: [indique el nombre la entidad que autoriza]

Fechada el [indique el día] día de [indique el mes] de [indique el año]

Declaración de Desempeño sobre Explotación y Abuso Sexual (EAS) y/o Acoso Sexual (ASx)

[El siguiente cuadro debe ser completada por el Licitante y cada miembro de la APCA o JV y cada subcontratista propuesto por el Licitante]

Nombre del Licitante: *[indicar el nombre completo]*
Fecha: *[insertar día, mes, año]*
SDO No. y Título: *[insertar la referencia de la SDO]*
Página *[insertar número de página] de [insertar número total] páginas*

Declaración EAS y /o ASx
Nosotros: ☐ (a) no hemos sido objeto de descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS/ASx. ☐ (b) no estamos sujetos a descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS/ASx ☐ (c) hemos sido descalificados por el Banco por incumplimiento de las obligaciones sobre EAS/ASx pero fuimos excluidos de las empresas descalificadas Se ha dictado un laudo arbitral en el caso de descalificación a nuestro favor.
[Si (c) anterior es aplicable, adjunte evidencia de un laudo arbitral que revierta las conclusiones sobre los problemas subyacentes a la descalificación.]

Formulario de Declaración de Mantenimiento de Oferta

[El Licitante completará este Formulario de Declaración de Mantenimiento de Oferta de acuerdo con las instrucciones indicadas].

Fecha: *[indique día, mes y año de presentación de la oferta]*.
Oferta n.°: *[número del proceso de la SDO]*.
Alternativa n.°: *[indique el n.° de identificación si se trata de una oferta por una alternativa]*.

Para: *[indique el nombre completo del Comprador]*.

Los suscriptos declaramos que:

Entendemos que, de acuerdo con sus condiciones, las Ofertas deberán estar respaldadas por una Declaración de Mantenimiento de Oferta.

Aceptamos que seremos declarados automáticamente inelegibles para participar en cualquier licitación de contrato con el Comprador por un período especificado en la Sección II - Datos de la Licitación (DDL), si incumplimos nuestras obligaciones derivadas de las condiciones de la oferta, a saber:

(a) si retiramos nuestra Oferta antes de la fecha de expiración de la validez de la Oferta especificado en la Carta de la Oferta, o cualquier fecha extendida otorgada por nosotros, o

(b) si, una vez que el Comprador nos ha notificado de la aceptación de nuestra Oferta antes de la fecha de expiración de la validez de la Oferta especificada en la Carta de la Oferta, o cualquier fecha extendida otorgada por nosotros, (i) no firmamos o nos negamos a firmar el Contrato, o (ii) no suministramos o nos negamos a suministrar la Garantía de Cumplimiento de conformidad con las IAL.

Entendemos que esta Declaración de Mantenimiento de Oferta expirará en el caso de que no seamos seleccionados, y (i) si recibimos una notificación con el nombre del Licitante seleccionado, o (ii) han transcurrido 28 días después de la fecha de expiración de la validez de nuestra Oferta, lo que ocurra primero.

Nombre del Licitante*:

Nombre de la persona debidamente autorizada para firmar la Oferta en nombre del Licitante**: _____

Cargo de la persona firmante del Formulario de la Oferta: _____

Firma de la persona nombrada anteriormente: _____

Fecha de la firma: El día _____ del mes _____ del año _____.

***** En el caso de las Ofertas presentadas por una APCA, especifique el nombre de la APCA que actúa como Licitante.

** La persona que firme la Oferta deberá contar con el poder otorgado por el Licitante. El poder deberá adjuntarse a los Formularios de la Oferta.

[Nota: En caso de que se trate de una APCA, la Declaración de Mantenimiento de Oferta deberá emitirse en nombre de todos los miembros de la APCA que presenta la Oferta].

Autorización del Fabricante

[NO APLICA]

[El Licitante solicitará al Fabricante que complete este formulario de acuerdo con las instrucciones indicadas. Esta carta de autorización deberá estar escrita en papel membretado del Fabricante y deberá estar firmada por una persona debidamente autorizada para firmar documentos que comprometan jurídicamente al Fabricante. El Licitante lo deberá incluirá en su Oferta, si así se establece en los DDL].

Fecha: *[indique día, mes y año de presentación de la oferta]*.
SDO n.°: *[Indique el número del proceso de la SDO]*.
Alternativa n.°: *[indique el n.° de identificación si se trata de una oferta por una alternativa]*.

Para: *[indique el nombre completo del Comprador]*.

POR CUANTO

Nosotros *[indique nombre completo del Fabricante]*, como fabricantes oficiales de *[indique el nombre de los bienes fabricados]*, con fábricas ubicadas en *[indique la dirección completa de las fábricas]*, autorizamos mediante el presente a *[indique el nombre completo del Licitante]* a presentar una Oferta con el propósito de suministrar los siguientes Bienes de nuestra fabricación *[nombre y breve descripción de los bienes]*, y a posteriormente negociar y firmar el Contrato.

Por este medio extendemos nuestro aval y plena garantía, conforme a la IAL 28 de las Condiciones Generales del Contrato, respecto de los Bienes ofrecidos por la firma antes mencionada.

Nosotros confirmamos que no hemos incurrido o empleado trabajo forzoso o personas sujetas a trata de personas o trabajo infantil de conformidad con la Cláusula 14 de las Condiciones Generales del Contrato.

Firma: *[indique firma de los representantes autorizados del Fabricante]*.

Nombre: *[indique el nombre completo de los representantes autorizados del Fabricante]*.

Cargo: *[indique el cargo]*.

Fechado el día _____ de _____del año _____ *[fecha de la firma]*.

Sección V. Países Elegibles

Elegibilidad para el suministro de bienes, obras y servicios distintos de los de consultoría en adquisiciones financiadas por el Banco

Con referencia a las IAL 4.8 y 5.1 de las Instrucciones a los Licitantes (IAL), para información de los Licitantes, las firmas, los bienes y los servicios de los siguientes países están excluidos actualmente de participar en este Proceso de Licitación:

En virtud de las IAL 4.8 (a) y 5.1: *"ninguno".*

En virtud de las IAL 4.8 (b) y 5.1: *"ninguno".*

Sección VI. Fraude y Corrupción

(La Sección VI no deberá modificarse)

1. Propósito

1.1 Las Directrices del Banco de Lucha Contra el Fraude y la Corrupción y esta sección se aplicarán a las adquisiciones en el marco de las operaciones de Financiamiento para Proyectos de Inversión del Banco.

2. Requisitos

2.1 El Banco exige que los Prestatarios (incluidos los beneficiarios del financiamiento del Banco), licitantes (postulantes / proponentes) , consultores, contratistas y proveedores, todo subcontratista, subconsultor, prestadores de servicios o proveedores, todo agente (haya sido declarado o no), y todo miembro de su personal, observen las más elevadas normas éticas durante el proceso de adquisición, la selección y la ejecución de contratos financiados por el Banco, y se abstengan de prácticas fraudulentas y corruptas.

2.2 Con ese fin, el Banco:

a. Define de la siguiente manera, a los efectos de esta disposición, las expresiones que se indican a continuación:

i. Por “práctica corrupta” se entiende el ofrecimiento, entrega, aceptación o solicitud directa o indirecta de cualquier cosa de valor con el fin de influir indebidamente en el accionar de otra parte.

ii. Por “práctica fraudulenta” se entiende cualquier acto u omisión, incluida la tergiversación de información, con el que se engañe o se intente engañar en forma deliberada o imprudente a una parte con el fin de obtener un beneficio financiero o de otra índole, o para evadir una obligación.

iii. Por “práctica colusoria” se entiende todo arreglo entre dos o más partes realizado con la intención de alcanzar un propósito ilícito, como el de influir de forma indebida en el accionar de otra parte.

iv. Por “práctica coercitiva” se entiende el perjuicio o daño o la amenaza de causar perjuicio o daño directa o indirectamente a cualquiera de las partes o a sus bienes para influir de forma indebida en su accionar.

v. Por “práctica obstructiva” se entiende:

(a) la destrucción, falsificación, alteración u ocultamiento deliberado de pruebas materiales referidas a una investigación o el acto de dar falsos testimonios a los investigadores para impedir materialmente que el Banco investigue denuncias de prácticas corruptas, fraudulentas, coercitivas o colusorias, o la amenaza, persecución o intimidación de otra parte para evitar

que revele lo que conoce sobre asuntos relacionados con una investigación o lleve a cabo la investigación, o

(b) los actos destinados a impedir materialmente que el Banco ejerza sus derechos de inspección y auditoría establecidos en el párrafo 2.2 e, que figura a continuación.

b. Rechazará toda propuesta de adjudicación si determina que la empresa o persona recomendada para la adjudicación, los miembros de su personal, sus agentes, subconsultores, subcontratistas, prestadores de servicios, proveedores o empleados han participado, directa o indirectamente, en prácticas corruptas, fraudulentas, colusorias, coercitivas u obstructivas para competir por el contrato en cuestión.

c. Además de utilizar los recursos legales establecidos en el convenio legal pertinente, podrá adoptar otras medidas adecuadas, entre ellas declarar que las adquisiciones están viciadas, si determina en cualquier momento que los representantes del prestatario o de un receptor de una parte de los fondos del préstamo participaron en prácticas corruptas, fraudulentas, colusorias, coercitivas u obstructivas durante el proceso de adquisición, o la selección o ejecución del contrato en cuestión, y que el prestatario no tomó medidas oportunas y adecuadas, satisfactorias para el Banco, para abordar dichas prácticas cuando estas ocurrieron, como informar en tiempo y forma a este último al tomar conocimiento de los hechos.

d. Podrá sancionar, conforme a lo establecido en las Directrices del Banco de Lucha Contra la Corrupción y a sus políticas y procedimientos de sanciones vigentes, a cualquier empresa o persona en forma indefinida o durante un período determinado, lo que incluye declarar a dicha empresa o persona inelegibles públicamente para: (i) obtener la adjudicación o recibir cualquier beneficio, ya sea financiero o de otra índole, de un contrato financiado por el Banco[1]; (ii) ser nominada[2] como subcontratista, consultor, fabricante o proveedor, o prestador de servicios de una firma que de lo contrario sería elegible a la cual se le haya adjudicado un contrato financiado por el Banco, y (iii) recibir los fondos de un préstamo del Banco o participar más activamente en la preparación o la ejecución de cualquier proyecto financiado por el Banco.

e. Exigirá que en los documentos de solicitud de ofertas/propuestas y en los contratos financiados con préstamos del Banco se incluya una cláusula en la

---

1 A fin de disipar toda duda al respecto, la inelegibilidad de una parte sancionada en relación con la adjudicación de un contrato implica, entre otras cosas, que la empresa o persona no podrá: (i) presentar una solicitud de precalificación, expresar interés en una consultoría, y participar en una licitación, ya sea directamente o en calidad de subcontratista nominado, consultor nominado, fabricante o proveedor nominado, o prestador de servicios nominado, con respecto a dicho contrato, ni (ii) firmar una enmienda mediante la cual se introduzca una modificación sustancial en cualquier contrato existente.

2 Un subcontratista nominado, consultor nominado, fabricante o proveedor nominado, o prestador de servicios nominado (se utilizan diferentes nombres según el documento de licitación del que se trate) es aquel que: (i) ha sido incluido por el licitante en su solicitud de precalificación u oferta por aportar experiencia y conocimientos técnicos específicos y esenciales que permiten al licitante cumplir con los requisitos de calificación para la oferta particular; o (ii) ha sido designado por el Prestatario.

que se exija que los licitantes (postulantes / proponentes), consultores, contratistas y proveedores, así como sus respectivos subcontratistas, subconsultores, prestadores de servicios, proveedores, agentes y personal, permitan al Banco inspeccionar[3] todas las cuentas, registros y otros documentos referidos a la presentación de ofertas y la ejecución de contratos, y someterlos a la auditoría de profesionales nombrados por este.

[3] Las inspecciones que se llevan a cabo en este contexto suelen ser de carácter investigativo (ej. forense). Consisten en actividades de constatación realizadas por el Banco o por personas nombradas por este para abordar asuntos específicos relativos a las investigaciones/auditorías, como determinar la veracidad de una denuncia de fraude y corrupción a través de los mecanismos adecuados. Dicha actividad incluye, entre otras cosas, acceder a la información y los registros financieros de una empresa o persona, examinarlos y hacer las copias que corresponda; acceder a cualquier otro tipo de documentos, datos o información (ya sea en formato impreso o electrónico) que se considere pertinente para la investigación/auditoría, examinarlos y hacer las copias que corresponda; entrevistar al personal y otras personas; realizar inspecciones físicas y visitas al emplazamiento, y someter la información a la verificación de terceros.

PARTE 2. Requisitos de los Bienes y Servicios Conexos

Sección VII. Requisitos de los Bienes y Servicios Conexos

Índice

1. Lista de Bienes y Cronograma de Entregas 116
2. Lista de servicios conexos y cronograma de cumplimiento…...……..125
3. Especificaciones Técnicas..... 126

1. Lista de bienes y Cronograma de entregas

[El comprador completará este cuadro, excepto la columna "Fecha de entrega ofrecida por el Licitante", la cual será completada por el Licitante].

N.º de artículo	Descripción de los bienes	Cantidad	Unidad física	Lugar de entrega final, según se indica en los DDL	Fecha de entrega[6] (de acuerdo con los Incoterms)		
					Fecha más temprana de entrega	Fecha límite de entrega	Fecha de entrega ofrecida por el licitante *[la proporcionará el Licitante]*
[Indique el n.º].	*[Indique la descripción de los bienes].*	*[Indique la cantidad de los artículos por suministrar].*	*[Indique la unidad física de medida de la cantidad].*	*[Indique el lugar de entrega].*	*[Indique el número de días después de la fecha de entrada en vigor del Contrato].*	*[Indique el número de días después de la fecha de entrada en vigor del Contrato].*	*[Indique el número de días después de la fecha de entrada en vigor del Contrato].*
1	Computadora de Escritorio Tipo 1	210	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
2	Computadora de Escritorio Tipo 2	71	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

[6] El plazo máximo para la entrega de los bienes será de hasta setenta y cinco (75) días calendario contados desde el día siguiente de la firma del Contrato. Los Licitantes podrán ofertar un plazo menor, el cual será considerado como factor de evaluación conforme al Plan de Entregas de los Bienes (IAL 34.6), aplicándose el ajuste económico correspondiente para efectos de comparación de Ofertas, según lo establecido en las Bases de Licitación.

3	Monitor para Computadoras	696	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
4	Teclado y Mouse	281	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
5	Soporte para 03 Monitores para Computadoras de Escritorio Tipo 1	210	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
6	Equipo Portátil	09	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
7	Auricular Monoaural	210	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
8	Micrófono	115	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
9	Altavoces	115	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
10	PPT de pie	210	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

11	Cámara Web	281	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
12	Teléfonos IP Tipo 1	201	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
13	Teléfonos IP Tipo 2	62	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
14	Teléfonos IP Tipo 3	16	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
15	Teléfonos IP Tipo 4	4	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
16	Botonera para teléfono IP 4	1	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
17	Pantalla para Monitoreo	2	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
18	Videoconferencia	4	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

19	Impresora tipo personal	13	Und	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
20	Impresora tipo mediano volumen	5	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
21	Proyector Multimedia	4	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
22	Tabletas Rugerizadas	37	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
23	Switches Spine Data Center	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
24	Switches Leaf Data Center	8	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
25	Solución de Orquestador DC	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
26	Switch Core LAN Campus	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

27	Switch de acceso 48 puertos PoE	23	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
28	Switch de acceso 24 puertos PoE	4	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
29	Switch DMZ	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
30	Switch de Gestión Fuera de Banda	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
31	Controlador inalámbrico	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
32	Access Point	47	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
33	Solución de Administración y Gestión Campus	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
34	Solución de Control de Acceso	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

35	Hardware de Hiperconvergencia	4	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
36	Software Hiperconvergencia	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
37	Servidor para backup	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
38	Servidor de inmutabilidad	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
39	Almacenamiento para backup	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
40	Librería de backup	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
41	Software de backup	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
42	Firewall NGFW (Perimetral)	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

43	Firewall Interno	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
44	Consola de analítica y reportes	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
45	XDR (Extended Detection & Response)	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
46	ZTNA (Zero Trust Network Access)	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
47	Seguridad para correo electronico	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
48	WAF - Seguridad para Aplicaciones Web	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
49	SIEM	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
50	Plataforma de detección y respuesta de amenazas externas e internas	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
52	ADC (application Delivery Controller)	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
53	Anti - DDos	2	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
54	MFA - Administración de identidad y acceso	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
55	PAM - Administración de acceso privilegiado	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
56	NDR (Network Detection and Response)	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
57	Sandboxing	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	
58	Solución de Análisis de Tráfico de Red	1	Unid	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	Hasta setenta y cinco (75) días calendario para la entrega de los bienes.	

2. Lista de servicios conexos y cronograma de cumplimiento

Servicio	Descripción del servicio	Cantidad[1]	Unidad física	Lugar donde los servicios serán prestados	Fecha(s) final(es) de ejecución de los servicios
[Indique el n.º del servicio].	*[Indique descripción de los servicios conexos].*	*[Indique la cantidad de rubros de servicios por proveer].*	*[Indique la unidad física de medida de los rubros de servicios].*	*[Indique el nombre del lugar].*	*[Indique la(s) fecha(s) de entrega requerida(s)].*
1	Servicio de implementación (instalación, configuración, pruebas y comisionamiento)	1	Servicios	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	Hasta noventa (90) días calendario para la implementación integral de la solución, incluyendo instalación, configuración, integración, pruebas y puesta en operación, contabilizados a partir del día siguiente de la suscripción del Contrato.
2	Mesa de Servicio	12	Meses	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	12 meses, contabilizado a partir del dia siguiente de la aceptacion operativa.
3	SOC	12	Meses	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	12 meses, contabilizado a partir del dia siguiente de la aceptacion operativa.
4	Garantía y Soporte de los Bienes	12	Meses	Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.	12 meses, contabilizado a partir del dia siguiente de la aceptacion operativa.

3. Especificaciones Técnicas



"Año de la Esperanza y el Fortalecimiento de la Democracia"

ADQUISICIÓN DE EQUIPAMIENTO OFIMÁTICO Y DE REDES LAN PARA LA CENTRAL 911 EN EL MARCO DEL PROYECTO CREACIÓN DE UN SISTEMA DE ATENCIÓN DE EMERGENCIAS, URGENCIAS E INFORMACIÓN MEDIANTE UN NÚMERO ÚNICO EN LIMA METROPOLITANA Y EL CALLAO – PROYECTO 911





Índice

1. Marco General ... 3
1.1. Base Normativa ... 3
1.2. Objetivo de la Contratación ... 3
1.3. Glosario de Términos ... 4
1.4. Información General ... 5
2. Alcance, Descripción de la Solución y Arquitectura Tecnológica ... 8
2.1. Equipamiento Ofimático ... 10
2.2. Red LAN ... 13
3. Soporte y Ciberseguridad ... 20
3.1. Mesa de Servicio ... 20
3.2. SOC ... 24
4. Implementación, Planificación y Gestión del Proyecto ... 32
4.1. Gestión del Proyecto ... 32
4.2. Personal Clave para la gestión ... 32
4.3. Personal clave para la Implementación. ... 33
4.4. Personal Clave para la administración de las soluciones tecnológicas durante el periodo de soporte y garantía. ... 34
4.5. Personal Clave para el soporte a usuario final durante el periodo de soporte y garantía ... 35
4.6. Personal NO Clave ... 35
4.7. Implementación ... 35
4.8. Aceptación Operativa ... 35
4.9. Recursos y Servicios para entregar por el Comprador ... 36
4.10. Gestión de Activos ... 36
4.11. Embalaje y/o Rotulado ... 36
4.12. Salud y Seguridad ... 36
4.13. Logistica y Control ... 36
4.14. Acreditación y Control de Acceso ... 37
4.15. Integraciones ... 37
4.16. Entrenamiento Técnico ... 37
4.17. Lugar y Plazo de Entrega ... 37
ANEXO 1 – CARACTERÍSTICAS TECNICAS ... 39
ANEXO 2 – DIAGRAMA TOPOLOGICO ... 123
ANEXO 3 – GARANTÍA Y SOPORTE DE LOS BIENES ... 124
ANEXO 4 – ACCESORIOS / CONSUMIBLES ... 126

1. Marco General

El Proyecto de implementación de la Central de Atención y Gestión de Emergencias 911 constituye una iniciativa estratégica del Estado Peruano, orientada a garantizar la atención oportuna, continua y coordinada de emergencias para Lima Metropolitana y el Callao. Dada la naturaleza crítica del servicio, la Central 911 ha sido concebida para operar de manera ininterrumpida (24x7x365), incluso ante escenarios de desastre, lo que exige una infraestructura tecnológica altamente disponible, resiliente, segura y escalable.

El Edificio de la Central 911 ha sido diseñado bajo estándares de misión crítica, incorporando redundancia en energía, comunicaciones, climatización y estabilidad estructural, así como un Centro de Datos y sistemas tecnológicos especializados. En este contexto, la experiencia en proyectos similares y los análisis técnicos realizados evidencian que la confiabilidad del servicio depende directamente de contar con una red LAN moderna y equipamiento informático adecuadamente dimensionados, capaces de soportar plataformas críticas como el sistema SAGE, videovigilancia, radiocomunicaciones, telecomunicaciones, hiperconvergencia y ciberseguridad avanzada.

Asimismo, la complejidad del ecosistema tecnológico, la necesidad de integración con múltiples soluciones provistas por terceros y el cumplimiento de principios de seguridad como Zero Trust, hacen indispensable establecer especificaciones técnicas claras, homogéneas y verificables. La ausencia de estos lineamientos podría generar riesgos de indisponibilidad, vulnerabilidades de seguridad, sobrecostos operativos y afectación directa a la continuidad del servicio de atención de emergencias.

En virtud de lo expuesto, las presentes Especificaciones Técnicas se sustentan en la criticidad del servicio 911, en los antecedentes técnicos del proyecto y en la necesidad de garantizar una plataforma tecnológica confiable, segura y sostenible, que asegure la correcta implementación, operación y transferencia de las soluciones tecnológicas que soportan la atención de emergencias a nivel metropolitano.

1.1. Base Normativa

- Contrato de Préstamo Nº 9039-PE, para el Financiamiento del Proyecto 911, suscrito el 16 de julio de 2020 entre el Banco Internacional de Reconstrucción y Fomento y la Republica del Perú.
- Regulaciones de Adquisiciones para prestatarios de Inversión: Bienes, Obras, Servicios de No consultoría y Servicios de Consultoría, julio 2016, Revisión noviembre 2017 y agosto 2018 aprobado por Resolución Ejecutiva N° 097-2020-MTC/24 y sus modificatorias.
- Manual de Operaciones, disposiciones para la ejecución del Proyecto 911
- Resolución Ministerial Nº 0311-2020-MTC/01.03, que aprueba el Manual de Operaciones del Programa Nacional de Telecomunicaciones – PRONATEL.

1.2. Objetivo de la Contratación

El objetivo de la presente contratación es adquirir e implementar de manera integral el equipamiento ofimático y la red LAN de la Central de Atención y Gestión de Emergencias 911, garantizando una infraestructura tecnológica de misión crítica, segura, altamente disponible y escalable, que asegure la operación continua 24x7x365 de los sistemas y servicios esenciales de atención de emergencias, su correcta integración con las plataformas existentes y el cumplimiento de los estándares técnicos y normativos aplicables.

1. Marco General

El Proyecto de implementación de la Central de Atención y Gestión de Emergencias 911 constituye una iniciativa estratégica del Estado Peruano, orientada a garantizar la atención oportuna, continua y coordinada de emergencias para Lima Metropolitana y el Callao. Dada la naturaleza crítica del servicio, la Central 911 ha sido concebida para operar de manera ininterrumpida (24x7x365), incluso ante escenarios de desastre, lo que exige una infraestructura tecnológica altamente disponible, resiliente, segura y escalable.

El Edificio de la Central 911 ha sido diseñado bajo estándares de misión crítica, incorporando redundancia en energía, comunicaciones, climatización y estabilidad estructural, así como un Centro de Datos y sistemas tecnológicos especializados. En este contexto, la experiencia en proyectos similares y los análisis técnicos realizados evidencian que la confiabilidad del servicio depende directamente de contar con una red LAN moderna y equipamiento informático adecuadamente dimensionados, capaces de soportar plataformas críticas como el sistema SAGE, videovigilancia, radiocomunicaciones, telecomunicaciones, hiperconvergencia y ciberseguridad avanzada.

Asimismo, la complejidad del ecosistema tecnológico, la necesidad de integración con múltiples soluciones provistas por terceros y el cumplimiento de principios de seguridad como Zero Trust, hacen indispensable establecer especificaciones técnicas claras, homogéneas y verificables. La ausencia de estos lineamientos podría generar riesgos de indisponibilidad, vulnerabilidades de seguridad, sobrecostos operativos y afectación directa a la continuidad del servicio de atención de emergencias.

En virtud de lo expuesto, las presentes Especificaciones Técnicas se sustentan en la criticidad del servicio 911, en los antecedentes técnicos del proyecto y en la necesidad de garantizar una plataforma tecnológica confiable, segura y sostenible, que asegure la correcta implementación, operación y transferencia de las soluciones tecnológicas que soportan la atención de emergencias a nivel metropolitano.

1.1. Base Normativa

- Contrato de Préstamo N° 9039-PE, para el Financiamiento del Proyecto 911, suscrito el 16 de julio de 2020 entre el Banco Internacional de Reconstrucción y Fomento y la Republica del Perú.
- Regulaciones de Adquisiciones para prestatarios de Inversión: Bienes, Obras, Servicios de No consultoría y Servicios de Consultoría, julio 2016, Revisión noviembre 2017 y agosto 2018 aprobado por Resolución Ejecutiva N° 097-2020-MTC/24 y sus modificatorias.
- Manual de Operaciones, disposiciones para la ejecución del Proyecto 911
- Resolución Ministerial Nº 0311-2020-MTC/01.03, que aprueba el Manual de Operaciones del Programa Nacional de Telecomunicaciones – PRONATEL.

1.2. Objetivo de la Contratación

El objetivo de la presente contratación es adquirir e implementar de manera integral el equipamiento ofimático y la red LAN de la Central de Atención y Gestión de Emergencias 911, garantizando una infraestructura tecnológica de misión crítica, segura, altamente disponible y escalable, que asegure la operación continua 24x7x365 de los sistemas y servicios esenciales de atención de emergencias, su correcta integración con las plataformas existentes y el cumplimiento de los estándares técnicos y normativos aplicables.

1.3. Glosario de Términos

A continuación, se lista el glosario de términos que permitirán el entendimiento de aspectos particulares para tener en cuenta para la lectura del presente requerimiento técnico:

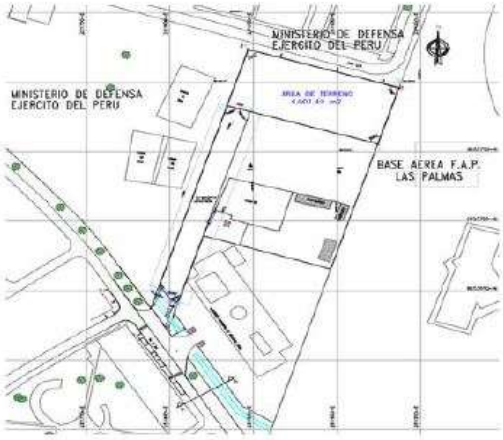
- **Centro de Atención de Llamadas:** Es un área donde operadores, reguladores, despachadores, supervisores o ejecutivos, especializados en servicio al usuario, realizan o reciben llamadas desde o hacia las personas (ciudadanía) u otras entidades.
- **Comprador**: Es la Entidad Contratante, Programa Nacional de Telecomunicaciones.
- **Contratista Obra:** Es la empresa constructora del edificio de la Central 911.
- **Despachador:** Personal de una entidad de primera respuesta – EPR, encargado de asignar los recursos necesarios, coordinar, dar seguimiento y soporte para la atención eficiente y oportuna de una emergencia o urgencia.
- **Edificio de la Central 911:** Esta locación es el sitio donde se realizará la implementación del presente requerimiento, y está ubicada en Av. El Sol S/N, Distrito de Chorrillos, Provincia y Departamento de Lima.
- **EPR:** Conjunto de las Entidades de Primer Respuesta (PNP, SAMU y Bomberos).
- **Implementación:** Hace referencia a la instalación, configuración, pruebas individuales y pruebas integrales que realizará el proveedor del presente requerimiento.
- **Línea 100:** Servicio especializado en atención telefónica gratuita a nivel nacional que tiene como finalidad brindar información, orientación, consejería y soporte emocional a las personas afectadas o involucradas en hechos de violencia familiar o sexual y a quienes conozcan sobre algún caso de maltrato en su entorno.
- **Médico Regulador:** Médico capacitado y entrenado en la atención prehospitalario, encargado del triaje telefónico, clasificará las prioridades de la atención médica y discriminará el uso de recursos para la atención (envío de ambulancia para prioridad I y II, y/o la asistencia médica en las prioridades III y IV).
- **Operador Telefónico:** Profesional que trabaja en un centro de atención telefónica que se encarga de atender y recibir las llamadas de los ciudadanos que marcan a la línea de emergencia, está encargado de determinar la pertinencia de la llamada.
- **Proveedor:** Es la empresa que se adjudique el presente requerimiento.
- **Proveedor SAGE:** Es la empresa que provee el software SAGE, que incluye hardware y software dedicado de la solución del SAGE.
- **Proveedor Servicios de Telecomunicaciones:** Es la empresa que provee los servicios de telecomunicaciones a la Central 911 (Servicio de Internet, Servicio de Telefonía fija y Servicios de Enlaces Dedicados).
- **Proveedor de Solución TETRA:** Es la empresa que provee la solución de TETRA en el Edificio de la Central 911.
- **SAGE:** El Sistema de Atención y Gestión de Emergencias – SAGE, es componente fundamental de la plataforma tecnológica y como sistema informático, está compuesto entre otros, por un sistema de despacho asistido por computadora (CAD- Computer-Aided Dispatch), un sistema de comunicaciones, sistema de geolocalización, sistema de información geográfica, entre otros sistemas, que permiten la atención centralizada y despacho descentralizado de emergencias, urgencias e información; que integra servicios como la geolocalización de las llamadas, la gestión de los recursos para la asistencia, la integración de las cámaras de vigilancia, la integración de las comunicaciones de radio, telefonía celular y analógica y el completo registro de la información (audio y video) generada como consecuencia de la atención.
- **Supervisor Obra:** Es la empresa especializada y dedicada a la Supervisión de las actividades del Contratista de Obra.
- **Spare:** Contingencia en bienes.
- **Gerente de Proyectos:** Será asignado por el comprador, y será el responsable de dirigir, coordinar y controlar la implementación del presente requerimiento en la Central 911, asegurando que los componentes de infraestructura, comunicaciones, plataformas, servicios TI, integración de sistemas y soporte operativo se ejecuten conforme al alcance, cronograma, calidad, seguridad y objetivos institucionales definidos en el presente requerimiento.

1.4. Información General

Edificio de la Central 911

Con la finalidad de contextualizar el proyecto general se describe que el Edificio de la Central 911 se ubica en la Avenida el Sol S/N, Distrito de Chorrillos, Provincia y departamento de Lima, con un área de 4,001.49 m2. Tiene los siguientes linderos y medida perimétricas:

- Por el Norte con Ministerio de Defensa Ejercito del Perú con 94.50 ml.
- Por el Oeste con la Ministerio de Defensa Ejercito del Perú con 41.99 ml.
- Por el Sur con la pista de acceso y terreno de INDECI con 94.50 ml.
- Por el este con la Base Aérea de Las Palmas con 42.70 ml.



El edificio tiene la función de estar operativo durante las 24 horas del día los 365 días del año, incluso cuando haya habido un evento devastador en la ciudad. Por lo tanto, tiene redundancia de servicios de comunicaciones, energía y abastecimiento de agua y desagüe, como también una estabilidad estructural a prueba de sismos de gran magnitud, por lo que cuenta con aisladores sísmicos.

La función principal del edificio es albergar al personal que reciba las llamadas de emergencia y éstas, luego de ser verificadas, serán canalizadas a las Entidades de Primera Respuesta (EPR) como la Policía Nacional, los Bomberos, el SAMU y la Línea 100, quienes se encargarán de darle solución a las diferentes emergencias.

El edificio se ha distribuido en un sótano y tres pisos distribuido de la siguiente manera:

Sótano:

Se accede desde la pista de acceso por una rampa al nivel -3.75 y cuenta con 48 estacionamientos de autos (incluyendo 2 para discapacitados), 2 ambulancias, 1 estacionamiento para descarga de materiales, 1 estacionamiento para un vehículo de abastecimiento a la cocina y estacionamientos para 16 motos y 20 bicicletas se ha considerado también una toma de energía para la carga de 2 unidades de autos eléctricos.

Cuenta con una Subestación Eléctrica y Área para Tableros, un Área para Grupos Electrógenos (3), Depósito General, Cuarto de Comunicaciones, Cuarto de Sistema Ininterrumpido, Área de mantenimiento con Baño, Área de Soporte Técnico, Camerinos para hombres y mujeres destinado a los ciclistas, 2 baños, un

depósito y un área para lavar las camillas que está destinado para las ambulancias del SAMU, Cuarto de basura, Cuarto para desechos eléctricos (RAEE), Ductos de Comunicaciones 1 y 2, Cuarto y Ducto Eléctrico y Hall de ascensores y escalera. También se ubica un área de camerinos y baños para el personal de la cocina con montacargas para abastecimiento de esta y una escalera de escape.

En el mismo nivel, pero ingresando desde el primer piso del estacionamiento de personalidades se encuentran las Cisternas de Consumo Humano divididas en 2, con dotaciones que permiten el uso ininterrumpido del edificio en caso de un desabastecimiento, un Cuarto de Bombas para 2 grupos de bombas de presión constante y una motobomba contra incendios y una Cisterna de Agua Contra Incendio.

Bajo el nivel de sótano se encuentra la cimentación del edificio, la cual está dotada de aisladores sísmicos que deben ser monitoreados permanentemente y al cual se accede mediante las trincheras que se encuentran alrededor del edificio, en este nivel se ha ubicado un ambiente para un acelerografo. Estas trincheras tendrán un tratamiento paisajístico con muros verdes dotadas de especies con poca necesidad de agua para generar vistas agradables a los ambientes que tiene acceso a ellas.

El aforo permanente de este piso son 6 personas.

Primer Piso:

En el Primer Piso se ubica una Garita de control vehicular y peatonal, el Ingreso Vehicular se realiza a través de una rampa y el Ingreso Peatonal accede a una plaza interior que da acceso al Lobby, en donde se encuentra la Recepción y el Hall Principal de ascensores que lleva a los diferentes niveles. En este nivel también se encuentra un Ingreso Vehicular desde la Base Aérea de las Palmas dejando un pase también al Terreno del futuro Proyecto del Edificio de Defensa Civil destinado a personalidades VIP, las cuales tienen la misión de tomar las decisiones en caso de emergencia. Este acceso está destinado a 10 vehículos.

Por otro lado, se encuentra el Data Center como el ambiente técnico más importante del proyecto y el cual debe garantizar el funcionamiento del edificio en caso de un desastre, este ambiente tiene un piso técnico de 45 cm.

También se encuentran ambientes como la sala de prensa, la cual tiene conexión a la Plaza de acceso, el Salón de Usos Múltiples, el cual se puede dividir en 3 salones menores mediante tabiques acústicos móviles, para capacitaciones o reuniones y un área de ampliación destinada a la PNP. Frente a ellos se encuentra la Cafetería con capacidad para 120 personas la cual tendrá vista hacia un muro verde y la cocina.

Todas estas áreas están complementadas con un Tópico, un Lactario y los Servicios Higiénicos para hombres y mujeres, así como Servicios higiénicos para discapacitados y Cuarto de Limpieza.

También se ubican 2 Ductos de Comunicaciones y 2 Cuartos Eléctricos, ubicados en el mismo lugar en todos los pisos para poder distribuir flexiblemente y con seguridad las instalaciones de comunicaciones y energía y un segundo ambiente para un acelerógrafo.

Finalmente, en este nivel también se encuentra la Sala de Control y Monitoreo con baño.

El aforo de esta planta es de 354 personas.

Segundo Piso:
En el Segundo nivel se encuentran las Salas de Operadores (90 personas) y Despachadores de las Entidades de Primera Respuesta (EPR) como la Policía Nacional (40 personas), el Cuerpo de Bomberos (15 personas) y el SAMU (30 personas) así como la Línea 100 (15 personas), a las cuales se accede desde una esclusa de doble altura con una escalera helicoidal que relaciona funcional y espacialmente los ambientes del segundo y tercer piso. La sala de Despachadores tiene un techo escalonado para mantener las alturas máximas que establece el estudio aeronáutico exigido para el lote. Toda el área se ha diseñado con una gran integración visual entre los ambientes mediante tabiquerías de vidrio debido a la gran interacción entre el personal de esta área que demanda una coordinación constante.

El área de operadores y despachadores cuenta con un piso técnico de 30 cm de manera de ofrecer flexibilidad en las distribuciones de ellos puestos de trabajo debido a la gran cantidad de cables que se necesitan ya que cada puesto de trabajo deberá contar con redundancia en el suministro de datos y energía.

En este nivel también se encuentra la Sala de Descanso 1, la cual consta de un área para lockers, 7 dormitorios con 2 camarotes cada uno (pudiendo albergar 1 más cada 1) incluyendo uno de ellos habilitado para recibir personas con discapacidad, vestuarios para hombres y mujeres, así como el área propiamente de descanso con kitchenette.

Finalmente se ubican también tres módulos de Baños para hombres, mujeres, discapacitados y Cuarto de Limpieza, así como 2 Ductos de Comunicaciones y 2 Cuartos Eléctricos.

El aforo total de este piso es de 205 personas.

Tercer Piso:
En el Tercer nivel se encuentran la Sala de Crisis, la cual tiene contacto visual con la doble altura de la Sala de Operadores y su Video Wall para una mejor comunicación. A ellas se accede desde la esclusa de doble altura que relaciona espacialmente los ambientes mediante una escalera, también se accede desde el vestíbulo de ascensores. En este piso se ubica una sala para el Cuerpo de Bomberos y una sala para la Policía Nacional, así como un área de mesa de ayuda y un área para oficina de SAMU con depósito y dos terrazas, la cual permite el ingreso de iluminación a la doble altura reforzando la iluminación natural.

En este nivel también se encuentra el Área Administrativa con Archivo, la Alta Dirección, la Sala de Descanso 2 y el Cuarto de radiocomunicaciones.

Finalmente se ubican también un módulo de Baños para hombres, mujeres, discapacitados y Cuarto de limpieza.

El aforo total de este piso es de 81 personas.

Azotea:
En este nivel se considera el acceso desde la escalera de evacuación, los ductos de comunicaciones y energía, ductos de ventilación, un ambiente para la ubicación de un acelerógrafo, los equipos de aire acondicionado de precisión de la data Center los equipos de aire acondicionado del Edificio (Chillers), así como un cuarto para los equipos de radiocomunicaciones y una torre de radiocomunicaciones.

2. Alcance, Descripción de la Solución y Arquitectura Tecnológica

La presente contratación tiene por objeto la adquisición, suministro, entrega, instalación (cuando corresponda) y puesta en funcionamiento de equipamiento tecnológico, agrupados por especialidad:

- Equipamiento Ofimático
- Equipamiento para la Red LAN

Cuadro Nro. 01 – Lista total del equipamiento

Nro	Bienes Equipamiento Ofimático	Cantidad	Spare	Cantidad Total (*) (**)
1	Computadora de Escritorio Tipo 1	198	12	210
2	Computadora de Escritorio Tipo 2	70	1	71
3	Monitor para Computadoras	664	32	696
4	Teclado y Mouse	268	13	281
5	Soporte para 03 Monitores Computadoras de Escritorio Tipo 1	198	12	210
6	Equipo Portátil	8	1	9
7	Auricular Monoaural	198	12	210
8	Micrófono	108	7	115
9	Altavoces	108	7	115
10	PPT de pie	198	12	210
11	Cámara Web	268	13	281
12	Teléfonos IP Tipo 1	190	11	201
13	Teléfonos IP Tipo 2	60	2	62
14	Teléfonos IP Tipo 3	14	2	16
15	Teléfonos IP Tipo 4	2	2	4
16	Botonera para teléfono IP 4	1	0	1
17	Pantalla para Monitoreo	2	0	2
18	Videoconferencia	4	0	4
19	Impresora tipo personal	13	0	13
20	Impresora tipo mediano volumen	5	0	5
21	Proyector Multimedia	4	0	4
22	Tabletas Rugerizadas	35	2	37
Nro	**Bienes Equipamiento Red LAN**	**Cantidad**	**Spare**	**Cantidad Total (*) (**)**
23	Switches Spine Data Center	2	0	2
24	Switches Leaf Data Center	8	0	8
25	Solución de Orquestador DC	1	0	1
26	Switch Core LAN Campus	2	0	2
27	Switch de acceso 48 puertos PoE	22	1	23
28	Switch de acceso 24 puertos PoE	4	0	4
29	Switch DMZ	2	0	2
30	Switch de Gestión Fuera de Banda	2	0	2
31	Controlador inalámbrico	2	0	2
32	Access Point	43	4	47
33	Solución de Administración y Gestión Campus	1	0	1
34	Solución de Control de Acceso	1	0	1
35	Hardware de Hiperconvergencia	4	0	4
36	Software Hiperconvergencia	1	0	1
37	Servidor para backup	1	0	1
38	Servidor de inmutabilidad	1	0	1
39	Almacenamiento para backup	1	0	1
40	Librería de backup	1	0	1
41	Software de backup	1	0	1
42	Firewall NGFW (Perimetral)	2	0	2
43	Firewall Interno	2	0	2

44	Consola de analítica y reportes	1	0	1
45	XDR (Extended Detection & Response)	1	0	1
46	ZTNA (Zero Trust Network Access)	1	0	1
47	Seguridad para correo electronico	1	0	1
48	WAF - Seguridad para Aplicaciones Web	1	0	1
49	SIEM	1	0	1
50	Plataforma de detección y respuesta de amenazas externas e internas	1	0	1
51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	1	0	1
52	ADC (application Delivery Controller)	2	0	2
53	Anti - DDos	2	0	2
54	MFA - Administración de identidad y acceso	1	0	1
55	PAM - Administración de acceso privilegiado	1	0	1
56	NDR (Network Detection and Response)	1	0	1
57	Sandboxing	1	0	1
58	Solución de Análisis de Tráfico de Red	1	0	1

(*) Las cantidades totales, incluyen las unidades operativas y de spare, según corresponda.
(**) Todos los bienes a suministrar, incluido los spare, deben incluir sus accesorios o elementos necesarios para la instalación, interconexión y puesta en operación, tales como tranceivers, cables de energía, ventiladores entre otros necesarios para su puesta en operación de forma integral.

Para la presentación de propuestas, los postores deberán adjuntar una relación de los bienes ofertados, indicando: marca, modelo y año de fabricación.

Los bienes propuestos no deberán ingresar en condición de "fuera de soporte" ni "fin de vida" (End of Support / End of Life) durante los próximos cinco (5) años, contados a partir de la fecha de presentación de propuestas. Para acreditar lo anterior, el postor deberá presentar una carta emitida por el fabricante como sustento.

Para la implementación, el Proveedor deberá presentar un matriz de cumplimiento de cada una de las características técnicas del Anexo 1, la cual será revisada y aprobada por el equipo de implementación del Contratante. En caso alguna de las características no cumpla, esta será rechazada, por lo que Proveedor será responsable de reemplazar con un bien que si cumpla. El retraso que generé esto será de responsabilidad única y exclusiva del Proveedor.

A continuación, se realiza la descripción general de los bienes que conforman el presente requerimiento con el desagregado de cantidades de spare. El detalle de las características técnicas se describe en el Anexo 1 del presente documento.

2.1. Equipamiento Ofimático

A continuación, se describe de forma general todos los bienes, accesorios, y otros que forman parte del presente requerimiento referente al equipamiento ofimático a proveer.

Cuadro Nro. 02 – Lista total del equipamiento Ofimático

Nro	Bien	Cantidad	Spare	Cantidad Total
1	Computadora de Escritorio Tipo 1	198	12	210
2	Computadora de Escritorio Tipo 2	70	1	71
3	Monitor para Computadoras	664	32	696
4	Teclado y Mouse	268	13	281
5	Soporte para 03 Monitores para Computadoras de Escritorio Tipo 1	198	12	210
6	Equipo Portátil	8	1	9
7	Auricular Monoaural	198	12	210
8	Micrófono	108	7	115
9	Altavoces	108	7	115
10	PPT de pie	198	12	210
11	Cámara Web	268	13	281
12	Teléfonos IP Tipo 1	190	11	201
13	Teléfonos IP Tipo 2	60	2	62
14	Teléfonos IP Tipo 3	14	2	16
15	Teléfonos IP Tipo 4	2	2	4
16	Botonera para teléfono IP 4	1	0	1
17	Pantalla para Monitoreo	2	0	2
18	Videoconferencia	4	0	4
19	Impresora tipo personal	13	0	13
20	Impresora tipo mediano volumen	5	0	5
21	Proyector Multimedia	4	0	4
22	Tabletas Rugerizadas	35	2	37

2.1.1. Estaciones de Trabajo

Los equipos de cómputo serán dotados para las posiciones operativas y administrativas de la Central 911, conforme a la distribución definida por ambientes y turnos establecidos, asegurando un estándar homogéneo de configuración, continuidad operativa y soporte.

Todas las estaciones de trabajo serán aprovisionadas con una imagen base institucional, debidamente configuradas y agregadas a un dominio de red, con las aplicaciones autorizadas para operación (CAD, GIS, radiocomunicación, video y herramientas complementarias), y con endurecimiento (hardening) acorde a lineamientos de seguridad para puestos de operadores, despachadores y supervisores que se entregarán al Proveedor durante la implementación.

La preparación de los equipos comprende como mínimo lo siguiente:

- Configuración estándar (imagen base), inventario y etiquetado patrimonial.
- Unión a dominio, políticas de seguridad (GPO), control de privilegios y actualización.
- Lista de software base y parámetros de hardening entregados para despliegue y auditoría.
- Preparado para soporte 24x7 (mesa de ayuda, reposición y mantenimiento).
- Redundancia con doble tarjeta de red.

Computadoras de Escritorio Tipo 1 y 2

Se han definido dos tipos de computadora, de acuerdo a los perfiles del personal de la Central 911. Las cuales deberán considerar su accesorios generales y soporte para monitores, según el tipo de computadora. Para las computadoras tipo 1 se ha

considerado 03 monitores con su soporte para estos, mientras que las computadoras tipo 2 no se considera el componente de soporte. Las características técnicas se detallan en el Anexo 1 del presente documento, siendo las cantidades resumidas en el siguiente cuadro:

Cuadro Nro. 03

Nro	Tipo del componente	Cantidad	Spare	Total
1	Computadora de Escritorio Tipo 1	198	12	210
2	Computadora de Escritorio Tipo 2	70	1	71
3	Monitor para Computadoras	664	32	696
4	Teclado y Mouse	268	13	281
5	Soporte para 03 Monitores para Computadoras de Escritorio Tipo 1	198	12	210

Computadoras Portátiles

Como parte del parque informático, también se ha definido equipamiento portátil, siendo lo requerido un total de 09 unidades. Las características técnicas se detallan en el Anexo 1 del presente documento.

2.1.2. Periféricos Especializados

Componentes críticos de las posiciones operativas para asegurar la operación continua 24x7 de la Central 911, orientados a la atención de emergencias y a la integración con los módulos de CAD, GIS y radiocomunicación. Los periféricos especializados son: cámaras web, interruptores PTT (Push-To-Talk), micrófonos, altavoces y auriculares monoaurales, los cuales deberán ser compatibles con las estaciones de trabajo y plataformas de comunicaciones, contar con controladores estables y garantía local, para facilitar soporte, reposición y continuidad operativa.

La preparación de los periféricos comprende como mínimo lo siguiente:

- Instalación integral de los componentes periféricos.
- Compatibilidad técnica con estaciones, puertos y aplicaciones (audio/video/Radio).
- Calidad y confiabilidad para uso intensivo por turnos (misión crítica).
- Estandarización para reducir fallas recurrentes y tiempos de restauración.
- Considerar stock mínimo/backup para reemplazo inmediato y continuidad 24x7.

Las características técnicas se detallan en el Anexo 1 del presente documento, siendo las cantidades resumidas en el siguiente cuadro:

Cuadro Nro. 04

Nro	Tipo del componente	Cantidad	Spare	Cantidad Total
7	Auricular Monoaural	198	12	210
8	Micrófono	108	7	115
9	Altavoces	108	7	115
10	PPT de pie	198	12	210
11	Cámara Web	268	13	281

2.1.3. Teléfonos IP

Los teléfonos IP serán desplegados en la central 911 para las comunicaciones por voz que se requieran. Las características técnicas se detallan en el Anexo 1 del presente documento, siendo las cantidades resumidas en el siguiente cuadro:

Cuadro Nro. 05

Nro	Tipo del componente	Cantidad	Spare	Cantidad Total
12	Teléfonos IP Tipo 1	190	11	201
13	Teléfonos IP Tipo 2	60	2	62
14	Teléfonos IP Tipo 3	14	2	16
15	Teléfonos IP Tipo 4	2	2	4
16	Botonera para teléfono IP 4	1	0	1

2.1.4. Pantalla de Monitoreo

Se requiere la provisión de dos (02) pantallas para monitoreo, las cuales estarán ubicadas en la sala NOC de TI. Las características técnicas se detallan en el Anexo 1 del presente documento.

2.1.5. Videoconferencia

Se incorporará cuatro (04) soluciones de videoconferencia para coordinación interinstitucional, gestión operativa y soporte durante la operación de las actividades de la Central 911 garantizando audio y video de calidad, estabilidad y seguridad. La solución deberá integrarse al entorno de red, contemplar administración y configuración controlada, y operar bajo políticas institucionales de ciberseguridad.

La solución de videoconferencia comprende como mínimo lo siguiente:

- Cámara, audio, codec/terminal y accesorios según sala y aforo las cuales deben estar integrados.
- Conectividad y segmentación de red conforme a arquitectura aprobada.
- Cifrado/seguridad y actualización de firmware bajo control.
- Soporte y mantenimiento alineado a disponibilidad 24x7.

2.1.6. Impresoras/Suministros/consumibles

Los equipos de impresión monocromáticos de tipo personal y de mediano volumen, atenderán las necesidades operativas y administrativas de la Central 911, asegurando disponibilidad, rendimiento y control. Las impresoras deberán soportar carga de trabajo acorde al volumen esperado, conectividad segura a la red institucional y administración centralizada, permitiendo trazabilidad y reducción de riesgos por uso no controlado.

La preparación de los periféricos comprende como mínimo lo siguiente:

- Conectividad de red, gestión central y control de acceso.
- Impresión dúplex y rendimiento (ciclo mensual) alineado al uso real.
- Seguridad básica: credenciales, actualizaciones y segmentación según diseño.
- Soporte y repuestos con tiempos acordes a operación 24x7.

Del mismo modo, se considerarán suministros y consumibles necesarios para el inicio de las operaciones de la Central 911. Los suministros deberán corresponder a los modelos adquiridos y contemplar rendimiento por página y rotación, de forma que se garantice disponibilidad sin impactar la operación.

- Tóner/tinta, kits y repuestos consumibles según especificación del fabricante.

- Rendimiento declarado (yield) y control de inventario (kardex).
- Stock mínimo y reposición planificada para operación continua.
- Registro de consumo para control y proyección de demanda.

Las características técnicas se detallan en el Anexo 1 del presente documento, siendo las cantidades resumidas en el siguiente cuadro:

Cuadro Nro. 06

Nro	Tipo del componente	Cantidad Total
19	Impresora tipo personal	13
20	Impresora tipo mediano volumen	5

Estos equipos no tienen spare

2.1.7. Proyectores Multimedia

Se realizará el suministro, instalación, configuración y puesta en funcionamiento de tres (03) sistemas de proyección multimedia para salas de usos múltiples divisibles mediante tabiques móviles, permitiendo la operación independiente de cada ambiente o la operación conjunta de los tres ambientes como una sola sala. Asimismo, un (01) sistema de proyección para la Sala de Prensa.

2.1.8. Tabletas para SAMU

Se adquirirán treinta y siete (37) tabletas para uso operativo del SAMU orientadas a movilidad y continuidad de servicio en campo, permitiendo acceso a información y aplicaciones autorizadas vinculadas a la atención de emergencias. Los equipos deberán contar con controles de seguridad, conectividad estable y accesorios que aseguren operación segura en ambientes exigentes.

La preparación de los equipos comprende como mínimo lo siguiente:

- Cifrado, control de aplicaciones y borrado remoto.
- Conectividad (Wi-Fi/LTE según corresponda), GPS y autonomía.
- Accesorios: fundas, cargadores y soportes.
- Integración con procesos de mesa de ayuda (inventario, incidentes y reposición).
- Servicio de datos por el periodo de soporte y garantía (Consumo promedio 50 GB en alta velocidad mensual por dispositivo).

2.2. Red LAN

La Red LAN de la Central 911 constituye la plataforma de conectividad principal que soportará la operación continua, segura y de alta disponibilidad de los servicios tecnológicos y operativos del proyecto, incluyendo el equipamiento de usuario final, la telefonía IP, la red inalámbrica, la plataforma SAGE, la infraestructura de centro de datos, los servicios de respaldo, las plataformas de ciberseguridad y los demás componentes que forman parte del ecosistema tecnológico de la Central 911. Dada la naturaleza del servicio 911, esta infraestructura ha sido concebida y deberá implementarse como una red para un entorno de misión crítica, preparada para operar de manera ininterrumpida 24x7x365, con tolerancia a fallas, continuidad operativa ante incidentes, eventos adversos o mantenimientos programados, y con niveles de resiliencia acordes al carácter estratégico de la atención de emergencias.

De manera general, la solución esta diseñada en una arquitectura integrada de Campus y Data Center, conformada por un fabric de centro de datos tipo Spine-Leaf, un núcleo de red LAN Campus (Core LAN), una capa de acceso cableado PoE, una red inalámbrica con administración centralizada, una zona DMZ y una red de gestión fuera de banda (OOB), permitiendo la segregación funcional y lógica de los distintos servicios, así como la integración ordenada de las plataformas tecnológicas del proyecto. Esta arquitectura ha sido definida para un centro de misión crítica, por lo que prioriza la

eliminación de puntos únicos de falla, el crecimiento horizontal, la recuperación rápida ante contingencias y el soporte estable del tráfico asociado a la atención de emergencias, la coordinación interinstitucional, los sistemas de despacho, voz, video, monitoreo y los servicios internos del centro de datos.

La solución contempla mecanismos de alta disponibilidad en los componentes críticos mediante redundancia de equipos, enlaces duales, agregación de enlaces, balanceo de tráfico y esquemas de operación que garanticen continuidad aun ante la falla de dispositivos, enlaces o módulos individuales. Del mismo modo, deberá soportar capacidades avanzadas de conmutación y enrutamiento para la segmentación lógica de la red, la separación de dominios de tráfico y la aplicación de políticas centralizadas de acceso y seguridad, asegurando la convivencia ordenada de redes de usuarios, voz, video, administración, servicios críticos, respaldo, seguridad y demás segmentos requeridos para la operación de la Central 911, sin comprometer el desempeño, la disponibilidad ni los tiempos de respuesta esperados en una operación de misión crítica.

Como parte del alcance del presente requerimiento, la Red LAN deberá integrarse de forma nativa con la plataforma de hiperconvergencia, la solución de backup e inmutabilidad, los componentes de ciberseguridad multicapa, la infraestructura inalámbrica, la solución de control de acceso a la red (NAC), así como con las plataformas institucionales y de terceros que forman parte de la operación integral de la Central 911. Esta integración deberá permitir visibilidad, telemetría, monitoreo, trazabilidad, administración centralizada y operación coordinada entre todos los componentes tecnológicos, manteniendo el desempeño requerido para una infraestructura de misión crítica y asegurando que los servicios esenciales del 911 dispongan de conectividad confiable, segura y permanentemente disponible.

Asimismo, la solución deberá contemplar una gestión centralizada, capacidades de automatización, monitoreo permanente, control de versiones de firmware, registro de eventos, analítica y operación segregada mediante red de administración fuera de banda, con la finalidad de facilitar la implementación, operación, mantenimiento, soporte y crecimiento futuro de la plataforma tecnológica. Todo ello deberá realizarse considerando la operación de la infraestructura en doble pila IPv4/IPv6, sin afectar el desempeño integral de la red y conforme a los lineamientos establecidos en el presente requerimiento. En concordancia con el enfoque de misión crítica del proyecto, la red deberá facilitar actividades de operación y soporte sin introducir indisponibilidades no planificadas y con capacidad de administración segura ante escenarios degradados.

La topología base de referencia de la solución se presenta en el Anexo 2 – Diagrama Topológico, en el cual se muestra, de manera referencial, la interconexión general entre los componentes de campus, centro de datos, seguridad, respaldo, acceso inalámbrico, gestión y servicios asociados. Dicho anexo deberá entenderse como la representación de la arquitectura objetivo del proyecto para un entorno de misión crítica y servirá como insumo para la ingeniería de detalle que desarrollará el Proveedor durante la fase de implementación, sin perjuicio del cumplimiento íntegro de las características técnicas, funcionales y de desempeño establecidas en el presente documento.

A continuación, se describe de forma general todos los bienes y accesorios que forman parte de la Red LAN, el cual será provisto en el presente requerimiento.

Cuadro Nro. 07 – Lista total del equipamiento de Red LAN

Nro	Bien	Cantidad	Spare	Cantidad Total
23	Switches Spine Data Center	2	0	2
24	Switches Leaf Data Center	8	0	8
25	Solución de Orquestador DC	1	0	1
26	Switch Core LAN Campus	2	0	2
27	Switch de acceso 48 puertos PoE	22	1	23
28	Switch de acceso 24 puertos PoE	4	0	4
29	Switch DMZ	2	0	2

Nro	Bien	Cantidad	Spare	Cantidad Total
30	Switch de Gestión Fuera de Banda	2	0	2
31	Controlador inalámbrico	2	0	2
32	Access Point	43	4	47
33	Solución de Administración y Gestión Campus	1	0	1
34	Solución de Control de Acceso	1	0	1
35	Hardware de Hiperconvergencia	4	0	4
36	Software Hiperconvergencia	1	0	1
37	Servidor para backup	1	0	1
38	Servidor de inmutabilidad	1	0	1
39	Almacenamiento para backup	1	0	1
40	Librería de backup	1	0	1
41	Software de backup	1	0	1
42	Firewall NGFW (Perimetral)	2	0	2
43	Firewall Interno	2	0	2
44	Consola de analítica y reportes	1	0	1
45	XDR (Extended Detection & Response)	1	0	1
46	ZTNA (Zero Trust Network Access)	1	0	1
47	Seguridad para correo electronico	1	0	1
48	WAF - Seguridad para Aplicaciones Web	1	0	1
49	SIEM	1	0	1
50	Plataforma de detección y respuesta de amenazas externas e internas	1	0	1
51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	1	0	1
52	ADC (application Delivery Controller)	2	0	2
53	Anti - DDos	2	0	2
54	MFA - Administración de identidad y acceso	1	0	1
55	PAM - Administración de acceso privilegiado	1	0	1
56	NDR (Network Detection and Response)	1	0	1
57	Sandboxing	1	0	1
58	Solución de Análisis de Tráfico de Red	1	0	1

2.2.1.Switching

A continuación, se describe los aspectos del diseño considerados para este equipamiento. Siendo estos detallados en la ingeniería a detalle a realizarse previo a la implementación por parte del Proveedor. Asimismo, en el Anexo 2, se adjunta el diagrama de conexión definido como diseño base para la implementación de todas las soluciones.

- **Alta disponibilidad:** Redundancia N+1 en equipos críticos y enlaces duales hacia el fabric.
- **Simplicidad y Escalabilidad:** Topología Spine-Leaf con ECMP y crecimiento horizontal.
- **Segmentación y Seguridad: VRF**, **VXLAN/EVPN**, y control de acceso centralizado (NAC/TACACS+).
- **Operabilidad:** Orquestación, versiones controladas de firmware y telemetría continua.

- **Gestión segregada:** Red OOB independiente del plano de datos

Vista Lógica del Centro de Datos (Fabric Spine-Leaf)

- **Rol y ubicación de equipos**
  - **Spine Data Center (2 unidades):** En sala del Centro de datos; switch de agregación de alto rendimiento.
  - **Leaf Data Center (8 unidades, en pares MLAG):** En racks del DC; acceso a HCI, servicios y firewalls.
  - **Leaf Border (incluido en los Leaf):** Switch Leaf designado como frontera del fabric, responsable de la interconexión con redes y servicios externos (Firewall Interno, Firewall Perimetral, DMZ, SAGE y/o WAN), asegurando la aplicación de políticas de seguridad y segmentación definidas.
  - **Switch OOB (2 unidades):** Gestión fuera de banda para todos los equipos.

- **Interconexiones Obligatorias**
  - Cada Leaf deberá conectarse a ambos Spine mediante dos (2) enlaces de 100Gbps por cada Spine (mínimo), soportando ECMP.
  - Cada Leaf formará MLAG con su par/virtualización equivalente.
  - Cada nodo HCI contará con al menos cuatro (4) enlaces de 25Gbps hacia los Leaf (LACP), y un (1) enlace hacia el switch de gestión OOB.
  - Leaf Border conectará hacia Firewall Interno y DMZ.

- **Servicios L2/L3 del Fabric**
  - **Underlay:** BGP/OSPF para accesibilidad entre Spine/Leaf.
  - **Overlay:** VXLAN/EVPN (estático o dinámico) para extensibilidad L2 y movilidad de cargas.
  - **Gateway distribuido:** ARP/ND suppression, IRB y Anycast Gateway.
  - **Multicast:** IGMP/MLD snooping y PIM/EVPN-Multicast (según fabricante).

Vista Lógica del Campus

- **Core LAN (2 unidades, núcleo colapsado):** Conectado a los firewalls internos mediante enlaces de 10 Gbps.
- **Acceso (22 unidades × 48p PoE + 1 spare = 23 total; + 4 × 24p PoE):** Uplinks 10 Gbps al Core con stack hasta 8 equipos.
- **DMZ (02 unidades)**

2.2.2. Red Inalámbrica

La solución inalámbrica deberá proporcionar conectividad de alta disponibilidad mediante controladores WLAN en configuración N+1, con administración centralizada, políticas homogéneas y optimización automática del entorno radioeléctrico. La arquitectura deberá considerar:

- **Controladoras WLAN en HA (N+1)**
  - Con capacidad para manejar la totalidad de los APs y crecimiento proyectado.
  - Gestión centralizada de políticas de seguridad (WIPS/WIDS, detección de interferencias, optimización automática de canales y potencia).
  - Integración nativa con NAC (802.1X, MAB, perfiles basados en rol, segmentación dinámica).
  - Soporte para SSID corporativo, invitado, BYOD y servicios de localización.
  - Integración con la plataforma de analítica y telemetría

- **Equipamiento WLAN**
  La solución deberá incluir:
  - **43 Access Points + 4 en spare (total 47)** Wi-Fi 6/6E, MIMO 2x2, compatibles con PoE 802.3bt, soporte BLE/Zigbee y servicios IoT.

- Controladores WLAN en N+1, con puertos 10Gbps, DPI, WIPS, WIDS y firewall L7 integrado o deducible por políticas.
- Licenciamiento para toda la solución (AP + Controller + Analytics).

- **Interconexiones mínimas**
  La solución inalámbrica deberá cumplir con las siguientes interconexiones mínimas:
  - Cada controlador WLAN deberá conectarse al Core de la red LAN mediante dos (2) interfaces de 10Gbps, en configuración de alta disponibilidad.
  - Cada controlador WLAN deberá incluir una interfaz adicional para gestión fuera de banda (OOB).
  - Los puntos de acceso deberán conectarse a los puertos PoE de los switches de acceso los cuales deberán tener uplinks de mínimo 10Gbps hacia el Core de la Red LAN.
  - La solución deberá integrarse con la plataforma de control de acceso a red (NAC) mediante mecanismos estándar.
  - La solución deberá integrarse con la plataforma institucional de analítica, telemetría y monitoreo mediante protocolos estándar (Syslog, NetFlow/sFlow, APIs, o equivalentes).

2.2.3. Hiperconvergencia (HCI) - Arquitectura y Equipamiento

La solución de hiperconvergencia deberá integrar cómputo, virtualización y almacenamiento bajo un modelo totalmente definido por software, con administración centralizada y escalabilidad horizontal.

- **Requerimientos:**
  - Mínimo 4 nodos HCI, operando en clúster.
  - Soporte nativo para replicación, alta disponibilidad y auto-recuperación.
  - Conectividad a la red mediante cuatro (4) interfaces de 25Gbps agregadas vía LACP, distribuidas en pares MLAG a dos switches Leaf distintos.
  - Gestión fuera de banda obligatoria mediante Switch OOB.
  - Integración con la solución de respaldo para protección de máquinas virtuales.

- **Equipamiento HCI**
  - Nodos HCI con CPU de gama empresarial, almacenamiento SSD/NVMe, duplicación de controladoras, fuentes redundantes y hypervisor integrado.
  - Licencias completas para virtualización, administración y soporte del fabricante.

- **Interconexiones mínimas**
  La solución de hiperconvergencia deberá de cumplir con las siguientes interconexiones mínimas:
  - Cada nodo HCI deberá conectarse al fabric del centro de datos mediante cuatro (4) interfaces de 25Gbps, agregadas mediante LACP y distribuidas en pares hacia dos (2) switches Leaf distintos, asegurando alta disponibilidad y continuidad operativa ante la falla de uno de los dispositivos o enlaces.
  - Cada nodo HCI deberá contar con una interfaz adicional dirigida a la red de gestión fuera de banda (OOB), conectada a los switches de administración correspondientes.
  - Las interconexiones deberán permitir el tráfico simultáneo requerido por el clúster, incluyendo almacenamiento distribuido, replicación interna, sincronización del clúster, migración de máquinas virtuales y tráfico del hipervisor, sin generación de cuellos de botella.
  - La solución HCI deberá integrarse con la plataforma de respaldo mediante APIs, agentes o mecanismos equivalentes, garantizando

consistencia a nivel de hipervisor para operaciones de copia, restauración y protección.
- Todo el tráfico interno del clúster deberá operar en redes o segmentos específicos del centro de datos (Fabric / VRF correspondientes), evitando mezclarse con redes de usuarios, acceso o tráfico no relacionado al funcionamiento del clúster.

- **Servicios de red**
  El Proveedor deberá realizar el despliegue de servicios de red en los servidores como el AD, NTP, DNS, DHCP y entre otros que se requieran para poner en producción los servicios. Asimismo, deberá de garantizar su operación durante el año de soporte requerido en el presente requerimiento.

  Las características técnicas de todo el equipamiento de la solución de hiperconvergencia se detallan en el Anexo 1 del presente documento.

2.2.4.Sistema de Respaldo

El sistema de respaldo deberá garantizar la protección integral de cargas virtualizadas, servidores físicos y servicios críticos mediante una arquitectura escalable, segura y alineada a buenas prácticas internacionales.

La arquitectura deberá considerar:
- Servidor dedicado de Backup con recursos suficientes para procesamiento de tareas concurrentes.
- Repositorio de almacenamiento optimizado para operaciones de respaldo y restauración, incluyendo disco, inmutabilidad y/o cinta.
- Software de gestión de copias con retenciones configurables, verificación automática de integridad (health check) y compatibilidad con hipervisores, servidores, bases de datos y aplicaciones.
- Integración nativa con la plataforma HCI, servidores físicos, bases de datos y componentes críticos mediante APIs y agentes.
- Capacidad para realizar backups completos, incrementales y diferenciales, con optimización del tráfico.
- Definición de políticas de retención, ventanas de respaldo y mecanismos de restauración granular.

Equipamiento de Respaldo

El equipamiento mínimo requerido para la solución de respaldo incluye:
- Servidor de backup con almacenamiento interno de alto rendimiento, procesador empresarial, memoria suficiente y redundancia de energía.
- Repositorio de almacenamiento en disco dedicado para respaldos, con soporte para cifrado, protocolo NFS/SMB o S3 compatible, y capacidad dimensionada según la retención proyectada.
- Librería de almacenamiento en cinta, con capacidad dimensionada para retención prolongada y compatibilidad con tecnología LTO.
- Software de Backup licenciado para máquinas virtuales, servidores físicos, base de datos y aplicaciones, incluyendo módulos de replicación, verificación de integridad e integración con inmutabilidad.

Almacenamiento para Backups en Disco e Inmutabilidad (WORM)

Incorporar un repositorio de respaldo en disco on-premise para restauraciones rápidas y un repositorio inmutable que impida la eliminación o modificación de copias durante el período de retención definido.

Deberá incluir:
- **Repositorio en disco para backup**
  - Compatible con el software de backup propuesto (bloque/NFS/SMB o S3-compatible, según aplique).
  - Cifrado en reposo (AES-256) y en tránsito (TLS 1.2/1.3).
  - RBAC, autenticación multifactor y segregación de accesos.

- **Repositorio Inmutable**
  - Soporte de Object Lock / WORM en modo Compliance o equivalente, con retenciones y legal hold configurables.
  - Protección total contra eliminación o sobrescritura de backups durante la retención, incluso por administradores.
  - MFA-Delete o mecanismos equivalentes; auditoría inalterable exportable a SIEM.
  - Separación estricta de credenciales, dominios y funciones administrativas.
  - Integración nativa con el software de backup para aplicar inmutabilidad por política o por conjunto de trabajos.

- **Buenas Prácticas 3-2-1-1-0:** mantener 3 copias de datos, en 2 tipos de medios distintos, 1 copia off-site (o logical-airgap), 1 copia inmutable, y garantizar 0 errores mediante verificaciones automáticas de integridad del software de respaldo.

- **Telemetría y monitoreo:** exportación de eventos (retenciones, expiraciones, intentos de borrado) vía Syslog hacia el SIEM.

Interconexiones mínimas

La solución de respaldo deberá de cumplir con las siguientes interconexiones mínimas:

- El servidor de backup deberá conectarse al fabric del centro de datos mediante un mínimo de dos (2) interfaces de 10/25Gbps, configuradas en alta disponibilidad, para garantizar el rendimiento en operaciones de copia y restauración.
- El servidor de backup deberá contar con una interfaz adicional dedicada a la red de gestión fuera de banda (OOB) para operación y mantenimiento independiente del plano de datos.
- El repositorio de almacenamiento en disco deberá conectarse al fabric mediante interfaces de 10/25Gbps, utilizando protocolos estándar (NFS, SMB o S3-compatible), asegurando suficiente ancho de banda para respaldos y restauraciones de alta velocidad.
- La librería de cintas deberá conectarse directamente al servidor de backup mediante interfaces SAS, según lo requerido para operaciones de copia a largo plazo.
- Todo el tráfico asociado a operaciones de respaldo deberá operar sobre redes o segmentos específicos del centro de datos, evitando mezclarse con redes de producción, acceso o tráfico de usuario.
- Los eventos del sistema de respaldo (retenciones, expiraciones, verificaciones de integridad e intentos de eliminación) deberán enviarse mediante Syslog o mecanismo equivalente hacia la plataforma de monitoreo o SIEM.

2.2.5. Ciberseguridad

La solución de seguridad deberá cumplir los principios de Zero Trust Architecture (ZTA), garantizando inspección en múltiples capas, segmentación dinámica, autenticación continua, visibilidad completa del tráfico, y respuesta automatizada ante incidentes.

Incluye los siguientes componentes:

- **Firewall Perimetral NGFW en HA,** con IPS avanzado, inspección TLS/SSL, control de aplicaciones y filtrado web.
- **Firewall Interno** segmentando dominios críticos
- **Consola de Analítica y Reportes** para visibilidad unificada y cumplimiento.
- **XDR (Extended Detection & Response)** para endpoints, con análisis de comportamiento y respuesta integrada.

- **ZTNA (Zero Trust Network Access)** para accesos remotos basados en identidad y postura del dispositivo.
- **Seguridad para Correo Electrónico** con (antiexploit, antiphishing, sandboxing), reputacion y análisis avanzado.
- **WAF** para aplicaciones Web institucionales
- **SIEM** para correlación centralizada
- **Plataforma de Detección y Respuesta de Amenazas Externas e Internas,** para detección temprana de intrusiones.
- **SOAR** para automatización de flujos de respuesta y orquestación de incidentes.
- **ADC (application Delivery Controller)** para balanceo L4/L7, offloading SSL, optimización de aplicaciones y continuidad del servicio.
- **Anti-DDos** para mitigación de ataques volumétricos y de aplicación.
- **MFA** para administración de identidad y acceso.
- **PAM** para administración de acceso privilegiado
- **NDR (Network Detection and Response)** para detección avanzada basado en tráfico y comportamiento.
- **Sandboxing** para análisis dinámico de archivos sospechosos.
- **Solución de Análisis de Tráfico de Red**

3. Soporte y Ciberseguridad

3.1. Mesa de Servicio

En una operación de misión crítica como la Central 911, la Mesa de Servicio 24x7 no es un "soporte adicional", sino un control operativo esencial para asegurar la continuidad y disponibilidad de la infraestructura tecnológica implementada para la atención y gestión de emergencias. Este servicio debe considerarse porque habilita atención permanente con (3) tres niveles de escalamiento, gestión integral de incidentes y requerimientos con trazabilidad, mantenimiento preventivo/correctivo, y gestión de garantías/repuestos, reduciendo la probabilidad y el tiempo de indisponibilidad. Además, permite cumplir acuerdos de niveles de servicio con tiempos objetivo exigentes, respuesta en minutos y restauración en horas para criticidad alta, y asegurar control, evidencia y mejora continua, elementos indispensables para gobernar la operación 24x7 y evitar puntos únicos de falla. Este servicio deberá estar activo desde el inicio del soporte y garantía para el presente requerimiento.

Alcance

Asegurar la continuidad operativa del equipamiento tecnológico del presente requerimiento para la operación de la Central 911 mediante un servicio de Mesa de Servicio especializado, con atención permanente, escalamiento por niveles y cumplimiento de acuerdos de niveles de servicio.

- Atención permanente 24x7 para incidentes y requerimientos asociados al equipamiento tecnológico.
- Soporte nivel 1: registro, categorización, priorización, diagnóstico inicial, solución remota y escalamiento.
- Soporte nivel 2: diagnóstico avanzado, intervención presencial cuando corresponda, reinstalación, configuración, reemplazo de componentes y coordinación de garantías.
- Soporte nivel 3: resolución de fallas complejas, soporte a configuraciones avanzadas, análisis de causa raíz y coordinación con fabricantes o proveedores especializados.
- Mantenimiento preventivo planificado, mantenimiento correctivo y verificación de salud de equipos.
- Gestión de inventario y control de activos, incluyendo evidencia de intervenciones y cambios.
- Reportes operativos, seguimiento y plan de mejora continua.
- Catálogo de Servicios: definido por el proveedor en base todo al presente requerimiento, y actualizado durante el soporte y garantía.

Dotación de personal mínima

Cuadro Nro. 08

Nivel	Cobertura	Modalidad	Posición simultanea	Dotación total recomendada	Rol principal
Nivel 1	Atención continua	Presencial	Tres (3)	Once (11) 2 por turno (3x3=9) + 2 de relevo (descansos, vacaciones y contingencias).	Registro, diagnóstico inicial, solución remota y escalamiento
Nivel 2	Atención continua	Presencial	Cuatro (4)	Catorce (14) 2 por turno (4x3=12) + 2 de relevo (descansos, vacaciones y contingencias)	Soporte avanzado, intervención presencial, reemplazos y coordinación de garantías
Nivel 3	Atención continua	Presencial	Dos (2)	Ocho (8) 1 por turno (2x3=6) + 2 de relevo (descansos, vacaciones y contingencias)	Especialistas, análisis de causa raíz y coordinación con fabricantes

Turnos Operativos mínimos

Cuadro Nro. 09

Turno	Horario	Observación
Primer Turno	Turno de ocho (8) horas	Incluye traslape de quince minutos para transferencia de posición.
Segundo Turno	Turno de ocho (8) horas	Incluye traslape de quince minutos para transferencia de posición.
Tercer Turno	Turno de ocho (8) horas	Incluye traslape de quince minutos para transferencia de posición.

Nivel 1 Funciones mínimas de Analista de mesa de ayuda

- Recepción multicanal, registro y clasificación.
- Priorización según matriz de impacto y urgencia.
- Diagnóstico inicial y solución remota cuando aplique.
- Comunicación al usuario y escalamiento controlado.
- Gestión de base de conocimiento y cierre con evidencia.

Nivel 2 Funciones mínimas de Soporte Técnico

- Atención de incidencias de software, hardware, periféricos y conectividad del puesto.
- Atención presencial y/o remoto, reinstalación, configuración, reemplazo y pruebas.
- Gestión de repuestos y coordinación de garantías.
- Estandarización y control de configuraciones de estaciones y periféricos.

Nivel 3 Funciones mínimas de Soporte Especialista

- Resolución de fallas complejas no resueltas en niveles previos.
- Análisis de causa raíz, corrección permanente y prevención de recurrencia.
- Coordinación con fabricantes y proveedores especializados.
- Validación técnica de cambios que afecten continuidad operativa.

Gestión de componentes, repuestos, garantías y cambios

- Diagnóstico y evidencia: confirmar falla con checklist, registros y evidencia.
- Contención: reasignación de puesto o componente.
- Reemplazo: cambio por unidad equivalente y actualización de inventario con número de serie.
- Verificación: pruebas funcionales y conformidad del usuario.
- Cierre y trazabilidad: registro completo en el Nivel 1 y actualización de activos.
- Gestión de garantía: trámite de reparación o reemplazo del componente retirado para reconstituir stock mínimo.

Características generales del Software de Mesa de Servicio:

Cuadro Nro. 10

Componente funcional	Carácter	Descripción técnica	Resultado esperado
Gestión de tickets	Obligatorio	Registro, categorización, asignación, bitácora, adjuntos y estados.	Trazabilidad completa
Acuerdos de niveles de servicio	Obligatorio	Cálculo automático, alertas, escalamiento y semáforos por prioridad.	Control de cumplimiento
Catálogo de servicios	Obligatorio	Formularios, validaciones y aprobaciones por tipo de requerimiento.	Atención estandarizada
Gestión de activos	Obligatorio	Inventario con número de serie, ubicación, usuario, garantía y relación con tickets.	Inventario consistente
Base de conocimiento	Obligatorio	Artículos, versionado, revisión y publicación para nivel 1.	Resolución más rápida
Reportes	Obligatorio	Tableros de desempeño, tendencias, exportación y reportes programados.	Gobierno del servicio
Auditoría y seguridad	Obligatorio	Roles, permisos, bitácora de cambios y trazabilidad por usuario.	Cumplimiento y control

Módulo de Soporte Remoto	Obligatorio	Conexión segura, grabación de sesión Multisesión	Atención estandarizada
Aplicación IA/ Chatbot	Obligatorio	Triaje inteligente, resolución autónoma, traspaso fluido	Atención estandarizada

Alcance de implementación – entregables y criterios minimos de aceptación

Cuadro Nro. 11

Fase	Entregables	Criterios mínimos de aceptación	Cumplimiento
Planificación	Plan de despliegue; matriz de riesgos; plan de comunicaciones; plan de pruebas; matriz de roles y responsabilidades.	Aprobación formal; cronograma validado.	La planificación para la implementación de la mesa de servicio formará parte del Plan del Proyecto. El Proveedor deberá de implementar la mesa de servicio, detallando los procedimientos, catálogo de servicio, recursos, software, entre otros previo a la aceptación operativa del presente requerimiento, considerando lo establecido en el presente documento. El software de mesa de servicio podrá ser on-premise o en nube.
Preparación	Imágenes, configuraciones estándar, etiquetado, inventario inicial.	Muestra representativa validada; inventario trazable.	
Despliegue	Instalación física y lógica; checklist por puesto; evidencias.	Pruebas de aceptación aprobadas; incidencias registradas.	
Transferencia	Documentación técnica; capacitación; acta de transferencia.	Transferencia formal; base de conocimiento inicial.	

Indicadores mínimos para control del servicio durante el primer año de soporte y garantía:

Cuadro Nro. 12

Indicador	Definición	Meta referencial
Cumplimiento del tiempo máximo de respuesta	Porcentaje de tickets atendidos dentro del tiempo máximo de respuesta por prioridad	95% o superior
Cumplimiento del tiempo objetivo de restauración	Porcentaje de incidentes restaurados dentro del tiempo objetivo por prioridad	90% o superior en prioridad crítica
Tiempo promedio de restauración en prioridad crítica	Promedio desde registro hasta restauración para prioridad crítica	2 horas o menor

Resolución en primer contacto	Porcentaje de tickets resueltos por nivel 1 sin escalamiento	60% o superior (objetivo creciente)
Reincidencia de incidentes	Cantidad de incidentes repetidos por misma causa	Tendencia decreciente
Disponibilidad de la Mesa de Servicios	Disponibilidad efectiva del canal de atención y registro	99.9% o superior
Antigüedad de tickets abiertos	Tickets abiertos con más de 72 horas	Controlado y justificado
Satisfacción del usuario	Encuesta posterior al cierre	4 sobre 5 o superior
Cumplimiento de mantenimiento preventivo	Actividades preventivas ejecutadas frente a plan	95% o superior
Tiempo de reposición de periféricos o equipos con spare en sitio	Tiempo desde diagnóstico hasta reemplazo para periféricos o equipos con spare en sitio	1 hora

3.2. SOC

El Centro de Operaciones de Seguridad (SOC) constituye un control operativo esencial para asegurar la confidencialidad, integridad y disponibilidad de los activos tecnológicos que soportan la atención de emergencias. El SOC permite la vigilancia continua 24x7 de eventos de ciberseguridad, la detección temprana de actividades anómalas y amenazas (internas y externas), y la respuesta coordinada a incidentes de seguridad antes de que escalen a afectaciones operativas, para lo cual coordina permanentemente con la mesa de servicio para el registro respectivo de la incidencia u otro relacionado al alcance del SOC. Asimismo, el SOC asegura el cumplimiento de objetivos de seguridad operacional, y se integra con el servicio de seguridad del SAGE, de tal forma se tenga una seguridad de extremo a extremo con equipos multidiscplinarios y herramientas diversas para minimizar cualquier tipo de ataque o vulneración a la seguridad del 911.

El servicio SOC y todo lo inidicado debe estar implementado antes de la aceptación operativa, por lo que el Proveedor deberá presentar el plan de implementación de este servicio en el "Plan del Proyecto".

El Proveedor debe proporcionar un SOC con las siguientes características:

- Analizar y clasificar eventos mediante playbooks, clasificadores de severidad y la base de datos de amenazas y vulnerabilidades del laboratorio de amenazas de las soluciones adquiridas.
- Notificar a la Central 911 y otros Proveedores sobre amenazas verificadas y entregar recomendaciones de remediación a través del portal del servicio.
- Brindar acceso a un portal del servicio para visualizar eventos verificados, estatus de incidentes y descargar reportes.
- Escalar incidentes críticos a la Central 911 dentro de los 15 minutos posteriores a su confirmación, a través de correo electrónico y llamada telefónica.
- Escalar incidentes de alta severidad en máximo 45 minutos vía correo electrónico; de severidad media en 90 minutos y de severidad baja en un máximo de 6 horas.
- Proporcionar informes semanales resumidos de alertas, notificaciones y tickets del portal.
- Procesar y evaluar todos los eventos de seguridad recibidos de los dispositivos monitoreados para filtrar falsos positivos y generar notificaciones verificadas.
- Analizar y validar eventos, clasificándolos como incidentes verificados y notificando por correo electrónico.

- Generar tickets de incidente de seguridad con notificación inmediata según la matriz de escalamiento acordada.
- Registrar todas las interacciones y recomendaciones en los tickets creados.
- Brindar acceso al historial de eventos y tickets, con visualización de estado y detalle de incidentes.
- Permitir la visualización de reportes e informes generados por el servicio.
- Permitir el envío de solicitudes de ajuste de monitoreo o cambios en la recolección de logs mediante el portal proporcionado.
- Clasificar los incidentes de seguridad de acuerdo con su impacto potencial, utilizando la tabla de severidad descrita (Crítico, Alto, Medio, Bajo).
- Ajustar la prioridad del ticket de incidente conforme cambie el estado o impacto del incidente.
- Mantener abiertos los tickets el tiempo necesario para la evaluación.
- Permitir solicitudes de incorporación de nuevos dispositivos a través del portal.
- Debe de considerar alguno de los siguientes casos de uso alineados a MITRE:

Cuadro Nro. 13

Reconocimiento	
Reconocimiento: Casos de uso que detectan técnicas de recopilación de información de forma activa o pasiva.	
T1595	Escaneo activo
Militarización	
Ejecución: Casos de uso que detectan técnicas que implican crear, comprar o comprometer/robar recursos externos con el fin de comprometer las vulnerabilidades de la víctima.	
T1047	Instrumental de administración de Windows
Entrega	
Acceso inicial: Casos de uso que detectan sitios web, aplicaciones, acceso remoto, servicios o ataques de phishing comprometidos.	
T1133	Servicios Remotos Externos
T1189	Compromiso de intrusión
T1190	Aprovechar la aplicación de cara al público
T1566	Phishing
Explotación	
Ejecución: Casos de uso que detectan cuando se habilita código o software no autorizado en un sistema.	
T1072	Herramientas de implementación de software
T1059	Intérprete de comandos y secuencias de comandos
T1203	Explotación para la ejecución del cliente
Acceso a credenciales: Casos de uso que detectan intentos de robo de credenciales, como keyloggers o ataques de volcado de credenciales.	
T1003	Volcado de credenciales del sistema operativo
T1056	Captura de entrada
T1083	Detección de archivos y directorios
T1110	Fuerza bruta
Descubrimiento: Casos de uso que detectan cuándo los atacantes intentan obtener conocimientos sobre el sistema y las redes internas.	
T1018	Detección remota de sistemas
T1046	Escaneo de servicios de red
T1082	Descubrimiento de información del sistema
T1083	Detección de archivos y directorios
T1087	Descubrimiento de Cuentas
T1135	Detección de recursos compartidos de red
Evasión de la defensa: Casos de uso que detectan cuándo los atacantes intentan eludir los controles de protección.	
T1014	Rootkit

T1027	Archivos o información ofuscados
T1055	Inyección de proceso
T1070	Eliminación del indicador en el host
T1140	Desofuscar / Decodificar archivos o información
T1211	Explotación para la evasión de la defensa
T1212	Explotación para el acceso a credenciales
T1218	Ejecución de proxy binario firmado
T1497	Virtualización / Evasión de sandbox
T1539	Robar código de sesión web
T1548	Mecanismo de control de elevación de abuso
T1562	Deteriorar las defensas
T15740	Flujo de ejecución de secuestro
Escalada de privilegios: Casos de uso que detectan intentos de obtener permisos de nivel superior en un sistema o red.	
T1055	Inyección de proceso
T1068	Explotación para la escalada de privilegios
T1078	Cuentas válidas
T1134	Manipulación de tokens de acceso
T1548	Mecanismo de control de elevación de abuso
T1574	Flujo de ejecución de secuestro
Instalación	
Movimiento lateral: Casos de uso que detectan intentos de obtener acceso no autorizado a los sistemas de una red desde una fuente presuntamente confiable en la misma red.	
T1021	Servicios Remotos
T1072	Herramientas de implementación de software
T1210	Explotación de servicios remotos
T1534	Spearphishing interno
T1570	Transferencia lateral de herramientas
Persistencia: Casos de uso que detectan intentos de mantener el acceso a los sistemas a través de reinicios, credenciales modificadas y otras interrupciones que podrían cortar el acceso del adversario.	
T1176	Extensiones de navegador
T1133	Servicios Remotos Externos
T1136	Crear una cuenta
T1574	Flujo de ejecución de secuestro
Colección: Casos de uso que detectan técnicas utilizadas por los atacantes para recopilar información con fines de exfiltración.	
T1185	Secuestro de sesión del navegador
T1574	Captura de entrada
T1602	Datos del repositorio de configuración
Comando y control	
Comando y control: Casos de uso que detectan tráfico sospechoso que se origina desde el sistema interno a destinos externos.	
T1001	Ofuscación de datos
T1008	Canales de reserva
T1071	Protocolo de capa de aplicación
T1092	Comunicación a través de medios extraíbles
T1095	Protocolo de capa no aplicativa
T1104	Canales de varias etapas
T1105	Transferencia de herramientas de entrada
T1132	Codificación de datos
T1219	Software de acceso remoto
T1568	Resolución dinámica
T1571	Puerto no estándar
T1573	Canal encriptado
Acciones sobre objetivos	

Exfiltración: Casos de uso que detectan técnicas que los adversarios pueden utilizar para robar datos y evitar la detección mientras los eliminan.	
T1041	Exfiltración a través del canal C2
T1048	Exfiltración sobre protocolo alternativo
T1052	Exfiltración sobre medio físico
T1537	Transferir datos a una cuenta en la nube
T1567	Exfiltración a través del servicio web
Impacto: Casos de uso que detectan técnicas que los adversarios pueden utilizar para interrumpir la disponibilidad o comprometer la integridad mediante la manipulación de los procesos comerciales y operativos.	
T1485	Destrucción de datos
T1486	Datos encriptados para lograr un impacto
T1498	Denegación de servicio de red
T1499	Denegación de servicio de endpoints
T1561	Borrado de disco

- Se debe proporcionar un servicio complementario al SOC, el cual debe ser provisto por un fabricante de ciberseguridad e incluir servicios para preparación y respuesta ante incidentes, con las siguientes características:
  - Proporcionar un servicio de preparación y respuesta ante incidentes del fabricante de seguridad de las soluciones adquiridas que contemple asesoría y acompañamiento remoto en actividades de forense digital, análisis, contención y remediación de incidentes de ciberseguridad.
  - Garantizar 100 horas de análisis forense digital y respuesta a incidentes, debiendo ser provista por algunos de los fabricantes de las soluciones XDR, SIEM o SOAR adquiridas, por el periodo de soporte y garantía. De no ser usado el servicio, antes del término del contrato, se podrá acceder a un catálogo de opciones asesoría especializada.
  - Asegurar la disponibilidad de recursos técnicos especializados para la atención de incidentes y ejercicios proactivos de preparación durante toda la vigencia del servicio contratado.
  - Realizar una reunión remota inicial de onboarding para establecer los puntos de contacto, presentar el portal de gestión de incidentes y explicar las opciones de servicios disponibles.
  - Ejecutar una reunión remota de capacitación forense, explicando en detalle los procesos de respuesta a incidentes, capacidades y alcance, así como resolver todas las consultas relevantes.
  - Garantizar un tiempo de respuesta máximo de 02 horas desde la apertura del ticket de incidente crítico.
  - Brindar acceso continuo a servicios de soporte y asesoría para respuesta a incidentes durante toda la vigencia del contrato.
  - Realizar revisión integral del sistema de seguridad de la Central 911, incluyendo identificación de componentes comprometidos en caso de incidente.
  - Analizar logs relevantes provenientes de soluciones firewall/NetFlow, VPN, proxy web, IDS/IPS, SIEM y artefactos forenses complementarios.
  - Ejecutar análisis detallado de archivos y memoria con el fin de descubrir cargas maliciosas y técnicas utilizadas en el incidente.
  - Identificar y documentar hosts comprometidos, cuentas comprometidas, indicadores de compromiso (IOC), indicadores de exfiltración de datos, métodos de acceso inicial y paciente cero.
  - El servicio deberá evaluar el estado actual de preparación de la entidad ante incidentes y ataques. Esta evaluación se deberá realizar en conjunto con los expertos de la marca para evaluar la postura de seguridad actual.
  - Este servicio deberá Identificar y priorizar las mejoras más críticas. Desde la implementación completa de programas hasta la orientación estratégica para ayudarnos a establecer una ciberdefensa de primer nivel.

- Deberá establecer una base sólida, desarrollando las bases para una ciberdefensa sólida, incluidas políticas, procedimientos, estándares, flujos de trabajo, cuadros de personal y hojas de ruta estratégicas.
- Deberá descubrir y priorizar los riesgos de seguridad en toda la institución en términos de ciberdefensa.
- Adicionalmente deberá trabajar colaborativamente con el personal de la entidad para actuar ante los siguientes escenarios a demanda:

Cuadro Nro. 14

Tipo de Servicio	Servicio y Descripción
Servicio de Respuesta a Incidentes	Respuesta al incidente • Investigar y recuperarse de incidentes de seguridad y violaciones de datos: ▪ Contener y erradicar la amenaza ▪ Determinar el punto de acceso inicial ▪ Determinar el alcance de la actividad no autorizada ▪ Determinar a qué datos, si los hubo, se accedió o se robaron • Análisis de malware e ingeniería inversa Investigación de ransomware • Involucrar al actor de amenazas en nombre de la Entidad. • Buscar pruebas de que el atacante puede descifrar los datos • Remitir a la Entidad y a los proveedores de servicios de pago para adquirir claves de cifrado para la recuperación de datos. • Aplicar ingeniería inversa a la utilidad de descifrado proporcionada por el atacante para garantizar que no exista ningún código malicioso • Proporcionar tutorial al equipo de la Entidad para demostrar cómo descifrar archivos • Proporcionar soporte remoto para la resolución de problemas Compromiso de correo electrónico corporativo • Contener el incidente y recomendar medidas de seguridad adicionales; Investigue y determine la causa raíz, la ventana de compromiso, la actividad del atacante y revise los datos a los que se accede para cuantificar la información confidencial. Compromiso web • Contenga amenazas e implemente salvaguardas, analice registros, revise código, cuantifique la exposición o pérdida de información confidencial y recomiende contramedidas de refuerzo de diseño. Respuesta a la brecha en la nube • Identifique el vector de ataque inicial y el alcance del acceso no autorizado y la exfiltración, contenga el incidente, identifique el alcance de los sistemas para la remediación y recomiende/implemente medidas de seguridad adicionales y verificaciones continuas. Investigación PCI • Contenga los incidentesdispo e implemente medidas de seguridad, navegue por el proceso de PFI, responda a supuestas violaciones, identifique el vector de ataque y la ventana de compromiso, cuantifique la cantidad de tarjetas expuestas

Análisis Forense Digital	• Investigaciones digitales, incluidos asuntos relacionados con amenazas internas, empleados que se han ido y robo de propiedad intelectual. • Análisis forenses de medios digitales, incluidas computadoras de escritorio/portátiles, servidores, teléfonos móviles/tabletas y/o datos de registro para cumplir objetivos específicos, incluida la identificación del acceso, movimiento, exfiltración y/o destrucción de datos. • Análisis forense de hardware para determinar la funcionalidad de un dispositivo o extraer datos de dispositivos IoT, nuevas tecnologías o hardware creado por atacantes • Investigaciones de datos estructurados ▪ Asesorar sobre la recopilación y liderar el análisis de entornos de bases de datos SQL y NoSQL, incluidos, entre otros, la revisión de esquemas, tablas, procedimientos y registros recopilados de los sistemas de bases de datos afectados, para evaluar la actividad de los actores de amenazas y el riesgo de exposición de datos.
Servicios de Prueba y Evaluación	Revisión de preparación para infracciones (BRR) • Evaluación de riesgos de ciberseguridad específica centrada en controles de detección, personas, procesos y tecnologías necesarios para responder de manera efectiva a las amenazas cibernéticas. • Incluye recomendaciones de remediación, mejoras de control y una hoja de ruta estratégica para lograr un estado objetivo de preparación para infracciones. Desarrollo del Programa de Respuesta a Incidentes • Facilitar el desarrollo de un programa de respuesta a incidentes para ayudar a establecer o mejorar el plan, las políticas, los procedimientos y los manuales de respuesta a incidentes actuales. Pruebas de penetración (Penetration Test): ejercicios de equipo morado y rojo • Simula un ciberataque del mundo real para evaluar la fuerza de las contramedidas e identificar vulnerabilidades de seguridad ocultas. • Defina un alcance, reglas de compromiso y establezca objetivos, y luego identifique rutas de ataque y cadenas de explotación que un actor de amenazas probablemente aprovecharía para obtener acceso a datos confidenciales o aplicaciones comerciales críticas. Análisis de vulnerabilidades • Evaluación técnica interna y/o externa diseñada para generar tantas vulnerabilidades como sea posible en el entorno, junto con la gravedad y la prioridad de remediación recomendada. Análisis de Aplicaciones Web • Evalúe las aplicaciones web en busca de vulnerabilidades, incluidas las fallas en el desarrollo, la configuración, la implementación, el proceso de actualización, las integraciones de API, el mantenimiento o los complementos de terceros. Evaluaciones de aplicaciones móviles • Probar y mejorar la seguridad de las aplicaciones móviles. Enumere la superficie de ataque, buscando vulnerabilidades,

	configuraciones incorrectas o fallas lógicas que conduzcan a caminos probables de compromiso y/o exfiltración de datos. Ejercicios de phishing por correo electrónico • Probar y mejorar la conciencia de seguridad cibernética en la Entidad y reduzca la susceptibilidad a los ataques de phishing. Evaluación de Compromisos / Cacería de Amenazas (Threat Hunting) • Revisar las redes de la Central 911 y los comportamientos de los terminales para determinar si hay evidencia de acceso o actividad no autorizados. Evaluación de la seguridad del correo electrónico • Llevar a cabo una revisión exhaustiva de la configuración de seguridad del entorno de correo electrónico que incluya la revisión de la administración de la cuenta, las reglas de reenvío de correo electrónico, las políticas de la bandeja de entrada, los controles de autenticación.
Servicios de Asesoría Estratégica	Director virtual de seguridad de la información (vCISO) • Un vCISO de El fabricante ayuda a desarrollar e implementar una estrategia de seguridad cibernética, identificar riesgos y proporcionar recomendaciones para medidas de reducción de riesgos. • Un vCISO puede responder a las preguntas de la junta directiva o de la alta dirección sobre los puntos de referencia y la madurez del programa de seguridad, la preparación para infracciones, la eficacia y la idoneidad, etc. • Estrategia de riesgo cibernético y hojas de ruta de mitigación • Desarrolle planes estratégicos personalizados que establezcan un camino, un cronograma y un presupuesto para lograr los objetivos de resiliencia cibernética de una organización. • Revisión de la estrategia de seguridad del Directorio (Board of Directors o BoD) • Evaluación y revisión para identificar el riesgo cibernético, crear un perfil de estado actual y crear una estrategia de seguridad clara para compartir con sus ejecutivos y la Junta. • Maduración del desarrollo de programas cibernéticos, políticas y estándares • Desarrollar o mejorar políticas y estándares de ciberseguridad. Teniendo en cuenta los estándares específicos de la industria, los objetivos de la Central 911 y las metas futuras. • Evaluación SOC • Diseñar y asesorar sobre la construcción de un centro de operaciones de seguridad de próxima generación y/o un programa de seguridad de la información basado en las mejores prácticas. • Implementación discreta de proyectos cibernéticos • Asistencia experta con la arquitectura, la supervisión de la implementación y el ajuste de un proyecto crítico de ciberseguridad. • Servicios estratégicos y tácticos, por ejemplo, asesoramiento sobre el fortalecimiento de aplicaciones comerciales críticas, correo electrónico empresarial y controles de detección de última generación. • Servicios de asesoramiento de remediación y recuperación estratégica posterior a la vulneración • Orientación y priorización de remediación estratégica para evitar una mayor propagación de cualquier persistencia relacionada con el Incidente.

	• Evaluación del estado de los controles de seguridad, sistemas, proveedores de servicios gestionados, diseño de equipos y procedimientos destinados a identificar y prevenir el Incidente específico. • Con base en la evaluación, desarrollar y entregar un plan de remediación estratégico que incluya objetivos priorizados a corto, mediano y largo plazo para abordar las debilidades de seguridad expuestas por un incidente específico y reducir el riesgo de cualquier incidente continuo o recurrente.
Servicios de Gobierno, Riesgo y Cumplimiento	Evaluación CIS V8 • Informe CIS V8 y recomendaciones personalizadas. • Roadmap (hoja de ruta) de implementación de 12 a 24 meses. Evaluación del marco de ciberseguridad del NIST (NIST CSF) • Libro de trabajo de resultados del LCR del NIST. • Informe Ejecutivo de Hallazgos Temáticos. • Hoja de ruta de implementación de 12 a 24 meses. Evaluaciones de ciberseguridad reguladas y basadas en contratos (por ejemplo, CCPA, NYDFS, HIPAA, FINRA, PCI DSS, C2M2, GDPR) • Realizar un mapeo de evaluación a los requisitos de control de los marcos contractuales, estatales y/o regulatorios. • Evalúe los requisitos de control, encuentre y solucióne las brechas y demuestre el cumplimiento. Revisiones de debida diligencia cibernética de fusiones y adquisiciones • Evaluación específica en relación con la actividad pendiente de fusión/adquisición. Enfocada y táctica, esta evaluación está diseñada para brindar transparencia a los participantes del trato. • Identifique posibles señales de alerta, resalte los riesgos de ciberseguridad ocultos y obtenga una evaluación independiente de la madurez general del programa de seguridad de la información. Evaluación de riesgos de ciberseguridad de proveedores externos • Evaluación del riesgo de ciberseguridad basado en proveedores externos. • Evaluar y mejorar los requisitos del contrato relacionados con la seguridad de la información. • Desarrollar y/o mejorar las operaciones de seguridad relacionadas con el cumplimiento de los requisitos de seguridad por parte de proveedores externos.

4. Implementación, Planificación y Gestión del Proyecto

4.1. Gestión del Proyecto

El Proveedor deberá presentar el plan del proyecto a los quince (15) días calendarios contabilizados al día siguiente de firmado el Contrato. Este documento tiene que contener como mínimo las siguientes áreas de conocimiento:

- Gestión del Alcance
- Gestión del Cronograma
- Gestión de recursos
- Gestión de Calidad
- Gestión de las comunicaciones
- Gestión de riesgos
- Gestión de los interesados

Dicho plan será revisado por el Gerente del Proyecto del Comprador asignado a este contrato y será aprobado en un plazo no mayor de cinco (05) días calendarios después de haber sido presentado por el Proveedor en el caso de no existir observaciones. De existir observaciones, están deberán ser levantadas en un plazo no mayor de dos (2) días calendario y ser enviado nuevamente para revisión con el mismo plazo de aprobación. Asimismo, el Proveedor deberá habilitar en una herramienta en línea para 05 usuarios que permita visualizar todas estas áreas de conocimiento, con el cronograma en línea, estableciendo KPI de seguimiento. Asimismo, la gestión de riesgos debe ser una actividad semanal, con la finalidad de generar alertas tempranas de la ejecución del proyecto en todas sus áreas de conocimiento y propias del Contrato, visualizando el estado de la procura desde su requerimiento hasta la llegada a los almacenes del Proveedor y su traslado al almacén en la Central 911, con la finalidad de tener el tracking de estos.

Se establecerán semanalmente reuniones con el personal clave del Proveedor y el personal del equipo del proyecto 911 para realizar el seguimiento a las actividades.

El Proveedor deberá contar con un equipo de profesionales para realizar la gestión de proyectos, principalmente el Jefe de Proyectos y un Controller del Proyecto, quienes deberán generar y mantener en un repositorio en línea compartido con toda la documentación desde la firma del contrato. Asimismo, elaborar todas las actas de reuniones que se realicen durante la ejecución de estas. Este repositorio será de acceso restringido.

4.2. Personal Clave para la gestión

- ***01 Jefe de Proyecto:***

  Nivel Académico

  - Con título profesional en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. Colegiado y habilitado (para la firma de contrato se presentará la habilitación)

  Certificaciones

  - Certificación vigente PMP emitido institución PMI o Certificación SCRUM Máster.
  - Certificación ITIL V4
  - Certificación ISO27001 Seguridad de la información.
  - Certificación ISO22301 Continuidad del negocio.

  Experiencia

  - Con mínimo de diez (10) años de experiencia como jefe o gerente de proyecto en implementación de soluciones TIC.

  Nota: los licitantes en su propuesta deben considerar un controller del proyecto.

4.3. Personal clave para la Implementación.

Cuadro Nro. 15

Especialista	Perfil
01 Especialista en Networking	**Formación académica:** Con título profesional o bachiller en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante en Switching de la solución ofertada. **Experiencia:** Con mínimo cinco (05) años de experiencia como Especialista en Networking.
01 Especialista en Ciberseguridad	**Formación académica:** Con título profesional o bachiller en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes y/o Comunicaciones. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante de la solución de Firewall ofertada. **Experiencia:** Con mínimo cinco (05) años de experiencia como Especialista en Seguridad.
01 Especialista en Servidores	**Formación académica:** Con título profesional o bachiller en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante de la solución de Hardware y/o Software ofertada. **Experiencia:** Con mínimo cinco (05) años de experiencia como Especialista en Servidores.
01 Especialista en Servicios de TI	**Formación académica:** Con título profesional o bachiller en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. **Capacitaciones:** Capacitación mínima en 1 certificación en algunas de las soluciones ofertadas por el fabricante de la solución ofertada.

	Certificación en ITIL **Experiencia:** Con mínimo cinco (05) años de experiencia como Especialista en Gestión de Servicios de TI.

4.4. Personal Clave para la administración de las soluciones tecnológicas durante el periodo de soporte y garantía.

Cuadro Nro. 16

Especialista	Perfil	Cantidad
Jefe de Soporte TI	**Formación académica:** Con título profesional en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Ingeniero Administrativo, **Capacitación** • Curso o taller o Certificación en Dirección de Proyectos • Curso o taller o Certificación ITIL V4 • Curso o Taller Certificación SCRUM Máster. **Experiencia:** • Con mínimo de cinco (05) años de experiencia como Coordinador o Gerente de Servicio de soluciones TIC. Colegiado y habilitado (para la firma de contrato se presentará la habilitación)	01
Soporte en redes	**Formación académica:** Con título profesional o bachiller o técnico en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante en Switching de la solución ofertada. **Experiencia:** Con mínimo dos (02) años de experiencia como Especialista en Networking.	03
Soporte en Ciberseguridad	**Formación académica:** Con título profesional o bachiller o técnico en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes y/o Comunicaciones. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante de la solución de Firewall ofertada. **Experiencia:**	03

	Con mínimo dos (02) años de experiencia como Especialista en Seguridad.	
Soporte en Servidores	**Formación académica:** Con título profesional o bachiller o técnico en Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Computo y/o Industrial y/o Redes. **Capacitaciones:** Capacitación en la solución ofertada acreditado mediante certificación del fabricante de la solución ofertada. **Experiencia:** Con mínimo dos (02) años de experiencia como Especialista en Servidores.	03

4.5. Personal Clave para el soporte a usuario final durante el periodo de soporte y garantía

Para el primer año el soporte y garantía, el Proveedor debe brindar el soporte 24x7, para lo cual deberá considerar 3 turnos.

El servicio debe estar estructurado como mínimo en tres niveles de atención, con escalamiento controlado y responsabilidades diferenciadas. La dotación se proyecta considerando continuidad 24x7 y una base instalada de equipamiento para operación.

El personal deberá considerar como mínimo los siguientes puestos para brindar el soporte requerido en 03 turnos con la finalidad de cubrir el servicio de 24x7:

- Analista de mesa de servicio,
- Soporte técnico para las diversas especialidades a nivel de usuario final.

4.6. Personal NO Clave

El Proveedor puede considerar otro personal al exigido de forma complementaria, sin que reemplace las actividades del personal clave, para la gestión, implementación y soporte y garantía.

4.7. Implementación

El Proveedor, previo a la instalación, configuración y pruebas, deberá presentar la topología final, plan de numeración en IPv4 e IPv6, plan de configuración, planes de despliegue, planes de rollback, plan de pruebas final, entre otros documentos que considere para su implementación. Esto deberá presentarlo por equipo o solución integral tres (03) días antes de su implementación en la Central 911, y será aprobado mediante acta por el Gerente de Proyectos asignado por el Comprador.

Finalizada la instalación, configuración y pruebas, deberá actualizar los documentos finales, y entregarlos en sobre lacrado para la "Aceptación Operativa".

Nota: Todas las soluciones deberán ser configuradas en doble pila (IPv4/IPv6), para lo cual el Proveedor deberá considerar los complementos tecnológicos (hardware y/o software) necesarios para su operatividad y correcta operación, sin afectar el performance de la red en su integridad.

4.8. Aceptación Operativa

Finalizada la implementación, el comprador (Pronatel), a través del Gerente de Proyectos asignado a este requerimiento, solicita al Proveedor toda la documentación desde el diseño hasta las pruebas finales integrales, y de considerar solicitar pruebas adicionales. Asimismo, se revisa que el Proveedor presente toda la documentación

para la operación como planes BCP, DRP, SLAs, mesa de servicio y SOC 7x24, manuales, y que todos los sistemas estén debidamente integrados con las demás soluciones y operativas.

La Aceptación Operativa será realizada mediante acta firmada entre el Gerente del Proyecto del Comprador y el Jefe de proyectos del Proveedor. Esta acta con toda la documentación que forma parte de la aceptación operativa, deberá ser presentada por el Proveedor en la mesa de partes del Comprador para el proceso de pago final.

4.9. Recursos y Servicios para entregar por el Comprador

El Comprador, dará todas las facilidades de acceso a la Central 911, los planos finales del sistema de cableado estructurado, centro de datos y demás soluciones tecnológicas que requiera el Proveedor para el cumplimiento del presente requerimiento.

4.10. Gestión de Activos

El Proveedor es responsable de todo lo suministrado en el presente requerimiento desde su adquisición, traslado a sus almacenes, traslado a la Central 911, todo el proceso de implementación, hasta la aceptación operativa final otorgada por el Gerente de Proyectos del Comprador.

Deberán considerar el etiquetado de todo el equipamiento a entregar, para lo cual cargará en el software de mesa de servicio todos los activos, donde se detalle, ubicación, área, usuarios, marca, modelo, # serie, entre otros datos de los bienes provistos por el Proveedor en este requerimiento.

4.11. Embalaje y/o Rotulado

El proveedor será responsable de que el embalaje, rotulado, identificación y documentación de los bienes objeto de la contratación sean adecuados, completos y suficientes para garantizar su correcta protección, identificación y control durante el transporte, almacenamiento y entrega.

El embalaje deberá ser nuevo y apropiado para equipos de TI. El rotulado deberá ser claro, legible e indeleble, colocado en el interior y exterior de los paquetes, e incluir como mínimo la identificación del proveedor, descripción del bien, cantidad, número de serie (cuando corresponda) y referencias del contrato y del Proyecto 911.

El incumplimiento de lo señalado será causal de observación, rechazo o no conformidad de los bienes, sin perjuicio de las acciones correctivas que correspondan, siendo de exclusiva responsabilidad del proveedor, sin generar costos adicionales para el Comprador.

4.12. Salud y Seguridad

El personal del Proveedor deberá tener SCTR en salud y pensión, desde el inicio de los trabajos, con los Equipos de Protección Personal (EPP) según el tipo de trabajo, para lo cual deberá de presentar su Plan de Seguridad, Salud y Trabajo en el Plan de Proyecto, con la matriz IPERC.

Previo a los trabajos en la Central 911, deberá recibir la charla de inducción respectiva. Este será dado por el Especialista SSOMA del Proveedor, quien lidera y coordina con sus pares del Contratista de la Obra, la Supervisión de la Obra y con el personal del Comprador.

4.13. Logistica y Control

Traslado y entrega

El Proveedor será plenamente responsable del traslado, transporte y entrega de los bienes objeto del contrato hasta el lugar de la Central 911, incluyendo las maniobras de carga, descarga, estibas necesarias e incluso el almacenaje con seguridad del Proveedor.

Seguro de Transporte
El Proveedor deberá contratar, bajo su exclusivo costo y responsabilidad, un seguro de transporte que cubra los bienes desde el punto de origen hasta su entrega final y conformidad, amparando los riesgos de pérdida, robo, daño, deterioro, siniestro, accidente u otros riesgos habituales durante el traslado o almacenaje.

Transporte y Almacenaje
Cualquier daño, pérdida o menoscabo que sufran los bienes durante el transporte, almacenaje, instalación hasta la aceptación operativa será responsabilidad exclusiva del Proveedor, quien deberá proceder a la reposición inmediata de los bienes afectados, sin costo adicional para el Comprador y sin perjuicio de la aplicación de las penalidades que correspondan.

4.14. Acreditación y Control de Acceso
El personal del Proveedor deberá estar debidamente identificado con su fotocheck y vestimenta con los logos que identifiquen al Proveedor, tanto en camisa, chalecos, polos y casco.

Para el acceso, el Proveedor deberá enviar una semana antes del inicio de sus actividades en la Central 911, la lista del personal adjuntado DNI y antecedentes penales.

4.15. Integraciones
El Proveedor en su plan de proyecto deberá incluir un acápite para las integraciones tecnológicas con las soluciones implementadas en la Central 911, para lo cual el Proveedor podrá solicitar las reuniones de coordinación y técnicas necesarias al Gerente de Proyectos del Comprador para que sean realizadas con el Contratista de la Obra, la Supervisión de la Obra y el resto de Los proveedores presentes en la Central 911.

Estas integraciones son:
- Integración entre la red LAN y Equipamiento Ofimático
- Integración entre la red LAN y el SAGE
- Integración entre la red LAN y el Centro de datos
- Integración entre la red LAN y los servicios de Telecomunicaciones
- Integración entre la red LAN y el Sistema TETRA

4.16. Entrenamiento Técnico
El Proveedor deberá presentar el plan de entrenamiento técnico para su aceptación operativa, el cual será realizado para 2 personas por cada solución que se lista a continuación: Switches, Red inalámbrica, Firewall, Hiperconvergencia, XDR, SIEM, SOAR, NDR, PAM y la Solución de respaldo.

El entrenamiento técnico será realizado en el primer semestre del soporte y garantía, y serán cursos oficiales a nivel fundamentos emitidos por cada fabricante propuesto. Siendo responsabilidad del Proveedor asumir todos los gastos como traslados, impuestos, y otros que se consideren para la correcta ejecución del entrenamiento técnico.

4.17. Lugar y Plazo de Entrega

Lugar:
La entrega de los equipos previo a la instalación será realizada en la Central 911, para lo cual el Proveedor deberá instalar un almacen con todas las condiciones físicas, ambientales y de seguridad para su posterior implementación, previa coordinación con el Gerente de Proyecto del Contrato.

El servicio se realizará en las instalaciones del Edificio de la Central 911 se ubica en la Avenida el Sol S/N, Distrito de Chorrillos, Provincia y departamento de Lima de forma presencial.

Plazo:
El plazo de entrega de bienes es de hasta 75 días calendarios contabilizados al día siguiente de la firma del Contrato.

El plazo para la implementación es de 90 días calendarios contabilizados al día siguiente de la firma del Contrato.

La garantía y soporte del Proveedor están indicados en el Anexo 3 del presente documento. Con relación a la mesa de servicio y SOC, estas inician con el soporte y garantía por un periodo de 12 meses, y estarán habilitados para garantizar la continuidad del Proyecto y su correcta transferencia al MININTER.

El entrenamiento se realizará dentro del primer semestre de año de garantía y soporte.

La puesta en Operación del servicio será posterior a la aceptación operativa y a través de un acta firmada entre el Jefe de Proyectos del Proveedor y el Gerente de Proyectos del Comprador en donde se establecerá la fecha de inicio para el Soporte y Garantía.

"Año de la Esperanza y el Fortalecimiento de la Democracia"

ANEXO 1 – CARACTERÍSTICAS TECNICAS

Equipamiento Ofimático

Estaciones de trabajo

1. Computadora de Escritorio Tipo 1 (210 Unidades)

Factor de forma	Mini
Sistema Operativo	Windows 11 LTSC
Procesador	Intel Core i7 de última generación
Memoria RAM	16GB DDR5 5600MHz
Tarjeta de Video	Dedicada PCIe de 4Gb DDR6 Compatible con DirectX 10.0 con 256 MB.
Unidad de Almacenamiento	500Gb PCIe M.2 SSD.
Bios	Instalado UEFI BIOS, de la misma marca del fabricante del equipo. -Precargado el número de serie de la computadora. -Herramienta de diagnóstico capaz de generar análisis de sistema y códigos de error. -Actualización del BIOS del equipo mediante descarga de software de la WEB del fabricante
Puertos	3x HDMI y/o MiniHDMI (con sus adaptadores) y/o 3x Displayport y/o 3x MiniDP 6x USB SuperSpeed Tipo A 10Gbps. 1x USB 3.2, 1x USB-C.
Audio	Integrado de Alta Definición soporta múltiple transmisión. 1x mini-jack universal de 3.5mm.
Conectividad	2x puertos de red RJ45, 10/100/1000 Mbps.
Certificación	Energy Star.
Fuente de Alimentación	CA 120/230 V (50/60 HZ). Estándar de 200 Watts certificada.

2. Computadora de Escritorio Tipo 2 (71 Unidades)

Factor de forma	Mini / SFF
Sistema Operativo	Windows 11 Profesional de 64 bits OEM
Procesador	Intel Core i7 de última generación
Memoria RAM	16Gb. DDR5 5600MHz
Unidad de Almacenamiento	500Gb PCIe M.2 SSD.
Bios	Instalado UEFI BIOS, de la misma marca del fabricante del equipo. -Precargado el número de serie de la computadora. -Herramienta de diagnóstico capaz de generar análisis de sistema y códigos de error. -Actualización del BIOS del equipo mediante descarga de software de la WEB del fabricante
Puertos	1 x HDMI 1 x DisplayPort 1.4 integrado 4 x USB-A de 5Gbps delanteros 4 x USB-A de 5Gbps traseros

	2 x Ethernet 1GbE RJ-45 1 x USB-C
Audio	Integrado de Alta Definición soporta múltiple transmisión. 1x mini-jack universal de 3.5mm.
Conectividad	2x puertos de red RJ45, 10/100/1000 Mbps. Wi-Fi integrada. Bluetooth 5.0.
Ofimática	Office LTSC 2024
Certificación	Energy Star
Fuente de Alimentación	Estándar de 200 Watts certificada.

3. Monitor para Computadoras (696 Unidades)

Tamaño	23-24 pulgadas
Tipo:	LED
Resolución	1920x1080p
Tipo de Panel	TN
Tiempo de Respuesta	<5 ms
Brillo	250 cd/m2
Interfaz	HDMI y/o Displayport
Fuente de Alimentación	CA 120/230 V (50/60 HZ).
Certificación	Energy Star

4. Teclado y Mouse (281 Unidades)

Teclado	Alámbrico en español.
Mouse	Alámbrico tres botones Sensor óptico Ambidiestro y/o Ergonómico
Conexión	USB
Compatible	Windows 11 professional

5. Soporte para 03 Monitores para Computadoras de Escritorio Tipo 1 (210 Unidades)

Compatibilidad	De 13 a 24 pulgadas.
VESA compatible	75x75, 100x100mm
Carga	7 kg (Por pantalla)
Giro	+90°~-90°
Inclinación	+45°~-45°
Rotación	+180°~-180°
Extensión del Brazo	658mm
Altura del Poste	443mm
Material	Acero, plástico.
Color	Negro
Gestión de cables	SI
Cantidad de Monitores	03 por soporte. Los monitores a soportar son los que se proveerán en el numeral 1.3 de este Anexo.

6. Equipo Portátil (09 Unidades)

Procesador	Intel Core I9 (Décimo cuarta generación) y/o su equivalente en AMD
Memoria RAM	16GB.
Almacenamiento	Disco SSD 512 GB
Pantalla	LCD retroiluminación LED, HD de 14".
Puertos	USB, HDMI, RJ45/Ethernet, Audio y Micrófono 3.5mm
Teclado	En español.
Multimedia	Cámara WEB HD, Micrófono integrado, altavoces.
Conectividad	Wifi, 10/100/1000 Mbps.
Fuente de alimentación	Adaptador de alimentación de 220V.
Software	Windows 11 professional (64bits en español). Office 2024.

Perifericos Especializados

7. Auricular Monoaural (210 Unidades)

Tipo de conexión	USB (audio y alimentación)
Material almohadillas	Cuero Sintético y/o similar
Micrófono	Omnidireccional, 35 Hz a 21 kHz Sensibilidad -40 ± 3dB
Parlante	< 6 mm, 20Hz a 20 KHz
Tasa señal / ruido	> 50dB
Peso	< 55 gramos
Longitud de Cable	> 2 metros

8. Micrófono (115 Unidades)

Tipo de Micrófono	Cuello de ganso flexible
Tipo de Conexión	USB (audio y alimentación)
Frecuencia	150 - 12500 Hz a 48 KHz de tasa de muestreo
Distorsión Armónica	<5%
Cancelación de ruido	20dB de cancelación activa
Longitud de Cable	> 2 metros

9. Altavoces (115 Unidades)

Tipo de Conexión	USB 3 (audio y alimentación)
Respuesta en frecuencia	120 - 10300 Hz a 48 KHz de tasa de muestreo
Frecuencia	150 - 12500 Hz a 48 KHz de tasa de muestreo
Distorsión Armónica	<5%
Nivel de potencia de audio máxima	95 dB SPL a 50 cm (aproximadamente 10W)
Control de Volumen	Dedicado
Montaje	Opciones de montaje flexible
Longitud de cable	> 2 metros

10. PPT de pie (210 Unidades)

Tipo de Conexión	USB 3 (audio y alimentación)
Material	Hierro fundido pesado
Base	Antideslizante
Longitud de cable	> 3 metros
Homologación	*El sistema ha sido homologado con pedaleras Kinesis FS22AJ-JSB. Modelos adicionales deben ser validados*

	previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.
Control de Volumen	Dedicado
Montaje	Opciones de montaje flexible
Longitud de cable	> 2 metros

11. Cámara Web (281 Unidades)

Tipo de Conexión	USB 3 (audio y alimentación)
Resolución	1080p
Micrófono	Micrófono omnidireccional estéreo
Cable	1.15 m.

Teléfonos IP

12. Teléfonos IP Tipo 1 (201 Unidades)

Marca	Mitel
Modelo	6865i
Pantalla	LCD monocromática 3.4" (128×48) con retroiluminación
Teclas físicas	8 teclas programables con LED; 2 teclas de línea "hard" con LED
Red	Doble puerto Gigabit Ethernet (10/100/1000) con switch integrado (LAN + PC)
Auriculares	Soporte nativo DHSG/EHS para headset analógico
Alimentación	PoE IEEE 802.3af Clase 2 o adaptador de corriente
Capacidad de líneas (call lines)	Hasta 24 call lines con LED
Homologación	Compatibilidad con el modelo de la central telefónica MX-ONE y versión del sistema operativo 7.7.1.0.15. Modelos adicionales deben ser validados previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.

13. Teléfonos IP Tipo 2 (62 Unidades)

Marca	Mitel
Modelo	6920w
Protocolos	SIP y MiNet
Pantalla	LCD color 3.5" (QVGA, 320×240)
Líneas	Hasta 20 líneas
Teclas	18 teclas de función programables; 4 teclas contextuales
Wi-Fi	Dual band 802.11 a/b/g/n
Bluetooth	Bluetooth 5.2 (documentación reciente / quick reference)
Red	2× puertos Gigabit Ethernet (LAN + PC)
Audio	Altavoz full-duplex; "HD audio"; lista de códecs incluye G.711/G.729/G.722, etc.
Puertos / expansión	USB 2.0 host (500 mA); puerto "sidecar/expansion"
Seguridad / QoS	Voz cifrada; IEEE 802.1p/Q (VLAN/priority); IEEE 802.1X
Alimentación	PoE IEEE 802.3az (en este datasheet figura Clase 3) y soporte de fuente 48V
Homologación	Compatibilidad con el modelo de la central telefónica MX-ONE y versión del sistema operativo 7.7.1.0.15. Modelos adicionales deben ser validados previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.

14. Teléfonos IP Tipo 3 (16 Unidades)

Marca	Mitel
Modelo	6930t
Enfoque	Plásticos con tratamiento antimicrobiano
Protocolos	MiNet y SIP
Pantalla	4.3" color (480×272)
Líneas	Hasta 24 call lines
Teclas	Teclas programables + contextuales
Bluetooth	Bluetooth 4.1 (MobileLink)
Wi-Fi	No integrado
Red	2× puertos Gigabit Ethernet (LAN + PC)
Headset	USB + puerto analógico EHS/DHSG (y puerto modular 4-pin convertible)
USB host	USB 2.0 host (500 mA)
Alimentación	PoE Clase 2 + 48V local
Homologación	Compatibilidad con el modelo de la central telefónica MX-ONE y versión del sistema operativo 7.7.1.0.15. Modelos adicionales deben ser validados previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.

15. Teléfonos IP Tipo 4 (4 Unidades)

Marca	Mitel
Modelo	6940w
Pantalla	7" color touch (800×480)
Wi-Fi	Dual band 802.11 a/b/g/n
Bluetooth	Bluetooth 5.2
Líneas / teclas	Acceso mediante teclas programables "soft" a hasta 96 líneas (según plataforma)
Red	2× Gigabit Ethernet (LAN + PC)
USB	USB 2.0 host (500 mA)
QoS / Seguridad	QoS 802.1p/Q, 802.1X, voz cifrada
Alimentación	PoE Clase 3; soporte de fuente 48V. Ojo: si instalas DECT integrado y/o M695, requiere alimentación por adaptador 48V
Homologación	Compatibilidad con el modelo de la central telefónica MX-ONE y versión del sistema operativo 7.7.1.0.15. Modelos adicionales deben ser validados previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.

16. Botonera para teléfono IP 4 (1 Unidad)

Marca	Mitel
Modelo	Botonera
Pantalla del módulo	4.3" LCD color
Teclas	28 teclas programables × 3 páginas
Encadenamiento	Hasta 3 módulos enlazables
Compatibilidad	Soportado en 6920w / 6930w / 6940w
Alimentación	Se alimenta desde el teléfono, pero el fabricante recomienda/indica uso de adaptador de escritorio (no sólo PoE) para ciertos escenarios con accesorios
Homologación	Compatibilidad con el modelo de la central telefónica MX-ONE y versión del sistema operativo 7.7.1.0.15.

	Modelos adicionales deben ser validados previamente por el proveedor del sistema para garantizar compatibilidad y operatividad total del equipo.

17. Pantalla para Monitoreo (02 Unidades)

Pantalla:	Full HD (1920 x 1080) o superior.
Dimensiones:	55" diagonal o superior.
Tecnología:	IPS y/o D-LED o LCD
Vida útil:	50 mil horas o superior.
Entradas de video:	2 entradas DP 1.2, 2 entradas HDMI 2.0 o superior.
Salidas de video:	1 salida DP 1.2 o superior.
Puerto Ethernet:	Si
Wifi:	Si

18. Videoconferencia (04 Unidades)
Especificación técnica Sala 08 personas (01 Unidad)

Camara	• Resolución: 4K, 1440p, 1080p, 900p, 720p y SD a 30fps • Panorámica: Robotizada ±25° • Inclinación: Robotizada ±15° • Zoom: Zoom digital HD 4x • Campo visual diagonal: 120°, Campo visual horizontal: 113°, Campo visual vertical: 80.7° • Cobertura total de sala (campo visual + panorámica e inclinación): 163° horizontal x 110° vertical
Parlante Subwoofer	• Transductor: 70 mm • Sensibilidad: 92 dB SPL a 1 W, 99 dB SPL a 8.0 W, ambos +/-2 dB a 0.5 m • Potencia nominal: 8W • THD: 1 kHz < 2% a 1 W • Frecuencia de muestreo de bocina: 48 kHz • Impedancia: 4 ohmios
Parlante Altavoces	• Transductores: 2 de 43 mm • Sensibilidad: 84 dB SPL a 1 W/1 M • Potencia nominal: 4W • THD: 1 kHz < 2% a 1 W • Frecuencia de muestreo de bocina: 48 kHz • Impedancia: 4 ohmios
Micrófonos	• Respuesta de frecuencia: 90 Hz – 16 kHz • Sensibilidad: >-36 dBFS +/-1 dB a 1 Pa • Velocidad de salida de datos de micrófono: 48 kHz • Radio de captación: Hasta 7 m • Elementos de formación de haces: 6 micrófonos MEMS digitales omnidireccionales que forman 5 haces de difusión acústica adaptativa • Procesamiento de audio: AEC (Acoustic Echo Cancellation), VAD (Voice Activity Detector) • Supresión de ruido: Algoritmo de supresión de ruido basado en inteligencia artificial • Micrófonos adicionales: Admite hasta tres micrófonos adicionales

	• Visualización en cuadrícula: Detecta y encuadra a todos los participantes de la reunión para crear experiencias de reunión híbridas equitativas.
Interfaces	• Salida HDMI: 2 • Entrada HDMI: 1 • USB: 3 x Tipo A, 1x Tipo C • Red: Ethernet 10/100/1G • WiFi: 802.11a/b/g/n/ac • Entrada de micrófono externo: Sí • Control remoto: Bluetooth® Low Energy
Alimentación y cables	• Fuente de alimentación: Detección automática • Alimentación/Voltaje de servicio: 100-240 V, 19 V, 4,74 A • Cable de CC: 1,5 m, Cable de CA: 1 m, Cable HDMI 1.4: 2 m, Cable USB A a USB C 3.0: 2,2 m
Medioambiente	• Temperatura de funcionamiento: 0 °C a 40 °C • Temperatura de almacenamiento: -40 a 70°C • Humedad: 10 % a 95 % • BTU/h: 57 (en inactividad), 64 (durante reuniones)
Seguridad	• Cifrado de disco completo: AES-128 • Cifrado de datos: Claves simétricas, infraestructura de clave pública (PKI) • Identidad de dispositivos: Protección mediante atestación de estado de dispositivos • Acceso a dispositivos: Autenticación mediante API • Protección mediante clave: Arm TrustZone, RPMP
Accesorios	• Piezas de montaje: Pieza de montaje en pared para barras de video, pieza de montaje en TV para barras de video
Compatibilidad	• Sistemas operativos Windows 11 professional, macOS: 10.10 o posteriores y Chrome OS™ • El Proveedor debe garantizar la compatibilidad de todos sus accesorios y elementos que conforman la solución de videoconferencia para su correcta operación 24x7.
Pantalla	• LED 75" con sus accesorios a pared, y puerto red LAN / Wifi

Especificación técnica Sala 16 personas (02 Unidades):

Cámara	• Resolución: 4K, 1440p, 1080p, 900p, 720p y SD a 30fps • Panorámica: Robotizada ±25° • Inclinación: Robotizada ±15° • Zoom: Zoom 15X HD (óptico 5X y digital 3X) • Campo visual diagonal: 90°, Campo visual horizontal: 82,1°, Campo visual vertical: 52,2° • Cobertura total de sala (campo visual + panorámica e inclinación): 132,1° horizontal x 82,2° vertical
Altavoces	• Transductores: 2x 70 mm • Sensibilidad: 92 dB SPL a 1 W, 99 dB SPL a 8.0 W, ambos +/-2 dB a 0.5 m • Potencia nominal: 8W • THD: 1 kHz < 2% a 1 W • Frecuencia de muestreo de bocina: 48 kHz • Impedancia: 4 ohmios

Micrófonos	• Respuesta de frecuencia: 90 Hz - 16 kHz • Sensibilidad: >-36 dBFS +/-1 dB a 1 Pa • Velocidad de salida de datos de micrófono: 48 kHz • Radio de captación: Hasta 7 m • Elementos de formación de haces: 6 micrófonos MEMS digitales omnidireccionales que forman 5 haces de difusión acústica adaptativa • Procesamiento de audio: AEC (Acoustic Echo Cancellation), VAD (Voice Activity Detector) • Supresión de ruido: Algoritmo de supresión de ruido basado en inteligencia artificial • Micrófonos adicionales: Admite hasta cuatro micrófonos adicionales
Interfaces	• Salida HDMI: 2 • Entrada HDMI: 1 • USB: 3 x Tipo A, 1x Tipo C • Red: Ethernet 10/100/1G • WiFi: 802.11a/b/g/n/ac • Entrada de micrófono externo: Sí • Control remoto: Bluetooth® Low Energy
Alimentación y cables	• Fuente de alimentación: Detección automática • Alimentación/Voltaje de servicio: 100-240 V, 19 V, 4,74 A • Cable de CC: 1,5 m, Cable de CA: 1 m, Cable HDMI 1.4: 2 m, Cable USB A a USB C 3.0: 2,2 m
Medioambiente	• Temperatura de funcionamiento: 0 °C a 40 °C • Temperatura de almacenamiento: -40 a 70°C • Humedad: 10 % a 95 % • BTU/h: 57 (en inactividad), 64 (durante reuniones)
Seguridad	• Cifrado de disco completo: AES-128 • Cifrado de datos: Claves simétricas, infraestructura de clave pública (PKI) • Identidad de dispositivos: Protección mediante atestación de estado de dispositivos • Acceso a dispositivos: Autenticación mediante API • Protección mediante clave: Arm TrustZone, RPMP
Accesorios	• Pieza de montaje en pared para barras de video, pieza de montaje en TV para barras de video
Compatibilidad	• Sistemas operativos Windows 11 professional, macOS: 10.10 o posteriores y Chrome OS™. • El Proveedor debe garantizar la compatibilidad de todos sus accesorios y elementos que conforman la solución de videoconferencia para su correcta operación 24x7.
Pantalla	• LED 86" con sus accesorios a pared, y puerto red LAN / Wifi

Especificación técnica Sala 30 personas (01 Unidad):

Camara	• Zoom: - Zoom 15x HD (óptico 5x + digital 3x) • Panorámica: 180° (±90°) • Inclinación: 140° (+50° / -90°) • Campo visual • Diagonal: 90°

	• Horizontal: 82° • Vertical: 52° • Cobertura total de sala: 262° ancho x 192° alto (campo visual + panorámica e inclinación) Resoluciones @ 30fps: 4K Ultra HD, 1440p, 1080p, 900p, 720p, y SD Resoluciones @ 60fps: 1080p, 720p • Rango dinámico amplio (WDR), compensación de poca luz, reducción de ruido de video, optimización de saturación con poca luz • Privacidad: En modo de suspensión, la lente permanece en ángulo de -90° para garantizar la privacidad
Parlante	• Transductor de 76 mm de alto desempeño con imán de tierras raras • El sistema de suspensión pendiente de patente elimina el temblor de la cámara por vibración y las interferencias de audio • El cable Mini XLR se conecta al controlador de pantalla para proporcionar señal y alimentación • Volumen de bocina: 95 dB SPL a 1 W, 100 dB SPL a 7,5 W, ambos +/-2 dB a ½ metro • Sensibilidad: 95+/-2 dB SPL a ½ metro • Distorsión: 200 Hz–300 Hz <2,5%, 300 Hz– 10 kHz <1% a 7,5 W • Frecuencia de muestreo: 48 kHz
Micrófonos	• Radio de captación: 7 m de diámetro • Cuatro micrófonos omnidireccionales forman ocho haces acústicos • AEC: Cancelación de eco acústico • VAD: Voice Activity Detector (VAD), Supresión de ruido de fondo, Botón de silencio con LED indicador de estado, Cable cautivo de 12 patillas y 2,95 m, Conexión en serie de hasta 7 bases de micrófono • Respuesta de frecuencia: 90 Hz – 16 kHz • Sensibilidad: >-27 dB +/-1 dB a 1 Pa • Velocidad de datos de micrófono: 48 kHz
Interfaces	• Salida HDMI: 2 • Entrada HDMI: 1 • USB: 3 x Tipo A, 1x Tipo C • Red: Ethernet 10/100/1G • WiFi: 802.11a/b/g/n/ac • Entrada de micrófono externo: Sí • Control remoto: Bluetooth® Low Energy
Alimentación y cables	• USB 3.1 Tipo C a USB 3.1 Tipo C (2 m) • Computadora de sala de conferencias a controlador de pantalla o de sobremesa • USB 3.1 Tipo A a USB Tipo B (2 m)
Controlador de sobremesa	• Conexión de cable CAT6A individual • Detección de hablante activo: analiza cada 8 ms el audio de hasta 7 bases de micrófono y 56 haces • Conector de 12 patillas para base de micrófono • Paso de HDMI Tipo A a controlador de pantalla (x2) • Debe tener interfaz USB Tipo C, USB Tipo A, USB Tipo B y RJ45

Controlador de pantalla	• HDMI Tipo A: (x2) (conexión a pantallas), USB C (conexión a cámara), USB Tipo B (conexión a computadora de sala de reuniones) • Debe tener interfaz RJ45 y Mini XLR que alimenta una o dos bocinas
Accesorios	• Pieza de montaje en pared para barras de video, pieza de montaje en TV para barras de video
Compatibilidad	• Sistemas operativos Windows 11 professional, macOS: 10.10 o posteriores y Chrome OS™ • El Proveedor debe garantizar la compatibilidad de todos sus accesorios y elementos que conforman la solución de videoconferencia para su correcta operación 24x7.

19. Impresora tipo personal (13 Unidades)

Funciones Principales	Copia, impresión y escáner de red
Velocidad	40ppm
Tecnología de Impresión	Láser monocromático (blanco y negro)
Resolución de Impresión	1200 x 1200 ppp
Velocidad de escaneo	40 ipm
Tamaño de papel	Hasta A4
Memoria RAM	Hasta 512 MB
Tipo de escaneo y copia	Cama plana y alimentadora de documentos (adf)
Sistemas operativos soportados	Windows 10, Windows 11 en todas sus versiones
Conectividad	USB 2.0.
	LAN, WIFI
Impresión a doble cara	Automática (estándar)
Ciclo mensual de trabajo	Hasta 10 000
Voltaje de operación	220 V / 50/60 Hz.

20. Impresora tipo mediano volumen (05 Unidades)

Funciones Principales	Copia, impresión y escáner de red
Velocidad	Desde 50ppm
Tecnología de Impresión	Láser monocromático (blanco y negro)
Resolución de Impresión	1200 x 1200 ppp
Tamaño de papel	Hasta A4
Memoria RAM	2 GB
Tipo de escaneo y copia	Cama plana y alimentadora de documentos (adf)
Sistemas operativos soportados	Windows 10, Windows 11 en todas sus versiones
Conectividad	USB 2.0.
	LAN, WIFI
Impresión a doble cara	Automática (estándar)
Voltaje de operación	220 V / 50/60 Hz.

21. Proyector Multimedia (04 Unidades)

Proyector Multimedia	• Tecnología de proyección: Fuente de luz láser de estado sólido, basada en tecnología 3LCD, LCD, DLP o equivalente. • Resolución nativa mínima: WUXGA (1920 x 1200 píxeles). • Brillo mínimo: 7,000 lúmenes ANSI o ISO. • Relación de aspecto nativa: 16:10. • Compatibilidad con formatos 16:9 y Full HD. • Contraste dinámico mínimo: 2,500,000:1. • Vida útil de la fuente de luz: mínimo 20,000 horas. • Zoom óptico mínimo: 1.6x. • Lens Shift horizontal y vertical. • Corrección trapezoid • al horizontal y vertical. • Tamaño de imagen compatible con pantallas de 150 pulgadas o superiores. • Entradas mínimas: dos (02) HDMI, un (01) USB y un (01) puerto RJ45. • Administración y monitoreo mediante red. • Nivel de ruido máximo: 38 dB. • Alimentación eléctrica: 220 VCA, 60 Hz. • Instalación fija en techo mediante soporte metálico.
Ecran Motorizado	• Tipo: Pantalla de proyección motorizada eléctrica. • Formato: 16:9. • Tamaño mínimo: 150 pulgadas diagonales. • Área útil mínima de proyección: 3.30 m x 1.85 m. • Material de proyección: Tela blanca mate (Matte White) o equivalente. • Ganancia mínima: 1.0. • Ángulo de visión mínimo: 160°. • Bordes negros perimetrales. • Operación mediante motor eléctrico integrado. • Accionamiento mediante interruptor de pared. • Carcasa metálica de alta resistencia. • Instalación en techo o pared. • Operación silenciosa. • Tela resistente a deformaciones, arrugas y humedad.
Sistema de Distribución Audiovisual	• Matriz audiovisual digital profesional de cuatro (04) entradas por cuatro (04) salidas como mínimo. • Entradas mínimas: cuatro (04) puertos HDMI. • Salidas mínimas: cuatro (04) salidas HDBaseT o equivalente, pudiendo incluir salidas HDMI locales. • Resolución soportada mínima: 4K UHD. • Compatibilidad HDCP. • Capacidad de conmutación, distribución y replicación simultánea de una misma señal audiovisual hacia los proyectores instalados. • Capacidad de operación independiente por sala o en modo combinado para los tres ambientes. • Administración mediante panel frontal, interfaz web, red IP, RS-232 o equivalente. • Instalación en rack estándar de 19 pulgadas. • Transmisión de video, audio y señales de control mediante cableado estructurado categoría 6A o superior.

	• Deberá incluir receptores HDBaseT o interfaces equivalentes cuando los proyectores no cuenten con entrada HDBaseT integrada. • Deberá permitir la conexión de fuentes audiovisuales como computadoras portátiles, computadoras de sala, sistemas de videoconferencia, reproductores multimedia u otros equipos similares.
Accesorios	• Soportes de techo para proyectores. • Pantallas motorizadas. • Matriz audiovisual. • Receptores HDBaseT o interfaces equivalentes cuando sean requeridos por la solución propuesta. • Cableado de energía, señal y control. • Accesorios de fijación y montaje.

22. Tabletas Rugerizadas (37 Unidades)

Pantalla	Tamaño: 10" a 12". Resolución: >= 1920 x 1200.
Procesador / GPU	(Octa-core) o superior.
Memoria RAM	6 GB.
Almacenamiento	128 GB.
Conectividad	Wi-Fi 6, Bluetooth >= 5.0. 4G LTE + Nano-SIM y/o eSIM
Puertos	USB Type-C para carga y transferencia de datos.
Cámaras	Frontal >= 5 MP. Posterior >= 12 MP.
Audio	Altavoces estéreo. Micrófonos integrados para videollamadas.
Batería	Capacidad típica 7,000 mAh.
Sistema operativo	Android 11 o superior
Seguridad	Bloqueo biométrico (huella o reconocimiento facial). Cifrado del dispositivo.
Accesorios	Cargador (o fuente) y cable. Funda protectora.

Red LAN

Switching
23. Switches Spine Data Center (02 Unidades)

Características de Hardware	- Debe contar con 32 puertos QSFP28 (con capacidad de conectar transceivers a 40 ó 100 Gbps). - Factor de forma: Una unidad de rack. - Un (1) Puerto USB (USB-A o USB 2.0 o USB similar) para gestión de archivos. - Un (1) puerto de gestión fuera de banda RJ45. - Administración por Consola RJ-45 o USB-C. - Memoria RAM: Mínimo 16GB. - Memoria Flash o SSD: Mínimo 64GB. - Debe contar con fuentes de poder redundantes removibles en caliente y en la máxima configuración disponible tanto en cantidad de fuentes y de potencia de cada fuente. - Ventiladores redundantes. Mínimo 4 bandejas removibles en caliente. Flujo de aire Front-to-Back. - Se deberá incluir ocho (08) transceivers ópticos 100GE-SR4 con conectores LC en cada uno de los switches propuestos.
Capacidades de Procesamiento	- Buffer no menor a 32MB. - Capacidad de conmutación no menor a 6.4 Tbps. - Capacidad de reenvío de paquetes no menor a 2 Bpps. - Capacidad de tabla de direcciones MAC no menor a 90K. - Capacidad de rutas IPv4 mínima de 130K y rutas IPv6 de 30K.
Características del Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecientes al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso de APIs de tipo REST o similar. - Debe permitir el apilamiento de dos switches mediante la tecnología MC-LAG o similar manteniendo planos de control separados de modo que se maximice la alta disponibilidad del servicio. Estos dos switches apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. - Debe contar con una consola de configuración por la línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI ó web UI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la Consola Gráfica de Administración Integrada	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Deberá mostrar de manera gráfica el equipo, visualizando la distribución de puertos y el factor de forma.
Funcionalidades de Capa 2, Capa	- Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q)

3, de Seguridad y Gestión	- Spanning Tree (802.1w, 802.1s y 802.1d). - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad). - IEEE 802.1ab LLDP. - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping. - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP. - VXLAN estática. - VXLAN dinámica mediante BGP-EVPN. - Protocolos de enrutamiento: PBR, VRRP, RIPv2, RIPng, OSPFv2 y v3, BGP4 y MP-BGP. - BFD y ECMP. - DCBx, PFC, ETS, ECN. - VRF. - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP server para IPv4 e IPv6 y DNS. - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Soporte de "port mirroring" por puerto o grupo de puertos. - Jumbo Frames de al menos 9K bytes.

24. Switches Leaf Data Center (08 unidades)

Características de hardware	- Debe contar con 48 puertos SFP28 (con capacidad de conectar transceiver a 1, 10 ó 25 Gbps) y 6 puertos QSFP28 (con capacidad de conectar transceiver a 40 ó 100 Gbps) - Factor de forma: Una unidad de rack - Un (1) Puerto USB (USB-A o USB 2.0, etc). - Un (1) puerto de gestión fuera de banda RJ45 - Administración por Consola RJ-45 o USB-C. - Memoria RAM: Mínimo 32GB - Memoria Flash o SSD: Mínimo 64GB - Debe contar con fuentes de poder redundantes removibles en caliente y en la máxima configuración disponible tanto en cantidad de fuentes y de potencia de cada fuente. - Ventiladores redundantes. Mínimo 5 bandejas removibles en caliente. Flujo de aire Front-to-Back. - Se deberá incluir dieciséis (16) transceivers ópticos 100GE-SR4 con conectores LC a ser distribuidos entre los switches solicitados. - Se deberá incluir treinta y cuatro (34) transceivers ópticos 25GE-SR con conectores LC a ser distribuidos entre los switches solicitados. - Se deberá incluir cuatro (04) transceivers ópticos 10GE-SR con conectores LC a ser distribuidos entre los switches solicitados.

	- Se deberá incluir doce (12) transceivers 1000Base-T con conector RJ-45 a ser distribuidos entre los switches solicitados. - Se deberá incluir un (01) cable de apilamiento a 100 Gbps por cada switch para virtualizar/apilar los switches solicitados.
Capacidades de procesamiento	- Buffer no menor a 32 MB. - Capacidad de conmutación no menor a 3.6 Tbps. - Capacidad de reenvío de paquetes no menor a 2 Bpps. - Capacidad de tabla de direcciones MAC no menor a 98 K - Capacidad de rutas IPv4 mínima de 130 K y rutas IPv6 de 30 K.
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso APIs del tipo REST o similar. - Debe permitir el apilamiento de dos switches mediante la tecnología MC-LAG o similar manteniendo planos de control y enrutamiento separados de modo que se maximice la alta disponibilidad del servicio. Estos dos switches deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. - Soporte del balanceo de servidores de aplicaciones mediante Microsoft Network Load Balancer (NLB). - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola externa de administración de políticas	- La plataforma podrá estar compuesta por más de un software del mismo fabricante y en conjunto deberá como mínimo: ▪ Basarse en appliance físico o virtual. En caso de ser virtual, se deberá considerar todo el componente de hardware y software necesario para el funcionamiento de la herramienta. ▪ Debe incluir APIs que permita el desarrollo de futuras integraciones. ▪ Debe brindar visibilidad de los hosts conectados, máquinas virtuales, VLANs, servicios y cargas de trabajo ▪ Debe proveer una orquestación unificada para segmentación, seguridad y configuración de políticas ▪ Debe dar visibilidad sobre la red física y las cargas de trabajo que la utilizan ▪ Debe realizar optimización de las rutas de datos creando políticas de optimización de red para satisfacer las necesidades de las cargas de trabajo de aplicaciones críticas ▪ Debe permitir visualizar el estado de salud de los switches ▪ Permitir el descubrimiento de dispositivos de red
Funcionalidades de Capa 2, Capa 3, de seguridad y gestión	- Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d). - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad). - IEEE 802.1ab LLDP. - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping. - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP.

	- VXLAN estática. - VXLAN dinámica mediante BGP-EVPN. - Protocolos de enrutamiento: PBR, VRRP, RIPv2, RIPng, OSPFv2 y v3, BGP4 y MP-BGP. - BFD y ECMP. - DCBx, PFC, ETS, ECN. - VRF - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. No se aceptarán protocolos similares y/o propietarios. - Incluir TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos - Jumbo Frames de al menos 9K bytes

25. Solución de Orquestador DC (01 Unidad)

Características Generales	- La solución de orquestación debe ser definida por software y basada en APIs de modo que simplifique y acelere el aprovisionamiento de redes, la gestión de la seguridad y las operaciones diarias en infraestructura de red de Centros de Datos. - La solución deberá contar con la capacidad de orquestar los switches de Data Center spine y leaf ofertados como un único fabric, simplificando las operaciones y la resolución de problemas en infraestructura de red de Centros de Datos. - La solución deberá implementarse en alta disponibilidad.
Arquitectura y Capacidades Principales	- Debe permitir la definición y creación de topologías de centro de datos mediante software. - Debe permitir la automatización de las configuraciones VXLAN entre varias sedes. - Debe permitir la gestión unificada de múltiples fabrics a través de ubicaciones geográficas. - Debe permitir la visualización integral de mallas, VLANs, hosts, MVs y seguridad. - Debe contar con un mapa en tiempo real auto-documentado del entorno de red. - Debe brindar visibilidad integral, desde las MVs hasta los puertos físicos de switch. - Debe contar con una interfaz gráfica que permita señalar y hace clicks, para eliminar complejidades en su uso. - Debe contar con configuración asistida o guiada para implementaciones complejas. - Debe contar con asistentes intuitivos que permitan la automatización de EVPN.

	- Debe contar con APIs RESTful para integración con sistemas de orquestación de terceros y otros repositorios. - La solución deberá ser capaz de aprovisionar, configurar y optimizar la red propuesta en tiempo real, respondiendo a eventos de sistemas de terceros sin intervención manual.
Funcionalidades de Orquestación	- Debe permitir la configuración de virtualización/stacking de switches Leaf del DC. - Debe permitir la implementación de topologías Leaf and Spine en el DC. - Debe permitir la configuración de redes subyacentes (underlay) basadas en al menos BGP/OSPF u otros protocolos similares no propietarios. - Debe permitir la configuración de redes superpuestas (overlay) basadas en al menos BGP EVPN u otros protocolos similares no propietarios. - Debe permitir la gestión de la agregación de enlaces y de grupos VLANs. - Debe permitir la gestión de VRFs y EVPN - Debe permitir la gestión del firmware de los switches de DC.
Capacidades de Integración	- La solución debe ser compatible con los siguientes sistemas: SimpliVity, VMware vSphere, ESX, NSX, VSAN, Nutanix Prism y las soluciones de gestión del fabricante propuesto. - Debe permitir el descubrimiento y visualización de infraestructura virtual. - Debe permitir la respuesta automática a eventos del ciclo de vida de MVs. - Debe permitir la creación de políticas basadas en etiquetas de vSphere o nombres de MV.
Vistas Disponibles	- Debe contar con una "Vista de Host" que permita visualizar la conectividad integral desde MVs hasta NIC físicos. - Debe contar con una "Vista de Red" que permita visualizar la conectividad Spine and Leaf y la de los conmutadores virtuales.
Capacidades de Monitoreo	- Debe contar con capacidad de análisis de red para un monitoreo amplio de problemas. - Debe permitir el monitoreo de alertas de estado de hardware, CPU/memoria, transceptores. - Debe permitir la recolección de alertas syslog. - Debe permitir la gestión de telemetría continua/integral/distribuida/pervasiva para resolución de problemas.

26. Switch Core LAN Campus (02 Unidades)

Características de hardware	- Debe contar con 32 puertos SFP28 (con capacidad de conectar transceiver a 1, 10 ó 25 Gbps) y 4 puertos QSFP28 (con capacidad de conectar transceiver a 40 ó 100 Gbps). - Factor de forma: Una unidad de rack - Un (1) Puerto USB (USB-A o USB 2.0 o USB similar) para gestión de archivos. - Un (1) puerto de gestión fuera de banda RJ45 - Administración por Consola RJ-45 o USB-C. - Memoria RAM: Mínimo 16GB - Memoria Flash o SSD: Mínimo 32GB - Debe contar con fuentes de poder redundantes removibles en caliente y en la máxima configuración disponible tanto en cantidad de fuentes y de potencia de cada fuente. - Bandeja de ventiladores redundantes (mínimo 3 bandejas) removibles en caliente. Flujo de aire Front-to-Back. - Se deberá incluir un (01) transceiver óptico 25GE-SR con conectores LC en cada uno de los switches solicitados - Se deberá incluir ocho (08) transceivers ópticos 10GE-LR con conectores LC en cada uno de los switches solicitados. - Se deberá incluir cuatro (04) transceivers ópticos 10GE-SR con conectores LC en cada uno de los switches solicitados.

	- Se deberá incluir dos (02) transceivers ópticos 1000Base-T con conectores RJ-45 en cada uno de los switches solicitados. - Se deberá incluir un (01) cable de apilamiento a 100Gbps por cada switch para virtualizar/apilar los switches solicitados.
Capacidades de procesamiento	- Buffer no menor a 32MB - Capacidad de conmutación no menor a 2.4Tbps - Capacidad de reenvío de paquetes no menor a 1.7Bpps - Capacidad de tabla de direcciones MAC no menor a 80k - Capacidad de rutas IPv4 mínima de 130k y rutas IPv6 de 30k
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecientes al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso de APIs de tipo REST o similar. - Debe permitir el apilamiento de dos switches mediante la tecnología MC-LAG o similar manteniendo planos de control separados de modo que se maximice la alta disponibilidad del servicio. Estos dos switches apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI ó web UI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola grafica de administración integrada	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Deberá mostrar de manera gráfica el equipo, indicando la distribución de puertos y el factor de forma.
Funcionalidades requeridas de Capa 2, Capa 3, de seguridad y gestión	- Capacidad de asignar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d). - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad). - IEEE 802.1ab LLDP. - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping. - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP. - VXLAN estática. - VXLAN dinámica mediante BGP-EVPN. - Protocolos de enrutamiento: PBR, VRRP, RIPv2, RIPng, OSPFv2 y v3, BGP4 y MP-BGP. - BFD y ECMP.. - DCBx, PFC, ETS, ECN. - VRF. - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS.

	- Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos - Jumbo Frames de al menos 9K bytes

27. Switch de acceso 48 puertos PoE (22 Unidades + 01 unidad en spare)

Características de hardware	- El switch debe contar con 48 puertos RJ45 10/100/1000 Base-T con soporte de PoE 802.3at Clase 4 y 04 puertos de uplink SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps). - El switch debe contar con una capacidad PoE disponible ("PoE Budget") de 740W de modo que cualquiera de los 48 puertos RJ45 10/100/1000 Base-T pueda brindar hasta 30 W de potencia PSE mientras no se agote dicha capacidad PoE. - El switch debe contar con dicha capacidad PoE disponible ("PoE Budget") de 740W bajo cualquier situación de falla de una de las dos (02) fuentes de energía solicitadas. - Factor de forma: una (01) unidad de rack (RU: Rack Unit). - El switch debe contar con ASIC del mismo fabricante. - Un (01) puerto auxiliar USB (USB-A o USB 2.0 o similar). - Un (01) puerto de gestión fuera de banda 10/100/1000 RJ-45. - Administración por Consola RJ-45 o USB-C. - Capacidad de mantener el flujo de energización por los puertos Ethernet a los dispositivos cliente (Ej. Teléfono IP, cámaras IP, access point, etc.) incluso durante el proceso de reinicio del switch (PoE permanente). - Memoria RAM: Mínimo 8 GB. - Memoria Flash o SSD: Mínimo 8 GB. - Fuentes de poder reduntantes intercambiables en caliente (incluir fuente redundante). - Bandejas/Módulos de ventiladores redundantes, al menos dos, intercambiables en caliente. - Se deberá incluir once (11) transceivers ópticos 10GE-LR con conectores LC a ser distribuidos entre los switches solicitados. - Se deberá incluir dieciocho (18) cables de apilamiento de 1m de longitud a 10 Gbps a ser distribuidos entre los switches solicitados. - Se deberá incluir cuatro (04) cables de apilamiento de 3m de longitud a 10 Gbps a ser distribuidos entre los switches solicitados.
Capacidades de procesamiento	- Capacidad de reenvío no menor a 130 Mpps. - Capacidad de switching no menor a 176 Gbps. - Buffer mínimo de 6 MB. - Capacidad de tabla de direcciones MAC no menor a 32K. - Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K.
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecientes al mismo fabricante. El Motor de Analítica debe

	incluir monitoreo y diagnósticos avanzados mediante el uso de APIs de tipo REST o similar. - Debe permitir el apilamiento o stack clásico de hasta 8 switches de la misma familia. Se permitirá el uso de back plane stacking o de máximo dos de los puertos de uplink solicitados. Estos switches en stack o apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. Se debe incluir el hardware necesario para realizar el apilamiento o stack. - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola grafica de administración integrada	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Revisión del estado del PoE (cuando aplique), estatus, prioridad y uso por puerto. - Deberá mostrar de manera gráfica el equipo, indicando la distribución de puertos y el factor de forma. - Mostrar información de los dispositivos conectados al equipo. Se aceptará una consola de gestión externa licenciada con su respectivo hardware para cubrir dicho requerimiento.
Funcionalidades requeridas Capa 2, Capa 3, de seguridad y gestión	- Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d). - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad).. - IEEE 802.1ab LLDP. - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping. - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP. - Protocolos de enrutamiento: RIPv2, RIPng, OSPFv2 y v3. - VXLAN estática. - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS. - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - Control de acceso centralizado por RADIUS, para los usuarios de la red que se autentican vía 802.1x. - RADIUS y RADIUS CoA. - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo.

	- Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN. - Jumbo Frames de al menos 9K bytes.

28. Switch de acceso 24 puertos PoE (04 Unidades)

Características de hardware	- El switch debe contar con 24 puertos RJ45 10/100/1000 Base-T con soporte de PoE 802.3at Clase 4 y 04 puertos de uplink SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps). - El switch debe contar con una capacidad PoE disponible ("PoE Budget") de 740W de modo que cualquiera de los 24 puertos RJ45 10/100/1000 Base-T pueda brindar hasta 30 W de potencia PSE mientras no se agote dicha capacidad PoE. - El switch debe contar con dicha capacidad PoE disponible ("PoE Budget") de 740W bajo cualquier situación de falla de una de las dos (02) fuentes de energía solicitadas. - Factor de forma: una (01) unidad de rack (RU: Rack Unit). - El switch debe contar con ASIC del mismo fabricante. - Un (01) puerto auxiliar USB (USB-A o USB 2.0 o similar). - Un (01) puerto de gestión fuera de banda 10/100/1000 RJ-45. - Administración por Consola RJ-45 o USB-C. - Capacidad de mantener el flujo de energización por los puertos Ethernet a los dispositivos cliente (Ej. Teléfono IP, cámaras IP, access point, etc.) incluso durante el proceso de reinicio del switch (PoE permanente). - Memoria RAM: Mínimo 8 GB. - Memoria Flash o SSD: Mínimo 8 GB. - Fuentes de poder reduntantes intercambiables en caliente (incluir fuente redundante). - Bandejas/Módulos de ventiladores redundantes, al menos dos, intercambiables en caliente. - Se deberá incluir cinco (05) transceivers ópticos 10GE-LR con conectores LC a ser distribuidos entre los switches solicitados. - Se deberá incluir cuatro (04) cables de apilamiento de 3m de longitud a 10 Gbps a ser distribuidos entre los switches solicitados.
Capacidades de procesamiento	- Capacidad de reenvío no menor a 95 Mpps. - Capacidad de switching no menor a 128 Gbps. - Buffer mínimo de 6 MB. - Capacidad de tabla de direcciones MAC no menor a 32K. - Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K.
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecientes al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso de APIs de tipo REST o similar. - Debe permitir el apilamiento o stack clásico de hasta 8 switches de la misma familia. Se permitirá el uso de back plane stacking o de máximo dos de los puertos de uplink solicitados. Estos switches en stack o apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. Se debe incluir el hardware necesario para realizar el apilamiento o stack. - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola grafica	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el

de administración integrada	estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Revisión del estado del PoE (cuando aplique), estatus, prioridad y uso por puerto. - Deberá mostrar de manera gráfica el equipo, indicando la distribución de puertos y el factor de forma. - Mostrar información de los dispositivos conectados al equipo. Se aceptará una consola de gestión externa licenciada con su respectivo hardware para cubrir dicho requerimiento.
Funcionalidades requeridas Capa 2, Capa 3, de seguridad y gestión	- Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d). - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad). - IEEE 802.1ab LLDP. - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping. - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP. - Protocolos de enrutamiento: RIPv2, RIPng, OSPFv2 y v3. - VXLAN estática. - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS. - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - Control de acceso centralizado por RADIUS, para los usuarios de la red que se autentican vía 802.1x. - RADIUS y RADIUS CoA. - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN. - Jumbo Frames de al menos 9K bytes. -

29. Switch DMZ (02 Unidades)

Características de hardware	- Debe contar con 24 puertos SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps) y 04 puertos SFP56 (con capacidad de conectar transceivers a 1, 10, 25 ó 50 Gbps). - Factor de forma: Una unidad de rack - El switch debe contar con ASIC del mismo fabricante. - Un (01) Puerto USB (USB-A o USB 2.0 o similar).

	- Un (01) puerto de gestión fuera de banda RJ45. - Administración por Consola RJ-45 o USB-C. - Memoria RAM: Mínimo 8GB - Memoria Flash o SSD: Mínimo 32GB - Debe contar con fuentes de poder redundantes removibles en caliente y en la máxima configuración disponible tanto en cantidad de fuentes y de potencia de cada fuente. - Ventiladores redundantes, al menos dos módulos/bandejas de ventiladores, intercambiables en caliente. - Se deberá incluir ocho (08) transceivers ópticos 10GE-SR con conectores LC a ser distribuidos entre los switches solicitados. - Se deberá incluir ocho (08) transceivers 1000 Base-T con conectores RJ-45 a ser distribuidos entre los switches solicitados. - Se deberá incluir un (01) cable de apilamiento a 50Gbps por cada switch para virtualizar/apilar los switches solicitados.
Capacidades de procesamiento	- Capacidad de reenvío no menor a 654 Mpps. - Capacidad de switching no menor a 880 Gbps. - Buffer mínimo de 8MB - Capacidad de tabla de direcciones MAC no menor a 32K - Capacidad de rutas IPv4 mínima de 32K y rutas IPv6 de 16K
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso APIs del tipo REST o similar. - Debe permitir el apilamiento o stack clásico de hasta 8 switches de la misma familia. Se permitirá el uso de back plane stacking o de máximo dos de los puertos de uplink solicitados. Estos switches en stack o apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. Se debe incluir el hardware necesario para realizar el apilamiento o stack. - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola grafica de administración integrada	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Deberá mostrar de manera gráfica el equipo, indicando la distribución de puertos y el factor de forma. - Mostrar información de los dispositivos conectados al equipo. Se aceptará una consola de gestión externa licenciada con su respectivo hardware para cubrir dicho requerimiento.
Funcionalidades requeridas Capa 2, Capa 3, de seguridad y gestión	- Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d) - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad) - IEEE 802.1ab LLDP - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping

	- Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP - Protocolos de enrutamiento: PBR, VRRP, RIPv2, RIPng, OSPFv2 y v3, BGP4 y MP-BGP. - VXLAN estática. - VRF - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP - Control de acceso centralizado por RADIUS, para los usuarios de la red que se autentifican vía 802.1x. - RADIUS y RADIUS CoA - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN - Jumbo Frames de al menos 9K bytes

30. Switch de Gestión Fuera de Banda (02 Unidades)

Características de hardware	- El switch debe contar con 48 puertos RJ-45 10/100/1000 Base T con y 04 puertos SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps). - Factor de forma: una (01) unidad de rack (RU: Rack Unit). - El switch debe contar con ASIC del mismo fabricante. - Un (01) puerto auxiliar USB (USB-A o USB 2.0 o similar). - Un (01) puerto de gestión fuera de banda 10/100/1000 RJ-45. - Administración por Consola RJ-45 o USB-C. - Memoria RAM: Mínimo 8GB - Memoria Flash o SSD: Mínimo 8GB - Fuente de poder y ventiladores embebidos (fijos). - Se deberá incluir un (01) cable de apilamiento a 10Gbps por cada switch para virtualizar/apilar los switches solicitados.
Capacidades de procesamiento	- Capacidad de reenvío no menor a 130 Mpps. - Capacidad de switching no menor a 176 Gbps. - Buffer mínimo de 6MB - Capacidad de tabla de direcciones MAC no menor a 32K - Capacidad de rutas IPv4 mínima de 2K y rutas IPv6 de 1K
Características de Sistema Operativo	- Contar con configuración mediante API, que permita la automatización para el aprovisionamiento de los recursos de red. - El sistema operativo debe tener la capacidad de hacer puntos de chequeo de la configuración automáticamente para devolverse en el histórico de las mismas y realizar procesos de rollback. - La solución debe contar con motores de analítica internos o externos al switch y pertenecer al mismo fabricante. El Motor de Analítica debe incluir monitoreo y diagnósticos avanzados mediante el uso APIs del tipo REST o similar.

	- Debe permitir el apilamiento o stack clásico de hasta 8 switches de la misma familia. Se permitirá el uso de back plane stacking o de máximo dos de los puertos de uplink solicitados. Estos switches en stack o apilados deben ser vistos por los demás como una única entidad lógica de modo que se pueda agregar puertos entre ellos. Se debe incluir el hardware necesario para realizar el apilamiento o stack. - Debe contar con una consola de configuración por línea de comandos completa, soportar administración desde software centralizado y contar con interfaz gráfica incluida GUI. No se aceptarán soluciones de tipo SMB o Smart managed.
Características de la consola grafica de administración integrada	- La interfaz de gestión Web interna del equipo deberá mostrar de manera gráfica los logs, alertas críticas y advertencias, las versiones de firmware, el estado de temperatura, utilización del CPU, estado de fuente de poder y ventilación (cuando aplique). - Debe permitir la gestión del firmware del equipo: upgrades y downgrades. - Chequeo de enlaces agregados. - VLANs: gestión y estado de las interfaces. - Permitir hacer labores de diagnóstico. - Monitoreo del tráfico en tiempo real. - Deberá mostrar de manera gráfica el equipo, indicando la distribución de puertos y el factor de forma. - Mostrar información de los dispositivos conectados al equipo. Se aceptará una consola de gestión externa licenciada con su respectivo hardware para cubrir dicho requerimiento.
Funcionalidades requeridas Capa 2, Capa 3, de seguridad y gestión	- Capacidad de agregar VLANs en un mismo puerto físico o lógico (802.1Q) - Spanning Tree (802.1w, 802.1s y 802.1d) - Mecanismos de protección contra ataques tipo: BPDU spoofing, root bridge y loops. - Capacidad de agregar varios puertos físicos en uno lógico (LACP 802.3ad) - IEEE 802.1ab LLDP - Multicast: IGMP v1, v2 y v3, MLD v1 y v2, IGMP Snooping y MLD Snooping - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. - IEEE 802.1p y DSCP - Protocolos de enrutamiento: RIPv2, RIPng, OSPFv2 y v3. - VXLAN estática - Terminal monitor, capacidad de mostrar eventos en línea durante la sesión ssh. - Gestión a través de consola y terminales SSHv2. - SNMP v2 ó SNMP v2c. - SNMP v3. - NTP, DHCP y DNS - Transferencia de archivos a través de FTP y/o TFTP y/o SFTP. - Soporte de provisionamiento de tipo zero-touch. - Soporte de defensa contra ataques del tipo Denial of Service hacia el procesador. - Listas de control de acceso (ACL) basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP - Control de acceso centralizado por RADIUS, para los usuarios de la red que se autentifican vía 802.1x. - RADIUS y RADIUS CoA - Control de acceso centralizado por TACACS+ para los administradores del switch para autenticación, autorización y accounting. - Chip TPM o TAM para asegurar la autenticidad del hardware y del código del equipo. - Al menos 4 niveles de privilegios de acceso para administración por consola o por SSHv2. - Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN - Jumbo Frames de al menos 9K bytes.

Red Inalámbrica

31. Controlador Inalámbrico (02 Unidades)

- Deberá ser del tipo appliance y trabajar en conjunto con un servicio o software externo del mismo fabricante on-premise o en nube el cual se encargará de la gestión, monitoreo y la capa de control.
- Deberá ser una solución que permita extender el mismo registro/control que se realiza en la red inalámbrica a la red cableada (switches) propuesta.
- Características de controlador en formato appliance hardware:
  - Mínimo cuatro (04) puertos SFP+ (con capacidad de conectar transceivers a 1 ó 10 Gbps). Se deberá incluir dos (02) transceivers 10GE-SR por cada equipo ofertado.
  - Un (01) puerto consola RJ45 o similar.
  - Fuente redundante de energía.
  - Capacidad de poder registrar/controlar al menos 3000 dispositivos.
  - Capacidad de mantener conectados al menos 9000 clientes/endpoints simultáneos.
  - Capacidad de manejar 30,000 túneles.
  - Throughput no menor de 10 Gbps.
- La solución de controladores inalámbricos deberá implementarse bajo un esquema de redundancia N+1, de modo que, en caso de falla de un controlador, se pueda mantener conectados al menos 9000 clientes.
- En caso que en el futuro se requiera aumentar la capacidad de clientes conectados, la solución deberá permitirlo mediante la adición de más controladores.
- Debe manejar los estándares 802.11 a/b/g/n/ac/ax.
- Debe de operar conjuntamente con el resto de los equipos de la solución inalámbrica y cableada para soportar las aplicaciones de datos, voz y video.
- Deberá de contar con software o servicio que le permita adaptarse y administrar en tiempo real el entorno de RF. Entre estas funciones deberá de encontrarse:
  - Asignación dinámica de canales para optimizar la cobertura y desempeño.
  - Balanceo de carga de usuarios entre múltiples puntos de acceso inalámbricos.
  - Detección y corrección de huecos en la cobertura inalámbrica.
  - Control dinámico de potencia de acuerdo con las condiciones de la red.
- Incluir un firewall stateful embebido de al menos 2M de sesiones, con la capacidad de aplicar políticas basadas en L3, L4 y L7 o de lo contrario incluir un firewall de la misma marca de los switches y access points con las siguientes características:
  - Firewall stateful de 2M de sesiones
  - Throughput 10Gbps
  - 2 puertos SFP+ con dos (02) transceivers 10GE-SR
- Detección y clasificación de puntos de acceso inalámbricos no legítimos de manera automática, con opción a llevar acciones de contención como alguna de las siguientes:
  - Contención en el aire. Los puntos de acceso de la solución permiten contener al rogue incrementando su señal u otro mecanismo similar para que el cliente se asocie a la red adecuada.
  - Contención en la red. Integración con la plataforma de switches que permita identificar con la información de la red inalámbrica el punto de red a la cual se ha conectado el rogue. Debe de poder inclusive, realizar un apagado de puerto o bloquear el tráfico del AP no autorizado.
  - Enviar paquetes de interferencia al dispositivo ilegítimo para desconectarlo de la red inalámbrica.
- Capacidad de poder manejar autenticaciones basadas en web que pueda servir para la autenticación de usuarios invitados.
- Bloqueo de tráfico entre clientes asociados a un mismo SSID.
- Soporte de AAA mediante un servidor de RADIUS y TACACS+ para manejar las políticas de usuarios.
- Debe incluir o estar integrado a una solución DPI (Deep Packet Inspection) con la cual se pueda visualizar, analizar y controlar el uso de tráfico a nivel capa 7 (aplicación).
- Debe poder identificar las aplicaciones que usan los clientes con la finalidad de permitir o restringir su uso además de establecer la velocidad de carga y descarga de cada una (shaping).
- Deberá soportar y tener habilitada las siguientes funcionalidades de calidad de servicio:

  - Soporte de Wi-Fi Multimedia (WMM)
  - Soporte de DSCP
- Soporte de asignación de ancho de banda por perfil de usuario de acuerdo con su rol en la red o grupo en el directorio activo
- Debe tener la capacidad de funcionar como servidor de DHCP o DHCP Proxy o DHCP Relay.
- Para la administración como mínimo debe de soportar el acceso via HTTPS, SSH, SNMP v2 o v2c y v3.
- Debe manejar los estándares 802.11 d/e/h.
- Debe estar integrado con sistemas WIPS o WIDS o tener uno embebido en el mismo equipo que como mínimo permita:
  - Contar con mecanismos precisos y automáticos para la clasificación real de Access Points intrusos que se encuentren en la red.
  - Proveer mecanismos automáticos y eficientes de contención de Access Points intrusos.
  - Detección de ataques avanzados, habilitar acciones de contención o mitigación de amenazas avanzadas y colección de datos del WLAN.
  - Incluir la integración con un sistema de prevención de intrusos avanzado y completo, que permita tener total visibilidad de amenazas, identificación de firmas de ataques reconocidos, tomar acciones correctivas de mitigación y contención.
  - Detección y clasificación de puntos de acceso inalámbricos no legítimos (rogue) de manera automática, con opción a llevar acciones de contención.
- El equipo deberá permitir la aplicación política de red de forma automática según el usuario o dispositivo, eliminando la necesidad de configurar VLANs, ACLs o subredes manualmente, garantizando la separación y la seguridad del tráfico mediante segmentación dinámica.

32. Access Point (43 Unidades + 04 Unidades en Spare)

Especificaciones de radio WiFi	- Antenas omnidireccionales integradas para MIMO 2x2 - Access point para interiores de tres radios: 2.4Ghz, 5Ghz y 6Ghz. - Ganancia de antena mínimo de 4 dBi en 2.4GHz, 7 dBi en 5GHz y 6 dBi en 6Ghz. - Radio 5 GHz: 2 flujos espaciales con una tasa de datos de hasta 1.2 Gbps - Radio 2.4 GHz: 2 flujos espaciales con una tasa de datos de hasta 287 Mbps - Radio 6 GHz: 2 flujos espaciales con una tasa de datos de hasta 2.4 Gbps - DFS (Dynamic Frequency Selection) - Tecnologías de radio: ▪ 802.11b: DSSS (Direct-Sequence Spread-Spectrum) ▪ 802.11a/g/n/ac: OFDM (Orthogonal frequency-division multiplexing) ▪ OFDMA en 802.11 ax - Tipos de modulación: ▪ 802.11b: BPSK, QPSK, CCK ▪ 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM ▪ 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256- QAM ▪ 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256- QAM, 1024-QAM - Máxima potencia de transmisión : ▪ Por radio/banda de 2.4 GHz, 5 GHz y 6 GHz: +18 dBm por cadena, +21 dBm agregado.
Especificaciones de protocolos	- ACC (Advanced Cellular Coexistence) - MRC (Maximum Ratio Combining) - CDD/CSD (Cyclic Delay/Shift Diversity) - STBC (Space-Time Block Coding) - LDPC (Low-Density Parity Check) - TxBF (transmit beam-forming) - TWT (Target Wait Time) - FTM (Fine Timing Measurement)

	- BSS Coloring - Tasas de datos soportadas (Mbps): ▪ 802.11b: 1, 2, 5.5, 11 ▪ 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 ▪ 802.11n: 6.5 hasta 300 (MCS0 a MCS15, HT20 a HT40) ▪ 802.11ac: 6.5 hasta 867 (MCS0 a MCS9, NSS = 1 a 2, VHT20 a VHT80). ▪ 802.11ax: (2.4GHz): 3.6 hasta 574 (MCS0 a MCS11, NSS = 1 to 2, HE20 a HE40) ▪ 802.11ax (5GHz): 3.6 hasta 1,201 (MCS0 a MCS11, NSS = 1 to 2, HE20 a HE80) ▪ 802.11ax (6GHz): 3.6 a 2,402 (MCS0 a MCS11, NSS = 1 a 2, HE20 a HE160) - A-MPDU, A-MSDU
Interfaces	- Dos interfaces 100/1000/2500 BASE-T Ethernet (RJ-45) - Velocidad de enlace auto-sensing y MDI/MDX - EEE (Energy Efficient Ethernet) 802.3az - - PoE-PD (entrada): 48 Vdc (nominal) 802.3bt PoE - Radio BLE (Bluetooth Low Energy) y Zigbee (802.15.4) - Interface host USB 2.0 (conector Tipo A) - Interface serial de la consola
Características adicionales	- Módulo TPM o TAM para asegurar la autenticidad del hardware y del código del access point. - Debe incluir kit para instalación en techo o pared. - En caso se necesite, el AP debe poder funcionar sin necesidad de un controlador centralizado, es decir, mediante un controlador embebido. - Aspectos Regulatorios: ▪ FCC/ISED ▪ CE Marked ▪ Low Voltage Directive 2014/35/EU ▪ UL/IEC/EN 60950 o 62368-1 ▪ EN 60601-1-2 - Certificaciones: ▪ UL2043 plenum rating ▪ Wi-Fi Alliance (WFA) certificado 802.11a/b/g/n/ac/ax (incluyendo radio 6Ghz) ▪ WPA, WPA2 y WPA3 – Enterprise with CNSA option, Personal(SAE), Enhanced Open (OWE)

33. Solución de Administración y Gestión Campus (01 Unidad)

Características Generales	- La solución de administración y gestión de la infraestructura campus podrá ser implementada en premisa con appliance de propósito específico o en la nube. - En el caso de una solución en premisa, deberá incluir alta disponibilidad de todos sus servicios. Cada appliance físico deberá tener: ▪ Dos (02) interfaces de 10Gbps ▪ Fuente de poder redundante ▪ Altura no mayor a dos (02) Rack Units (RUs) ▪ Kit para poder ser instalado en rack de 19" - En el caso de una solución en nube, se deberá presentar documentación o carta del fabricante que indique un SLA no menor a 99.95%. No se aceptarán soluciones basadas en VMs que obliguen a la institución a gestionar o contratar un Tenant de nube pública. - Debe administrar tanto la infraestructura de switching como la de Wireless. No se aceptarán herramientas independientes con cross launch. - Debe realizar el aprovisionamiento de los dispositivos de red por medio de PnP (Plug and Play) o ZTP (Zero Touch Provisioning)

	- El licenciamiento debe ser perpetuo. En caso de estar basado en suscripción deberá considerarse por 12 meses contados desde la fecha que inicie la garantía y soporte.
Monitoreo	- La solución debe contar con una interfaz fácil de utilizar. - La solución debe mostrar información actualizada sobre el uso de la red y métricas de rendimiento de la misma. - La solución debe mostrar el mapa topológico de la red. - La solución debe proveer vistas de red de cada dispositivo (por ejemplo, puntos de acceso, switches, etc) bajo su gestión: ▪ En el caso de la red inalámbrica para cada dispositivo o radio se deberá contar cómo mínimo con información sobre la cantidad de dispositivos conectados, ancho de banda (bajada y subida), modelo y versión de software, utilización de canales, ruido, pérdidas, errores y retransmisiones, dirección IP, serie, y dirección MAC. ▪ En el caso de la red cableada para cada dispositivo deberá contar cómo mínimo con información sobre modelo, serie, dirección MAC, dirección IP, versión de software, estado de puertos (estado, utilización de subida y bajada, vlans configuradas, información de paquetes unicast, multicas, broadcast, errores y descartes), PoE consumido y disponible, utilización de CPU y memoria, estado de ventiladores y fuentes. - Debe proveer información sobre los clientes inalámbricos y cableados conectados a los dispositivos de red gestionados como: ▪ En el caso de los clientes inalámbricos se deberá mostrar como mínimo el nombre de usuario o hostname, dirección IP, MAC, vlan, estado (en línea, fuera de línea o fallido especificando el por qué) radio y canal de conexión inalámbrica, velocidad, throughput de subida y bajada. ▪ En el caso de los clientes cableados se deberá mostrar como mínimo el nombre de usuario o hostname, dirección IP, MAC, vlan, puerto y switch al cual está conectado, throughput de subida y bajada. - Incluir visibilidad de las aplicaciones en capa 7, con capacidad de al menos 3000 para usuarios conectados vía LAN y/o WLAN.
Diagnóstico y alertas	- Debe permitir la habilitación y configuración de alertas - Las alertas deben poder ser categorizadas por severidad. - Las alertas deben poder ser personalizadas de tal forma que se puedan definir umbrales y severidades. - Las alertas deben poder ser enviadas por correo electrónico. - Incluir IA que detecte posibles problemas que afecten el rendimiento de la red y ofrecer pistas sobre la causa raíz del problema para ayudar al administrador en la resolución (Insights) - Contar con una IA que permita analizar el desempeño de la red basado en SLAs o baselines obtenidos de otros sitios de modo que se pueda afinar la configuración de manera manual o automática. - Contar con una IA que permita determinar la calidad de la cobertura basado en el análisis del roaming de los clientes inalámbricos u otros parámetros. - Debe permitir el monitoreo de servicio de red, como mínimo AAA, DHCP y DNS, de modo que se pueda conocer si las transacciones contra estos servicios se están dando de manera exitosa o no. - Debe permitir la integración con soluciones terceras por medio de Webhooks para el envío de notificaciones.
Administración de configuraciones y firmware	- La plataforma deberá poder hacer cambios de configuración en la infraestructura de red ya sea de manera global, por grupos de equipos o de manera específica a un dispositivo en particular. - Debe manejar el inventario de los dispositivos de red, recopilando la dirección IP, la MAC Address

	- Debe permitir la creación de tags o etiquetas (labels) para realizar la agrupación o identificación de dispositivos que tengan alguna característica en común - Debe permitir la organización de los dispositivos de red en ubicaciones geográficas de modo que se pueda contar con el detalle de las redes por sitio. - Debe ser capaz de generar una plantilla de configuración o grupo de configuración. Este debe poder ser aplicada a uno o varios dispositivos de red. - Creación de SSID y configuración de parámetros de RF - Carga de planos para la visualización del mapa de calor de la red inalámbrica - Debe proveer información de auditoria para todos los cambios realizados en la red que incluya el nombre del usuario que hizo el cambio, así como la fecha/horas y detalle del cambio. - Debe proveer la opción de actualizar el firmware de uno o más dispositivos a la vez de manera inmediata o programada. - Se debe poder definir versiones de firmware mínimas aceptables por tipo de equipamiento o grupo de dispositivos. - Debe indicar si es que hay una versión de firmware superior a la utilizada en los dispositivos. Asimismo, debe recomendar una versión de firmware por tipo de dispositivo. - Clasificación de dispositivos finales utilizando capacidades de Machine Learning (ML) - Debe incluir workflows intuitivos - Debe incluir integración por medio de APIs. - Deberá poder definir perfiles de acceso para distintos tipos de usuarios de tal manera que se puedan asignar distintos privilegios de acceso a cada una de las secciones o módulos de la consola.
Seguridad	- La solución deberá utilizar todos los dispositivos de red inalámbrica bajo su gestión para detectar dispositivos no autorizados tales como puntos de acceso "rogue". - La solución deberá ser capaz de monitorear eventos de IDS tales como el descubrimiento de dispositivos no autorizados o interferencias. - Debe tener la capacidad de permitir o denegar tráfico basado en aplicaciones, categoría de aplicaciones, reputación y categorías de sitios web. - La solución deberá proveer mecanismos para remediar o contener dispositivos no autorizados encontrados en la red.
Reportes	- La solución deberá generar reportes. - Los reportes deberán poder generarse y enviarse vía correo electrónico de manera diaria, semanal o mensual. - Los reportes generados deberán poder ser exportados en formato pdf o csv.

34. Solución de Control de Acceso (01 Unidad)

Características generales	- Se requiere una solución de control de acceso redundante con la cual se puedan aplicar políticas de acceso basadas en usuario, dispositivo, lugar y medio de conexión a todos los dispositivos que se conectan a la red. - Deberá soportar la aplicación de políticas de control de acceso para redes de cualquier tipo (LAN, WLAN y VPN) - La solución debe centralizar el control de acceso de usuarios administradores a dispositivos de red de la entidad vía TACACS+ para autenticación, autorización y accounting. - La solución debe basarse en un esquema AAA (autenticación, autorización y accounting). - Interfaz basada en WEB para la configuración de políticas y troubleshooting.

	- El sistema deberá contar con funcionalidad habilitada para proporcionar integración con las siguientes fuentes de autenticación externas: Directorio Activo de Microsoft, Mobile Device Management (MDM), servidores RADIUS y RADIUS token server, entre otros. - El sistema deberá contar con funcionalidad habilitada de integrarse con soluciones de terceros de modo que se puedan compartir contextos e interoperar con el fin de realizar acciones de enforcement en conjunto. - Deberá soportar Auto Sign-On y/o single sign-on (SSO) mediante SAML - Deberá permitir autenticación 802.1x, no 802.1x y acceso basado en portal web. - Soporte de varias fuentes de autenticación tales como RADIUS, LDAP, AD, HTTP, SQL, Kerberos y Okta. - Los tipos de enforcements aplicados para cada uno de los servicios de autenticación deben ser como mínimo: ▪ RADIUS enforcement permit / deny / CoA ▪ Policy assignment ▪ SNMP enforcement ▪ DACL ▪ TACACS+ ▪ HTTP ▪ Filter Id - El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multi dominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario. - La solución debe soportar y tener habilitados los siguientes métodos de autenticación como mínimo: ▪ PAP ▪ CHAP ▪ EAP-MSCHAPv2 ▪ EAP-MD5 ▪ PEAP ▪ EAP-TLS ▪ EAP-GTC ▪ MAC Authentication ▪ WEB Authentication ▪ EAP-FAST ▪ EAP-PWD ▪ SAML ▪ OAuth2 - La solución debe, dependiendo del perfil del usuario autenticado, poder asignarle políticas de manera granular de acuerdo a las siguientes condiciones combinadas o independientes: ▪ Acceso a la red basado en tiempos: determinación de intervalos de tiempo en donde está permitido el usuario en la red. ▪ Acceso de red basado en la localización del usuario en la red: en determinados lugares de la red debe permitir el acceso del usuario. ▪ Acceso de red basado en el tipo de acceso:aAnte determinados medios de acceso como WLAN, VPN, LAN, etc., si el usuario está autorizado, darle acceso a la red. ▪ Atributos extraídos del directorio activo o personalizaciones vía APIs. - De acuerdo a las condiciones descritas anteriormente, poder aplicar algún tipo de política al usuario. Como mínimo las siguientes: ▪ Asignación dinámica de vlans ▪ Asignación dinámica de listas de control de acceso. ▪ Redirección hacia una URL. - Deberá permitir utilizar atributos de múltiples repositorios de identidad tales como Microsoft Active Directory, LDAP, base de datos SQL compatibles con OBDC, servidores de Token y base de datos interna, con

	el objetivo de utilizar estos atributos dentro de una política para un control granular.
Reconocimiento de dispositivos (profiling)	- Descubrir y clasificar los dispositivos finales, independientemente del tipo de dispositivo. Por ejemplo: Impresora, dispositivo móvil, computadora, teléfono, entre otros. - Identificación y clasificación (profiling) basada en datos contextuales tales como: ▪ MAC OUIs ▪ Nmap Scan ▪ DHCP fingerprints ▪ TCP fingerprints ▪ HTTP user agent ▪ SNMP traps ▪ LLDP ▪ Netflow / IPFIX ▪ WMI ▪ Span Port - La funcionalidad de profiling debe estar licenciada para el 100% de conexiones simultáneas, debe ser capaz de identificar cambios en perfilamiento y modificar dinámicamente la autorización de privilegios. Es decir, si una impresora que ya había sido autenticada en el pasado aparece como una Laptop Windows, el sistema de control de acceso debe denegar el acceso de manera automática. - Debe permitir al administrador sobrescribir la clasificación de perfilamiento hecha por el sistema, o agregar una nueva regla de clasificación para los atributos aprendidos, a modo de permitir que endpoints desconocidos sean categorizados de manera adecuada.
Administración de acceso para dispositivos headless	- Deberá permitir identificar a los dispositivos no administrados no 802.1x (headless) –impresoras, teléfonos y cámaras IP y clasificarlos como conocido o desconocido. - Esta funcionalidad deberá estar disponible y habilitada para su despliegue.
Gestión de visitantes	- Deberá permitir crear perfiles de accesos y la creación de cuentas temporales de invitados para el acceso a la red WIFI y cableada. - Deberá permitir la creación de más de un portal cautivo - El portal cautivo incluirá funcionalidades avanzadas de auto-registro, mediante las cuales el invitado podrá generar su propia cuenta de invitado sin comprometer la seguridad de la red. - El portal proporcionará diversos métodos para la entrega de credenciales de invitado: email, SMS o impresión de tickets. - El portal proporcionará métodos avanzados de aprobación de la visita por parte de la persona que recibe al invitado que permitan autorizar la visita de manera flexible y sin intervención de personal de IT. Es importante que los usuarios que aprueban el acceso no deban contar con ningún tipo autorización con privilegios de administración hacia la plataforma de control de acceso/guest. - Para la autenticación vía portal o Portal Authentication es necesario que el protocolo usado por el portal o captive portal sea el estándar y no uno propietario lo cual impide que la solución inalámbrica se integre con soluciones de control de acceso de terceros.
Control de salud de los dispositivos	- Deberá soportar la validación de la salud del dispositivo mediante el uso de agentes instalados en el dispositivo final. - Deberá informar sobre la integridad del dispositivo final como el estado del antivirus, anti-spyware, firewall, aplicaciones peer-to-peer, a los cuales se les definirá la autorización de su uso. - Deberá soportar la auto-remediación para los dispositivos que no cumplen las políticas de salud. - Deberá soportar la clasificación de los dispositivos como saludable o cuarentena.

	- El sistema deberá proporcionar un agente ligero NAC (Network Access Control) que garantice la integridad de los dispositivos. Este agente comprobará el estado y actualización de anti-virus, anti-spyware, firewalls, etc., y proporcionará instrucciones de remediación en caso de que el dispositivo viole las políticas corporativas. El agente deberá ser compatible con, al menos: Windows, Linux y MacOS - También debe realizar comprobaciones avanzadas como detección de programas P2P, utilización de llaves USB como dispositivos de almacenamiento y valores dentro de las llaves del REGEDIT.
Aprovisionamiento automático de dispositivos móviles corporativos (BYOD)	- Se deberá ser capaz de comportarse como una Entidad Certificadora (CA) la cual genere e instale automáticamente certificados digitales en los dispositivos móviles entregados por la empresa a sus colaboradores. - Deberá proveer un portal de auto-servicio para que los usuarios puedas aprovisionar sus dispositivos sin intervención de TI - Deberá incluir de manera embebida la funcionalidad de Autoridad Certificadora (CA), que permita generar certificados que incluya la información específica de los usuarios y sus dispositivos. - Deberá incluir dentro de sus workflows, la opción de integrarse con sistemas MDM/EMM y MFA para incrementar los niveles de seguridad - Deberá permitir limitar la cantidad de dispositivos por usuario - Deberá soportar el aprovisionamiento para dispositivos con los siguientes sistemas operativos: Windows, Mac OS X, iOS, Android y Ubuntu - Deberá ser capaz de configurar de manera automática los parámetros de red en los dispositivos personales, para que éstos se puedan conectar de manera segura a la red corporativa con 802.1x - Deberá realizar perfilamiento automático para identificar tipo de dispositivo, fabricante, modelo y sistema operativo - Deberá proveer estadísticas de uso e inventario de los dispositivos móviles - Deberá permitir la personalización de los workflows de aprovisionamiento, para que, por ejemplo, un miembro del staff de TI deba aprobar la solicitud antes de que el usuario pueda conectar su dispositivo.
Plataforma	- Plataforma de la solución en formato appliance, mínimo de dos (02) nodos (appliances físicos) redundantes, con capacidad de soportar cada uno al menos 60,000 dispositivos endpoints autenticados simultáneamente. - Cada nodo deberá tener dos (02) conexiones 10GE-SR para conectarse con la red. - Cada nodo (appliance físico) deberá contar con: un procesador de por lo menos 32 cores y 32 threads, RAM de al menos 128 GB y storage de 960 GB SSD. - Licenciamiento a perpetuidad. - Se deberá considerar que se tendrán 2,000 dispositivos finales (endpoints) conectados de manera concurrente/simultánea a la red, cantidad que será independiente del tipo de autenticación que usen (por usuario y password, por MAC, por certificado, via portal, etc.). Se deberá considerar incluir para esta cantidad de dispositivos finales todas las funcionalidades descritas en las secciones "características generales", "reconocimiento de dispositivos", "administración de acceso para dispositivos headless", y "gestión de visitantes". - Se deberá considerar que 500 usuarios podrán conectar a la red empresarial dispositivos BYOD hasta un máximo de un smartphone, una tablet y una computadora portátil por usuario, los cuales deberán aprovisionarse automáticamente con los certificados correspondientes. Se deberá considerar incluir para esta cantidad de usuarios todas las funcionalidades descritas en la sección "aprovisionamiento automático de dispositivos móviles corporativos (BYOD)". - Se deberá considerar que existirán 2000 dispositivos finales (endpoints) sobre los cuales se deberá realizar una evaluación avanzada de postura (control de salud) ya sea si su conexión es cableada, inalámbrica y/o por VPN. Se deberá considerar incluir para esta cantidad de usuarios todas

	las funcionalidades descritas en la sección "control de salud de los dispositivos".
Repositorios de identidad soportados	- Deberá soportar Microsoft Active Directory - Deberá soportar Kerberos - Deberá soportar LDAP - Deberá soportar SQL server compatible con ODBC - Deberá soportar listas estáticas - Deberá soportar base de datos internas.

Hiperconvergencia

35. Hardware de Hiperconvergencia (04 Unidades)

Descripción	Características técnicas mínimas
Cantidad	Cuatro (04) unidades.
Solución Hiperconvergente (HCI)	La solución hiperconvergente por definición es cómputo, virtualización y storage totalmente definido por software. Los nodos HCI deben encontrarse en la matriz de compatibilidad e interoperabilidad del fabricante del software. Los nodos HCI deben estar identificado en el portal del fabricante del hardware como appliance o sistema hiperconvergente.
Factor de forma	Rackeable, debe incluir los accesorios de rackeo.
Procesadores	Dos (02) procesadores x86 de la última generación, con fecha de lanzamiento 2026 como mínimo, de 12 cores como mínimo, de al menos 2.2GHz de frecuencia base y mínimo 48MB de cache L3. Debe soportar la tecnología Hyper-Threading o Multithreading.
Memoria RAM	512GB de memoria RAM de tecnología DDR5, en módulos de mínimo 64GB 6,400MHz RDIMM. Deberá soportar un crecimiento de al menos hasta 2TB de memoria RAM en su máxima configuración, añadiendo módulos de memoria, sin reemplazar los módulos solicitados. Deberá soportar como mínimo 32 slots DIMM.
Boot de hipervisor	Dos (02) discos M.2 SSD NVMe de mínimo 480GB configurados en RAID 1 por hardware.
Almacenamiento	Cada servidor o nodo HCI deberá contar con discos SSD NVMe intercambiables en caliente, deberá incluir al menos 10 bahías para discos SSD NVMe. La solución hiperconvergente (HCI) debe ser configurada para permitir la tolerancia de fallos ante la caída de un (01) servidor o nodo (N+1) La capacidad efectiva o usable total de almacenamiento de la solución HCI deberá ser de al menos 50TiB SSD NVMe en RF2 o RAID 1 o mirror, sin considerar factores de eficiencia como compresión y deduplicación. El dimensionamiento deberá ser sobre arquitectura de acceso directo a la capa de almacenamiento NVMe. La solución debe realizar réplicas de datos almacenados a través de los nodos de clúster.
Puertos de conectividad	Cuatro (04) puertos Ethernet de 25Gb SFP28, deben incluir sus respectivos transceivers SR SFP28 y cables de fibra LC-LC MM OM3 de mínimo 3 metros. los cuales se utilizarán para garantizar redundancia de conectividad LAN y para la interconexión de la solución hiperconvergente. La solución debe garantizar conectividad redundante hacia los switches de data center, el postor deberá considerar la configuración y compatibilidad de la solución con dicha infraestructura.
Fuentes de poder	Dos (02) fuentes poder redundantes de 220VAC de intercambio en caliente de mínimo 1,300W, con sus respectivos cables de poder C13-C14 de al menos 2 metros.

Seguridad	Soporte de TPM 2.0. La gestión del hardware del nodo HCI debe cumplir con los estándares FIPS 140-2 y NIST 0800-053. Debe contar con un sistema de arranque (boot) seguro, que garantice que solo se cargue software inmutable y firmado durante el tiempo de arranque, evitando que se cargue código malicioso y ayudando a prevenir ataques como la instalación de rootkits. Debe contar con una tapa de seguridad frontal con llave.
Análisis predictivo de fallas	Debe soportar análisis predictivo de fallas de componentes como: procesador, discos, memoria, ventiladores y fuentes de poder; y debe poder solicitarse el cambio por garantía desde el momento que se presenta una alerta de este tipo en algunos de estos componentes.
Puerto de gestión	Deberá incluir un (01) puerto de gestión de 1GbE RJ45, que proporcionen una interfaz de administración web, desde la cual se podrá supervisar y gestionar todos los componentes internos del servidor. Debe contar con todas sus funcionalidades habilitadas.
Software de administración de hardware	Factor de forma: máquina o appliance virtual. Deberá incluir el software y todas las licencias necesarias que permitan la administración centralizada de los servidores solicitados. Este software debe permitir la administración, control, gestión y manejo de toda la infraestructura de cómputo y realizar las siguientes funciones como mínimo: - Descubrir todo el hardware. - Realizar un inventario de la infraestructura de servidores. - Monitoreo del estado de la salud de los componentes. - Actualizaciones de firmware. - Configuración de patrones de los servidores. - El software deberá soportar la administración remota gráfica de cada servidor independientemente del sistema operativo del servidor. - Proveer acceso detallado a problemas de fallas del sistema. - Deberá de ser capaz de contactar al fabricante automáticamente para abrir un ticket y enviar datos de servicio siempre que el equipo notifique un error de hardware. - Capacidad de instalación remota de un servidor o grupo de servidores. - Capacidad de actualización del firmware remota de un servidor o grupo de servidores. - Funcionalidad de acceso remoto compartido entre por lo menos tres usuarios concurrentemente, independiente del sistema operativo del servidor. - Integración con herramientas de administración de recursos como basadas en Ansible, Chef y Puppet. - Las características descritas deberán entenderse como requerimientos funcionales abiertos, no vinculados a un fabricante específico, permitiendo la participación de soluciones equivalentes que cumplan o superen las funcionalidades solicitadas.
Consideraciones	Se deberá incluir la instalación física y configuración de la Solución Hiperconvergente (HCI) por parte del fabricante de los servidores o del software HCI. Todos los componentes, partes y accesorios deben ser originales y nuevos. El año de fabricación de los servidores o nodos HCI deberá ser como mínimo 2026.

36. Software Hiperconvergencia (01 Unidad)

Descripción	Características técnicas mínimas
Licencias	El licenciamiento del software debe ser por suscripción, del tipo OPEN, de forma que no esté vinculado a un solo fabricante de hardware.
Características del almacenamiento definido por software	La infraestructura de cómputo y almacenamiento deberá ser distribuida y completamente definida por software, armando un clúster con las siguientes características: - La solución deberá soportar tolerancia a fallas equivalente a un esquema de redundancia N+1, permitiendo la continuidad operativa del clúster ante la caída simultánea de hasta dos nodos sin pérdida de información ni indisponibilidad de servicios críticos. - La protección de datos deberá realizarse entre los múltiples nodos que componen el clúster, de manera distribuida. - Deberá tener la capacidad de distribuir los datos dentro del clúster y adicionalmente poder replicarlos internamente, para asegurar su disponibilidad. - En caso de una falla, la solución basada en software debe actuar de manera automática creando nuevas copias múltiples de los datos, de manera de mantener el nivel de protección hasta tanto se reemplace el componente que haya fallado. - Capacidad de generar almacenamiento compartido (distribuido) usando los discos internos de cada uno de los nodos generando un almacenamiento virtual, el cual pueda ser presentado a la capa de hypervisor para que los diferentes Hosts puedan hacer uso del almacenamiento de manera transparente y homogénea. - Los recursos de cómputo (CPU y memoria) deberán mantenerse dedicados a cada nodo físico. En el caso del almacenamiento, la solución deberá permitir la conformación de una malla o fabric de almacenamiento distribuido, donde los discos locales de cada nodo se integren en un pool lógico unificado presentado al clúster, garantizando distribución de datos, resiliencia y balanceo automático. - Cada nodo deberá contar con su propia controladora de almacenamiento virtual. - La solución debe escalar como mínimo hasta 16 nodos por clúster. - Debe incluir el soporte de vGPU y GPU Passthrough. - La solución deberá ser agnóstica al hipervisor y debe soportar distintos hipervisores como: VMware ESXi y basados en Linux KVM. - La solución deberá de ser capaz de actualizar el hipervisor en forma desatendida y automatizada. Así mismo la solución deberá de tener la capacidad de convertir la infraestructura de un hipervisor a otro en forma desatendida. - La solución deberá permitir las actualizaciones centralizadas del software en caliente, sin salida de servicio de las cargas (máquinas virtuales) que están corriendo. - La solución debe tener la capacidad de expandir la infraestructura en cualquiera de los tres componentes, procesamiento, memoria, y almacenamiento, sin que las cargas

	(máquinas virtuales) salgan de servicio. El software debe reconocer los recursos cuando se agregue un nodo. - Deberá soportar el crecimiento scale-out en nodos heterogéneos, o diferentes modelos para maximizar recursos de procesamiento, memoria o almacenamiento según requiera. - Proveer un crecimiento lineal, estable y predecible en su rendimiento a medida que se agreguen nodos. - Proveer alto rendimiento al presentar recursos de almacenamiento desde el mismo nodo en el que la máquina virtual se encuentra atendiendo los requerimientos de IOPS. Esto significa que el almacenamiento virtualizado, puede entregar recursos para administrar los requerimientos de I/O hecho por la máquina virtual local a cada nodo. - Cada nodo deberá manejar los IOPS de sus máquinas virtuales en forma local. Independientemente de que la máquina virtual sea original a ese nodo, o haya sido desplazada desde otro nodo. - Debe incluir la funcionalidad de asignar y redistribuir cargas de trabajo a los nodos que mejor se adapten a sus requisitos específicos de almacenamiento, ya sea en términos de rendimiento, latencia o capacidad, asegurando así una óptima utilización de los recursos disponibles. - La solución de almacenamiento deberá ser definida por software e incluir las siguientes funcionalidades: o Deduplicación y compresión. o Thin provisioning. o Snapshots ilimitados basados en punteros. o Sistemas de clones de máquinas virtuales sin consumo de espacio adicional. o Replicación asíncrona. - La solución de almacenamiento no requerirá de switches Fibra Canal, ni FCoE para su funcionamiento. Solamente utilizará switches para Data Center que trabajen stack TCP/IP sobre Ethernet. - La solución debe ser 100% definida por software, desacoplando la inteligencia del hardware y evitando la dependencia de componentes propietarios. Debe integrar en una sola plataforma recursos de cómputo, almacenamiento, virtualización y gestión centralizada, permitiendo una experiencia operativa coherente en centros de datos locales y nubes públicas. - La solución deberá incluir al menos 1 TiB de almacenamiento para servicios de archivos (NFS, SMB) u objetos compatibles con S3, incorporando funcionalidades de analítica que permitan visualizar comportamiento de usuarios y consumo. También podrá ser ofertado con Hardware y Software de terceros que se integren dentro de la solución.
Características del software virtualización	- El software de virtualización debe instalarse para todos los nodos que conforman el clúster. - El hipervisor debe ser compatible con servidores tipo x86 basados en procesadores multinúcleo compatibles con la arquitectura x86 de 64 bits. - El hipervisor deberá instalarse en cada servidor físico como parte de la arquitectura del clúster hiperconvergente, pudiendo coexistir con controladoras virtuales de almacenamiento distribuidas propias de la solución propuesta, siempre que no

	se comprometa el rendimiento, disponibilidad y seguridad de la plataforma. - Debe incluir el soporte para la migración de máquinas virtuales apagadas (Power off) de un servidor físico a otro tan solo indicando la acción de la máquina virtual seleccionada en la consola de administración. - Debe incluir el soporte para la migración de máquinas virtuales en ejecución o encendidas (Power On) desde un servidor físico a otro similar, sin interrupciones para los usuarios ni pérdidas de servicio, eliminando la necesidad de planificar tiempo fuera de servicio de aplicaciones para realizar el mantenimiento planificado de los servidores. - La solución de virtualización debe incluir alta disponibilidad, se entiende la capacidad que debe tener la plataforma de iniciar una máquina virtual en cualquier nodo disponible, en el caso de que el nodo que la alberga falle. - El software de virtualización debe permitir el reinicio de manera automatizada de todas las máquinas virtuales en forma inmediata en caso de un fallo de hardware. - La solución de virtualización debe tener la capacidad de creación y ejecución simultánea de múltiples máquinas virtuales sobre un mismo nodo. Con soporte de sistemas operativos como: o Microsoft Windows Server 2016, 2019 y 2022. o Red Hat Enterprise Linux 6, 7, 8 y 9. o SUSE Linux Enterprise 12 y 15. o Canonical Ubuntu 14, 16, 18, 19, 20 y 22.
Características del software de administración de la Plataforma Virtual	La solución deberá proveer una consola de administración única la cual deberá: - Ser accedida mediante un browser y estar basada en HTML5. - Proveer una única vista para todo el entorno (sistema) manteniendo múltiples puntos de acceso. - La consola permitirá administrar y monitorear a todo el stack que compone la solución, almacenamiento, hipervisor, redes, los nodos que conforman el clúster hiperconvergente. - La consola de Administración deberá ejecutarse sobre los mismos nodos del clúster que administra, aprovechando la tolerancia a fallos de este. La consola debe permanecer disponible ante la falla de cualquiera de los nodos. - Proveer accesos alternativos basados en SSH y/o interfaces seriales remotas estilo IPMI. - Contener autenticación LDAP, Active Directory, CAC Prompt y certificados firmados por SSL. - Gestión automática de dependencias. - Proceso de actualización unificado. - La consola facilitará la ejecución de las tareas de mantenimiento de la plataforma, actualizaciones del software, upgrades de hipervisor, upgrades de firmware de manera no disruptiva. - Permitir reportes y panel de control personalizable. - Permitir analizar de manera predictiva, el uso de los recursos del clúster (memoria, discos y procesamiento). - Permitir el análisis del comportamiento de una máquina virtual. - Permitir su optimización automatizada en caso no esté usando los recursos de manera eficiente.

	- Permitir analizar de manera gráfica, la estadística de las cargas de trabajo, permitir proyectar crecimientos, para luego recomendar un upgrade de recursos (memoria, disco y procesamiento) que soporte ese crecimiento futuro (Capacity Planning).
Seguridad	- Microsegmentación de la red: Debe incluir capacidades nativas de redes definidas por software para aplicar políticas de seguridad de «confianza cero» a nivel de la interfaz de red virtual, aislando las cargas de trabajo y las aplicaciones sin necesidad de realizar cambios en la red, también esta funcionalidad podrá ser ofertada con Hardware y Software de terceros que se integren dentro de la solución. - La solución debe incluir una funcionalidad nativa para análisis y gestión de políticas de seguridad que proporcione: o Monitoreo y visibilidad de VMs y políticas aplicadas. o Auditoría y remediación mediante análisis en tiempo real y acciones automatizadas para corregir desviaciones. o Cumplimiento continuo, automatizando verificaciones y validaciones normativas. o Planificación de seguridad, con visualización y clasificación del tráfico de red. o Investigación de incidentes y generación de mapas de calor para evaluar la postura de seguridad. o Pruebas automatizadas basadas en mejores prácticas. o Políticas listas para usar para cumplir normativas como HIPAA, PCI-DSS, CIS, entre otras. o Todo gestionado desde una única consola, sin recurrir a herramientas externas ni integraciones adicionales. - La solución de hiperconvergencia debe proveer la capacidad para la encripción de datos en reposo sin requerir un Key Management Server externo, sino entregar el manejo de las llaves de encriptación. También esta funcionalidad podrá ser ofertada con Hardware y Software de terceros que se integren dentro de la solución. - La solución debe contar con un nivel de aseguramiento (hardening) aplicado de fábrica y disponer de un mecanismo nativo que automatice la remediación de cualquier desviación respecto a dicho hardening durante todo el ciclo de vida, sin requerir tareas manuales por parte del administrador.
Sistema Operativo	- Windows Server 2025 Datacenter segurando el licenciamiento total de los cores físicos (2 paquetes de 12 cores). Adicionalmente, se requiere la compra de 300 CALs de Usuario de Windows Server 2025, las cuales deben cubrir al total de usuarios que interactuarán con el Directorio Activo y los servicios de red.

Sistema de Respaldo

37. Servidor para backup (01 Unidad)

Descripción	Características técnicas mínimas
Cantidad	Una (01) unidad.
Factor de forma	Rackeable, debe incluir los accesorios de rackeo.
Procesadores	Un (01) procesador x86 de la última generación, con fecha de lanzamiento 2025 como mínimo, cada procesador de 12 cores como mínimo, de al menos 2.2 GHz de frecuencia base y mínimo 48 MB de cache L3. El servidor debe soportar el crecimiento hasta dos (02) procesadores. Debe soportar la tecnología Hyper-Threading o Multithreading.
Memoria RAM	64GB de memoria RAM, de tecnología DDR5, en módulos de mínimo 16GB 6,400MHz RDIMM o superior. Deberá soportar como mínimo 32 slots DIMM.
Puertos de conectividad	Dos (02) puertos Ethernet de 25Gb SFP28, deben incluir sus respectivos transceivers SR SFP28 y cables de fibra LC-LC MM OM3 de mínimo 5 metros. Dos (02) puertos Fibra Canal (FC) de 32Gb, deben incluir sus respectivos transceivers y cables de fibra LC-LC MM OM3 de mínimo 5 metros, para la conexión con la Librería de Cintas solicitada.
Discos	Dos (02) discos SSD de 3.84TB configurados en RAID 1. Los discos deben poder ser intercambiables en caliente. Deberá incluir el backplane con soporte de al menos ocho (08) discos.
Tarjeta de arreglo	Con soporte de RAID 0, 11 10, 5, 50 y 60 como mínimo. Deberá tener 4GB de caché flash integrada Soporte de discos HDD y SSD.
Fuentes de poder	Dos (02) fuentes poder redundantes de 220VAC de intercambio en caliente de mínimo 1,300W, con sus respectivos cables de poder C13-C14 de al menos 2 metros.
Sistemas operativos soportado	Microsoft Windows Server 2022 y 2025 Red Hat Enterprise Linux 9 y 10. SUSE Linux Enterprise Server 15 y 16. VMware vSphere (ESXi) 8 y 9.
Licencia de Sistema Operativo	Deberá incluir la suscripción o licencia OEM del Sistema Operativo de 64 bits. Esta deberá ser compatible con el Software de Backup solicitado.
Análisis predictivo de fallas	Debe soportar análisis predictivo de fallas de componentes internos como: procesador, discos, memoria, ventiladores y fuentes de poder; y debe poder solicitarse el cambio por garantía desde el momento que se presenta una alerta de este tipo en algunos de estos componentes.
Seguridad	Soporte de TPM 2.0. El servidor debe cumplir con los estándares NIST SP800-193, NIST SP800-131A y NIST SP800-147B. Debe contar con un sistema de arranque (boot) seguro, que garantice que solo se cargue software inmutable y firmado durante el tiempo de arranque, evitando que se cargue código malicioso y ayudando a prevenir ataques como la instalación de rootkits.

	Debe contar con protección contra actualizaciones de firmware no autorizadas y corrupción, restaurando el firmware a un estado integral y monitoreo del firmware en busca de posibles compromisos de ataques cibernéticos.
Puerto de gestión	Deberá incluir un puerto de gestión fuera de banda, que proporcionen una interfaz de administración web, desde la cual se podrá supervisar y gestionar todos los componentes internos del servidor, así mismo deberá contar con mecanismos de despliegue o provisionamiento del sistema operativo, estas funciones deberán ser independientes al sistema operativo. Deberá ser un puerto de gestión dedicado de 1Gb RJ45 y con todas sus funcionalidades habilitadas.
Software de administración de hardware	Factor de forma: máquina o appliance virtual. Deberá incluir el software y todas las licencias necesarias que permitan la administración centralizada de los servidores solicitados. Este software debe permitir la administración, control, gestión y manejo de toda la infraestructura de cómputo y realizar las siguientes funciones como mínimo: - Descubrir todo el hardware. - Realizar un inventario de la infraestructura de servidores. - Monitoreo del estado de la salud de los componentes. - Actualizaciones de firmware. - Configuración de patrones de los servidores. - El software deberá soportar la administración remota gráfica de cada servidor independientemente del sistema operativo del servidor. - Proveer acceso detallado a problemas de fallas del sistema. - Deberá de ser capaz de contactar al fabricante automáticamente para abrir un ticket y enviar datos de servicio siempre que el equipo notifique un error de hardware. - Capacidad de instalación remota de un servidor o grupo de servidores. - Capacidad de actualización del firmware remota de un servidor o grupo de servidores. - Funcionalidad de acceso remoto compartido entre por lo menos tres usuarios concurrentemente, independiente del sistema operativo del servidor. - Integración con herramientas de administración de recursos como basadas en Ansible, Chef y Puppet.
Sostenibilidad	Certificado de no perjudicar la salud y/o presentar un impacto negativo al medio ambiente EPEAT. Certificado de eficiencia de energía (Energy Star).
Consideraciones	Todos los componentes, partes y accesorios, deben ser originales y nuevos. El año de fabricación del servidor deberá ser como mínimo 2026.

38. Servidor de inmutabilidad (01 Unidad)

Descripción	Características técnicas mínimas
Factor de forma	Rackeable, debe incluir los accesorios de rackeo.
Procesadores	Un (01) procesador x86 de la última generación, con fecha de lanzamiento 2025 como mínimo, cada procesador de 12 cores como mínimo, de al menos 2.2 GHz de frecuencia base y mínimo 48 MB de cache L3. El servidor debe soportar el crecimiento hasta dos (02) procesadores. Debe soportar la tecnología Hyper-Threading o Multithreading.
Memoria RAM	64GB de memoria RAM, de tecnología DDR5, en módulos de mínimo 16GB 6,400MHz RDIMM o superior. Deberá soportar como mínimo 32 slots DIMM.
Puertos de conectividad	Dos (02) puertos Ethernet de 25Gb SFP28, deben incluir sus respectivos transceivers SR SFP28 y cables de fibra LC-LC MM OM3 de mínimo 5 metros. Dos (02) puertos Fibra Canal (FC) de 32Gb, deben incluir sus respectivos transceivers y cables de fibra LC-LC MM OM3 de mínimo 5 metros, para la conexión con el Almacenamiento de Backup solicitado.
Discos	Dos (02) discos SSD de 1.92TB configurados en RAID 1. Los discos deben poder ser intercambiables en caliente. Deberá incluir el backplane con soporte de al menos ocho (08) discos.
Tarjeta de arreglo	Con soporte de RAID 0, 11 10, 5, 50 y 60 como mínimo. Deberá tener 4GB de caché flash integrada Soporte de discos HDD y SSD.
Fuentes de poder	Dos (02) fuentes poder redundantes de 220VAC de intercambio en caliente de mínimo 1,300W, con sus respectivos cables de poder C13-C14 de al menos 2 metros.
Sistemas operativos soportado	Microsoft Windows Server 2022 y 2025 Red Hat Enterprise Linux 9 y 10. SUSE Linux Enterprise Server 15 y 16. VMware vSphere (ESXi) 8 y 9.
Licencia de Sistema Operativo	Deberá incluir la suscripción del Sistema Operativo Linux de 64 bits, necesarias para la inmutabilidad del backup a disco.
Análisis predictivo de fallas	Debe soportar análisis predictivo de fallas de componentes internos como: procesador, discos, memoria, ventiladores y fuentes de poder; y debe poder solicitarse el cambio por garantía desde el momento que se presenta una alerta de este tipo en algunos de estos componentes.
Seguridad	Soporte de TPM 2.0. El servidor debe cumplir con los estándares NIST SP800-193, NIST SP800-131A y NIST SP800-147B. Debe contar con un sistema de arranque (boot) seguro, que garantice que solo se cargue software inmutable y firmado durante el tiempo de arranque, evitando que se cargue código malicioso y ayudando a prevenir ataques como la instalación de rootkits. Debe contar con protección contra actualizaciones de firmware no autorizadas y corrupción, restaurando el firmware a un estado integral y monitoreo del firmware en busca de posibles compromisos de ataques cibernéticos.

Puerto de gestión	Deberá incluir un puerto de gestión fuera de banda, que proporcionen una interfaz de administración web, desde la cual se podrá supervisar y gestionar todos los componentes internos del servidor, así mismo deberá contar con mecanismos de despliegue o provisionamiento del sistema operativo, estas funciones deberán ser independientes al sistema operativo. Deberá ser un puerto de gestión dedicado de 1Gb RJ45 y con todas sus funcionalidades habilitadas.
Software de administración de hardware	Factor de forma: máquina o appliance virtual. Deberá incluir el software y todas las licencias necesarias que permitan la administración centralizada de los servidores solicitados. Deberá contar con soporte y suscripción por el periodo de 12 meses. Este software debe permitir la administración, control, gestión y manejo de toda la infraestructura de cómputo y realizar las siguientes funciones como mínimo: - Descubrir todo el hardware. - Realizar un inventario de la infraestructura de servidores. - Monitoreo del estado de la salud de los componentes. - Actualizaciones de firmware. - Configuración de patrones de los servidores. - El software deberá soportar la administración remota gráfica de cada servidor independientemente del sistema operativo del servidor. - Proveer acceso detallado a problemas de fallas del sistema. - Deberá de ser capaz de contactar al fabricante automáticamente para abrir un ticket y enviar datos de servicio siempre que el equipo notifique un error de hardware. - Capacidad de instalación remota de un servidor o grupo de servidores. - Capacidad de actualización del firmware remota de un servidor o grupo de servidores. - Funcionalidad de acceso remoto compartido entre por lo menos tres usuarios concurrentemente, independiente del sistema operativo del servidor. - Integración con herramientas de administración de recursos como basadas en Ansible, Chef y Puppet.
Sostenibilidad	Certificado de no perjudicar la salud y/o presentar un impacto negativo al medio ambiente EPEAT. Certificado de eficiencia de energía (Energy Star).
Consideraciones	Todos los componentes, partes y accesorios, deben ser originales y nuevos. El año de fabricación del servidor deberá ser como mínimo 2026.

39. Almacenamiento para backup (01 Unidad)

Descripción	Características técnicas mínimas
Formato	Rackeable, deberá incluir su kit de montaje en rack. Si es necesario expansiones de discos se deben agregar y cada expansión debe ser en formato rack e incluir su kit de montaje en rack.

Disponibilidad	Deberá estar diseñado para una disponibilidad de 99.9999%, deberá poder ser verificado en la documentación pública del fabricante del sistema de almacenamiento. Deberá soportar actualizaciones de firmware sin interrupciones.
Controladoras	Dos controladoras en configuración activo-activo con balanceo de carga automático. La arquitectura de las controladoras debe estar basado en tecnología de procesadores x86.
Memoria cache	64GB como mínimo de memoria cache nativa por sistema. No se aceptará tarjetas o discos flash u otro elemento no nativo como componentes de cache.
Conectividad	iSCSI y Fibra Canal.
Puertos por controlador	Dos (02) puertos iSCSI de 10/25 Gb, deben incluir sus respectivos transceivers. Cuatro (04) puertos Fibra Canal a 32 Gb, deben incluir sus respectivos transceivers. Un (01) puerto 1GbE RJ45 para gestión.
RAID	Debe soportar RAID 0, 1, 5, 6 y 10 como mínimo. Soporte de Pool de discos dinámicos o similar.
Escalabilidad	Mínimo 3 expansiones de discos. Debe soportar escalar al menos hasta 1 PB RAW.
Tipo de discos soportados	SSD SAS o superior. HDD SAS. HDD NL-SAS. Los discos deberán ser reemplazables en caliente.
Capacidad instalada	Deberá contar como mínimo con 100TiB de capacidad usable, sin considerar funcionalidades de eficiencia de datos, con discos de estado sólido (SSD), deberá configurarse doble paridad y al menos un disco o capacidad spare.
Interoperabilidad	Deberá ser compatible con la conexión directa (DAS)
Fuentes de poder redundantes	Dos (02) fuentes de poder AC, Hot-Swap, activas y redundantes.
Sistemas Operativos Soportados	Microsoft Windows Server. Red Hat Enterprise Linux. SUSE Linux Enterprise Server. VMware vSphere.
Administración	La consola de administración deberá permitir: - La gestión centralizada vía web con distintos perfiles y privilegios de usuarios. - Visualizar datos de rendimiento, incluida la latencia de E/S, IOPS, la utilización de la CPU y el rendimiento. - Suministrar almacenamiento mediante conjuntos o grupos de volumen y crear cargas de trabajo de aplicaciones. - Realizar copias de seguridad y recuperación ante desastres mediante capturas y copias de volúmenes. - Comprobar el estado de los componentes. - Notificar a los administradores acerca de sucesos importantes que se producen en el almacenamiento. Las alertas se deberán enviar mediante correo electrónico, capturas SNMP y syslog. - Configurar la autenticación de los usuarios y funciones de rendimiento del sistema.

	- Ver datos de diagnóstico, gestionar actualizaciones y configurar el soporte automático, que permitirá supervisar el estado del almacenamiento y enviarlo automáticamente al centro de soporte técnico.
Funcionalidades incluidas	- Deberá incluir la funcionalidad de thin provisioning para generar volúmenes de espacio virtual sobre el espacio físico disponible. - Deberá incluir la capacidad de realizar snapshots. - Deberá incluir la capacidad de realizar copia de volúmenes. - Estas funcionalidades deberán incluir el licenciamiento por toda la capacidad soportada del sistema de almacenamiento.
Software de gestión de hardware	Deberá incluir el software y todas las licencias necesarias que permitan la administración centralizada de los servidores y almacenamiento solicitados. También se podrá proponer un software de terceros para esta funcionalidad.
Consideraciones	Todos los componentes, partes y accesorios, deben ser originales y nuevos. El año de fabricación del almacenamiento deberá ser como mínimo 2026.

40. Librería de backup (01 Unidad)

Descripción	Características técnicas mínimas
Formato físico	Debe ser modular y escalable. El módulo base debe ser en formato rack. Debe ser de tipo rackeable y debe incluir los accesorios para su montaje.
Unidades de lectura/escritura	La configuración de la librería debe incluir mínimo dos (02) tapes drives LTO9, cada uno con un (01) puerto de fibra canal (FC) de 8 Gbps como mínimo. - La configuración de la librería debe incluir la capacidad de instalar y sustituir los tapes drives en caliente sin afectar la operatividad de la librería. - El modelo de la librería debe soportar tape drives y cartuchos de tecnologías LTO8 y LTO9 en forma concurrente. - La librería requerida deberá soportar escalar hasta 21 tapes drives como mínimo, a partir de módulos de expansiones adicionales.
Slots y estaciones de Ingreso/Salida de cintas	- La librería deberá incluir cuarenta (40) slots para cartuchos de cinta magnética LTO en su máxima configuración.
Lector de barras y brazo robótico	- La configuración de la librería ofertada debe incluir la automatización de la manipulación, identificación (mediante etiquetas de código de barras) e inventario de cartuchos de cinta magnética LTO. - La configuración de la librería ofertada deberá incluir mínimo un (01) brazo robótico.
Cartuchos de cintas	- Debe incluir diez (10) cartuchos de cintas Ultrium 9 con sus etiquetas de código de barras. - Debe incluir como mínimo un (02) cartucho de limpieza.

Fuentes de poder y ventiladores	- Debe incluir fuentes de poder redundantes con la capacidad de instalar y sustituir las fuentes de poder en caliente.
Conectividad	- Cada tape drive LTO9 debe incluir como mínimo un (01) puerto en fibra canal (FC) para conectarse al servidor de backup solicitado, cada uno de estos puertos debe ser de 8 Gbps como mínimo. - Debe incluir como mínimo dos (02) puertos Ethernet para la gestión, cada uno de estos puertos debe ser de 10/100/1000 BASE-T como mínimo y deben tener soporte de protocolos IPv4 e IPv6.
Compatibilidad y actualización de firmware	- Debe ser compatible con el sistema operativo del servidor de backup solicitado. - Debe incluir la función de actualización del firmware de la Librería y de los tapes drives, sin que esta actividad afecte la operatividad de la totalidad de la Librería. - Compatibilidad con el software de backup solicitado.
Interfaces de administración y monitoreo	- Debe incluir una consola de administración. - Debe incluir una interfase de administración web browser y/o GUI. - La interface de administración de la librería debe incluir la función de mostrar el estado de la Librería y tapes drives. - Debe incluir la función de monitoreo y comunicación de alertas.
Consideraciones	- Todos los componentes, partes y accesorios, deben ser originales y nuevos. - El año de fabricación deberá ser como mínimo 2026.

41. Software de backup (01 Unidad)

- Tipo de licenciamiento por suscripción por 12 meses.
- Licenciamiento para proteger mínimo 80 cargas de trabajo (VMs, servidores físicos y estaciones).
- Debe ser compatible con software de hiperconvergencia.
- Compatibilidad con otros entornos como Microsoft Hyper-V, Windows Server (2016/2019/2022/2025) y distribuciones Linux (RHEL, SUSE, Ubuntu), etc.
- Soporte nativo para unidades de cinta LTO (hasta LTO-9) conectadas vía SAS o FC.
- Destinos de respaldo a disco, cinta, almacenamiento en red y nubes compatibles.
- La solución debería facilitar la recuperación de una copia de seguridad basada en agentes directamente en Google Platform, Amazon AWS o Microsoft Azure y Microsoft Azure Stack.
- Métodos de respaldo deben ser completos, incrementales y sintéticos. Programación flexible de tareas.
- Recuperación o restauración granular de archivos, VMs completas, objetos de aplicaciones.
- Optimizaciones como compresión, deduplicación, cambio por bloque, exclusiones, balanceo de carga.
- Cifrado en tránsito y en reposo. Control de acceso por roles. Registro de auditoría.
- La solución debe integrar analítica de seguridad a su consola proporcionada.
- La solución deberá asegurar las copias de seguridad en repositorios reforzados a prueba de malware y hackers con copias de seguridad inmutables, para prevenir el cifrado o eliminación por ransomware y debe admitir credenciales que se usan una sola vez y no ser almacenadas en la infraestructura de respaldo, así si el servidor de respaldo se ve comprometido, un atacante no puede obtener las credenciales y conectarse al repositorio reforzado.

- La solución debe ofrecer una Incident API que pueda ser consumida por cualquier herramienta de seguridad que al detectar un ataque o incidente pueda notificar del incidente y poder hacer un quick backup del equipo que está bajo ataque.
- La solución deberá asegurar las copias de seguridad en repositorios reforzados a prueba de malware y hackers con copias de seguridad inmutables, para prevenir el cifrado o eliminación por ransomware y debe admitir credenciales que se usan una sola vez y no ser almacenadas en la infraestructura de respaldo, así si el servidor de respaldo se ve comprometido, un atacante no puede obtener las credenciales y conectarse al repositorio reforzado
- La solución debe permitir el escaneo in-line de los backups con bajo impacto utilizando una base de datos de más de 4000 cepas de malware que se actualiza automáticamente.
- Consola de gestión gráfica web o cliente local. Reportes, alertas y administración centralizada.
- Escalabilidad, capacidad de ampliar licencias sin reinstalación.

Ciberseguridad

42. Firewalles NGFW Perimetral (02 Unidades)

- La solución debe ser ofrecida en alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones técnicas.
- Deberá tener un rendimiento de Prevención de Amenazas de 28 Gbps cuando opera en simultáneo: Application Control, firewall, IPS, Antivirus/Anti-Bot/Antispyware o 14 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7) teniendo las siguientes funcionalidades habilitadas de manera simultánea: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. La solución debe operar bajo una arquitectura de procesamiento único donde todas las funciones de seguridad se apliquen simultaneamente sobre el mismo flujo de tráfico. El postor deberá presentar documentación pública del fabricante que sustente el cumplimiento de la medición. No se aceptarán cartas de fabricante como sustentos para el cumplimiento del performance y condiciones de medición solicitadas.
- El equipo debe soportar como mínimo 20 millones de sesiones concurrentes medidas con transacciones TCP o 2.5 millones medidas con transacciones HTTP.
- El equipo debe soportar 800 mil nuevas sesiones por segundo medidas con transacciones TCP o 200 mil nuevas sesiones por segundo medidas con transacciones HTTP.
- Debe incluir mínimo 12 interfaces de 1G/2.5G/5G/10G RJ-45, 10 interfaces de 10Gbps SFP/ SFP+, 4 interfaces de 25Gbps SFP28 y 2 interfaces de 40G/100GGbps QSFP28.
- Debe contar con una interfaz de cobre RJ45 dedicada para la gestión del equipo
- Debe contar con 02 interfaces dedicadas para la alta disponibilidad.
- Debe contar con disco interno de estado sólido de 480 SSD.
- Debe contar con dos fuentes de poder redundantes.
- Debe estar licenciado y habilitado en simultaneo las funcionalidades: Firewall, IPS, Antivirus de red, Filtrado URL, Control de aplicaciones, identificación de usuarios, identificación y perfilado de dispositivos IoT/OT, prevención de Bots y amenazas DNS, SDWAN y Sandboxing cloud.
- El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- Capacidad de inspeccionar el contenido en túneles GRE, opcionalmente GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.
- Deberá soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based

forwarding, dual-stack, QoS y/o DSCP, NAT64, LLDP, BFD, DHCPv6 Relay, SNMP, opcionalmente ECMP y SLAAC

- La plataforma propuesta por el fabricante debe contar con certificación USGv6-r1 para las pruebas de Firewall, IDS e IPS.
- Debe realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas.
- Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.
- La solución deberá contar con capacidades nativas de auditoría y versionado de cambios de reglas de seguridad, permitiendo visualizar el historial de modificaciones, identificar usuario, fecha y acción realizada, así como consultar el estado previo y posterior de las reglas y comparar versiones de configuración. Estas funcionalidades deberán estar integradas en el propio equipo, sin requerir herramientas externas.
- Debe soportar la configuración de alta disponibilidad Activo/Pasivo, con despliegues de los equipos tanto en modo transparente y/o como en modo capa 3 (L3).
- Deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, RC4, AES128, AES256, CHACHA20-POLY1305; MD5, SHA1, SHA256, SHA384.
- Capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos y/o no fiables, a pesar de no descifrar el tráfico.
- Debe contar con un dashboard que muestre gráficamente la proporción del tráfico descifrado, aplicaciones y dominios con descifrado correcto, errores de descifrado.
- Debe contar con un panel de logs dedicados a monitorear el tráfico de descifrado SSL/TLS, estos logs deberán permitir una identificación rápida de problemas del descifrado.
- Desde la consola gráfica deberá mostrar todo el detalle de la sesión SSL/TLS identificada, tales como IP origen y destino, subject common name, issuer common name, server name indication, datos del certificado digital (fecha de expiración, serial number), versión de TLS, algoritmo asimétrico, algoritmo simétrico, hash, estado del descifrado (correcto o con error), motivo del error del descifrado. Este detalle de logs no deberá afectar el performance del equipo.
- Reconocer por lo menos 4500 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
- Las aplicaciones deberán estar clasificadas en al menos 30 categorias y/o subcategorias, de tal manera que se puedan configurar políticas en base al tipo de aplicación.
- Las aplicaciones deberán contar con atributos descriptivos tales como tipo, nivel de riesgo y etiqueta.
- Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.
- Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión y/o a través de una herramienta tercera del fabricante.
- Deberá contar con un módulo de aprendizaje que permita migrar las políticas basadas en puertos específicos y políticas con puertos ALL/ANY, a políticas basadas en aplicaciones.
- El módulo de aprendizaje deberá ser específico por cada política de seguridad.
- El módulo de aprendizaje deberá mostrar el nombre de la(s) aplicación(es) que han pasado por una política de seguridad, fecha de primera y última ocurrencia y volumen de datos transferido por cada aplicación.
- Deberá contar con un wizard que permita convertir una política basada en puertos (capa 4) a una política basada en aplicaciones (capa 7) en base al aprendizaje realizado.

- La solución debe permitir la creación de políticas de seguridad basadas en la identidad del usuario y grupo al cual pertenece, a través de la integración de servicios de autenticación como Active Directory, Novell eDirectory, Open LDAP y base de datos local.
- Debe contar con varios mecanismos para la identificación del usuario y la dirección IP del equipo en donde se encuentra autenticado. Como mínimo deberá poder integrarse a las siguientes plataformas para cubrir este requerimiento:
    - Eventos de login gestionados en Domain Controller y/o Microsoft Exchange.
    - Capacidad de leer eventos de login y logout usando el protocolo WinRM.
    - Terminal Server de Microsoft o Citrix
    - Consultando directamente a cada estación de trabajo a través del protocolo WMI
    - Lectura de la cabecera XFF al integrarse con soluciones terceras de Proxy
    - Capacidad de extraer la información de IP y usuarios a través de la lectura y extracción de datos del tráfico syslog.
- Deberá contar con un componente que permita integrarse a diversas plataformas de identidades tales como Azure LDAP, Google Directory, Okta, Cisco Duo, PingID.
- Deberá contar con un mecanismo que permita identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, inclusive si el tráfico entre la potencial víctima y su servidor DNS utilizado no pasa por el NGFW.
- Los algoritmos basados en inteligencia artificial deberán ser capaces de prevenir ataques como DGA (Domain Generation Algorithm) Random y de Diccionario, DNS Tunneling, Fast Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS.
- Soportar proteger contra ataques de día cero y malware desconocido a través de un servicio de sandboxing del fabricante provisto desde su nube (Debe soportar emulacion en Windows, MacOS y Linux).
- El sandbox debe identificar los ataques de phishing al momento de emular los potenciales archivos maliciosos en: swf, html, lnk y js.
- Luego del análisis realizado por el sandbox, éste deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.
- El análisis en tiempo real deberá determinar si la página web desconocida (no categorizada en la base de datos del fabricante), tiene contenido javascript malicioso, phishing, actividad de command and control y otros tipos de contenido malicioso.
- Debe contar con medidas de antievasión como Cloaking, Captcha falsos, codificación de caracteres HTML, entre otros.
- Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de robo de credenciales.
- Debe incluir capacidades de identificación y perfilado de dispositivos conectados a la red (incluyendo dispositivos IoT/OT), permitiendo su clasificación, evaluación de riesgo y aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, sin requerir la instalación de agentes adicionales.
- La solución debe incluir la capacidad de poder monitorear la salud de los enlaces en términos de jitter, latencia y pérdida de paquetes, tomando decisiones inteligentes de enrutamiento basado en la condición de los enlaces de manera dinámica.
- Debe permitir realizar la detección y bloqueo de archivos por su extensión.
- Deberá integrarse de forma nativa con la plataforma SIEM, proporcionando telemetría de seguridad enriquecida y correlacionada en tiempo cercano a real, incluyendo como mínimo información de aplicaciones de red en capa 7, cabeceras HTTP, consultas DNS, tráfico DHCP y atributos de dispositivos (tipo, categoría, fabricante y sistema operativo). Dicha telemetría deberá ser consistente y utilizable directamente para análisis, correlación y automatización, sin requerir procesos adicionales de normalización, parsing complejo o integraciones personalizadas.
- En total para la solución de Firewall externo, se debe incluir 04 transceiver de SFP+ 10Gbps MMF.

- En total para la solución de Firewall externo, se debe incluir 04 transceiver de SFP28 25Gbps MMF.

43. Firewall Interno (02 Unidades)

- La solución debe ser ofrecida en alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones técnicas.
- Deberá tener un rendimiento de Prevención de Amenazas de 110 Gbps cuando opera en simultáneo: Application Control, firewall, IPS, Antivirus/Anti-Bot/Antispyware o 48 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7) teniendo las siguientes funcionalidades habilitadas de manera simultánea: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. La solución debe operar bajo una arquitectura de procesamiento único donde todas las funciones de seguridad se apliquen simultaneamente sobre el mismo flujo de tráfico. El postor deberá presentar documentación pública del fabricante que sustente el cumplimiento de la medición, el cual será validado durante la implementación, según la metodología que sustente el Proveedor.
- El equipo debe soportar como mínimo 80 millones de sesiones concurrentes medidas con transacciones TCP o 7 millones medidas con transacciones HTTP.
- El equipo debe soportar 1.2 millones de nuevas sesiones por segundo medidas con transacciones TCP o 370 mil nuevas sesiones por segundo medidas con transacciones HTTP.
- Debe incluir mínimo 8 interfaces de 1G/2.5G/5G/10G RJ-45, 12 interfaces de 1G/10G SFP/ SFP+, 4 interfaces de 25Gbps SFP28 y 4 interfaces de 40G/100GGbps QSFP28.
- Debe contar con una interfaz de cobre RJ45 dedicada para la gestión del equipo
- Debe contar con 02 interfaces dedicadas para la alta disponibilidad.
- Debe contar con disco interno de estado sólido de 480 SSD.
- Debe contar con dos fuentes de poder redundantes.
- Debe estar licenciado y habilitado en simultaneo las funcionalidades: Firewall, IPS, Antivirus de red, Control de aplicaciones, identificación de usuarios, identificación y perfilado de dispositivos IoT/OT, prevención de Bots y amenazas DNS y Sandboxing cloud.
- El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- Capacidad de inspeccionar el contenido en túneles GRE, opcionalmente GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.
- Deberá soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based forwarding, dual-stack, QoS y/o DSCP, NAT64, LLDP, BFD, DHCPv6 Relay, SNMP, opcionalmente ECMP y SLAAC
- La plataforma propuesta por el fabricante debe contar con certificación USGv6-r1 para las pruebas de Firewall, IDS e IPS.
- Debe realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas.
- Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.
- La solución deberá contar con capacidades nativas de auditoría y versionado de cambios de reglas de seguridad, permitiendo visualizar el historial de modificaciones, identificar usuario, fecha y acción realizada, así como consultar el estado previo y posterior de las reglas y comparar versiones de configuración. Estas funcionalidades deberán estar integradas en el propio equipo, sin requerir herramientas externas.

- Debe soportar la configuración de alta disponibilidad Activo/Pasivo, con despliegues de los equipos tanto en modo transparente y/o como en modo capa 3 (L3).
- Deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, RC4, AES128, AES256, CHACHA20-POLY1305; MD5, SHA1, SHA256, SHA384.
- Capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos y/o no fiables, a pesar de no descifrar el tráfico.
- Debe contar con un dashboard que muestre gráficamente la proporción del tráfico descifrado, aplicaciones y dominios con descifrado correcto, errores de descifrado.
- Debe contar con un panel de logs dedicados a monitorear el tráfico de descifrado SSL/TLS, estos logs deberán permitir una identificación rápida de problemas del descifrado.
- Desde la consola gráfica deberá mostrar todo el detalle de la sesión SSL/TLS identificada, tales como IP origen y destino, subject common name, issuer common name, server name indication, datos del certificado digital (fecha de expiración, serial number), versión de TLS, algoritmo asimétrico, algoritmo simétrico, hash, estado del descifrado (correcto o con error), motivo del error del descifrado. Este detalle de logs no deberá afectar el performance del equipo.
- Reconocer por lo menos 4500 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
- Las aplicaciones deberán estar clasificadas en al menos 30 categorias y/o subcategorias, de tal manera que se puedan configurar políticas en base al tipo de aplicación.
- Las aplicaciones deberán contar con atributos descriptivos tales como tipo, nivel de riesgo y etiqueta.
- Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.
- Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión y/o a través de una herramienta tercera del fabricante.
- Deberá contar con un módulo de aprendizaje que permita migrar las políticas basadas en puertos específicos y políticas con puertos ALL/ANY, a políticas basadas en aplicaciones.
- El módulo de aprendizaje deberá ser específico por cada política de seguridad.
- El módulo de aprendizaje deberá mostrar el nombre de la(s) aplicación(es) que han pasado por una política de seguridad, fecha de primera y última ocurrencia y volumen de datos transferido por cada aplicación.
- Deberá contar con un wizard que permita convertir una política basada en puertos (capa 4) a una política basada en aplicaciones (capa 7) en base al aprendizaje realizado.
- La solución debe permitir la creación de políticas de seguridad basadas en la identidad del usuario y grupo al cual pertenece, a través de la integración de servicios de autenticación como Active Directory, Novell eDirectory, Open LDAP y base de datos local.
- Debe contar con varios mecanismos para la identificación del usuario y la dirección IP del equipo en donde se encuentra autenticado. Como mínimo deberá poder integrarse a las siguientes plataformas para cubrir este requerimiento:
    - Eventos de login gestionados en Domain Controller y/o Microsoft Exchange.
    - Capacidad de leer eventos de login y logout usando el protocolo WinRM.
    - Terminal Server de Microsoft o Citrix
    - Consultando directamente a cada estación de trabajo a través del protocolo WMI
    - Lectura de la cabecera XFF al integrarse con soluciones terceras de Proxy
    - Capacidad de extraer la información de IP y usuarios a través de la lectura y extracción de datos del tráfico syslog.
- Deberá contar con un componente que permita integrarse a diversas plataformas de identidades tales como Azure LDAP, Google Directory, Okta, Cisco Duo, PingID.
- Deberá contar con un mecanismo que permita identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, inclusive si el tráfico entre la potencial víctima y su servidor DNS utilizado no pasa por el NGFW.
- Los algoritmos basados en inteligencia artificial deberán ser capaces de prevenir ataques como DGA (Domain Generation Algortihm) Random y de Diccionario, DNS Tunneling, Fast

Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS.

- Soportar proteger contra ataques de día cero y malware desconocido a través de un servicio de sandboxing del fabricante provisto desde su nube (Debe soportar emulacion en Windows, MacOS y Linux).
- El sandbox debe identificar los ataques de phishing al momento de emular los potenciales archivos maliciosos en: swf, html, lnk y js.
- Luego del análisis realizado por el sandbox, éste deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- Debe incluir capacidades de identificación y perfilado de dispositivos conectados a la red (incluyendo dispositivos IoT/OT), permitiendo su clasificación, evaluación de riesgo y aplicación de políticas de seguridad basadas en tipo, comportamiento o nivel de riesgo del dispositivo, sin requerir la instalación de agentes adicionales.
- Debe permitir realizar la detección y bloqueo de archivos por su extensión.
- Deberá integrarse de forma nativa con la plataforma SIEM, proporcionando telemetría de seguridad enriquecida y correlacionada en tiempo cercano a real, incluyendo como mínimo información de aplicaciones de red en capa 7, cabeceras HTTP, consultas DNS, tráfico DHCP y atributos de dispositivos (tipo, categoría, fabricante y sistema operativo). Dicha telemetría deberá ser consistente y utilizable directamente para análisis, correlación y automatización, sin requerir procesos adicionales de normalización, parsing complejo o integraciones personalizadas.
- En total para la solución de Firewall interno, se debe incluir 08 transceiver de SFP+ 10Gbps MMF.
- En total para la solución de Firewall interno, se debe incluir 08 transceiver de SFP28 25Gbps MMF.

44. Consola de analítica y reportes (01 Unidades)

- Debe incluir una consola de analítica y reportería local provista en la nube del fabricante, que debe de estar licenciada para poder administrar todos los NGFW solicitados.
- La solución debe ser una plataforma unificada de gestión y operaciones impulsada por IA para toda la infraestructura de seguridad de red, permitiendo la gestión de politicas y gestión de eventos de los firewalls perimetrales y los firewalls internos
- La solución deberá contar con una plataforma de almacenamiento centralizado de logs de seguridad, que permita la ingesta continua de telemetría sin restricciones por volumen de datos y que incluya una capacidad de retención de logs de al menos un (01) año.
- La capacidad de almacenamiento deberá estar incluida de forma nativa en el licenciamiento de la solución, sin requerir dimensionamiento previo ni adquisición incremental de almacenamiento para cumplir con el período de retención requerido.
- Con el objetivo de que la Institución cuente con autonomía para evaluar si el NGFW se encuentra configurado acorde a las buenas prácticas y evitar que el postor sea juez y parte del control de calidad de ésta, la consola de analítia y reportes debe permitir evaluar automáticamente si el NGFW se encuentra configurado acorde a las buenas prácticas del fabricante en materia de los diferentes módulos de seguridad que se le haya activado.
- Esta plataforma deberá ser única y consolidar la información de todos los NGFW incluidos en este proyecto.
- Debe contar con gráficos ejecutivos que permitan mostrar el nivel de adopción de los módulos de seguridad del NGFW en las políticas de seguridad.
- Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red.
- La solución debe tener Alertas de Salud del Hardware, Software, Licencias
- La solución debe detectar vulnerabilidades de software de los NGFW
- La solución debe tener análisis de causa raíz para problemas de rendimiento.
- La solución debe predecir averías y evitar el impacto en la red por interrupciones del firewall y conexiones de servicio con pronósticos y recomendaciones de soluciones hasta 90 días antes de una interrupción.

- La solución debe tener Análisis de Mejores Prácticas del fabricante.
- La solución debe tener Verificaciones de Configuración Personalizadas.
- La solución debe ofrecer mejores prácticas en tiempo real y proactivas con la aplicación.
- La solución debe tener un Analizador de Políticas (ML).
- La solución debe tener Optimizador de Políticas (ML).
- La solución debe aprovechar el análisis impulsado por IA para detectar, resolver y optimizar anomalías en las políticas, como políticas ocultas y redundantes, y reglas demasiado permisivas o no utilizadas.
- La solución debe mejorar la postura de seguridad con recomendaciones de mejores prácticas integradas y mantener el cumplimiento de los estándares de la industria y de InfoSec.
- La solución debe tener verificaciones de mejores prácticas predefinidas.
- La solución debe tener verificaciones de mejores prácticas personalizadas.
- La solución debe tener recomendaciones y aplicación de mejores prácticas en línea para cerrar las brechas de seguridad existentes.
- La solución debe tener limpieza de configuración de reglas y objetos no utilizados.
- La solución debe proporcionar recomendaciones en tiempo real y análisis automatizado sobre deficiencias de implementación, configuración y seguridad para una resolución de problemas más rápida.
- La solución debe permitir evaluaciones diarias de la configuración para identificar brechas, mantener las mejores prácticas y garantizar una postura de seguridad óptima.
- La solución debe garantizar el cumplimiento de los estándares de la industria (CIS, NIST) y verificaciones personalizadas para un cumplimiento continuo, reduciendo el riesgo.
- La solución debe optimizar la gestión de configuraciones y políticas en todos los puntos de aplicación desde una única interfaz.
- La solución debe proporcionar recomendaciones de actualización de software basadas en las funciones habilitadas y las vulnerabilidades CVE conocidas para NGFW.
- La solución debe tener paneles para Resumen Ejecutivo, Sandboxing, Seguridad DNS, SD-WAN y personalizados.
- La solución debe incluir un asistente basado en inteligencia artificial que permita realizar consultas en lenguaje natural para resolución de problemas, consultas técnicas, explicación de alertas y asistencia en la configuración de políticas de seguridad.
- La solución debe incluir capacidades de asistencia basada en inteligencia artificial que permitan analizar eventos de seguridad y generar reportes mediante consultas asistidas y visualización interactiva de datos.

45. XDR (Extended Detection & Response) – 01 solución

- La solución deberá ser de tipo XDR (Extended Detection & Response) y permitir la operación centralizada de capacidades de detección, análisis y respuesta para endpoints, formando parte de una plataforma unificada de operaciones de seguridad que integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.
- La solución XDR deberá permitir la integración con la solución SIEM propuesta, habilitando el envío y consumo de telemetría de seguridad, de forma nativa y estructurada, sin requerir desarrollos personalizados o procesos complejos de normalización, garantizando su uso para correlación, análisis y respuesta automatizada.
- Se deberán licenciar 1000 agentes XDR que incluyan todas las capacidades descritas en el requerimiento.
- El agente deberá ser ligero, que incluso pueda convivir con cualquier otro software instalado en el endpoint.
- El agente deberá soportar las siguientes versiones de sistemas operativos como mínimo:
    - Windows 11 professional
    - Windows Server 2025
    - MacOS 26

- Deberá estar protegido ante intentos de desinstalación o manipulación del agente.
- Deberá ser posible definir diferentes password de seguridad para diferentes grupos de endpoints.
- Deberá contar con capacidades nativas de prevención de exploits basadas en la detección y bloqueo de técnicas de explotación que afecten a sistemas Windows (Workstations y Servidores), Linux y MacOS. No debe depender de firmas por CVEs, ni heurísticas tradicionales.
- La capacidad de bloqueo de técnicas de explotación no deberá limitarse únicamente a aplicaciones predeterminadas. La plataforma deberá permitir extender la protección a procesos adicionales, incluyendo aplicaciones desarrolladas internamente (in-house), permitiendo especificar explícitamente los nombres de los procesos a proteger.
- Deberá proteger contra la explotación de vulnerabilidades del sistema operativo y de aplicaciones, incluso cuando estas no cuenten con el parche de seguridad instalado, mitigando riesgos asociados a ventanas de exposición.
- Los mecanismos de protección contra vulnerabilidades deberán ser independientes de la existencia o identificación de un CVE, permitiendo detectar y bloquear intentos de explotación de vulnerabilidades conocidas y de día cero, aun cuando estas no cuenten con un identificador público.
- El agente dedeberá ser capaz de enviar automáticamente archivos sospechosos y/o desconocidos a un entorno de sandbox para su emulación y análisis, esta capacidad deberá estar soportada al menos para Windows, Linux y MacOS.
- El entorno de sandbox podrá ser provisto por el mismo fabricante de la solución o por un tercero, siempre que se encuentre debidamente integrado con la plataforma.
- El sandbox deberá soportar el análisis de al menos 500,000 archivos diarios y permitir el análisis de archivos de hasta 100 MB de tamaño.
- Debe permitir gestionar los puertos USB que permitan conectar dispositivos como: discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles, unidades lectoras de discos floppy externas.
- Las políticas de control de dispositivos deben poder asignar a nivel de hostnames, grupos de hosts, usuarios, grupos de Active Directory.
- Debe de permitir la creación de excepciones temporales a partir de una alerta registrada, para permitir el dispositivo solo durante un tiempo configurable
- Toda la telemetría colectada del endpoint se deberá realizar de manera continua y en línea, así exista o no exista una alerta de seguridad de por medio, el agente debe colectar la siguiente telemetría, enviarlo automáticamente y de manera cifrada hacia la nube de la solución y almacenarse en formato estructurado para labores de analítica y threat hunting.
- El agente deberá capturar, como mínimo, la siguiente telemetría para equipos Windows:
    - Ejecución de procesos, incluyendo tiempo de inicio y tamaño del archivo.
    - Operaciones sobre archivos: creación, escritura, modificación, renombrado y eliminación.
    - Carga de DLLs, incluyendo ruta completa, dirección base, ID del proceso, tamaño de imagen, firma digital y hashes MD5 y SHA256.
    - Creación y finalización de procesos, con atributos como: proceso padre, PID, ruta completa, argumentos de línea de comando, hashes y detalles de firma o certificado.
    - Inyección de hilos, incluyendo ID del hilo padre, ID del hilo creado o terminado y proceso originador.
    - Interacciones de red, incluyendo IP y puertos origen/destino, estado de conexión (exitosa o fallida), protocolo (TCP/UDP), solicitudes y respuestas de DNS y actividad HTTP.
    - Estadísticas de red, considerando volúmenes de tráfico TCP de subida y descarga.
    - Acciones sobre el Registro de Windows, incluyendo creación, modificación, eliminación, restauración y guardado de claves y valores, con ruta y datos afectados.

  - Eventos de sesión del sistema, tales como inicio y cierre de sesión, conexión y desconexión.
  - Eventos .NET, tales como carga de DLL, intentos de bypass de AMSI.
  - Llamadas RPC y llamadas al sistema (syscalls).
  - Eventos de Windows, incluyendo logs de Seguridad y Aplicación, con soporte para al menos 60 tipos de eventos, entre ellos: 4880, 4881, 4896, 4898, 6272, 6280, 4624, 4625, 4634, 4647, 4649, 4776, 4800, 4801, 4720, 4722, 4723, 4724, 4725, 4726, 4727, 4731, 4754, 4728, 4732, 4756, 4735, 4737, 4755, 4764, 4741, 4742, 4743, 4698.
- El mismo agente de Endpoint Protectión deberá ser capaz de colectar la siguiente telemetría para equipos MacOS y Linux:
  - Logs de eventos de autenticación
  - Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
  - Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma digital.
  - Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
  - Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.
- Deberá poder almacenar toda la telemetría de los endpoints por al menos 30 días.
- La solución deberá presentar una secuencia gráfica del incidente de seguridad, construida automáticamente mediante los mecanismos de inteligencia artificial de la plataforma, que correlacione múltiples alertas y eventos con el objetivo de identificar la causa raíz del incidente.
- La secuencia gráfica deberá mostrar la información de los procesos correlacionados, incluyendo como mínimo: ruta de ejecución, usuario que ejecutó el proceso, entidad firmante del ejecutable, hash SHA256, veredicto del análisis en sandbox y línea de comandos utilizada., timestamp, hostname, dirección IP local y remota, TTPs de MITRE ATT&CK, actividad de red generada por cada proceso, actividad de archivos y directorios, actividad a nivel de claves de registro, llamadas RPC, Syscalls, Event Logs generados.
- La solución deberá permitir mostrar el catálogo de reglas de detección por comportamiento predefinidas en la plataforma, de tal forma que éstas se puedan clonar y crear reglas personalizadas de detección.
- La solución deberá permitir mostrar el catálogo de reglas de detección basadas en inteligencia artificial (IA), los cuales no deberán estar basadas en reglas estáticas, sino en el aprendizaje individual de cada activo.
- La solución deberá permitir la creación de reglas personalizadas de detección, basadas en el comportamiento de usuarios y hosts. Para ello se podrá hacer uso de cualquier evento colectado de telemetría.
- Deberá poder generar un inventario de las aplicaciones instaladas en las computadoras con sistema operativo Windows, MacOS y Linux
- Deberá generar un inventario de características de hardware del endpoint, como mínimo cantidad de memoria RAM; tipo, marca y capacidad de procesador; almacenamiento del disco duro; identificar si es servidor, desktop o laptop; sistema operativo y arquitectura.
- Deberá poder listar los usuarios locales creados en el endpoint y su respectivo estado (activo o inactivo)
- Deberá poder listar los autoruns, servicios/daemons y unidades o carpetas compartidas.
- Deberá ser capaz de guardar un histórico diario de estos inventarios, para poder comparar cambios que hubiesen ocurrido. Este histórico deberá estar disponible por al menos 30 días.

- A partir de la telemetría recolectada de los endpoints y de la información contextual de usuarios y hosts obtenida mediante las integraciones, la plataforma deberá aprender de forma automática un perfil base (baseline) del comportamiento de cada activo.
- Los perfiles de comportamiento deberán ser generados dinámicamente mediante algoritmos de aprendizaje de máquina no supervisado, permitiendo modelar el comportamiento normal sin necesidad de reglas predefinidas o umbrales estáticos
- Con base en el comportamiento aprendido, el módulo de UEBA deberá ser capaz de detectar y alertar actividades inusuales o desviaciones significativas respecto al perfil base establecido. Deberá tener al menos 150 casos de uso nativos, generados por machine learning, incluyendo los siguientes:
    - Comandos anómalos ejecutados en el endpoint
    - Múltiples procesos LOLBINs ejecutados
    - Procesos raros ejecutados sobre el endpoint
    - Eventos de Pass the ticket
    - Proceso conectándose a un sitio externo inusual
    - Comandos de powershell inusuales
    - Cifrado de datos sospechoso en el endpoint
    - Carga de driver inusual
    - Conexión anómala usando WMI
    - Servicio detenido de manera inusual
    - Tráfico LDAP generado desde un proceso inusual
    - Transferencia inusual de archivos por SMB
- La plataforma deberá asignar un puntaje de riesgo (risk score) a usuarios y hosts, considerando la frecuencia, severidad y correlación de eventos sospechosos y/o anómalos, con el objetivo de facilitar el triage y la priorización de incidentes.

46. ZTNA (Zero Trust Network Access) – 01 Solución

- La solución ZTNA deberá proporcionar acceso seguro a aplicaciones mediante un cliente de acceso remoto, aplicando políticas basadas en identidad de usuario, aplicación y contexto, sin exponer la red interna.
- La solución ZTNA deberá ser una solución dedicada o formar parte los NGFW Perimetrales. Debiendo integrarse a la Consola de Analítica y Reportes para permitir la aplicación de políticas de seguridad y control de acceso de manera unificada.
- La solución ZTNA debe soportar al menos 200 usuarios, debiendo incluir el licenciamiento necesario.
- Deberá ser capaz de validar si el equipo que intenta acceder a algún recurso de red (IP o IPs destino) cuenta con una postura de seguridad adecuada.
- La restricción al recurso de red debe ser personalizable, es decir, deberá permitir acceder de manera total o parcial al recurso de red destino en base al nivel de cumplimiento de la postura de seguridad del equipo. Por ejemplo, si cumple parcialmente con la postura de seguridad únicamente se le dará acceso para hacer PING a un servidor, sí cumple completamente podrá acceder vía RDP.
- La validación de la postura de seguridad del endpoint deberá ser continua; el NGFW automáticamente deberá restringir el acceso si es que luego de la conexión establecida el equipo modifica su postura de seguridad.
- Como mínimo la postura de seguridad del endpoint deberá validar lo siguiente:
    - Sistema operativo del equipo
    - Serial number del equipo
    - Pertenencia al dominio corporativo
    - Software antivirus instalado y habilitado en tiempo real
    - Software antivirus con la base de datos de firmas actualizada en un número de días personalizable
    - Haber realizado un escaneo del malware en un equipo dentro de un número de días personalizable
    - Marca del software antivirus
    - Parche de seguridad instalado, según su nivel de criticidad, o en su defecto mostrar las vulnerabilidades del endpoint (por CVE).

  - Firewall de host habilitado
  - Permitir validaciones personalizadas en base a registros de REGEDIT
- Las políticas de validación de postura del endpoint deberán poder ser aplicadas a un grupo de usuarios o direcciones IP.
- Deberá permitir configurar un mensaje personalizado, el cual permita notificar al usuario que controles no está cumpliendo.
- Esta verificación se podrá realizar a través de un agente instalado en los endpoints. Debe tener soporte como mínimo para Windows y MacOS.
- La solución podrá integrarse a una plataforma de Network Access Control (NAC) para cumplir los requerimientos listados. Se deja libertar al postor de elegir la plataforma NAC que se pueda integrar.
- Debe tener capacidad de integrarse con plataformas de Doble Factor de Autenticación (2FA).
- Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN, incluyendo el soporte de Split DNS.
- El Split Tunnel debe permitir elegir el tipo tráfico que se enrutará por el túnel VPN, basado en el nombre de la Aplicación y el Dominio.
- Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
  - Antes del usuario se autentique en la estación.
  - Después de la autenticación del usuario en la estación usando Single Sign On (SSO).
  - A demanda, de forma manual por parte del usuario.
- El agente de VPN client-to-site debe ser compatible al menos con: Windows 10, Windows 11 professional
- , MacOS X, Linux, Android y iOS.
- La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada, de manera manual y automática. Los equipos en cuarentena no deberán tener conexión con ningún recurso de red protegido por la solución. Esta capacidad deberá tener cobertura dentro de la red interna, sin necesidad de hacer túneles VPN.
- Para el caso de usuarios externos, dispositivos no gestionados o escenarios de acceso temporal, la solución deberá permitir el acceso seguro a aplicaciones críticas mediante navegador web, sin requerir la instalación de agentes en el endpoint. Esto a fin de reducir la superficie de ataque, evitar la exposición de la red interna y garantizar un control granular sobre el acceso y uso de la información sensible.
- La solución ZTNA adicionalmente deberá incluir capacidades de acceso seguro a aplicaciones a través de navegador web (agentless), permitiendo el acceso controlado a recursos críticos sin requerir la instalación de software en el endpoint.
- El acceso ZTNA mediante navegador web seguro debe estar licenciada para un minimo de 200 usuarios.
- El acceso ZTNA mediante navegador web deberá estar basado en validación de identidad del usuario y contexto de la sesión, permitiendo aplicar políticas de seguridad consistentes con las definidas para el acceso mediante cliente.
- El acceso ZTNA mediante navegador web deberá permitir la aplicación de controles granulares sobre la sesión web, incluyendo como mínimo restricciones de descarga, carga de archivos, copiado/pegado, impresión y transferencia de información.
- Este navegador web debe permitir el acceso seguro desde dispositivos no gestionados o de terceros, garantizando el aislamiento de la sesión y la protección de la información accedida.
- El acceso mediante navegador web seguro deberá integrarse con la plataforma de analítica y reportes, permitiendo la aplicación consistente de políticas de acceso y controles de seguridad definidos para el modelo ZTNA.
- El navegador web seguro deberá permitir la visibilidad y registro de las actividades realizadas durante la sesión, incluyendo usuario, aplicación accedida, acciones ejecutadas y duración de la sesión, para fines de auditoría y análisis.
- El navegador web seguro deberá permitir la aplicación de controles basados en tipo de aplicación (por ejemplo, aplicaciones web internas o SaaS), sin exponer directamente la red interna.

47. Seguridad para Correo Electrónico – 01 solución

- El servicio de correo electrónico es Zimbra, por lo que la solución deberá integrarse mediante protocolos SMTP, operando como gateway de correo electrónico a través de registros MX, permitiendo la inspección completa del tráfico entrante y saliente antes de su entrega.
- La solución deberá proteger un mínimo de 1000 buzones de correo electrónico bajo un modelo de licenciamiento por usuario, permitiendo escalabilidad automática en arquitectura SaaS, sin requerir adquisición de infraestructura adicional ni afectar el rendimiento del servicio
- La solución deberá implementar un modelo de análisis multicapa basado en riesgo, que combine técnicas de reputación, machine learning, análisis heurístico y análisis dinámico mediante sandboxing selectivo, permitiendo evaluar los correos electrónicos y sus componentes de manera eficiente según su nivel de riesgo.
- La solución deberá analizar todas las URLs y archivos adjuntos contenidos en los correos electrónicos entrantes mediante un modelo de análisis multicapa basado en riesgo, que combine técnicas de reputación, análisis estático y análisis dinámico selectivo para la detección de amenazas conocidas y desconocidas.
- La solución deberá permitir a los administradores acceder a información detallada del análisis de cada correo electrónico procesado, incluyendo trazabilidad completa del mensaje, clasificación de la amenaza, motores de detección utilizados y las razones específicas por las cuales el correo ha sido identificado como malicioso
- La solución deberá permitir la clasificación diferenciada de tipos de correo no deseado, incluyendo spam, graymail y campañas masivas, así como la aplicación de políticas específicas para cada categoría
- La solución deberá incorporar inteligencia de amenazas global que combine fuentes internas y externas, análisis basado en aprendizaje automático y correlación de eventos a gran escala, permitiendo la detección proactiva de amenazas conocidas y desconocidas en el tráfico de correo electrónico.
- La solución deberá incorporar motores antivirus como parte de una arquitectura de seguridad multicapa, permitiendo la detección de amenazas conocidas en el tráfico de correo electrónico, complementadas con mecanismos avanzados de análisis para la identificación de amenazas emergentes y sofisticadas.
- La solución deberá incorporar capacidades avanzadas de detección que no dependan exclusivamente de firmas tradicionales, utilizando inteligencia de amenazas, aprendizaje automático, análisis de comportamiento y correlación global para identificar amenazas conocidas, variantes y campañas emergentes.
- La solución deberá ofrecer protección frente a phishing, spear phishing, robo de identidad y phishing mediante códigos QR, utilizando análisis lingüístico del contenido, visión por ordenador, aprendizaje automático, evaluación de reputación y correlación de inteligencia de amenazas para identificar intentos de engaño dirigidos a usuarios."
- La solución deberá brindar protección frente a ataques de tipo Business Email Compromise (BEC), mediante el uso de análisis contextual, comportamiento del remitente, inteligencia de amenazas y validación de mecanismos de autenticación como SPF, DKIM y DMARC.
- La solución deberá detectar y proteger contra ataques de suplantación (spoofing), incluyendo la identificación de suplantación de nombres visibles (display name spoofing), suplantación de dominios y ataques dirigidos a usuarios VIP, mediante análisis contextual y de comportamiento del remitente
- La solución deberá contar con mecanismos para proteger contra ataques de tipo zero-day y N-day, mediante el uso de análisis de comportamiento, inteligencia de amenazas, machine learning y capacidades de análisis dinámico en entornos controlados.
- La solución deberá contar con mecanismos avanzados de protección de URLs que permitan analizar los enlaces contenidos en los correos electrónicos mediante técnicas como reescritura de URLs, evaluación de reputación en tiempo real y análisis dinámico en el momento de interacción del usuario (time-of-click), con el fin de identificar y bloquear enlaces maliciosos antes y después de su entrega al usuario final.
- La solución deberá contar con capacidades de análisis avanzado de archivos adjuntos mediante tecnología de sandboxing, integrada dentro de un modelo de protección multicapa que combine técnicas de análisis estático, reputación, machine learning y

análisis dinámico selectivo, permitiendo la detección de amenazas conocidas y desconocidas en archivos

- La solución deberá garantizar que los procesos de análisis de archivos adjuntos se realicen sin alterar su estructura ni contenido original, utilizando mecanismos de análisis seguros como entornos aislados (sandbox) y técnicas de inspección que operen sobre copias del archivo, manteniendo la integridad del contenido original
- La solución deberá ser capaz de detectar macros maliciosas y contenido sospechoso dentro de documentos adjuntos, mediante el uso de análisis de comportamiento, sandboxing e inteligencia de amenazas, permitiendo identificar actividades maliciosas y vectores de ataque embebidos en archivos.
- La solución deberá proporcionar herramientas de investigación que permitan analizar correos, archivos o enlaces previamente procesados, mediante interfaces de consulta y análisis desde la consola de administración
- La solución deberá ser capaz de analizar contenido comprimido y archivos embebidos dentro de los correos electrónicos, incluyendo estructuras anidadas, permitiendo identificar archivos, documentos y enlaces ocultos para su evaluación mediante mecanismos de análisis de seguridad multicapa
- La solución deberá ser capaz de identificar archivos protegidos por contraseña dentro de los correos electrónicos y aplicar políticas de seguridad configurables para su tratamiento, tales como bloqueo, cuarentena o entrega controlada, en caso de que el contenido no pueda ser inspeccionado
- La solución deberá ser capaz de analizar archivos comprimidos contenidos en los correos electrónicos, permitiendo extraer y evaluar su contenido mediante mecanismos de análisis de seguridad multicapa, con el fin de identificar amenazas ocultas en archivos y estructuras anidada
- La solución deberá contar con reconocimiento en reportes de analistas del mercado de seguridad de correo electrónico, tales como Magic Quadrant, Forrester Wave u otros estudios equivalentes, evidenciando su posicionamiento y capacidad de ejecución en el segmento
- La solución deberá ser nativa en la nube (cloud-native), operando bajo un modelo SaaS completamente alojado en infraestructura cloud, sin requerir la instalación de componentes on-premise, y permitiendo la integración con el servicio de correo mediante mecanismos estándar como SMTP/MX.
- La solución deberá operar bajo un modelo SaaS que garantice la actualización automática y continua de sus capacidades de seguridad, motores de detección e inteligencia de amenazas, sin requerir intervención manual por parte de la Entidad.
- La solución deberá operar bajo un modelo cloud-native que permita escalar automáticamente en función de la demanda, adaptándose al crecimiento de la Entidad sin requerir la adquisición de hardware adicional, y garantizando niveles adecuados de rendimiento y experiencia de usuario.
- La solución deberá permitir su implementación en modo de prevención de amenazas en línea (inline), inspeccionando el tráfico de correo electrónico antes de su entrega a los servidores, con el fin de detectar y bloquear amenazas antes de que lleguen al usuario final.
- La solución deberá operar mediante un modelo Secure Email Gateway (SEG) en modo inline, integrándose con el servicio de correo mediante registros MX, permitiendo la prevención de amenazas en tránsito antes de la entrega al usuario final.
- La solución deberá permitir el despliegue de la protección a nivel de dominio, aplicando controles de seguridad de manera centralizada sobre todos los usuarios.
- La solución deberá contar con una consola de administración centralizada que permita visualizar información detallada sobre incidentes de seguridad, reportes de amenazas y políticas aplicadas al tráfico de correo electrónico, proporcionando visibilidad completa para la gestión y monitoreo del servicio.
- La solución deberá permitir la definición y aplicación de políticas de control basadas en listas blancas y negras (whitelisting y blacklisting), utilizando parámetros como direcciones IP, dominios, remitentes, URLs y tipos de archivos, integradas dentro de un modelo de seguridad multicapa.
- La solución deberá permitir que los usuarios finales reporten de manera sencilla correos sospechosos o incorrectamente clasificados (falsos positivos o falsos negativos), integrando estos reportes en los procesos de análisis y respuesta de seguridad

- La solución deberá permitir el envío de notificaciones y resúmenes periódicos a los usuarios finales, incluyendo información sobre correos en cuarentena y acciones aplicadas, facilitando su visibilidad e interacción con los mensajes filtrados.

48. WAF - Seguridad para Aplicaciones Web (01 Unidades)

Modalidad del Servicio

- Tipo de Despliegue: La solución debe ser entregada bajo la modalidad de Software as a Service (SaaS) basado en la nube.
- Arquitectura: El servicio debe actuar como un proxy inverso en la nube, inspeccionando el tráfico antes de que este llegue a la infraestructura on-premise.
- Propósito: La solución debe proteger contra ataques en capa de aplicacion web en nube que soporte despliegues siempre activos, a través de modificación de DNS y que no requieran modificación alguna de Hardware o Sofware del lado de los servidores a proteger.

Licenciamiento

- Capacidad de Tráfico: El licenciamiento debe cubrir un ancho de banda (Throughput) de inspección adecuado para la demanda de las aplicaciones publicadas.
- Protección de Aplicaciones: Debe proteger un total de 10 aplicaciones con ancho de banda máximo de 100 Mbps.
- El servicio de Cloud WAAP debe soportar un modelo de integración basado en API que no requiera cambios de DNS o BGP para proteger las aplicaciones y que cuente tenga las siguientes características:
  - En la arquitectura basada en API no se requiere compartir el certificado digital.
  - En la arquitectura basada en API los requerimientos van directamente a la aplicación.

Capacidades de Seguridad

- La solución debe contar con un mecanismo que permita el bloqueo automático y temporal de direcciones IP de origen (source-blocking), basado en el análisis de los ataques realizados por un mismo actor a las diferentes aplicaciones protegidas. Este mecanismo debe ser automático, basado en ML, y permitir definir la sensibilidad de la activación.
- La solución debe contar con un mecanismo que permita visualizar los subdominios y/o URLs que invocan los scripts de java (JS) desde el navegador de los usuarios que consumen las aplicaciones, así como el nivel de amenaza de los mismos y si es que estos cuentan o no con certificados de seguridad.
- El servicio de Cloud WAAP debe proveer una protección basada en firmas que proteja la aplicación contra vulnerabilidades conocidas.
- El servicio debe proveer una protección contra comandos de SQL, comandos de shell y ataques de cross-site scripting, usando un algoritmo de reducción para detectar posibles segmentos de código en los parámetros. La protección debe cubrir al menos las siguientes amenazas: Cross Site Scripting (XSS), SQL Injections, Injection Flaws, Command Execution, Database Sabotage, Stealth Commanding, Backdoor.
- La solución deberá permitir al administrador, crear firmas custom (Custom Signatures). Mediante este mecanismo el administrador podra incorporar a las protecciones incluidas en la solución patrones especificos que desee tratar como eventos de seguridad.
- Gestión de Botnet: El servicio debe incluir protección contra ataques de tipo BOT (ataques automatizados) basado en firmas, siendo capaz de mitigar como minimo, bots de GEN 1 y GEN 2 (scripts y headless browsers)
- El servicio debe detectar y bloquear tráfico de bots en donde existan las siguientes anomalías de User-Agent:

- User-Agents invalidos.
- Headless Chrome.
- Navegadores Antiguos.

- El portal permitirá automatizar la creación de Certificados Digitales para las aplicaciones que así lo requieran. Este servicio no deberá representar costos adicionales para el cliente y permitira como minimo la creación de un certificado por aplicacion protegida
- Políticas de Seguridad Positiva y Negativa: Las políticas de seguridad debe implementar filtros de seguridad que soporten modelos de seguridad positivos y negativos.
- El portal debe contar con un servicio de Inteligencia reputacional, que permita a los operadores visualizar insights sobre las direcciones IP consultadas.
- El servicio debe garantizar la disponibilidad mínima de la infraestructura de red del servicio debe ser de 99.999% con un PoP de mitigación local.
- El servicio de Cloud WAAP debe ser un servicio de seguridad administrado por el fabricante con disponibilidad 7x24x365.

Gestión y Visibilidad

- El portal de servicios debe permitir visualizar los eventos de seguridad por aplicación. La información mínima que deben tener estos logs:
  - Acción tomada por el servicio
  - Dirección IP origen
  - País de Origen
  - Aplicación
  - Fecha y hora del evento
  - Severidad
  - Tipo de ataque
  - Clasificación del ataque de acuerdo al OWASP Top 10 2021
  - Entregar el detalle del encabezado del request de HTTP del ataque

49. SIEM (01 solución)

- La solución deberá realizar monitoreo, correlación y análisis de eventos de seguridad (SIEM), formando parte de una plataforma unificada de operaciones de seguridad que integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.
- La solución deberá permitir la ingesta, normalización y correlación automatizada de eventos en tiempo cercano a real, generando alertas consolidadas y permitiendo la ejecución de acciones de respuesta desde una única consola.
- La solución debe operar en modalidad SaaS (basada en la nube), permitiendo el uso de componentes locales (máquinas virtuales o agentes) únicamente para la recolección e integración de fuentes de datos internas, sin requerir infraestructura on-premise para el procesamiento, almacenamiento o correlación de eventos.
- La plataforma deberá estar basada en nube, con el objetivo de no tener limitaciones de hardware para el procesamiento de los algoritmos de Inteligencia Artificial (IA) en las fases de detección, investigación y respuesta ante amenazas.
- La nube desde donde se brinde el servicio deberá contar con las siguientes características para garantizar la confidencialidad, integridad y disponibilidad de los datos de la entidad:
  - Contar con la certificación SOC2 Plus de AICPA y CSA START Nivel 2 (Cloud Security Alliance)
  - Contar con certificaciones ISO 27001, ISO 27017, ISO 27018 e ISO 27701
  - Contar con doble factor de autenticación para el login proporcionado de manera nativa por la plataforma.
- Para el cifrado de los datos alojados en el tenant, la plataforma deberá soportar el mecanismo de BYOK (Bring Your Own Keys), permitiendo a la Entidad generar, importar y gestionar sus propias claves de cifrado, mediante un servicio de administración de claves, manteniendo control y auditabilidad sobre el acceso y el cifrado de los datos y apoyando cumplimiento regulatorio.

- La integración entre los distintos componentes deberá ser nativa, sin requerir desarrollos personalizados, procesos complejos de parsing o integraciones externas para la correlación de eventos.
- Debe soportar al menos 4,000 eventos por segundo y 50 dispositivos, o soportar ingesta de 350 GB por día.
- Debe permitir crecimiento de capacidad a demanda sin límites y únicamente adquiriendo licenciamiento adicional en caso la Entidad lo requiera a futuro.
- Deberá soportar múltiples mecanismos de ingesta/colección de logs, con conectores nativos para cientos de plataformas y la capacidad de integrar cualquier otra fuente donde no exista un conector nativo mediante mecanismos genéricos. Como mínimo, deberá soportar:
    - Syslog, en formato CEF, LEEF, RAW
    - API Polling/Pull: la solución extrae los logs de una plataforma externa.
    - API Receiver (HTTP Collector): la solución recibe logs enviados desde una plataforma externa.
    - Webhook
    - Netflow Collector
    - Windows Event Collector (WEC): colección de logs de Servidores Windows sin necesidad de desplegar agentes.
    - File Share Collector: colección de archivos de logs en formatos RAW, JSON, CEF, LEEF, CSV, TSV, almacenados en carpetas compartidas
    - FTP Server Collector: colección de archivos de logs en formatos RAW, JSON, CEF, LEEF, CSV, TSV, almacenados en servidores FTP/FTPS/SFTP.
    - Database Collector: colección de logs almacenados en tablas de bases de datos MySQL, MSSQL, Oracle, PostgreSQL.
    - Agentes de Colección: agentes
    - livianos para colectar logs de Auditoria, IIS, DNS, DHCP, entre otros, en servidores Windows y Linux.
- Todos los eventos, logs y telemetría recolectada deberán ser almacenados de manera normalizada y estructurada en tablas, datasets o índice de datos. El presente documento usará el término "tablas" para estandarizar el concepto.
- Deberá ser capaz de recolectar y almacenar centralizadamente logs y telemetría de endpoints provenientes de agentes EDR/XDR, ya sean del mismo fabricante o de terceros. El Postor deberá incluir el licenciamiento necesario para habilitar esta capacidad. Se entiende por telemetría no solo las alertas generadas por el EDR/XDR, sino también la actividad detallada del endpoint, incluyendo como mínimo: procesos (creación/árbol/command-line), archivos (creación/modificación/lectura), registro (Windows Registry), sesiones e identidad (logon/logoff), actividad de red (conexiones/DNS), y otros eventos relevantes de seguridad
- Deberá tener conectores nativos para más de 1000 plataformas de terceros y ser capaz de normalizar los eventos de manera nativa, sin necesidad de escribir reglas de correlación
- Debe ser capaz de monitorear en tiempo real el estado de salud de las fuentes de eventos y generar una alerta de manera automática ante estas ocurrencias. Por cada alerta deberá mostrar las causas del problema o posibles causas (tales como errores de conexión por API y otro), y debe tener la capacidad de ejecutar un playbook automatizado para el tratamiento de estos problemas.
- Deberá calcular automáticamente una línea base (baseline) de recepción de logs por cada fuente y generar alertas ante desviaciones significativas respecto a dicha línea base.
- Debe realizar la colección de eventos de los dispositivos en las premisas mediante la implementación de una máquina virtual (colector) o hardware appliance.
- Los colectores deberán tener la capacidad de ser desplegados en Alta Disponibilidad para tener resiliencia en la recolección de eventos.
- Deberá estar licenciado para almacenar todos los logs por al menos 30 días en formato de Hot Storage (almacenamiento en caliente para acceder a la data de manera constante) y 180 días en formato Cold Storage (almacenamiento en frio, que no requiere acceso constante a la data). Esta capacidad deberá ser granular, permitiendo elegir sobre que fuentes se requiere mayor periodo de retención.

- Debe ser capaz de almacenar la telemetría de los EDR/XDR integrados por al menos 30 días en formato Hot Storage (almacenamiento en caliente para acceder a la data de manera constante
- El método principal de detección deberá estar basado en inteligencia artificial. Es decir, la inteligencia artificial de la plataforma deberá ser capaz de procesar todos los logs y telemetría recolectada de las distintas fuentes para generar casos de uso de detección y alertar posibles incidentes.
- Cada alerta de seguridad debe ser enriquecida con atributos asociados a Tácticas y Técnicas de Ataque, Tipo de Amenaza, Severidad, Categoría.
- Los perfiles de comportamiento deberán de ser generados mediante el uso de perfiles estadísticos y algoritmos de machine learning.
- El motor de analítica debe procesar los eventos (red, autenticación, endpoint, cloud, etc.) para construir una línea base de actividad y generar alertas cuando identifique anomalías.
- Cada detector debe trabajar con intervalos de tiempo definidos: un periodo de activación/perfilado (tiempo de "calibración") para reunir datos suficientes y reducir falsos positivos; un periodo de evaluación para comparar la actividad reciente contra la línea base; y un periodo de entrenamiento (línea base) como histórico para calcular y ajustar continuamente y de manera automática los umbrales por cada activo.
- Debe contar con al menos 500 casos de uso de detección de amenazas. Todos estos casos de uso deberán estar activados de manera automática, sin necesidad de construir una regla de correlación o afinamiento manual.
- Deberá permitir la creación de reglas de correlación que permitan configurar casos de uso utilizando los eventos recolectados de las diversas fuentes.
- Las reglas de correlación deberán poder construirse en base a umbrales, filtros, rangos de tiempo y otros parámetros.
- Las reglas de correlación deberán poder construirse con más de una tabla (dataset o índice de eventos), es decir, una regla de correlación deberá poder usar distintas fuentes de logs.
- Un incidente deberá contener uno o varias alertas de seguridad, la plataforma deberá ser capaz de contextualizar y correlacionar automáticamente alertas de múltiples fuentes (cross-correlation) que formen parte de un mismo incidente.
- Las alertas de seguridad deberán tener un periodo de almacenamiento mínimo de 180 días.
- La solución deberá contar con un lenguaje de consulta especializado, diseñado para hacer consultas (querys) de forma directa a todos los eventos de seguridad recolectados desde fuentes externas integradas y de la Telemetría del Endpoint.
- El lenguaje deberá incluir operadores avanzados que permitan manipular, transformar y sintetizar la información, facilitando el análisis eficiente de grandes volúmenes de eventos.
- Deberá contar con capacidades de IA generativa que permitan asistir la construcción de consultas (queries) a partir de prompts en lenguaje natural, generando consultas en el lenguaje especializado de la plataforma, esto con la finalidad de facilitar el trabajo del analista.
- Debe tener más de 200 integraciones nativas con plataformas de inteligencia de amenazas, de los cuales se permita recolectar Feeds de manera automática, tales como: AbuseIPDB, Virus Total, Alienvault, Censys, Cyren, Domain Tools, Feedly, IP-API, IPQS, IPInfo, MISP, MITRE ATT&CK Feeds, MXtoolbox, Pwned, Shodan, Azure Feed.
- Con el objetivo de facilitar las labores de triage, la plataforma deberá ser capaz de correlacionar alertas provenientes de distintos mecanismos de detección y agruparlas automáticamente en un incidente unificado, de acuerdo a la naturaleza y similitudes de las alertas. Asimismo, deberá permitir la agrupación manual de alertas e incidentes cuando sea requerido por el analista.
- Debe permitir crear alertas e incidentes de manera manual, donde se pueda definir el nombre del evento, severidad, categoría, TTPs acorde a MITRE ATT&CK, y un playbook de respuesta.
- Por cada incidente se deberá mostrar las técnicas y tácticas de MITRE ATT&CK que fueron detectadas en ese incidente.
- La solución deberá contar con un módulo de reglas de puntaje de riesgo (risk scoring), que permita asignar un nivel de severidad cuantitativo (por ejemplo, en una escala de 0

a 100) a las amenazas detectadas, considerando la criticidad de los activos afectados y el tipo de amenaza.
- Debe tener un dashboard para monitorear el MTTR (mean time to response) en la gestión de incidentes.
- Debe tener un dashboard que permita dar seguimiento a los incidentes abiertos
- El soporte del fabricante deberá incluir un servicio que permita a la Entidad a optimizar la plataforma adquirida, para ello deberá tener como mínimo los siguientes alcances:
  - Verificar el estado de los componentes de la solución
  - Asistir en la configuración y corrección de parsing rules
  - Proveer recomendaciones para adoptar las configuraciones alineadas a las buenas prácticas
  - Proveer workshops y demostraciones del producto sobre nuevas capacidades que se publiquen a lo largo del servicio
  - Asistir a la Entidad con el afinamiento de las alertas e incidentes
  - Asistir a la Entidad a optimizar los playbooks de automatización
  - Proveer workshops a medida acorde a los objetivos de la Entidad
  - Realizar health checks completos de la plataforma al menos con una periodicidad anual

50. Plataforma de Detección y Respuesta de Amenazas Externas e Internas (01 solución)
- La solución deberá proporcionar capacidades de detección y análisis de amenazas externas mediante la identificación y evaluación de la superficie de ataque expuesta.
- La solución deberá formar parte de una plataforma unificada de operaciones de seguridad que permita complementar estas capacidades con la detección y respuesta de amenazas internas, mediante la integración y correlación de telemetría proveniente de diferentes fuentes de seguridad.
- La solución deberá permitir la correlación de riesgos externos con eventos internos, proporcionando una visión integral del riesgo de seguridad y facilitando la priorización de acciones de mitigación.
- La gestión deberá realizarse desde una plataforma centralizada, permitiendo la visibilidad unificada de amenazas, exposiciones y eventos de seguridad.
- La solución deberá descubrir de forma continua la superficie de ataque externa, atribuyendo activos públicos a la organización (incluyendo activos conocidos y no conocidos) mediante análisis de registros IP, dominios (WHOIS), Número de Sistema Autónomo (ASN), certificados y datos de escaneo, sin requerir agentes ni instalaciones adicionales.
- Deberá descubrir servicios cloud expuestos a Internet que no estén gestionados y/o no sean conocidos por la Entidad.
- Deberá permitir cargar activos al inventario mediante la interfaz (por ejemplo, importando un archivo CSV).
- Deberá soportar como mínimo la carga de dominios, subdominios y rangos IP.
- Deberá tener al menos 600 políticas predefinidas para detectar amenazas sobre activos expuestos.
- Deberá permitir evaluar rápidamente el nivel de exposición frente a amenazas emergentes tipo zero-day, identificando y priorizando los activos potencialmente afectados.
- Deberá inventariar certificados digitales usados para comunicaciones cifradas, registrando sus principales metadatos (emisor, clave pública/algoritmo, subject, organización y país/estado) y ejecutar clasificaciones básicas de "salud criptográfica" (por ejemplo, auto-firmado, wildcard, validación de control de dominio, expiración, tamaño de clave y algoritmo de firma).
- Deberá inventariar dominios externos atribuidos a la Entidad, indicando si tienen resolución reciente.
- Deberá recolectar información de dominios y DNS mediante técnicas globales de recolección activa y pasiva, incluyendo escaneos que permitan identificar servidores DNS.
- Deberá mantener un inventario de servicios expuestos a Internet atribuidos a la Entidad, y que respondan a escaneos sobre Internet público.

- Deberá clasificar cada servicio según el análisis basado en fingerprinting (software, tecnologías y comportamientos), indicando si cada clasificación está activa o inactiva según observaciones recientes.
- Deberá recolectar y presentar información adicional del servicio descubierto (por ejemplo, banner, respuestas y encabezados) para enriquecer el análisis y la priorización.
- Deberá escanear sitios web expuestos a Internet para identificar sitios inseguros, componentes y tecnologías usadas, manteniendo un inventario actualizado.
- Por cada sitio web, deberá detectar el uso de tecnologías/librerías de terceros, configuraciones inseguras, tecnologías vulnerables, incumplimiento de buenas prácticas, fechas de primera y última observación, host, tipo de HTTP, direcciones IP, estado de actividad, puerto, categoría del sitio.
- Deberá diferenciar dominios, servicios externos y sitios web, reflejando su relación (un dominio puede no tener sitio; un sitio puede depender de uno o más servicios HTTP).
- Por cada sitio web, deberá mostrar una captura de pantalla reciente y un enlace directo para facilitar la investigación.
- Deberá permitir agregar o retirar activos del inventario de forma manual desde la consola.
- Debe permitir adoptar medidas de contención rápida cuando se incumpla una política de seguridad, por ejemplo, restringiendo acceso al puerto no autorizado.
- Deberá validar la remediación de alertas de ASM mediante un escaneo de confirmación que verifique que el riesgo ya no es observable.
- Deberá descubrir vulnerabilidades y malas configuraciones en activos expuestos a Internet mediante pruebas controladas diarias, reduciendo la verificación manual.
- Deberá realizar escaneos únicamente a servicios externos accesibles públicamente y seleccionados para evaluación, ejecutando cada prueba solo donde aplique según el tipo de servicio del activo expuesto.
- Deberá ser capaz de detectar credenciales por defecto de los servicios expuestos
- Debe permitir seleccionar el nivel de intrusión al momento de realizar un escaneo, considerando al menos 4 niveles:
    - No intrusivo
    - Mínima intrusión
    - Impacto medio
    - Alto impacto
- Deberá permitir administrar los test de escaneo, permitiendo habilitar o deshabilitar los test. Por cada test deberá mostrar información como software afectado, identificadores de vulnerabilidad (CVE/CWE), score de severidad (CVSS), probabilidad de explotación (EPSS), referencias, guía de remediación, estado de habilitación y cantidad de servicios confirmados como vulnerables.
- Deberá ofrecer una vista centralizada de vulnerabilidades emergentes/zero-days para identificar rápidamente los eventos que puedan impactar a la organización, mostrando métricas clave (por ejemplo, CVSS y EPSS).
- Deberá brindar contexto detallado por cada evento, tales como, resumen, posibles impactos, evidencia de explotación. Asimismo, debe permitir evaluar el impacto en la superficie externa, incluyendo servicios/softwares afectados.
- Deberá incluir guía para remediación ante las vulnerabilidades emergentes.
- Deberá permitir consultar información global sobre Direcciones IP, dominios y certificados, enriqueciendo los resultados con información contextual (registro, geolocalización, certificados relacionados, servicios observados, ASNs y DNS pasivo), incluso si la consulta corresponde a otros valores no asociados a las alertas de superficie de ataque.
- Deberá tener capacidades de protección digital de marca, considerando al menos las siguientes funcionalidades:
- Detectar dominios de riesgo asociados a suplantación de marca y reportarlos para reducir riesgos como phishing, fraude, propagación de malware y robo de información.
- Identificar credenciales filtradas reportadas externamente y priorizar las ocurridas en una ventana reciente (por ejemplo, últimos seis meses).

51. SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta (01 solución)

- La solución deberá contar con capacidades de orquestación y automatización de la respuesta ante incidentes de seguridad (SOAR), formando parte de una plataforma unificada de operaciones de seguridad que integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.
- La solución deberá contar con un catálogo de al menos 800 playbooks predefinidos, orientados a automatizar la respuesta ante incidentes de seguridad. Dichos playbooks deberán poder personalizarse según las necesidades de la Entidad.
- La plataforma deberá permitir la creación y edición de playbooks, sin establecer un límite en la cantidad de playbooks que puedan ser definidos.
- Deberá permitir la construcción de playbook de manera amigable, usando mecanismos como drag-and-drop de las tareas/scripts y otros playbooks.
- La plataforma deberá soportar la reutilización de automatizaciones, permitiendo que un playbook pueda ser contenido dentro de otro, con el fin de estandarizar y optimizar los procesos de respuesta.
- La solución deberá permitir crear bucles dentro de un playbook principal mediante sub-playbooks, donde cada iteración calcule sus valores usando los datos del sub-playbook.
- La solución deberá permitir controlar el comportamiento del bucle (por ejemplo, máximo de iteraciones y tiempos de espera) para evitar impactos de rendimiento, y deberá iterar automáticamente cuando la entrada a una tarea del playbook sea un campo tipo arreglo (array), sin requerir configurar un bucle manual.
- La solución deberá contar con capacidades de filtrado, que permitan extraer información relevante desde estructuras complejas, utilizando criterios definidos por el analista y reutilizando los resultados en tareas posteriores.
- La solución deberá incluir funciones de transformación de datos, orientadas a normalizar, formatear y adaptar la información para su análisis, toma de decisiones o ejecución de acciones automatizadas.
- Deberá ser posible encadenar múltiples transformaciones, definiendo el orden de ejecución, y utilizar los resultados como inputs dinámicos dentro del playbook.
- Los playbook deberán ser capaces de manejar flujos de errores, de tal forma que si una tarea falla, la siguiente acción del playbook sea trasladado a un flujo que pueda gestionar este error.
- Permitir el uso de tareas estándar para ejecutar acciones automáticas o semiautomáticas, tales como enriquecimiento de indicadores, interacción con integraciones externas, ejecución de scripts, apertura de tickets, entre otros.
- Soportar tareas condicionales, que permitan evaluar resultados, atributos o respuestas previas y dirigir la ejecución del playbook mediante lógica de decisión y ramificación del flujo.
- Deberá soportar "sondeo" (espera activa) en playbooks para pausar la ejecución hasta que una acción remota en un producto externo finalice (por ejemplo, detonación/análisis de archivos o URLs, o consultas de larga duración), consultando periódicamente el estado y reanudando automáticamente cuando el proceso termine.
- Deberá permitir tareas de recolección de datos, orientadas a capturar input de usuarios o analistas, almacenando dicha información como contexto del incidente para su uso en pasos posteriores.
- Las tareas de captura de input del usuario deben permitir el envío de notificaciones (correo electrónico y/u otros canales) y soportar distintos tipos de respuesta (selección de alternativas, texto libre, numérico, fecha y carga de adjuntos), de modo que el playbook pueda continuar su ejecución automáticamente una vez recibido el input.
- Debe permitir que el formulario donde el usuario deba acceder para colocar el input, soporte mecanismos de acceso con y sin autenticación.
- Deberá permitir gestionar temporizadores a tareas específicas del playbook, con el objetivo de controlar el cumplimiento del SLA por etapa (por ejemplo, asignación y remediación)
- La solución deberá incorporar tareas basadas en inteligencia artificial, que permitan procesar prompts en lenguaje natural y generar salidas dinámicas, tales como análisis, resúmenes, reportes o comunicaciones automatizadas.

- La plataforma deberá permitir organizar los playbooks en secciones lógicas, facilitando la gestión, navegación y mantenimiento de flujos complejos.
- Debe tener la capacidad de ejecutar playbooks en modo debug, de tal forma que permita observar la ejecución paso a paso del mismo y resolver cualquier inconveniente de ser necesario
- Debe permitir crear scripts personalizados, para lo cual la solución deberá estar en la capacidad de consumir las API de las plataformas externas a integrar.
- El módulo SOAR deberá tener un IDE de desarrollo embebido para poder desarrollar los scripts personalizados. Este IDE deberá soportar al menos el lenguaje Python, JavaScript y Powershell.
- Los playbooks deben poder ser ejecutados como tareas programadas, es decir, sin necesidad de que exista una alerta o incidente de seguridad un playbook puede ejecutarse de manera periódica (permitiendo especificar la periodicidad) para automatizar alguna tarea.
- La solución deberá permitir crear reglas de automatización, donde se detalle bajo qué condiciones de una alerta de seguridad se gatillará la ejecución automática de un playbook.
- La solución debe sugerir automáticamente que playbook puede ser asociado a una alerta de seguridad, ante aquellas alertas que no tengan un playbook de respuesta asignado.
- La respuesta deberá tener cobertura a nivel de los endpoints para proteger contra amenazas altamente avanzadas, esto incluye:
  - Capacidad de poder colocar los malware en una carpeta de cuarentena
  - Capacidad de extraer el malware o archivo sospechoso del endpoint hacia la consola, para poder ser analizado por el investigador
  - Debe ser posible aislar el endpoint de la red para que no tenga comunicación con ningún dispositivo de la red interna o externa.
  - Deberá ser posible realizar una conexión remota a cada endpoint que forme parte de una investigación para ejecutar las siguientes acciones:
    - Listar procesos y archivos
    - Ejecutar instrucciones por línea de comandos (CMD y Powershell para el caso de Windows; Bash para el caso de Linux y MacOS).
    - Ejecutar scripts basados en Python
  - Capacidad de ejecutar scripts remotamente a múltiples endpoints de manera concurrentes.
  - Capacidad de tareas remotas a múltiples endpoints, como mínimo cerrar procesos, eliminar archivos, eliminar y/o modificar claves de registro.
- La solución deberá integrar capacidades avanzadas de inteligencia artificial para optimizar las operaciones de seguridad, permitiendo investigación asistida y ejecución de acciones automatizadas sobre la infraestructura.
- La plataforma deberá ofrecer una interfaz unificada para interactuar con agentes de IA predefinidos y personalizados, capaces de planificar y ejecutar flujos de trabajo de múltiples pasos.
- Debe permitir la creación de agentes de IA personalizados para investigación y respuesta, capaz de crear y ejecutar planes compuestos por acciones (playbooks, scripts, comandos y prompts).
- Debe proveer un módulo de administración para gestionar agentes y acciones, tales como, habilitar/deshabilitar, asignar acciones, crear acciones personalizadas.
- Deberá incorporar controles de seguridad en los prompts, validando automáticamente permisos y contexto antes de ejecutar cualquier acción, bloqueando solicitudes ambiguas, potencialmente maliciosas.
- Debe permitir marcar acciones sensibles que requieran aprobación explícita antes de ejecutarse, y ofrecer búsqueda/filtrado y trazabilidad para la gestión operativa de los agentes.
- Deberá garantizar la privacidad de las conversaciones del asistente, manteniendo al mismo tiempo trazabilidad completa mediante registros de auditoría que documenten de forma detallada quién inició una acción, qué acción se ejecutó y cuándo.
- Deberá permitir interacción conversacional con IA, utilizando el contexto del caso para investigar amenazas y ejecutar acciones como comandos, playbooks o scripts.
- Deberá permitir el uso de lenguaje natural para crear, ajustar y desplegar scripts de automatización, facilitando la interacción del analista.

- Deberá soportar integraciones con herramientas y fuentes externas, mediante protocolos estandarizados, para acceder a datos y ejecutar acciones en plataformas terceras.
- Deberá permitir la inclusión de tareas de inteligencia artificial generativa dentro de playbooks, como pasos independientes para análisis o generación de contenido.
- Deberá ser capaz de generar automáticamente resúmenes técnicos de incidentes, consolidando telemetría y datos de impacto para acelerar el triage y la comunicación.
- El asistente deberá organizar y gestionar el historial de conversaciones por periodos de tiempo, permitiendo revisar, retomar, renombrar o eliminar investigaciones previas de forma sencilla.
- Deberá garantizar la protección y cifrado de datos sensibles, con separación estricta entre clientes y control de acceso basado en identidades.
- Deberá asegurar que los datos procesados por la IA se utilicen exclusivamente para la respuesta inmediata, sin ser almacenados para entrenamiento ni compartidos con terceros.
- Debe integrarse con sistemas externos mediante MCP, permitiendo que los agentes consulten datos y ejecuten acciones en herramientas de terceros (ejm. Jira, GitHub).
- Debe permitir configurar múltiples instancias por integración, probar conectividad y mantener el estado habilitado/deshabilitado desde la consola.

52. ADC (application Delivery Controller) (02 Unidades)

Arquitectura y Capacidad de Hardware

- Procesamiento: Debe contar con una arquitectura multi-core optimizada, incluyendo un procesador de al menos 12 núcleos.
- Almacenamiento y Memoria: Debe incluir una unidad de estado sólido (SSD) de al menos 0.5 TB para logs y sistema operativo.
- Fuentes de Poder: Para garantizar la alta disponibilidad, cada unidad debe contar con doble fuente de poder redundante.

Rendimiento y Licenciamiento

- La solución debe incluir un pool de licencia flexible de throughput de 1 Gbps como mínimo.
- La solución ofertada debe incluir licenciamiento para un pool de 8 instancias de ADC (application delivery controllers).
- La solución debe incluir 2 equipos físicos operando en alta disponiblidad.
- La solución debe permitir remover la capacidad instalada de una instancia específica para que esta sea liberada y pueda ser reasignada a otras instancias de balanceo, para cualquiera de los factores de formas.
- La solución debe incluir una consola gráfica que permita administrar el pool de licencias, teniendo como mínimo las siguientes funcionalidades:
  - Aprovisionamiento de las licencias de throughput y funcionalidades.
  - Modificar las licencias asignadas a una instancia específica.
  - Desinstalación de las licencias de las instancias.
  - Visualizar la asignación del pool de licencias adquirido.
- Capacidad de Sesiones: Debe soportar un mínimo de 46 millones de conexiones concurrentes en Capa 4.
- Transacciones por Segundo L7: Capacidad para procesar al menos 1.8 millones de peticiones por segundo (RPS).
- Transacciones por Segundo L4: Capacidad para procesar al menos 1 millon de conexiones por segundo (CPS).
- La solución debe estar configurada en alta disponibilidad y debe soportar Stateful Failover.
- La solución debe permitir sincronizar la configuración entre equipos de forma manual o automática.
- La solución debe soportar balanceo transparente a través de filtros, en donde se realice inspección del tráfico, clasificación y envío a uno o más grupos de balanceo, sin alterar el paquete original y sin necesidad de exponer una IP virtual.
- La solución debe incluir una métrica por proximidad que correlacione la latencia y el número de saltos hacia un origen determinado, para el balanceo de salida y desde un origen determinado para el balanceo entrante.

Virtualización y Escalabilidad

- Instancias Virtuales (vADC): La solución debe soportar la partición del hardware en instancias lógicas independientes. Se debe incluir licenciamiento para un mínimo de 8 instancias vADC activas desde el primer día.
- Aislamiento: Cada vADC debe tener recursos de CPU y memoria garantizados para asegurar que el tráfico de una aplicación no afecte a las demás.

Conectividad Física y Escalabilidad

- El appliance debe contar con una densidad de puertos que garantice la integración en arquitecturas de alta velocidad y baja latencia, cumpliendo con los siguientes requisitos mínimos:
- Puertos de Cobre: Al menos ocho (08) puertos 10/100/1000 Mbps Base-T (RJ45) para gestión y servicios auxiliares.
- Puertos de Fibra (Acceso/Agregación): Al menos ocho (08) puertos con soporte nativo para 10 GbE (SFP+).
- Puertos de Alta Velocidad (Core): Al menos cuatro (04) puertos con soporte nativo para 25 GbE (SFP28) para interconexión de alta velocidad.
- Consola: Puerto dedicado para administración local (RJ45/USB).

Gestión Centralizada y Visibilidad

- Analíticas: Debe proporcionar visibilidad en tiempo real y reportes históricos sobre el rendimiento de las aplicaciones y el estado de salud de los servicios.
- La solución debe proveer visibilidad SSL/TLS para ambos, el tráfico hacia el Datacenter y el tráfico saliente a Internet, permitiendo a la solución ser la responsable de la orquestación y distribución dinámica de tráfico entre dispositivos de seguridad.

53. Anti – DDoS (02 Unidades)

Arquitectura y Componentes de la Solución

- Provisión de Hardware: La solución debe contemplar la entrega de 02 appliances físicos de alto rendimiento en configuración redundante.
- La solución de mitigación de ataques DDoS debe tener la siguiente configuración de interfaces para su integración a la red.
  - Como mínimo, 4 Interfaces de Cobre GE de entrada.
  - Como mínimo, 4 Interfaces de Cobre GE de salida.
- La solución de mitigación de ataques DDoS se debe integrar a la red de forma transparente en capa 2.
- Mecanismo de Bypass: Los puertos de cobre deben contar con un mecanismo de derivación (bypass) físico incorporado para garantizar la continuidad del tráfico en caso de fallo del equipo.
- La solución de mitigación de ataques DDoS debe soportar un número ilimitado de sesiones concurrentes de ataque.
- La solución de mitigación de ataques DDoS debe incluir doble fuente de poder hot swappable

Rendimiento y Performance

- La solución de mitigación de ataques DDoS debe estar licenciada para un throughput de tráfico legítimo de al menos 2 Gbps por equipo.
- La solución de mitigación de ataques DDoS debe soportar crecimiento de throughput por licenciamiento sobre el mismo hardware de hasta 5 Gbps por equipo.
- La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 10 Gbps por equipo
- Tasa de Paquetes: Debe soportar una tasa de procesamiento de hasta 12 Millones de Paquetes por Segundo (Mpps) para inundaciones de red.
- Latencia Máxima: La inspección del tráfico debe mantener una latencia ultra-baja, no superior a los 60 microsegundos.

Capacidades de Detección y Mitigación

- La solución debe tener la capacidad de crear y aplicar firmas para ataques DDoS de Dia Cero (Zero-Day) en menos de 20 segundos.
- Análisis de Comportamiento: La solución debe contar con protección de ataques DDoS DNS basada en análisis de comportamiento para detectar anomalías de tráfico y prevenir ataques de día cero incluyendo al menos los siguientes tipos de inundaciones de Queries DNS: A, AAAA, HTTPS, MX, PTR, TXT, SOA, NAPTR, SRV, Other.
- Protección Multicapa (L3-L7): Mitigación contra ataques de inundación TCP (SYN, SYN-ACK, RST, FIN-ACK.
- Anti-Spoofing: La solución debe identificar y filtrar los queries falsificados (spoofed) y prevenir contra ataques de Inundación DNS, Ataques de amplificación, fuerza bruta y DNS water torture.
- La protección contra ataques HTTPS debe soportar las siguientes versiones del protocolo SSL usando hardware dedicado interno sin requerir soluciones externas: TLS1.0, TLS 1.1, TLS 1.2 y TLS 1.3
- La solución debe ser capaz de detectar y mitigar ataques de randomización de encabezados y métodos HTTPS, a partir de los fingerprinting de TLS utilizados por la aplicación.
- La protección contra ataques HTTPS flood debe contar con al menos dos métodos de autenticación: 302 Redirect, Java Script.

Licenciamiento y Servicios Críticos

- Licencia de Capacidad: Deberá habilitar un rendimiento total de 10 Gbps del hardware sin restricciones lógicas.
- Servicio de Reputación (IP Reputation): Suscripción activa por 12 meses.

Gestión, Reportes y Monitoreo

- La solución debe incluir un elemento de gestión y control centralizado el cual soporte la administración y monitoreo de todos los mitigadores que hacen parte de la propuesta.
- Analítica Forense: La solución debe proporcionar una visualización completa de los detalles del ataque para los eventos de detección que lo ameriten, incluyendo ID del ataque, objeto protegido, hora de inicio, duración, nombre del ataque, firmas asociadas y atributos contextuales como IPs de origen/destino, puertos y protocolos.
- Métricas en Tiempo Real: La análitica de red debe incluir como mínimo la siguiente información para cada activo protegido.
  - Gráficos de Tráfico.
  - TOP IP Origen.
  - TOP IP Destino.
  - TOP Aplicaciones.
  - TOP Protocolos.
  - TOP Países
  - Tendencias de la última semana.

54. MFA - Administración de Identidad y Acceso (01 solución)

- La solución propuesta deberá ofrecerse como servicio (SaaS) y al menos tener las certificaciones SOC 2 Type 2, SOC 3, ISO27001, ISO 27017, ISO 27018 entre otras.
- La solución deberá proporcionar capacidades de autenticación multifactor (MFA) como parte de una plataforma de administración de identidad y acceso (IAM), permitiendo el control seguro de acceso a aplicaciones y recursos.
- La solución debe estar licenciada para 300 usuarios y deberá proveer 10 token mobiles, que se deberán integrar a la solución de gestión de identidad.
- La solución se debe basar en algoritmos de aprendizaje de máquina (machine learning) no supervisados. Es decir, los modelos estadísticos con los casos de uso ya deben estar listos y calibrados.
- La solución debe medir el riesgo de la autenticación verificando el comportamiento histórico de la identidad a través del conjunto de los siguientes atributos: - GeoVelocidad;

Geolocalizacion; Dia de la semana; Horario de acceso; Sistema operativo; Fallas de login consecutivas

- La solución debe permitirles a los administradores personalizar los rangos de puntuación (0 a 100) para las categorías:
  - Sin riesgo
  - Riesgo bajo
  - Riesgo medio
  - Riesgo alto
- El riesgo calculado durante la autenticación por el motor de análisis del comportamiento de los usuarios debe compartirse con los módulos (SSO y MFA) que realizan el login, para los casos de uso citados en este documento, y utilizarlo como contexto para:
  - Solicitar autenticación de múltiples factores de forma dinámica
  - Permitir el login sin el uso de múltiples factores
  - Negar la autenticación
- Debe brindarles a los administradores de la solución la capacidad de explorar los datos históricos a través de dashboards, filtros y gráficos configurables, verificar las alertas y los factores que los influenciaron y explorar los eventos capturados y sus atributos.
- Debe proveer gráficos de línea de tiempo, donuts, mapas con la geolocalización de los eventos, gráficos de barras, tablas analíticas y mapas de relación. Sus dimensiones y categorías deben ser personalizables.
- Debe brindarles a los administradores de la solución la capacidad de explorar los datos históricos a través de dashboards, filtros y gráficos configurables, verificar las alertas y los factores que los influenciaron y explorar los eventos capturados y sus atributos.
- Debe proveer gráficos de línea de tiempo, donuts, mapas con la geolocalización de los eventos, gráficos de barras, tablas analíticas y mapas de relación. Sus dimensiones y categorías deben ser personalizables.
- Debe ser capaz de exportar los datos de alertas, riesgos calculados y eventos a PDF y CSV y, además, grabar las visualizaciones en la solución para consultas posteriores.
- Debe estar integrada a fuentes de inteligencia cibernética de terceros reconocidas en el mercado como, por ejemplo, Palo Alto Cloud.
- Debe poseer interfaz para el envío de alertas de forma automatizada. Debe soportar, como mínimo:
  - Correo electrónico con contenido de alerta
  - Webhooks como, por ejemplo, envío de mensaje a un canal de Microsoft Teams o Slack
- Poseer dashboards configurados previamente con informaciones y gráficos con las siguientes características:
  - Utilización de motor de análisis del comportamiento de los usuarios
  - Comportamiento de los usuarios en la utilización de las aplicaciones
  - Visión sobre la seguridad de las aplicaciones
  - Mapa con la geolocalización de las autenticaciones
  - Visión sobre el comportamiento de los Endpoints (móviles y computadoras)
  - Visión sobre el comportamiento de las identidades
- La solución debe permitir configurar dashboards personalizados.
- Debe permitir compartir los dashboards con otros usuarios.
- La solución debe proveer un catálogo de aplicaciones web con modelos de configuración de SSO que contenga al menos 1000 ítems, incluidas las aplicaciones más conocidas del mercado, para facilitar la configuración de estas integraciones.
- La solución debe permitir configurar el SSO para aplicaciones web, como mínimo, a través de los siguientes protocolos y métodos:
  - OpenID connect
  - SAML 2.0
  - WS-Federation
  - Oauth 2.0 modo client
  - Oauth 2.0 modo server
  - NTLM
  - HTTP Basic
  - Extensión en el navegador para capturar aplicaciones web que utilicen formulario con usuario y contraseña, y completar automáticamente el login y la

contraseña. Está información se debe guardar de forma segura en la solución, para completar automáticamente futuros login en estas aplicaciones.

- La solución debe ofrecer un componente/software para intermediar el SSO en aplicaciones web que se encuentren en el centro de procesamiento de datos de la entidad, sin necesidad de exponer a estas aplicaciones al uso de internet o de VPN.
- La solución debe proveer una extensión de navegador avanzada solamente para los administradores de la solución para realizar el mapeo de los campos de los formularios (en general, login y contraseña) y después incluirlos como una aplicación web para SSO en el catálogo general. Este recurso ayudará en el SSO de aplicaciones que no soportan protocolos más modernos de federación, como SAML Oauth, y con diferentes contraseñas.
- Soporte para SSO mediante IWA (Integrated Windows Authentication), que reutiliza el login de red para autenticación en las aplicaciones web sin necesidad de ingresar con usuario y contraseña nuevamente.
- Ofrecer soporte para personalizar las respuestas SAML (SAML Response) como, por ejemplo, mapear atributos de los directorios para atributos SAML, tener la capacidad de incluir lógicas complejas para manipular las respuestas SAML y, en lo posible, visualizar la respuesta SAML configurada antes de su implantación.
- La solución debe proveer un portal web para el usuario final con las siguientes características:
    - Después de efectuar el login, debe presentar las aplicaciones web disponibles para realizar el SSO a través de un conjunto de íconos, donde cada uno represente una aplicación en la que el usuario tiene derecho a efectuar el SSO.
    - Que permita realizar cambios en los atributos de identidad, como teléfono celular, correo electrónico y foto.
    - Que verifique las actividades de su identidad a través de dashboard con la siguiente información:
        - Geolocalización de sus login
        - Verificación de la geolocalización actual de sus dispositivos registrados
        - Login totales.
        - Fallas de login totales.
        - Utilización de las aplicaciones.
        - Historial de eventos importantes, como adición de nueva aplicación en su portal de SSO o fallas de login, entre otros
- La solución debe poseer un servicio de directorio para almacenar identidades en la nube de la solución, sin depender de la sincronización con otros servicios de directorio locales (on-premises) o en la nube de terceros.
- El servicio de directorio de la solución debe ser capaz de realizar la extensión de su esquema a través de la configuración de atributos personalizados, para responder a requisitos de negocios complejos.
- El servicio de directorio de la solución debe ser autoescalable, para soportar millones de identidades y miles de autenticaciones simultaneas.
- Debe ser capaz de forzar la complejidad de las contraseñas, como mínimo, a través de los siguientes requisitos:
    - Exigir tamaño mínimo
    - Exigir tamaño máximo
    - Exigir cantidad mínima de números
    - Exigir letras mayúsculas y minúsculas
    - Exigir caracteres especiales (símbolos)
    - Limitar caracteres consecutivos
    - Forzar la expiración de contraseñas dependiendo de su antigüedad
    - Guardar el historial de contraseñas para evitar su reutilización
- Notificar sobre la expiración de la contraseña por correo electrónico.
- Registrar fallas de login repetidas para bloqueo de usuario.
- Al mismo tiempo, la solución debe soportar la integración con servicios de directorio locales (on-premises) y en la nube. Como mínimo, los siguientes:
    - Microsoft Active Directory
    - Microsoft Azure AD
    - Google Directory
    - Directorios LDAP

- Las integraciones realizadas con directorios de terceros no deben realizar sincronismo con estas bases, es decir, cargar todo el directorio configurado a la nube. La solución debe actuar como un intermediario ("broker") entre los servicios de directorio de terceros y la solución.
- La solución debe poseer integración con proveedores de identidades sociales, para delegar la autenticación a tales proveedores y responder ante posibles requisitos de negocio. Debe soportar, como mínimo, los siguientes proveedores:
  - Facebook
  - Google
  - LinkedIn
  - Microsoft
- La solución debe ser capaz de configurar IDPs (Identity Providers) de socios de negocio de la entidad, para permitir el acceso de las identidades federadas a nuestras aplicaciones de negocio sin la necesidad de crear una nueva identidad en nuestra infraestructura. Esta federación se debe realizar a través del protocolo SAML.
- El portal SSO (inicio de sesión único) debe permitir a los usuarios administrar usuarios y contraseñas para aplicaciones que no están integradas con SSO pero que les gustaría almacenar estos usuarios y contraseñas para otras aplicaciones web de forma segura, agregando una experiencia de SSO después de guardar estas credenciales.
- La solución debe permitir a los usuarios compartir estas credenciales y el flujo de SSO con otros usuarios sin depender del administrador de la solución. Cuando se comparte, debe elegir:
  - Compartir sin necesidad de ver credenciales
  - Compartir con visualización de las credenciales.
  - Compartir siendo posible editar las credenciales.
- También debería ser posible que el administrador de la solución defina las credenciales y los flujos de SSO para las aplicaciones web que están disponibles para los usuarios finales en función de sus perfiles de acceso en la solución.
- Estas credenciales (nombre de usuario y contraseñas) se pueden almacenar de forma segura en la nube de la solución o en la solución de bóveda de contraseñas local del mismo proveedor.
- La solución debe tener la capacidad de crear perfiles dinámicos basados en atributos de la identidad, por ejemplo, su departamento. Estos perfiles se pueden utilizar para autorizar o solicitar diferentes métodos de MFA al acceder a una aplicación web integrada en la plataforma.
- Debería ofrecer widgets personalizados para MFA y pantalla de inicio de sesión para la integración con las aplicaciones web de la empresa. Generar un código HTML para ser incrustado en la página de inicio de sesión de estas aplicaciones web.
- La solución debe ser capaz de cumplir mínimamente los siguientes casos de uso para solicitar uno y más factores de autenticación:
  - Aplicaciones web integradas en la autenticación simplificada - funciones SSO.
  - En las pantallas de inicio de sesión y desbloqueo de los sistemas operativos Windows
  - Autenticación multifactor para soluciones VPN a través de RADIUS o SAML.
  - Cualquier dispositivo o sistema operativo que admita RADIUS.
  - Complemento para ADFS (IDP, proveedor de identidad), servicios de federación de Active Directory.
  - A petición mediante el protocolo Oauth y las API de REST.
  - Para realizar el restablecimiento de contraseña de servicio automático o desbloqueo de usuario.
- La solución debe ser capaz de ofrecer mínimamente los siguientes métodos para múltiples factores de autenticación: Usuario y contraseña de los directorios admitidos en la solución:
  - A través de la aplicación móvil iOS y Android, que ofrece soporte para:
  - Biometría FaceID.
  - Biometría a través del lector digital.
  - Inserción de smartphone (Notificación para aprobar o rechazar una autenticación).
  - Geolocalización a través de GPS coordenadas e IDatabase.
  - Soporte tokens OATH OTP.

  - Autenticación en la pantalla de inicio de sesión a través de QRcode (Passwordless) sin necesidad de introducir el usuario y la contraseña, con la opción de forzar la biometría en el dispositivo móvil.
- Llamada telefónica para solicitar un PIN previamente configurado.
- Mensaje de texto vía SMS que ofrezca el código para entrada manual y también una URL única, que permita aprobar o rechazar la autenticación sin necesidad de digitar el código manualmente.
- Confirmación de código vía correo electrónico que ofrezca el código para entrada manual y también una URL única, que permita aprobar o rechazar la autenticación sin necesidad de digitar el código manualmente.
- Clientes de tipo OATH OTP.
- Autenticadores que soporten FIDO2/U2F. Como mínimo, debe soportar:
  - MacOS TouchID
  - Yubikey
  - Google Titan Key
- Preguntas y respuestas configuradas previamente.
- Permitir que los usuarios realicen el autoservicio de restablecimiento de contraseña y desbloqueo de usuario, utilizando los métodos citados en el ítem 8.2 y sus subítems, para la verificación positiva a través del portal web de la solución.
- Para cada caso de uso o conjunto de casos de uso citados en el ítem 8.2 y sus subítems, la solución debe ser capaz de identificar los atributos de contexto de cada autenticación, para proporcionar los mejores métodos definidos para la autenticación. Como mínimo, debe soportar:
  - Dirección IP.
  - Día de la semana.
  - Fechas específicas.
  - Intervalos de tiempo entre dos fechas.
  - Intervalos de tiempo entre horarios (ejemplo: horario comercial).
  - Tipo de sistema operativo.
  - Tipo de navegador (browser).
  - Perfiles configurados en la solución.
  - País desde el que se accede.
  - Si se trata de un dispositivo gestionado.
  - Autenticación vía certificado.
  - Nivel de riesgo de la autenticación medido por un motor de análisis de comportamiento de los usuarios (UBA, User Behavior Analytics)
- La solución debe ser capaz de detectar casos de uso o perfiles de autenticación ya validados por el usuario y no solicitar nuevamente la autenticación durante un período de tiempo configurado por el administrador de la solución, para evitar repetidas validaciones en un corto período de tiempo.
- Los factores de autenticación que fueron proporcionados durante el acceso deben basarse en las reglas especificadas y separarse de la siguiente manera:
  - Conjunto de aplicaciones.
  - Una única aplicación.
  - Reglas para realizar el autoservicio de restablecimiento de contraseña o desbloqueo de usuario
  - Portal del Administrador.
  - Portal del Usuario.
- La solución debe proveer un portal web para el usuario final con las siguientes características:
  - Permitir que el usuario realice el registro de sus propios factores de autenticación, como preguntas y respuestas, FIDO2 tokens, OATH OTP, definir PIN para llamada telefónica, TouchID, FaceID, entre otros.
  - Permitir que el usuario redireccione la autenticación de múltiples factores a otros usuarios (si está permitido), por ejemplo, para su gerente.
  - Permitir que los usuarios gestionen sus dispositivos registrados, como mínimo:
  - Smartphones Android y IOS.
  - Sistemas operativos Windows y MacOS.
  - Para cada dispositivo registrado, los usuarios deberán tener las siguientes capacidades de gestión:

  - Deshabilitar el SSO remotamente.
  - Habilitar el SSO remotamente.
  - Registrar nuevos dispositivos móviles.
- La solución debe proveer una aplicación móvil para Android y IOS con las siguientes características:
  - Después de efectuar el login, debe presentar las aplicaciones web disponibles para realizar el SSO a través de un conjunto de íconos, donde cada uno represente una aplicación en la que el usuario tenga derecho a efectuar el SSO ya integrado con los navegadores instalados en los dispositivos móviles.
  - Que permita el login a través del escaneo de código QR en el portal web, para permitir SSO sin identificación de usuario y contraseña.
  - Que permita configurar OATH OTP adicionales provenientes de otras soluciones.
  - Que permita configurar OATH OTP para autenticación de múltiples factores en los sistemas operativos Windows y MacOS (pantalla de login y bloqueo) sin conexión a Internet.
  - Que verifique los dispositivos registrados (dispositivos móviles y sistemas operativos).
  - Que cuente con integración nativa con FaceID, TouchID, lector biométrico de los dispositivos móviles e impulse su uso para la autenticación biométrica durante el login en las aplicaciones.
  - Que reporte coordenadas GPS a los sistemas que utilizan geolocalización.
  - Que detecte ROOT en dispositivos Android y Jailbreak en dispositivos IOS, para detectar actividades maliciosas y, como consecuencia, deshabilitar el uso de la aplicación.
- La aplicación móvil (IOS y Android) debe soportar la autenticación de tipo push, en que el usuario puede elegir si aceptar o rechazar el desafío. Esta notificación debe contener, como mínimo, la siguiente información:
  - Fecha y hora.
  - Ciudad/geolocalización de acceso.
  - Aplicación a la que se accede.
- Durante la creación de un perfil de autenticación con sus métodos multifactor, la solución debe indicar en qué nivel de confianza de autenticación el administrador de la solución configura dicho perfil de autenticación, según la publicación especial de NIST SP 800-63-3, sobre el guía de identidad digital que clasifica una autenticación en 3 niveles, AAL1, AAL2, AAL3 (Authenticator Assurance Level). Siendo 1 el menos seguro y 3 el más seguro posible con los métodos actuales de autenticación multifactor.

55. PAM - Administración de Acceso Privilegiado (01 solución)

- La solución propuesta deberá ofrecerse como servicio (SaaS) y al menos tener las certificaciones SOC 2 Type 2, SOC 3, ISO27001, ISO 27017, ISO 27018 entre otras.
- La solución debe estar licenciada para 50 usuarios privilegiados.
- La solución propuesta deberá tener un repositorio seguro o boveda digital, el cual debe estar patentado por el fabricante, esto quiere decir que no deberá tener software de bases de datos comerciales para resguardar la informacion.
- La solución ofertada deberá contar con una boveda (vault) segregado, con cifrado y hardening propietario certificado (FIPS/NIST), no dependiente de OS estándar.
- La solución propuesta debe tener una boveda patentada que debe estar certificada por el Common Criteria y tener un nivel de certificacion minima de Evaluation Assurance Level (EAL) 2+.
- La solución ofertada no debe requerir establecer enlaces VPNs IPSec o Direct Connect con la nube de la solución SaaS.
- La solución propuesta no debe de tener limites en cuanto a conexiones concurrentes por usuarios, estas deben ser ilimitadas.
- La solución propuesta, no debe tener limite en cuanto a la cantidad de dispositivos, integraciones o cuentas a proteger.
- La comunicación a internet necesaria por la solución debe ser solo de salida (outbound)
- La solución propuesta deberá tener la capacidad de cifrar, en reposo y en tránsito todos los datos que utilice. Incluyendo contraseñas, reportes almacenados, grabaciones y

registros de usuarios. Lo anterior utilizando algoritmos que cumplan con los estándares en FIPS 140-2, como AES-256 y RSA-2048.

- La solución debe ayudar a la organización a administrar y monitorear los accessos privilegiados y el uso de las credenciales privilegiadas, utilizadas por identidades humanas y no humanas, asociadas a infraestructura en ambientes híbridos; incluyendo servidores, bases de datos, dispositivos de comunicaciones, soluciones de seguridad y apliaciones en un centro de datos, así como en ambientes de nube pública
- Deberá tener la capacidad de ejecutar operaciones de forma masiva (bulk operations) sobre las cuentas privilegiadas, como altas y modificaciones.
- La solución de Seguridad de Cuentas Privilegiadas deberá tener la capacidad de administrar la plataforma de forma centralizada a través de un portal web y capacidad para restringir accesos a través de zonas de red confiables.
- El SLA del servicio debe ser mínimo de 99.9%
- La solución ofertada al ser SaaS, deberá contar con mecanismos de alta disponibilida entre regiones, sin incurrir en costos adicionales.
- La solución ofertada al ser SaaS, deberá de estar disponible minimo en 8 zonas de disponibilidad.
- La solución debe tener la capacidad de soportar el uso de aplicaciones y servicios que se ejecuten en un sistema hibrido, esto quiere decir en entornos nube y en la premisa.
- La solución propuesta deberá tener la capacidad de proporcionar un esquema Bring-your-own key (BYOK), de tal manera que le permita al cliente retirar la llave que descifra la informacion de la boveda cuando lo vea conveniente.
- La solución propuesta deberá tener la capacidad de permitir al cliente definir su propia llave de cifrado y reemplazar la llave de cifrado predeterminada de la plataforma cuando crea conveniente. Esto le permite a la solución ofertada acceder a su llave de cifrado y que la solución la utilice para cifrar sus datos.
- La solución deberá tener la capacidad de descubrir cuentas privilegiadas humanas y no-humanas, sin la necesidad de agentes.
- La solución deberá tener la capacidad de descubrir cuentas de servicio que tengan dependencias con aplicaciones o servicios ejecutados en la organizacion (ej: tareas programadas, archivos de sistema, servicios de windows, entre otros).
- La solución deberá tener la capacidad de descubrir usuarios y llaves SSH sobre sistemas Unix y Linux.
- La solución deberá tener la capacidad de descubrir usuarios o cuentas privilegiadas en Windows y MACoS
- La solución deberá tener la capacidad de descubrir usuarios o cuentas privilegiadas en bases de datos, minimo MS SQL Server, Oracle y PostgresSQL.
- La solución ofertada deberá tener la capacidad de descubrir credenciales en ambientes de nube publica, obteniendo el contexto no solo de cuentas sino tambien de roles y grupos que puedan tener privilegios.
- La solución ofertada deberá proporcionar capacidades de escaneos de una sola vez o de manera recurrente para el proceso de descubrimiento.
- La solución ofertada deberá tener la capacidad de programar los escaneos.
- La solución ofertada deberá tener la capacidad de crear politicas para que las cuentas que se descubran sean protegidas en un esquema automático.
- La solución ofertada debe permitir importación y exportación de conjuntos de reglas de descubrimiento y proteccion permitiendo a los administradores reutilizar las reglas en diferentes entornos de forma eficiente.
- La solución ofertada deberá tener componentes de IA que utilicen las capacidades basadas en la experiencia operativa y los conocimientos que el fabricante ha acumulado durante muchos años en la gestión de sistemas de seguridad de identidad, sin costo adicional.
- La solución ofertada deberá tener un asistente conversacional basado en IA que le permita interactuar con los servicios de la solución a través del lenguaje natural para generar consultas, obtener información importante sobre el sistema, ejecutar comandos, configuraciones y mantener fácilmente su sistema, sin costo adicional.
- La solución ofertada deberá tener componentes de IA que trabajen de forma integrada en las funciones claves para proteger la identidad y el acceso de los usuarios. Esto incluye la detección de cuentas y recomendaciones para la baja de cuentas. Estas

funciones le ayudan a encontrar rápidamente cuentas importantes o a eliminar las que ya no necesita, sin costo adicional.

- La solución propuesta deberá tener mecanismos de detección y alerta cuando se detecta una desviación en el patrón de comportamiento de un usuario humano al recuperar/obtener un secreto de la boveda digital o de la plataforma. Esta detección puede indicar un abuso de la plataforma de identidades y la vulnerabilidad o brecha de la identidad del usuario.
- La solución ofertada deberá incorporar mecanismos de Inteligencia Artificial (IA) y/o Machine Learning que permitan procesar y analizar las sesiones privilegiadas de los usuarios. Dichos mecanismos deberán:
    - Generar un veredicto automático sobre la sesión (ej. categorización como normal, riesgosa o anómala).
    - Detectar comportamientos atípicos o desviaciones respecto a patrones de uso establecidos.
    - Proveer un informe resumido y auditable del veredicto, con trazabilidad y evidencia que sustente la clasificación realizada.
    - Permitir la integración con sistemas de monitoreo y alertamiento para la gestión de incidentes de seguridad.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de los siguientes Sistemas Operativos: Windows, Unix, Linux, IBM iSeries, Z/OS, HP Tandem, MAC OS, ESX/ESXi, XenServers, Linux RedHat, etc. Detallar todos los Sistemas Operativos que son soportados por la solución.
- La solución propuesta debe permitir que los administradores de la solución no tengan acceso a las contraseñas almacenadas si así se define por el negocio.
- La solución propuesta deberá tener la capacidad de permitir que ciertos administradores no puedan visualizar las contraseñas que son controladas por otros departamentos de la compañía, como por ejemplo que los administradores de Windows Server no puedan visualizar las contraseñas ni accesos a instancias de bases de datos SQL Server. Esto es para garantizar la separación de roles lo más posible para evitar el uso indebido de las cuentas privilegiadas protegidas por la solución.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de las siguientes Bases de datos: Oracle, MSSQL, DB2, Postgresql, mongoDB, Teradata, etc. Detallar todos los motores de base de datos SQL y NOSQL que son soportados por la solución.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas basadas en los siguientes servicios de directorio: Microsoft AD, Azure AD, Google. Detallar todos los servicios de directorio que son soportado por la solución.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de dispositivos de red (Firewalls, Routers, Switches, APs, etc). Detallar un listado completo con todos los diferentes dispositivos de Red que son soportados por la solución.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de Aplicaciones Cloud como Facebook, Google G Suite, Google Gmail, GitHub, Docker, Puppet,Cloudflare, Aqua, IBM Cloud, LinkedIn,instagram, Twitter, Amazon, Azure, VMware, Office 365,Paloalto, RedHat Ansible/OpenShift, salesforce. Detallar para que servicios SAS que son soportados por la solución "out of the box"
- En el caso que la cuenta privilegiada de una plataforma SaaS (ejemplo consola Cloud) posea un doble factor de autenticación en el inicio de sesion, en este escenario la solución debe poder permitir que el usuario agregue el factor necesario a lo menos en cuentas AWS y Azure. Detallar
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de aplicaciones de Nube/DevOps y controlar el acceso de herramientas a consolas de nube que utilicen mecanismos modernos de integracion tales como SAML, OpenID y WS-Federation, entregando una experiencia nativa, sin utilizar el jumpserver.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de redes sociales: Facebook, Instagram, Whatsapp, Linkedin, etc. Sin pasar por el jumpserver y garantizando los mecanismos de control, proteccion y grabacion de sesion.
- La solución propuesta deberá ser capaz de soportar cualquier dispositivo de red mediante conexión SSH.
- La solución propuesta deberá ser capaz de soportar cualquier repositorio de datos mediante conexión ODBC

- La solución propuesta deberá ser capaz de permitir a través de un administrador definir y agregar cuentas privilegiadas.
- La solución propuesta deberá ser capaz de soportar Conecciones de tipo Ad Hoc.
- La solución propuesta deberá permitir busquedas dentro de los videos de auditoria.
- La solución propuesta deberá ser capaz de detectar automáticamente nuevos dispositivos Laptops o PCs Windows, Servicios Windows(Windows Services), Scheduled Tasks, IIS Service Accounts, etc. para su administración en la solución. Detallar como se realiza este proceso.
- Integración con SIEM (Security Información and Event Management). Detallar un listado de las soluciones que se integra "out of the box"
- Integración con HSM (Hardware Security Module). Detallar un listado con las marcas soportadas.
- Integración con soluciones 2FA. Detallar un listado con las marcar que se integran "out of the box".
- Integración con soluciones de análisis de vulnerabilidades.
- La solución debe disponer de un servicio REST API (Application Programming Interface) vía WebServices para administrar y aprovisionamiento de la solución, que permita entre otras cosas automatizar procesos.
- La solución debe tener la capacidad de entregar un acceso remoto seguro (externo a la red corporativa) a los usuarios sin necesidad de instalación de clientes VPN en los dispositivos de usuarios remotos y garantizando un acceso seguro con MFA sin necesidad de modificar los recursos de autenticación corporativos como el AD,
- Debe supervisar las sesiones privilegiadas, grabar, detectar, correlacionar y mitigar comportamientos anormales, en todas las sesiones soportadas por PAM, entre ellos servidores Linux/Unix, Windows, controladores de dominio de Microsoft Active Directory, estaciones de trabajo Windows, diversos activos de red y de Seguridad, así como aplicaciones Cliente servidor/Web y servicios en Nube ya sean IaaS, SaaS o PaaS.
- Debe proveer un motor de UBA, que ademas de supervisar y adaptase segun el comportamiento, debe tambien tener la capacidad de detectar acciones en sesiones privilegiadas, con al menos soporte para SSH, Windows, SQL, Entradas de Teclado y SCP.
- La Solución debe entregar sesiones administrativas a las que se acceda y monitoree en tiempo real, con el uso compartido de pantalla y el control de periféricos, como el teclado y el ratón (asistencia remota), y mediante la grabación de comandos y vídeos de los mismos, en formato estándar de ejecución no propietaria de la solución, permitiendo que los comandos y vídeos generados se puedan indexar para futuras búsquedas, permitiendo el filtro de comandos y acciones realizadas a lo largo de la sesión grabada , lo que le permite buscar acciones específicas en la sesión grabada;
- La solución debe ser capaz de detectar comportamientos que tipifican abusos, comportamientos anormales y fuera de los estándares aprendidos/asignados, aplicando acciones atenuantes automáticas como la re-autenticación, suspensión y terminación de sesiones y rotación de credenciales privilegiadas en caso de actividad sospechosa de alto riesgo, detectando al menos los siguientes casos: 1- Durante horarios irregulares (cuando un usuario recupera una contraseña de cuenta con privilegios en un momento irregular según su perfil de comportamiento); Durante días irregulares (cuando un usuario recupera una contraseña de cuenta con privilegios en un día irregular de acuerdo con su perfil de comportamiento); A través de IP irregular y desconocida (cuando un usuario accede a cuen-tas con privilegios de una dirección IP o subred inusual, de acuerdo con su perfil de comportamiento); (cuando se realiza una conexión a un equipo con una cuenta con privilegios que no se administra en la solución).
- La solución propuesta deberá ser en formato SaaS, pero que incluya a lo menos los componentes de Proxy (Jump Server) y procesos de cambio de contrasena, en ambientes on-prem, cercano a los usuarios y aplicaciones, con el fin de optimizar el trafico, y seguridad junto con interrupciones de microcorte que no afecte las sesiones locales.
- La solución de Seguridad de Cuentas Privilegiadas debe ser una solución basada en software y debe estar disponible como SaaS o en modelo de suscripción para implementación en ambientes de Nube (AWS, Azure y Google Cloud) y/o instalable sobre entorno físico o virtualizado con infraestructura (servidores / software en entorno virtualizado, S.O., capa de balanceo de tráfico / redirección, etc.

- La solución debe ser modular y escalable para adaptarse a crecimientos de utilización o expansión de funcionalidades e incluso esquemas de Alta Disponibilidad de roles y/o componentes. Es decir, debe poder crecer por cada rol de forma independiente según sea requerido, sin incurrir en licenciamiento adicional
- La solución propuesta deberá contar con la capacidad de integrarse con el modulo SIEM de la Plaforma de Operaciones de Ciberseguridad.
- La solución propuesta deberá tener la capacidad de integrarse a directorios terceros de nube de forma nativa (sin la necesidad de utilizar agentes o maquinas intermediarias), tales como Entra-ID, Google Directory, entre otros.
- La solución propuesta deberá tener la capacidad de integrarse con directorios LDAP/AD y LDAPS, asi como con sistemas Radius.
- La solución propuesta deberá tener la capacidad de integrarse a sistemas de Ticketing/HelDesk/Change Management y permitir la validación de tickets antes de establecer la sesión.
- La solución propuesta deberá tener la capacidad de mostrar en un quick view todas las actividades relativas a una cuenta privilegiada, como el release de un password o sesiones de administración utilizando dicha cuenta
- La solución propuesta deberá tener la capacidad de generar todos los reportes de forma periódica, bajo demanda o en forma programada
- La solución propuesta deberá tener la capacidad de generar reportes detallados y programados con la siguiente información:
    - Entitlements Reports
    - Actividad de usuarios
    - Inventario de cuentas privilegiadas
    - Inventario de aplicaciones
    - Reportes de Cumplimiento
- La solución propuesta deberá tener la capacidad de auditar y generar reportes de todos los cambios administrativos realizados en el sistema
- La solución propuesta deberá cumplir con las siguientes normativas:
    - Ley 25.326 de Protección de Datos Personales
    - GDPR
    - ISO27001
    - PCI-DSS
    - NIST 800-53
- La solución propuesta deberá proporcionar la rotación de contraseñas y llaves en entornos complejos (Mainframe, AS/400, dispositivos OT, aplicaciones legacy) con soporte probado y certificado.
- La solución propuesta deberá tener la capacidad de cambiar passwords cada X días, meses, años
- La solución propuesta deberá tener la capacidad de cambiar múltiples passwords en una sola vez para un solo sistema o sistemas agrupados bajo un solo criterio
- La solución propuesta deberá tener la capacidad de cambiar un password o un grupo de passwords:
    - De acuerdo a una política (cada x días u 'on-demand')
    - Cambios manuales efectuados por un usuario
    - Automáticamente, cuando un password no ha sido sincronizado (falla en verificación)
- La solución propuesta deberá tener la capacidad de asignar passwords a un valor random
- La solución propuesta deberá tener la capacidad de cambiar manualmente un password por un administrador en cualquier momento
- La solución propuesta deberá tener la capacidad de cambiar automáticamente el valor de un password después de un tiempo especificado de un "chek out" del password
- La solución propuesta deberá tener la capacidad de cambiar automáticamente el password de una cuenta que acaba de ser definida en el sistema
- La solución propuesta deberá tener la capacidad de verificación automática del valor de un password en el sistema correspondiente
- La solución propuesta deberá tener la capacidad de automáticamente reconciliar passwords que se hayan detectado como "out of sync" o que se hayan perdido, sin utilizar herramientas externas de restauración

- La solución propuesta deberá tener la capacidad de configurar una longitud mínima de contraseña y complejidad para cuentas de súper-usuarios de todos los sistemas
- La solución propuesta deberá tener la capacidad de mantener el historial de contraseñas, ej. Las últimas tres contraseñas o por periodo de tiempo y proveer fácil acceso a ellas a través de la interfaz web del producto
- La solución propuesta deberá tener la capacidad de administrar cuentas de súper-usuario que han sido renombradas de su nombre por default
- La solución ofertada deberá proporcionar mecanismos de acceso privilegiado seguro a aplicaciones web empresariales sin requerir el uso de un jump server tradicional. Dicho acceso deberá:
    - Ofrecer una experiencia nativa de usuario (el usuario ingresa directamente a la aplicación sin interfaces intermedias forzadas).
    - Establecer sesiones seguras mediante protocolos estándar (ej. HTTPS/TLS) con aislamiento de credenciales, de forma que éstas nunca sean expuestas al usuario.
    - Soportar Single Sign-On (SSO) y federación de identidades (SAML, OIDC, Kerberos, etc.) para un acceso simplificado y seguro.
    - Incorporar registro y monitoreo de la sesión en segundo plano para garantizar auditoría y trazabilidad completas.
    - Permitir integración con MFA/biometría como paso adicional de seguridad antes de conceder privilegios.
- La solución propuesta deberá tener la capacidad de soportar conexiones transparentes a un dispositivo target, sin la necesidad de ver o teclear la contraseña como parte de la conexión. Detallar los requerimientos para realizar esta funcionalidad.
- La solución propuesta deberá tener la capacidad de soportar conexión directa a dispositivos UNIX/LINUX de administración (SSH) pudiendo grabar la sesion, con una experiencia de conexion nativa, esto quiere decir utilizando los clientes o herramientas instaladas en la estacion de trabajo y sin la necesidad de acceder al portal de la plataforma de gestion de accesos privilegiados.
- La solución debe permitir establecer sesiones de bases de datos de manera nativa, tales como SQL Server, PostgresSQL, Oracle, MySQL, Snowflake y MongoDB utilizando el cliente nativo correspondiente al que el usuario y/o administrador utiliza en su estacion de trabajo (SQL Server Management Studio, PGAdmin, PL/SQL Developer, entre otros), sin mostrar la contraseña.
- La solución debe permitir establecer sesiones de RDP, SSH y SCP de manera nativa ejecutando el cliente correspondiente instalado (MSTSC, Putty Manager, Moba Xterm, entre otros.) en la estación de trabajo del usuario y/o administrador, sin mostrar la contraseña.
- La solución debe permitir establecer sesiones a ambientes de Kubernetes de manera nativa, ejecutando el cliente correspondiente instalado (Kubectl) en la estación de trabajo del usuario y/o administrador, sin mostrar la contraseña.
- La solución propuesta debe permitir conexiones VPN-less de manera nativa, esto quiere decir que permita conexiones remotas hacia equipos destino sin la necesidad del uso de conexiones IPSec o de agentes VPN instalados.
- La solución propuesta deberá contar con mecanismos de MFA-Caching de tal manera que agilite el acceso privilegiado dentro de las multiples sesiones diarias que puede generar un usuario.
- La solución ofertada debe proporcionar un de acceso basado en el privilegio minimo y con experiencia nativa.
- La solución ofertada deberá soportar diferentes principios de acceso privilegiado de tal manera que pueda robustecer los accesos en ambientes estaticos y dinamicos, asi como disminuir el riesgo e impacto en el acceso otorgado.
- La solución ofertada debe proporcionar un esquema de acceso privilegiado "permanente", en cual se tienen capacidades como almacenamiento de cuentas en boveda digital, rotacion, aislamiento, monitoreo y grabacion de sesion.
- La solución ofertada debe proporcionar un esquema de acceso privilegiado "JIT (Just-In-Time)", en el cual el acceso privilegiado puede ser dado al momento, pero a intervalos limitados de tiempo con procesos de elevacion o aprobacion de acceso.
- La solución ofertada debe proporcionar un acceso privilegiado "Temporal", en el cual se controle el acceso y el privilegio, de esta forma se va a proporcionar el privilegio al

momento de generar la sesion de acceso privilegiado mediante un rol y/o cuenta privilegiada de manera temporal, dentro de un intervalo de tiempo especifico y basado en el minimo privilegio.
- La plataforma ofertada deberá tener la granuralidad para definir politicas de acceso basados en atributos o características propias de la nube, tales como VPC, Subnets, Segmentos y tags.
- La solución propuesta deberá tener la capacidad de grabar sesiones privilegiadas en: Windows, Virtual Servers, Linux, equipos de comunicaciones, Bases de Datos, Aplicaciones Web. Detallar cuales son los requerimientos para realizar esta capacidad.
- La solución propuesta deberá tener la capacidad de hacer búsquedas de comandos privilegiados dentro de las grabaciones de video. Detallar los requerimientos para realizar esta operacion.
- La solución propuesta deberá tener la capacidad de grabar las sesiones privilegiadas sin necesidad de un agente instalado en los targets o en los origenes del sistema operativo desde donde se genera la sesion.
- La solución propuesta deberá almacenar los videos de grabacion de manera cifrada, utilizando algoritmos de cifrado robustos, tales como aes-256.
- La solución propuesta deberá contar con la funcionalidad de terminar la sesion cuando el auditor o administrador lo requiera, de tal manera de poder generar un mecanismo de accion inmediato ante algun incidente presentado.
- La solución propuesta deberá contar con la funcionalidad de monitorear la sesion en tiempo real, sin requerir el control remoto de la sesion establecida de tal manera que se respete el principio de no-repudio y se mantenga la integridad de la sesion generada.
- La solución propuesta deberá tener la capacidad de mantener la grabacion de sesiones como minimo 2 años, y contará con almacenamiento ilimitado durante ese tiempo.
- La solución propuesta deberá tener la capacidad de contar con un método para detectar llaves SSH pares, llaves huérfanas y relaciones de confianza en la organización
- La solución propuesta deberá tener la capacidad de almacenar de forma segura y controla el acceso a las llaves privadas SSH
- La solución propuesta deberá tener la capacidad de permitir la automatización de rotación de llaves.

56. NDR (Network Detection and Response) – 01 solución

- La solución debe consistir en una plataforma capaz de detectar amenazas que se propagan por la red, así como comportamientos anómalos asociados a un ciberataque. Debiendo integrarse o formar parte de una plataforma unificada de operaciones de seguridad que integre de manera nativa múltiples fuentes de telemetría (endpoint, red y otros componentes de seguridad), sobre un modelo de datos común que permita la correlación automatizada de eventos, la generación de alertas consolidadas y la ejecución de acciones de respuesta desde una única consola.
- Deberá integrarse a un dispositivo de tipo hardware conectado a la red interna de la Entidad y extraer información del tráfico para la detección de amenazas.
- El dispositivo deberá tener una capacidad de inspección de 28 Gbps de tráfico, e incluir 02 interfaces de Fibra de 1G/10G (formato SF/SFP+) y 04 interfaces de Cobre 1G RJ45.
- Se deberá incluir 02 transceiver SFP+ 10Gbps MMF.
- El sensor debe ser capaz de recolectar y enviar automáticamente la siguiente telemetría de red:
    - Logs avanzados o telemetría detallada, es decir eventos que incluyan contenido de la aplicación de red en capa 7, cabecera HTTP, querys de DNS, información del tráfico DHCP y otros datos de la telemetría de red.
    - Eventos del tráfico mostrando: IP y puerto origen y destino, nombre de la aplicación en capa 7, país origen y destino, IP NAT de origen y destino, usuario de dominio, Bytes enviados y recibidos, Paquetes enviados y recibidos, DNS Querys, información sobre tráfico DHCP.
    - Nombre, serial number, nombre de la política y/o regla de seguridad de los Firewalls.
    - Nombre, tipo, categoría y severidad de la amenaza identificada.
    - Nombre del archivo transferido a través del tráfico de red.

  - Logs de tráfico URL, detallando URL accedida, categoría, severidad, hora, IP origen/destino, usuario, país de la URL, User-Agent de los paquetes HTTP.
  - Atributos de los dispositivos de red, tales como tipo de dispositivo, categoría, marca, sistema operativo, fabricante del dispositivo.

- La solución deberá ser una plataforma de autoaprendizaje con enfoque adaptativo, que utilice inteligencia artificial validada para modelar el comportamiento normal del entorno, permitiendo detectar, analizar y responder a desviaciones anómalas de la actividad esperada.
- La plataforma deberá ser capaz de identificar comportamientos anómalos en el entorno, resaltándolos de forma clara y contextualizada para su análisis e investigación por parte del equipo de seguridad.
- La solución deberá emplear algoritmos avanzados de inteligencia artificial y aprendizaje automático, incluyendo como mínimo Machine Learning supervisado, no supervisado y técnicas de Deep Learning, orientados a la detección de amenazas conocidas y desconocidas.
- La plataforma deberá asociar automáticamente cada alerta o incidente de seguridad con las tácticas y técnicas del framework MITRE ATT&CK, facilitando el análisis, priorización y entendimiento del ataque.
- La solución deberá contar con al menos 80 casos de uso predefinidos para la detección de anomalías en la red, orientados a identificar comportamientos sospechosos y patrones de ataque.
  - Accesos recurrentes a IP sospechosas
  - Sesiones SMB sospechosas hacia un host remoto
  - Uso de aplicaciones de red inusuales
  - Llamada EFSRPC sospechosa al domain controller
  - Subida masiva de información a sitios de storage
  - Escaneo de red y puertos
  - Sesiones SMTP anómalas
  - Subida de información anómala y excesiva por HTTPS, FTP u otro puerto no estándar.
  - Recurrente acceso a un Dominio y/o IP inusual
  - Acceso no-web a un sitio como Pastebin o similar
  - Proceso no-web accediendo a un website
  - Transferencias de archivos sospechosas vía protocolo SMB
  - Conexión inusual de túnel de red
  - Múltiples conexiones fallidas de DNS que puedan representar C&C
  - DNS Tunneling
  - Paquetes ICMP sospechoso con posible ataque de tunneling de protocolo
  - Posible cryptominer en un host
  - Fuzzing de subdominios
- La solución deberá contar con un módulo de monitoreo, descubrimiento, identificación y clasificación de dispositivos como teléfonos IP, cámaras de vigilancia, consolas de videojuegos, impresoras, dispositivos médicos, equipos industriales, entre otros.
- Por cada dispositivo identificado deberá mostrar la marca del fabricante, tipo de dispositivo, serial number, sistema operativo, dirección IP, dirección MAC, tipo de conexión (cableada o wireless), nombre del SSID o Puerto del switch al cual está conectado, según corresponda. Deberá ser capaz de crear grupos basados en el tipo de dispositivo.

57. Sandboxing (01 solución)

- La plataforma sandbox deberá proporcionar capacidades de análisis dinámico de amenazas (sandboxing) como un componente centralizado, orientado a la detección de malware avanzado y amenazas desconocidas.
- Esta plataforma deberá operar de forma integrada y transversal con los diferentes componentes de la arquitectura de seguridad propuesta, incluyendo como mínimo: los equipos NGFW, la solución XDR, la solución NDR, la solución SIEM, la solución SOAR y automatización (SOAR).
- La plataforma de Sandbox podrá ser ofrecido en Nube (Cloud), On-premise o ambos.
- Deberá ser capaz de emular el potencial malware en entornos Windows, Linux y MacOS.

- Los firewalls deberán ser capaces de de enviar 5000 archivos por hora al sandbox.
- El sandbox deberá ser capaz de analizar 5000 archivos por hora realizando análisis dinámico del archivo (entiéndase por análisis dinámico aquel que no está basado en firmas, ni prefiltros, sino en emulación completa del potencial malware).
- También se aceptará soluciones sandbox terceras de otro fabricante distinto al NGFW.
- En caso de tratarse de una plataforma de Sandbox Cloud, deberá cumplir con los siguientes requerimientos:
    - Deberá tener una disponibilidad de al menos 99.9% contabilizados mensualmente.
    - Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II Plus de AICPA, ISO 27001, ISO 27017 e ISO 27018.
- En caso de tratarse de una plataforma de Sandbox On-premise, deberá cumplir con los siguientes requerimientos:
    - Deberá soportar un throughput de 8 Gbps por cada equipo.
    - Deberá ser desplegado en Alta Disponibilidad (Activo-Pasivo) en cada sede, con el objetivo de mantener los controles de seguridad en caso de contingencia.
    - Debe proveer información forense sobre las acciones realizadas por el malware, tales como resumen del comportamiento visto, actividad sobre los archivos, peticiones DNS, conexiones de red, actividad de los archivos, procesos y registros. Esta información deberá poder se extraída en un reporte PDF.
    - Deberá ser capaz de analizar archivos sospechosos que se transfieran por los protocolos SMTP, POP3, IMAP, SMB, FTP, HTTP y HTTPS.
    - Debe ser capaz de identificar amenazas de tipo Fileless.
- Deberá contar con al menos 20 técnicas patentadas para realizar el análisis del malware.
- El sandbox debe identificar los ataques de phishing al momento de emular los potenciales archivos maliciosos: swf, html, lnk y js.
- Luego del análisis realizado por el sandbox, éste deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. Las firmas deben estar basadas en patrones del malware y no únicamente hashes, de tal forma que sea capaz de bloquear el malware polimórfico con una única firma.
- Debe permitir al administrador la descarga del archivo original analizado por el sandbox.
- Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.
- Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico.
- Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
- La solución debe incorporar un motor avanzado de prevención de malware para la inspección de tráfico en tiempo real. Dicho motor deberá estar potenciado por inteligencia artificial (Inline Malware Prevention) y/o aprendizaje automático (Inline machine learning) para la detección proactiva de amenazas, incluyendo las de día cero.

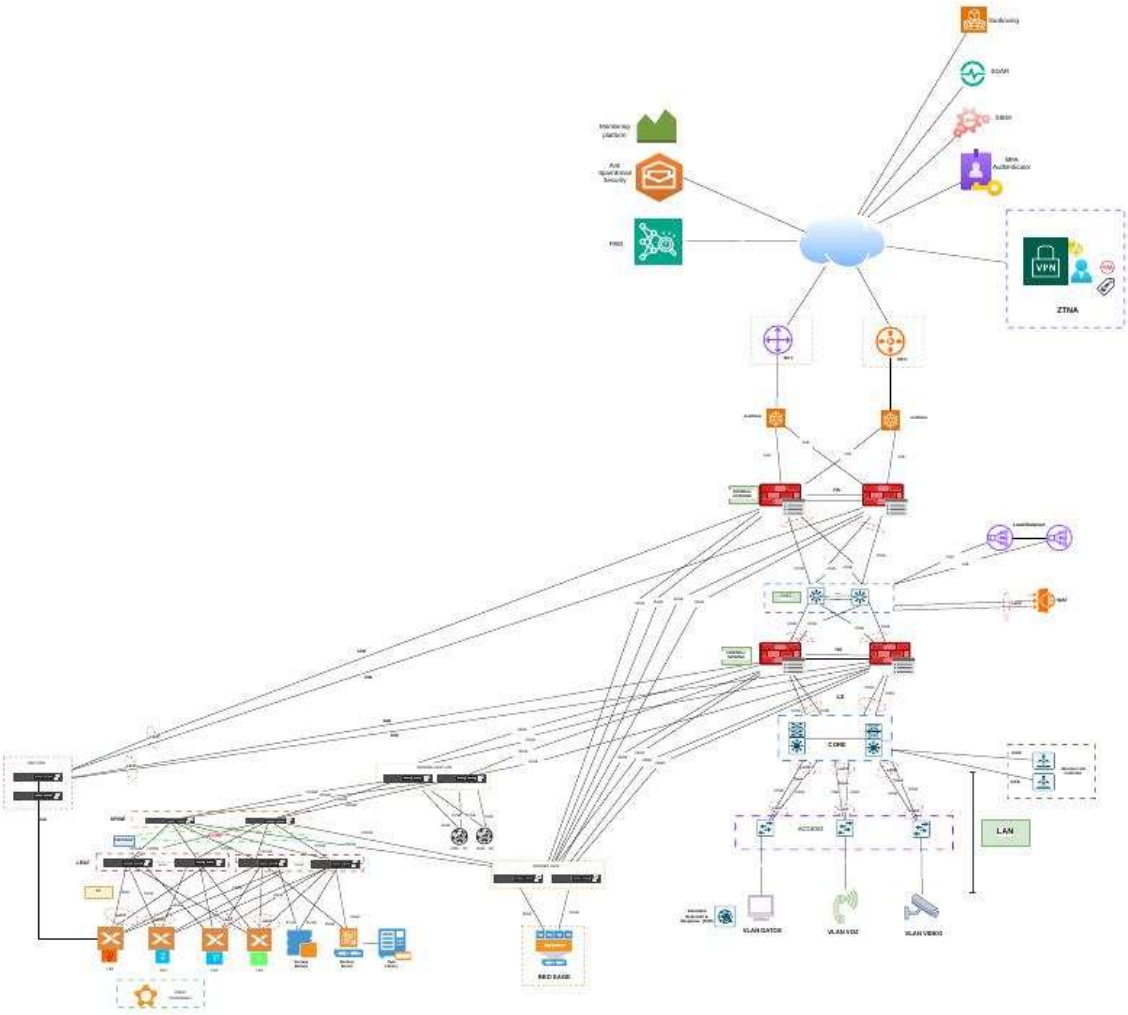
58. Solución de Análisis de Tráfico de Red - (01 Solución)

- La solución podrá ser provista en appliance físico del mismo fabricante, virtual appliance o bajo modelo SaaS (Cloud).
- El postor deberá incluir el hardware o los requerimientos necesarios para el montaje y operación de la instancia.
- No se aceptará que algún componente de la solución sea freeware, trial u open-source sin soporte del fabricante.
- Debe poder monitorear al menos 100 dispositivos, servidores o nodos de red.
- Debe contar con una vista de alto nivel del estado de la infraestructura que permita agrupar y explorar dinámicamente nodos, identificando de inmediato los puntos conflictivos.
- Debe ofrecer opciones de agrupamiento por grupo de instancia, etiqueta, tipo de dispositivo o sitio.

- Debe permitir la navegación jerárquica a través de los distintos niveles de la topología conservando filtros y modalidades de agrupamiento.
- Debe posibilitar la creación de vistas guardadas, capturando configuración de filtros y agrupamientos para acceso rápido.
- Debe exponer en una sola página la disponibilidad, rendimiento, incidentes y configuración de monitoreo de la instancia
- Debe disponer de un panel de acciones rápidas para agregar mantenimiento, aplicar plantillas.
- Debe permitir la creación de nuevos paneles de control definiendo propiedades como nivel de acceso y disponibilidad pública mediante URL.
- Debe permitir monitorear servidores y servicios accesibles públicamente utilizando una red de sondas distribuidas o colectores locales.
- Debe permitir el uso de un colector local para lograr monitoreo en profundidad y alcanzar de forma segura dispositivos detrás del firewall.
- Debe permitir el monitoreo de métricas clave de salud del sistema operativo y rendimiento de aplicaciones mediante protocolos estándar o agentes.
- Debe permitir agregar monitoreo a un servidor o dispositivo manualmente, seleccionando los servicios o aplicaciones y configurando las métricas.
- Debe monitorear para asegurar que las aplicaciones y servicios estén disponibles, funcionales y cumplan con las expectativas en tiempo real.
- Debe permitir recolectar información detallada sobre la calidad de la red de enlaces activos y de respaldo.
- Debe presentar el rendimiento a nivel de dispositivo y a nivel de puerto/interfaz mediante gráficos de línea y estadísticas de entrada/salida.
- Debe soportar la recepción de traps SNMP, permitiendo configurar alertas basadas en OID y severidad.
- Las notificaciones deben poder enviarse a través de canales directos e integraciones con herramientas de terceros.

ANEXO 2 – DIAGRAMA TOPOLOGICO

Se adjunta el diagrama topológico de la red LAN para la Central 911


VPN
ZTNA
CORE
LAN

"Año de la Esperanza y el Fortalecimiento de la Democracia"

ANEXO 3 – GARANTÍA Y SOPORTE DE LOS BIENES

La garantía y soporte será de 12 meses 24x7 on-site, con cuatro (04) horas de tiempo de respuesta, por el periodo con actualizaciones permanentes y condiciones indicado en el siguiente cuadro:

Cuadro Nro. 01

Nro	Bien	Cantidad	Características de la garantía y soporte.
1	Computadora de Escritorio Tipo 1	210	12 meses onsite por el proveedor
2	Computadora de Escritorio Tipo 2	71	12 meses onsite por el proveedor
3	Monitor para Computadoras	696	12 meses onsite por el proveedor
4	Teclado y Mouse	281	12 meses onsite por el proveedor
5	Soporte de Monitores Computadoras de Escritorio Tipo 1	210	12 meses onsite por el proveedor
6	Equipo Portátil	9	12 meses onsite por el proveedor
7	Auricular Monoaural	210	12 meses onsite por el proveedor
8	Micrófono	115	12 meses onsite por el proveedor
9	Altavoces	115	12 meses onsite por el proveedor
10	PPT de pie	210	12 meses onsite por el proveedor
11	Cámara Web	281	12 meses onsite por el proveedor
12	Teléfonos IP Tipo 1	201	12 meses onsite por el proveedor
13	Teléfonos IP Tipo 2	62	12 meses onsite por el proveedor
14	Teléfonos IP Tipo 3	16	12 meses onsite por el proveedor
15	Teléfonos IP Tipo 4	4	12 meses onsite por el proveedor
16	Botonera para teléfono IP 4	1	12 meses onsite por el proveedor
17	Pantalla para Monitoreo	2	12 meses onsite por el proveedor
18	Videoconferencia	4	12 meses onsite por el proveedor
19	Impresora tipo personal	13	12 meses onsite por el proveedor
20	Impresora tipo mediano volumen	5	12 meses onsite por el proveedor
21	Proyector Multimedia	4	12 meses onsite por el proveedor
22	Tabletas Rugerizadas	37	12 meses onsite por el proveedor
23	Switches Spine Data Center	2	12 meses onsite por el proveedor
24	Switches Leaf Data Center	8	12 meses onsite por el proveedor
25	Solución de Orquestador DC	1	12 meses onsite por el proveedor
26	Switch Core LAN Campus	2	12 meses onsite por el proveedor
27	Switch de acceso 48 puertos PoE	23	12 meses onsite por el proveedor
28	Switch de acceso 24 puertos PoE	4	12 meses onsite por el proveedor
29	Switch DMZ	2	12 meses onsite por el proveedor
30	Switch de Gestión Fuera de Banda	2	12 meses onsite por el proveedor
31	Controlador inalámbrico	2	12 meses onsite por el proveedor
32	Access Point	47	12 meses onsite por el proveedor
33	Solución de Administración y Gestión Campus	1	12 meses onsite por el proveedor
34	Solución de Control de Acceso	1	12 meses onsite por el proveedor
35	Hardware de Hiperconvergencia	4	12 meses onsite por el proveedor
36	Software Hiperconvergencia	1	12 meses onsite por el proveedor
37	Servidor para backup	1	12 meses onsite por el proveedor
38	Servidor de inmutabilidad	1	12 meses onsite por el proveedor
39	Almacenamiento para backup	1	12 meses onsite por el proveedor
40	Librería de backup	1	12 meses onsite por el proveedor
41	Software de backup	1	12 meses onsite por el proveedor
42	Firewall NGFW Perimetral	2	12 meses onsite por el proveedor

43	Firewall Interno	2	12 meses onsite por el proveedor
44	Consola de analítica y reportes	1	12 meses onsite por el proveedor
45	XDR (Extended Detection & Response)	1	12 meses onsite por el proveedor
46	ZTNA (Zero Trust Network Access)	1	12 meses onsite por el proveedor
47	Seguridad para correo electronico	1	12 meses onsite por el proveedor
48	WAF - Seguridad para Aplicaciones Web	1	12 meses onsite por el proveedor
49	SIEM	1	12 meses onsite por el proveedor
50	Plataforma de detección y re spuesta de amenazas externas e internas	1	12 meses onsite por el proveedor
51	SOAR - Solución de Orquestación de Seguridad, Automatización y Respuesta	1	12 meses onsite por el proveedor
52	ADC (application Delivery Controller)	2	12 meses onsite por el proveedor
53	Anti-DDos	2	12 meses onsite por el proveedor
54	MFA - Administración de identidad y acceso	1	12 meses onsite por el proveedor
55	PAM - Administración de acceso privilegiado	1	12 meses onsite por el proveedor
56	NDR (Network Detection and Response)	1	12 meses onsite por el proveedor
57	Sandboxing	1	12 meses onsite por el proveedor
58	Solución de Análisis de Tráfico de Red	1	12 meses onsite por el proveedor

Deberá presentar en su propuesta la carta por cada fabricante y/o declaración jurada del proveedor indicando el cumplimiento de la garantía y soporte exigido.

"Año de la Esperanza y el Fortalecimiento de la Democracia"

ANEXO 4 – ACCESORIOS / CONSUMIBLES

1. **Accesorios y consumibles en sitio**
   Corresponde a elementos destinados a reposición por falla, desgaste, mantenimiento preventivo/correctivo o continuidad del servicio.

   Con la finalidad de garantizar la continuidad operativa de las soluciones tecnológicas en el presente requerimiento, el Proveedor deberá entregar los siguientes accesorios adicionales de solo los equipos detallados en el presente anexo, para cambios inmediatos ante fallas:

Componente Tecnológico - Data Center (Spine – Leaf)	Cantidad
Transceivers 100GE-SR4	04
Transceivers 25GE-SR	04
Transceivers 10GE-SR	02
Transceivers 1000Base-T	02

Componente Tecnológico - Campus (Core – Acceso)	Cantidad
Transceivers 25GE-SR	02
Transceivers 10GE-LR	04
Transceivers 10GE-SR	02
Transceivers 1000Base-T	02

Componente Tecnológico - NAC	Cantidad
Transceivers 10GE-SR	02

Componente Tecnológico - Wireless Controller	Cantidad
Transceivers 10GE-SR	02

Componente Tecnológico - DMZ	Cantidad
Transceivers 10GE-SR	02
Transceivers 1000Base-T	02

Componente Tecnológico - Firewall Externo	Cantidad
Transceivers SFP+ 10GE	02
Transceivers SFP28 25GE	02

Componente Tecnológico - Firewall Interno	Cantidad
Transceivers SFP+ 10GE	02
Transceivers SFP28 25GE	02

Componente Tecnológico - Impresoras	Cantidad
Fusor para impresora de tipo personal	01
Fusor para impresora de tipo mediano volumen	02

Asimismo, se deberá proveer los siguientes consumibles para impresoras:

Componente Tecnológico - Impresoras	Cantidad
Toner+Tambor integrado para impresora de tipo personal	26
Toner para impresora de tipo mediano volumen	26
Tambor para impresora de tipo mediano volumen	26

Nota: Durante el periodo de garantía y soporte, estos repuestos y consumibles se ubicarán en el almacen de TI del Edificio de la Central 911, y administrado por el Proveedor durante el periodo indicado para su atención oportuna a través de la mesa de servicio, bajo la Supervisión de la Entidad.

PARTE 3. Contrato

Sección VIII. Condiciones Generales del Contrato

Índice

1. Margen de preferencia (IAL 33) 258

2. Documentos del Contrato 259

3. Fraude y Corrupción 259

4. Interpretación 259

5. Idioma 261

6. Asociación en Participación, Consorcio o Asociación 261

7. Elegibilidad 261

8. Notificaciones 262

9. Ley aplicable 262

10. Solución de controversias 262

11. Inspecciones y auditorías a cargo del Banco 263

12. Alcance de los suministros 263

13. Entrega y documentos 263

14. Responsabilidades del Proveedor 263

15. Precio del Contrato 265

16. Condiciones de Pago 265

17. Impuestos y derecho 265

18. Garantía de Cumplimiento 266

19. Derechos de Autor 266

20. Confidencialidad de la información 267

21. Subcontratación 268

22. Especificaciones y normas 268

23. Embalaje y documentos 268

24. Seguros 269

25. Transporte y servicios conexos 269

26. Inspecciones y pruebas 270

27. Liquidación por daños y perjuicios 271

28. Garantía de los Bienes 271

29. Patentes y exención de responsabilidad 272

30. Limitación de responsabilidad 273

31. Cambio en las leyes y regulaciones 274

32. Fuerza Mayor 274

33. Órdenes de cambio y enmiendas al Contrato 275

34. Prórroga de los plazos 276

35. Resolución 277

36. Cesión 278

37. Restricciones a la exportación 278

Sección VIII. Condiciones Generales del Contrato

1. Definiciones

1.1 Las siguientes palabras y expresiones tendrán los significados que aquí se les asigna:

(a) Por "Banco" se entiende el Banco Mundial y se refiere al Banco Internacional de Reconstrucción y Fomento (BIRF) o a la Asociación Internacional de Fomento (IDA).

(b) Por "Contrato" se entiende el Convenio de Contrato celebrado entre el Comprador y el Proveedor, junto con los Documentos del Contrato allí referidos, incluyendo todos los anexos y apéndices, y todos los documentos incorporados allí por referencia.

(c) Por "Documentos del Contrato" se entiende los documentos enumerados en el Convenio de Contrato, incluyendo cualquier enmienda.

(d) Por "Precio del Contrato" se entiende el precio pagadero al Proveedor según se especifica en el Convenio de Contrato, sujeto a las condiciones y ajustes allí estipulados o deducciones propuestas, según corresponda en virtud del Contrato.

(e) Por "día" se entiende día calendario.

(f) Por "cumplimiento" se entiende la prestación de los Servicios Conexos por parte del Proveedor de acuerdo con los términos y condiciones establecidas en el Contrato.

(g) Por "CGC" se entiende las Condiciones Generales del Contrato.

(h) Por "Bienes" se entiende todos los productos, materia prima, maquinaria y equipos, y otros materiales que el Proveedor deba proporcionar al Comprador en virtud del Contrato.

(i) El "País del Comprador" es el país especificado en las **Condiciones Especiales del Contrato (CEC)**.

(j) Por "Comprador" se entiende la entidad que compra los Bienes y Servicios Conexos, según **se indica en las CEC**.

(k) Por "Servicios Conexos" se entiende los servicios incidentales relativos a la provisión de los bienes, tales como seguro, instalación, capacitación y mantenimiento

inicial y otras obligaciones similares del Proveedor en virtud del Contrato.

(l) Por "CEC" se entiende las Condiciones Especiales del Contrato.

(m) Por "Subcontratista" se entiende cualquier persona física, entidad privada o pública, o una combinación de estas, a las cuales el Proveedor ha subcontratado para que suministren parte de los Bienes o presten parte de los Servicios Conexos.

(n) Por "Proveedor" se entiende la persona física o entidad privada o pública, o una combinación de estas, cuya oferta para ejecutar el Contrato ha sido aceptada por el Comprador y es denominada como tal en el Convenio de Contrato.

(o) Por "emplazamiento del Proyecto", donde corresponde, se entiende el lugar citado en las **CEC**.

2. Documentos del Contrato

2.1 Con sujeción al orden de precedencia establecido en el Convenio de Contrato, se entiende que todos los documentos que forman parte integral del Contrato (y todos sus componentes allí incluidos) son correlativos, complementarios y recíprocamente aclaratorios. El Convenio de Contrato deberá leerse de manera integral.

3. Fraude y Corrupción

3.1 El Banco requiere el cumplimiento de sus Directrices Contra el Fraude y la Corrupción y de sus políticas y procedimientos de sanciones vigentes incluidos en el Marco de Sanciones del Grupo Banco Mundial, conforme a lo estipulado en el Apéndice 1 de las CGC.

3.2 El Comprador exige al Proveedor que divulgue aquellas comisiones u honorarios que pudieran haber sido pagados o que hayan de ser pagados a los agentes o cualquier otra parte con relación al proceso de Licitación o ejecución del Contrato. La información divulgada deberá incluir al menos el nombre y domicilio del agente o de la otra parte, el monto y la moneda, y el propósito de la comisión, gratificación u honorario.

4. Interpretación

4.1 Si el contexto así lo requiere, el singular significa el plural, y viceversa.

4.2 Incoterms

(a) El significado de cualquier término comercial, así como los derechos y obligaciones de las partes serán los prescritos en los Incoterms, **conforme se especifica en las CEC**, a menos que sea incongruente con alguna disposición del Contrato.

(b) El uso de los términos EXW, CIP, FCA, CFR y otros similares se regirá por las normas establecidas en la edición vigente de los Incoterms especificada en las **CEC** y publicada por la Cámara de Comercio Internacional en París, Francia.

4.3 Totalidad del acuerdo

El Contrato constituye la totalidad de lo acordado entre el Comprador y el Proveedor y sustituye todas las comunicaciones, negociaciones y acuerdos (escritos o verbales) realizados entre las partes con anterioridad a la fecha de la celebración del Contrato.

4.4 Enmienda

Ninguna enmienda u otra variación al Contrato será válida, a menos que sea hecha por escrito, esté fechada, se refiera expresamente al Contrato y esté firmada por un representante de cada una de las partes debidamente autorizado.

4.5 Limitación de dispensas

(a) Con sujeción a lo indicado en la Subcláusula 4.5 (b) siguiente de las CGC, ninguna dilación, tolerancia, demora o aprobación por cualquiera de las partes al hacer cumplir algún término y condición del Contrato, así como tampoco el otorgamiento de prórrogas por una de las partes a la otra, perjudicará, afectará o limitará los derechos de esa parte en virtud del Contrato. Asimismo, ninguna dispensa concedida por cualquiera de las partes por incumplimiento del Contrato servirá de dispensa para incumplimientos posteriores o continuos del Contrato.

(b) Toda dispensa de los derechos, facultades o remedios de una de las partes en virtud del Contrato deberá otorgarse por escrito, llevar la fecha y estar firmada por un representante autorizado de la parte que la otorga, y deberá especificar la obligación que está dispensando y el alcance de la dispensa.

4.6 Divisibilidad

Si cualquier disposición o condición del Contrato fuese prohibida o resultase inválida o inejecutable, dicha prohibición, invalidez o falta de ejecución no afectará la validez o el cumplimiento de las otras disposiciones o condiciones del Contrato.

5. Idioma

5.1 El Contrato, así como toda la correspondencia y documentos relativos al Contrato intercambiados entre el Proveedor y el Comprador, deberán ser escritos en el idioma especificado en las **CEC**. Los documentos de respaldo y el material impreso que formen parte del Contrato pueden estar en otro idioma, siempre que vayan acompañados de una traducción fidedigna de las partes pertinentes al idioma especificado, en cuyo caso dicha traducción prevalecerá para a los efectos de la interpretación del Contrato.

5.2 El Proveedor será responsable de todos los costos que implique traducir al idioma principal los documentos que proporcione, así como de todos los riesgos derivados de las posibles imprecisiones de dicha traducción.

6. Asociación en Participación, Consorcio o Asociación

6.1 Si el Proveedor es una Asociación en Participación, Consorcio o Asociación ("APCA"), un consorcio o una asociación, todas las partes que lo conforman serán solidariamente responsables frente al Comprador por el cumplimiento de las disposiciones del Contrato y deberán designar a una de ellas para que actúe como representante con facultades para obligar jurídicamente a la APCA, el consorcio o la asociación. La composición o constitución de la APCA no podrá modificarse sin el previo consentimiento del Comprador.

7. Elegibilidad

7.1 El Proveedor y sus Subcontratistas deberán tener la nacionalidad de un país elegible. Se considera que un Proveedor o Subcontratista tiene la nacionalidad de un país si es un ciudadano o está constituido o inscripto en él y opera de conformidad con sus normas y leyes.

7.2 Todos los Bienes y Servicios Conexos que hayan de suministrarse en el marco del Contrato con financiamiento del Banco deberán tener su origen en países elegibles. Por "origen" se entiende, a los fines de esta instrucción, el país donde los bienes han sido extraídos, cosechados, cultivados, producidos, fabricados o procesados, o donde, como resultado de la manufactura, el procesamiento o el ensamblaje, se genera otro artículo reconocido comercialmente que difiere en gran medida de las características básicas de sus componentes.

8. Notificaciones

8.1 Todas las notificaciones entre las partes en virtud de este Contrato deberán cursarse por escrito a la dirección indicada en las **CEC**. El término "por escrito" se refiere a toda comunicación en forma escrita con prueba de recibo.

8.2 Las notificaciones serán efectivas en la fecha de entrega y en la fecha de la notificación, la que sea posterior.

9. Ley aplicable

9.1 El Contrato se regirá por las leyes del País del Comprador, y se interpretará conforme a dichas leyes, a menos que en las **CEC** se indique otra cosa.

9.2 Durante la ejecución del Contrato, el Proveedor deberá cumplir con las prohibiciones relativas a la importación de bienes y servicios del País del Comprador cuando:

(a) como consecuencia de las leyes o regulaciones oficiales, el país del Prestatario prohibiera las relaciones comerciales con dicho país;

(b) por un acto realizado en cumplimiento de una decisión del Consejo de Seguridad de las Naciones Unidas adoptada conforme al Capítulo VII de la Carta de las Naciones Unidas, el país del Prestatario prohíba cualquier importación de bienes de aquel país, o pagos a cualquier país, persona o entidad de aquel país.

10. Solución de controversias

10.1 El Comprador y el Proveedor harán todo lo posible para resolver amigablemente, mediante negociaciones directas informales, cualquier desacuerdo o controversia que se haya suscitado entre ellos en relación con el Contrato.

10.2 Si, transcurridos 28 (veintiocho) días, las partes no han podido resolver la controversia o diferencia mediante dichas consultas mutuas, el Comprador o el Proveedor podrá notificar a la otra parte sobre sus intenciones de iniciar un proceso de arbitraje con respecto al asunto en disputa, conforme a las disposiciones que se indican a continuación, y no podrá iniciarse un proceso de arbitraje con respecto a dicho asunto, a menos que se haya cursado dicha notificación. Cualquier controversia o diferencia respecto de la cual se haya notificado la intención de iniciar un proceso de arbitraje de conformidad con esta cláusula se resolverá definitivamente mediante arbitraje. El proceso de arbitraje podrá comenzar antes o después de la entrega de los Bienes en virtud del Contrato. El arbitraje se llevará a cabo según el reglamento de procedimientos **estipulado en las CEC.**

10.3 Sin perjuicio de las referencias al arbitraje que figuran en este documento,

(a) ambas partes deben continuar cumpliendo con sus respectivas obligaciones derivadas del Contrato, a menos que acuerden otra cosa;

(b) el Comprador pagará al Proveedor el dinero que le adeude.

11. Inspecciones y auditorías a cargo del Banco

11.1 El Proveedor deberá mantener, y realizar todos los esfuerzos razonables para que sus Subcontratistas mantengan, cuentas exactas y sistematizadas, así como registros contables relativos a los Bienes de forma tal que permitan identificar los tiempos de cambios pertinentes y los costos.

11.2 De conformidad con el párrafo 2.2 (e). del Apéndice 1 de las Condiciones Generales, el Proveedor permitirá, y procurará que sus agentes (hayan sido declarados o no), subcontratistas subconsultores, prestadores de servicios, proveedores y personal permitan, que el Banco o las personas designadas por el Banco inspeccionen las instalaciones y/o las cuentas, los registros y otros documentos relacionados con los procesos de calificación, selección y/o la ejecución del Contrato, y dispongan que dichas cuentas, registros y otros documentos sean auditados por medio de auditores designados por el Banco. El Proveedor y sus Subcontratistas y subconsultores deberán prestar atención a lo estipulado en la Cláusula 3.1 (Fraude y Corrupción), que establece, *inter alia*, que las acciones encaminadas a impedir sustancialmente el ejercicio de los derechos del Banco de realizar auditorías e inspecciones constituyen una práctica prohibida sujeta a la resolución del contrato (además de la determinación de inelegibilidad con arreglo a los procedimientos de sanciones vigentes del Banco).

12. Alcance de los suministros

12.1 Los Bienes y Servicios Conexos se suministrarán según lo estipulado en los Requisitos de los Bienes y Servicios Conexos.

13. Entrega y documentos

13.1 Con sujeción a lo dispuesto en la Subcláusula 33.1 de las CGC, la entrega de los Bienes y la Finalización de los Servicios Conexos se realizará de acuerdo con el Cronograma de Entregas y de Cumplimiento indicado en los Requisitos de los Bienes y Servicios Conexos. Los detalles de los documentos de embarque y otros que deberá suministrar el Proveedor se especifican en las **CEC**.

14. Responsabilidades del Proveedor

14.1 El Proveedor deberá proporcionar todos los Bienes y Servicios Conexos incluidos en el alcance de suministros de conformidad con la Cláusula 12 de las CGC, el Cronograma de Entregas

y de Finalización, de conformidad con la Cláusula 13 de las CGC.

14.2 El Proveedor, incluidos sus Subcontratistas, no empleará ni contratará trabajo forzoso o personas sujetas a trata, como se describe en las Subcláusulas 14.3 y 14.4 de las CGC.

14.3 El trabajo forzoso consiste en cualquier trabajo o servicio, no realizado voluntariamente, que se exige a un individuo bajo amenaza de fuerza o sanción, e incluye cualquier tipo de trabajo involuntario u obligatorio, como trabajo en régimen de servidumbre o acuerdos laborales similares.

14.4 La trata de personas se define como el reclutamiento, transporte, traslado, albergue o recepción de personas mediante la amenaza o el uso de la fuerza u otras formas de coerción, secuestro, fraude, engaño, abuso de poder o de una posición de vulnerabilidad o de dar o recibir pagos o beneficios para lograr el consentimiento de una persona que tiene control sobre otra, con fines de explotación.

14.5 El Proveedor, incluidos sus Subcontratistas, no empleará ni contratará a un niño menor de 14 años a menos que la ley nacional especifique una edad superior (la edad mínima).

14.6 14.6 El Proveedor, incluidos sus Subcontratistas, no deberá emplear ni contratar a un niño entre la edad mínima y la edad de 18 años de una manera que pueda ser peligrosa, o que interfiera con la educación del niño, o que sea dañina para el niño. salud o desarrollo físico, mental, espiritual, moral o social.

14.7 14.7 El trabajo considerado peligroso para los niños es aquel que, por su naturaleza o las circunstancias en las que se lleva a cabo, puede poner en peligro la salud, la seguridad o la moralidad de los niños. Tales actividades laborales prohibidas para los niños incluyen el trabajo:

(a) con exposición a abuso físico, psicológico o sexual;

(b) bajo tierra, bajo el agua, trabajando en alturas o en espacios reducidos;

(c) con maquinaria, equipo o herramientas peligrosos, o que impliquen manipulación o transporte de cargas pesadas;

(d) en entornos insalubres que expongan a los niños a sustancias, agentes o procesos peligrosos, o a temperaturas, ruidos o vibraciones perjudiciales para la salud; o

(e) en condiciones difíciles, como el trabajo durante muchas horas, durante la noche o en confinamiento en las instalaciones del contratante.

14.8 El Proveedor cumplirá y exigirá a sus Subcontratistas, si los hubiere, que cumplan con todas las reglamentaciones, leyes, directrices y cualquier otro requisito de salud y seguridad que se establezca en las Especificaciones Técnicas.

14.9 El Proveedor deberá cumplir con las obligaciones adicionales que se especifican en las **CEC**.

15. Precio del Contrato

15.1 Los precios que cobre el Proveedor por los Bienes proporcionados y los Servicios Conexos prestados en virtud del Contrato no podrán ser diferentes de los cotizados por el Proveedor en su Oferta, salvo que se trate de un ajuste de precios autorizado en las **CEC**.

16. Condiciones de Pago

16.1 El Precio del Contrato, incluyendo cualquier pago por anticipo, si corresponde, se pagará según se establece en las **CEC**.

16.2 La solicitud de pago del Proveedor al Comprador deberá formularse por escrito e ir acompañada de recibos que describan, según corresponda, los Bienes entregados y los Servicios Conexos prestados, y de los documentos presentados de conformidad con la Cláusula 13 de las CGC y en cumplimiento de las obligaciones estipuladas en el Contrato.

16.3 El Comprador efectuará los pagos prontamente, pero en ningún caso podrá hacerlo una vez transcurridos 60 (sesenta) días de la fecha en que el Proveedor haya presentado una factura o una solicitud de pago, y el Comprador la haya aceptado.

16.4 Las monedas en las que se pagará al Proveedor en virtud de este Contrato serán aquellas que el Proveedor hubiese especificado en su Oferta.

16.5 Si el Comprador no efectuara cualquiera de los pagos al Proveedor en las fechas de vencimiento correspondientes o dentro del plazo establecido en las **CEC**, el Comprador le pagará intereses sobre los montos de los pagos en mora a la tasa establecida en las **CEC**, por el período de la demora y hasta que se haya efectuado el pago completo, ya sea antes o después de cualquier sentencia judicial o laudo arbitral.

17. Impuestos y derechos

17.1 En el caso de bienes fabricados fuera del País del Comprador, el Proveedor será totalmente responsable por todos los

impuestos, timbres, comisiones por licencias y otros cargos similares impuestos fuera de dicho país.

17.2 En el caso de bienes fabricados en el País del Comprador, el Proveedor será totalmente responsable por todos los impuestos, gravámenes, comisiones por licencias y otros cargos similares que se abonen hasta la entrega de los Bienes contratados al Comprador.

17.3 El Comprador arbitrará todos los medios necesarios para que el Proveedor se beneficie con el mayor alcance posible de cualquier exención impositiva, concesión o privilegio legal que pudiese serle aplicable en el País del Comprador.

18. Garantía de Cumplimiento

18.1 Si así se estipula en las **CEC**, el Proveedor, dentro de los 28 (veintiocho) días posteriores a la notificación de la adjudicación del Contrato, deberá suministrar la Garantía de Cumplimiento del Contrato por el monto establecido en las **CEC**.

18.2 Los recursos de la Garantía de Cumplimiento serán pagaderos al Comprador como indemnización por cualquier pérdida que pudiera ocasionarle el incumplimiento de las obligaciones del Proveedor en virtud del Contrato.

18.3 Como se establece en las CEC, la Garantía de Cumplimiento, en caso de ser requerida, deberá estar denominada en la(s) misma(s) moneda(s) del Contrato o en una moneda de libre convertibilidad aceptable para el Comprador, y deberá presentarse en uno de los formatos estipulados por el Comprador en las CEC o en otro formato que este considere aceptable.

18.4 A menos que se indique otra cosa en las **CEC**, la Garantía de Cumplimiento será liberada por el Comprador y devuelta al Proveedor a más tardar 28 (veintiocho) días contados a partir de la fecha de Cumplimiento de las obligaciones del Proveedor en virtud del Contrato, incluyendo cualquier obligación relativa a la garantía de los bienes.

19. Derechos de Autor

19.1 Los derechos de autor respecto de todos los planos, documentos y otros materiales que contengan datos e información proporcionados por el Proveedor al Comprador seguirán siendo de propiedad del Proveedor. Si esta información fue suministrada al Comprador directamente o a través del Proveedor por un tercero, incluyendo proveedores de materiales, el derecho de autor de dichos materiales seguirá siendo de propiedad de dichos terceros.

20. Confidencialidad de la información

20.1 El Comprador y el Proveedor deberán mantener bajo estricta confidencialidad y en ningún momento divulgarán a terceros, sin el consentimiento de la otra parte, documentos, datos u otra información que hubiera sido directa o indirectamente proporcionada por la otra parte en relación con el Contrato antes, durante o después de su ejecución. Sin perjuicio de ello, el Proveedor podrá proporcionar a sus Subcontratistas los documentos, datos e información recibidos del Comprador a fin de que estos puedan llevar a cabo su trabajo en el marco del Contrato. En tal caso, el Proveedor obtendrá de dichos Subcontratistas un compromiso de confidencialidad similar al que debe asumir el Proveedor en virtud de la Cláusula 20 de las CGC.

20.2 El Comprador no utilizará dichos documentos, datos u otra información recibidos del Proveedor para ningún fin que no esté relacionado con el Contrato. Asimismo, el Proveedor no utilizará los documentos, datos u otra información recibidos del Comprador para ningún otro fin que el de la ejecución del Contrato.

20.3 No obstante, la obligación de las partes derivada de las Subcláusulas 20.1 y 20.2 de las CGC no se aplicará a información que:

(a) el Comprador o el Proveedor deba compartir con el Banco u otras instituciones que participan en el financiamiento del Contrato;

(b) actualmente o en el futuro pase a ser de dominio público sin culpa de la parte en cuestión;

(c) pueda comprobarse que estaba en poder de dicha parte al momento de ser divulgada y que no fue obtenida previamente, de manera ni indirecta, de la otra parte, o

(d) que un tercero que no tenía obligación de confidencialidad puso a disposición de esa parte.

20.4 Las disposiciones precedentes de esta Cláusula 20 de las CGC no modificarán de modo alguno ningún compromiso de confidencialidad asumido por cualquiera de las partes de este instrumento antes de la fecha del Contrato con respecto a los Suministros o a cualquier parte de ellos.

20.5 Las disposiciones de la Cláusula 20 de las CGC seguirán siendo válidas luego del cumplimiento o la extinción del Contrato, sea cual fuere el motivo.

21. Subcontratación

21.1 El Proveedor informará al Comprador por escrito acerca de todos los subcontratos que adjudique en virtud del Contrato, siempre que no los hubiera especificado en su Oferta. La Notificación del Proveedor para agregar cualquier subcontratista que no haya sido designado en el Contrato deberá estar acompañada de la declaración del Subcontratista de conformidad con el Apéndice 2 de las CGC - Declaración de Desempeño en materia de Explotación y Abuso Sexual (EAS) y/o Acoso Sexual (ASx). Dicha notificación, en la Oferta original u Ofertas posteriores, no eximirá al Proveedor de las obligaciones, deberes y compromisos o responsabilidades contraídas en virtud del Contrato.

21.2 Todos los subcontratos deberán cumplir con las disposiciones de las Cláusulas 3 y 7 de las CGC.

22. Especificaciones y normas

22.1 Especificaciones técnicas y planos

(a) Los Bienes y Servicios Conexos proporcionados en el marco de este Contrato deberán ajustarse a las especificaciones técnicas y a las normas estipuladas en la Sección VI, "Requisitos de los Bienes y Servicios Conexos", y, cuando no se haga referencia a una norma aplicable, la norma será equivalente o superior a las normas oficiales cuya aplicación sea apropiada en el país de origen de los Bienes.

(b) El Proveedor tendrá derecho a deslindar su responsabilidad por cualquier diseño, dato, plano, especificación u otro documento, o por cualquier modificación de estos, proporcionado o diseñado por el Comprador o en nombre de él, notificando a este último de dicho deslinde.

(c) Cuando en el Contrato se haga referencia a códigos y normas conforme a los cuales este deberá ejecutarse, la edición o versión revisada de dichos códigos y normas será la especificada en los Requisitos de los Bienes y Servicios Conexos. Cualquier cambio de dichos códigos o normas durante la ejecución del Contrato se aplicará solamente con la aprobación previa del Comprador y dicho cambio estará regido por la Cláusula 33 de las CGC.

23. Embalaje y documentos

23.1 El Proveedor embalará los Bienes en la forma necesaria para impedir que se dañen o deterioren durante el transporte al lugar de destino final indicado en el Contrato. El embalaje deberá ser adecuado para resistir, entre otras cosas, la manipulación descuidada, la exposición a temperaturas extremas, la sal y las precipitaciones, y el almacenamiento en espacios abiertos. En el tamaño y peso de los embalajes se tendrá en cuenta,

cuando corresponda, la lejanía del lugar de destino final de los bienes y la carencia de equipos para la carga y descarga de materiales pesados en todos los puntos en que los bienes deban transbordarse.

23.2 El embalaje, las identificaciones y los documentos que se coloquen dentro y fuera de los bultos deberán cumplir estrictamente con los requisitos especiales que se hayan estipulado expresamente en el Contrato, y cualquier otro requisito, si lo hubiere, especificado en las CEC y en cualquier otra instrucción dispuesta por el Comprador.

24. Seguros

24.1 A menos que se disponga otra cosa en las **CEC**, los Bienes suministrados en el marco del Contrato deberán estar completamente asegurados, en una moneda de libre convertibilidad de un país elegible, contra riesgo de extravío o daños incidentales ocurridos durante la fabricación, adquisición, transporte, almacenamiento y entrega, de conformidad con los Incoterms aplicables o según se disponga en las **CEC**.

25. Transporte y servicios conexos

25.1 A menos que se disponga otra cosa en las **CEC**, la responsabilidad por los arreglos de transporte de los Bienes se regirá por los Incoterms indicados.

25.2 Podrá exigirse al Proveedor que suministre alguno o la totalidad de los siguientes servicios, además de los servicios adicionales, si los hubiere, especificados en las CEC:

(a) funcionamiento o supervisión *in situ* del ensamblaje o puesta en marcha de los Bienes suministrados;

(b) provisión de herramientas de ensamblaje o mantenimiento de los Bienes suministrados;

(c) provisión de un manual detallado de operaciones y de mantenimiento apropiado para cada una de las unidades de los Bienes suministrados;

(d) funcionamiento o supervisión o mantenimiento o reparación de los Bienes suministrados, por un período de tiempo acordado entre las partes, entendiéndose que este servicio no exime al Proveedor de ninguna de las garantías de funcionamiento derivadas de este Contrato; y

(e) capacitación del personal del Comprador, en la planta del Proveedor o en el sitio de entrega, en relación con el ensamblaje, el inicio, la operación, el mantenimiento o la reparación de los Bienes suministrados.

25.3 Los precios que cobre el Proveedor por los servicios conexos, si no estuvieran incluidos en el Precio Contractual de los Bienes, serán acordados por las partes con antelación y no excederán las tarifas que el Proveedor normalmente cobre a otras partes por servicios similares.

26. Inspecciones y pruebas

26.1 El Proveedor realizará, por su cuenta y sin costo alguno para el Comprador, todas las pruebas o inspecciones de los Bienes y Servicios Conexos según se dispone en las **CEC**.

26.2 Las inspecciones y pruebas podrán realizarse en las instalaciones del Proveedor o de su Subcontratista, en el lugar de entrega o en el lugar de destino final de los Bienes o en otro lugar en el País del Comprador establecido en las **CEC**. De conformidad con la Subcláusula 26.3 de las CGC, cuando dichas inspecciones o pruebas se realicen en establecimientos del Proveedor o de sus Subcontratistas, se proporcionará a los inspectores todas las facilidades y asistencia razonables, incluido el acceso a los planos y datos sobre producción, sin cargo alguno para el Comprador.

26.3 El Comprador o su representante designado tendrá derecho a presenciar las pruebas o inspecciones mencionadas en la Subcláusula 26.2 de las CGC, siempre y cuando asuma todos los costos y gastos que ocasione su participación, incluidos, entre otros, gastos de viaje, alojamiento y alimentación.

26.4 Cuando el Proveedor esté listo para realizar dichas pruebas e inspecciones, notificará oportunamente al Comprador indicándole el lugar y la hora. El Proveedor obtendrá del tercer o del fabricante que corresponda el permiso o consentimiento necesario para permitir al Comprador o a su representante designado presenciar las pruebas o inspecciones.

26.5 El Comprador podrá exigir al Proveedor que realice algunas pruebas o inspecciones que no estén contempladas en el Contrato, pero que considere necesarias para verificar que las características y el funcionamiento de los Bienes cumplan con los códigos de las especificaciones técnicas y normas establecidas en el Contrato. Los costos y gastos adicionales razonables que sufrague el Proveedor por dichas pruebas e inspecciones se sumarán al Precio del Contrato. Asimismo, si dichas pruebas o inspecciones impidieran el avance de la fabricación o el cumplimiento de otras obligaciones del Proveedor derivadas del Contrato, deberán realizarse los ajustes correspondientes a las fechas de entrega y de finalización y a las otras obligaciones afectadas.

26.6 El Proveedor presentará al Comprador un informe de los resultados de dichas pruebas o inspecciones.

26.7 El Comprador podrá rechazar cualquiera de los Bienes o cualquier componente de estos que no pase las pruebas o inspecciones o que no se ajuste a las especificaciones. El Proveedor deberá rectificar o reemplazar dichos Bienes o componentes rechazados o hacer las modificaciones necesarias para cumplir con las especificaciones, sin costo alguno para el Comprador. Asimismo, deberá repetir las pruebas o inspecciones, sin costo alguno para el Comprador, una vez que notifique al Comprador de conformidad con la Subcláusula 26.4 de las CGC.

26.8 El Proveedor está de acuerdo en que ni la realización de pruebas o inspecciones de los Bienes o de parte de ellos, ni la presencia del Comprador o de su representante, ni la emisión de informes con arreglo a la Subcláusula 26.6 de las CGC lo eximirán de las garantías u otras obligaciones derivadas del Contrato.

27. Liquidación por daños y perjuicios

27.1 Con excepción de lo dispuesto en la Cláusula 32 de las CGC, si el Proveedor no cumple con la entrega de la totalidad o parte de los Bienes en la(s) fecha(s) establecida(s) o con la prestación de los Servicios Conexos dentro del período especificado en el Contrato, el Comprador, sin perjuicio de los demás recursos de que disponga en virtud del Contrato, podrá deducir del Precio del Contrato, por concepto de liquidación por daños y perjuicios, una suma equivalente al porcentaje del precio de entrega de los Bienes atrasados o de los Servicios no prestados establecido en las **CEC** por cada semana o parte de la semana de retraso hasta alcanzar el máximo del porcentaje especificado en dichas **CEC**. Una vez alcanzado el máximo establecido, el Comprador podrá dar por rescindido el Contrato de conformidad con la Cláusula 35 de las CGC.

28. Garantía de los Bienes

28.1 El Proveedor garantiza que todos los Bienes suministrados en virtud del Contrato son nuevos, no tienen uso previo y corresponden al modelo más reciente o actual, y que incorporan todas las mejoras recientes en cuanto a diseño y materiales, a menos que el Contrato disponga otra cosa.

28.2 De conformidad con la Subcláusula 22.1 (b) de las CGC, el Proveedor garantiza que todos los Bienes suministrados estarán libres de defectos derivados de sus actos y omisiones, o derivados del diseño, los materiales o la manufactura, durante el uso normal en las condiciones que imperen en el país de destino final.

28.3 Salvo que en las **CEC** se indique otra cosa, la garantía seguirá vigente durante 12 (doce) meses a partir de la fecha en que los Bienes, o cualquier parte de ellos, según el caso, hayan sido entregados y aceptados en el punto final de destino indicado en las **CEC**, o 18 (dieciocho) meses a partir de la fecha de embarque en el puerto o lugar de carga en el país de origen, si dicho período concluye primero.

28.4 El Comprador notificará al Proveedor consignando la naturaleza de los defectos y proporcionará toda la evidencia disponible inmediatamente después de haberlos descubierto. El Comprador otorgará al Proveedor una oportunidad razonable para inspeccionar tales defectos.

28.5 Al recibir dicha notificación, el Proveedor deberá reparar o reemplazar, dentro del plazo establecido en las **CEC**, los Bienes defectuosos o sus partes, sin costo alguno para el Comprador.

28.6 Si el Proveedor, tras haber sido notificado, no corrige los defectos dentro del plazo establecido en las **CEC**, el Comprador, dentro de un tiempo razonable, podrá proceder a tomar las medidas necesarias para remediar la situación, por cuenta y riesgo del Proveedor y sin perjuicio de otros derechos que el Comprador pueda tener contra el Proveedor en el marco del Contrato.

29. Patentes y exención de responsabilidad

29.1 El Proveedor eximirá al Comprador, siempre que este cumpla con lo establecido en la Subcláusula 29.2 de las CGC, así como a sus empleados y funcionarios, de toda responsabilidad derivada de litigios, acciones legales o procedimientos administrativos, reclamos, demandas, pérdidas, daños, costos y gastos de cualquier naturaleza, incluyendo gastos y honorarios por representación legal, que deba sufragar como resultado de la transgresión o la supuesta transgresión de derechos de patente, uso de modelo, diseño registrado, marca registrada, derecho de autor u otro derecho de propiedad intelectual registrado o ya existente en la fecha del Contrato debido a:

(a) la instalación de los Bienes por el Proveedor o el uso de los Bienes en el país donde se encuentra emplazado el proyecto; y

(b) la venta, en cualquier país, de los productos generados por los Bienes.

Dicha exención de responsabilidad no procederá si los Bienes o una parte de ellos fuesen utilizados para fines no previstos en el Contrato o que no pudieran inferirse razonablemente de este. Tampoco abarcará ninguna transgresión que resultará del uso

de los Bienes o parte de ellos, o de cualquier producto generado en asociación o combinación con otro equipo, planta o materiales no suministrados por el Proveedor en virtud del Contrato.

29.2 Si se entablara un proceso o una demanda contra el Comprador como resultado de alguna de las situaciones indicadas en la Subcláusula 29.1 de las CGC, este notificará sin demora al Proveedor y este último, por su propia cuenta y en nombre del Comprador, llevará adelante dicho proceso o reclamo, y realizará las negociaciones necesarias para llegar a un acuerdo respecto de dicho proceso o reclamo.

29.3 Si dentro de los 28 (veintiocho) días posteriores a la fecha en que recibió dicha comunicación el Proveedor no notifica al Comprador de su intención de llevar adelante dicho proceso o reclamo, el Comprador tendrá derecho a iniciar dichas acciones en su propio nombre.

29.4 El Comprador se compromete a prestar al Proveedor, cuando este se lo solicite, toda la asistencia posible para que pueda llevar adelante dicho proceso o reclamo, y el Proveedor le reembolsará todos los gastos razonables que hubiera realizado al hacerlo.

29.5 El Comprador eximirá de toda responsabilidad al Proveedor, así como a sus empleados, funcionarios y Subcontratistas, por cualquier litigio, acción legal o procedimiento administrativo, reclamo, demanda, pérdida, daño, costo y gasto de cualquier naturaleza, incluyendo honorarios y gastos de abogados, que pudieran afectarlo como resultado de cualquier transgresión o supuesta transgresión de derechos de patentes, modelo de utilidad, diseño registrado, marca registrada, derecho de autor u otro derecho de propiedad intelectual registrado o ya existente a la fecha del Contrato que pudiera derivarse de cualquier diseño, dato, plano, especificación, u otros documentos o materiales que hubieran sido suministrados o diseñados por el Comprador o a su nombre.

30. Limitación de responsabilidad

30.1 Excepto en casos de negligencia grave o conducta dolosa,

(a) el Proveedor no tendrá ninguna responsabilidad contractual, extracontractual o de otra índole frente al Comprador por pérdidas o daños indirectos o eventuales, pérdidas de uso, pérdidas de producción, o pérdidas de ganancias o por costo de intereses; esta exclusión no se aplicará a ninguna de las obligaciones del Proveedor de pagar al Comprador los daños y perjuicios previstos en el Contrato; y

(b) la responsabilidad total del Proveedor frente al Comprador, ya sea contractual, extracontractual o de otra índole, no podrá exceder el Precio del Contrato; tal limitación de responsabilidad no se aplicará a los costos provenientes de la reparación o reemplazo de equipos defectuosos ni afecta la obligación del Proveedor de eximir de responsabilidad al Comprador por transgresiones de derechos de patentes.

31. Cambio en las leyes y regulaciones

31.1 A menos que se indique otra cosa en el Contrato, si después de 28 días antes de la fecha de presentación de Ofertas, cualquier ley, reglamento, decreto, ordenanza o estatuto con carácter de ley entrase en vigencia, se promulgase, se derogase o se modificase en el lugar del País del Comprador donde está ubicado el Emplazamiento del Proyecto (incluyendo cualquier cambio en la interpretación o aplicación por parte de las autoridades competentes) que afecte posteriormente la Fecha de Entrega o el Precio del Contrato, dicha Fecha de Entrega o Precio del Contrato se incrementarán o reducirán según corresponda, en la medida en que el Proveedor se haya visto afectado por estos cambios en el cumplimiento de obligaciones derivadas del Contrato. Sin perjuicio de ello, dicho incremento o disminución del costo no se pagará separadamente ni se acreditará si ya se ha tenido en cuenta en las disposiciones de ajuste de precio cuando corresponda, de conformidad con la Cláusula 15 de las CGC.

32. Fuerza Mayor

32.1 El Proveedor no estará sujeto a la ejecución de su Garantía de Cumplimiento, liquidación por daños y perjuicios o terminación por incumplimiento en la medida en que la demora o el incumplimiento de sus obligaciones en virtud del Contrato sea el resultado de un evento de Fuerza Mayor.

32.2 A los fines de esta cláusula, por "Fuerza Mayor" se entiende un evento o situación fuera del control del Proveedor que es imprevisible, inevitable y no se origina por descuido o negligencia del Proveedor. Tales eventos pueden incluir, entre otros, actos del Comprador en su capacidad soberana, guerras o revoluciones, incendios, inundaciones, epidemias, restricciones de cuarentena y embargos de cargamentos.

32.3 Si se produce un hecho de Fuerza Mayor, el Proveedor notificará al Comprador, por escrito y sin demora, de dicha situación y de su causa. A menos que el Comprador disponga otra cosa por escrito, el Proveedor seguirá cumpliendo con las obligaciones que le impone el Contrato en la medida en que sea razonablemente práctico, y buscará todos los medios alternativos de cumplimiento que no estuviesen afectados por la situación de Fuerza Mayor existente.

33. Órdenes de cambio y enmiendas al Contrato

33.1 El Comprador podrá, en cualquier momento, ordenar al Proveedor, mediante notificación conforme a lo dispuesto en la Cláusula 8 de las CGC, que realice cambios dentro del alcance general del Contrato en uno o más de los siguientes aspectos:

(a) planos, diseños o especificaciones, cuando los Bienes que deban suministrarse en virtud al Contrato hayan de fabricarse específicamente para el Comprador;

(b) la forma de embarque o de embalaje;

(c) el lugar de entrega; y

(d) los Servicios Conexos que deba brindar el Proveedor.

33.2 Si cualquiera de estos cambios causara un aumento o disminución en el costo o en el tiempo necesario para que el Proveedor cumpla cualquiera de las disposiciones del Contrato, se realizará un ajuste equitativo al Precio del Contrato o al Cronograma de Entregas y de Cumplimiento, o a ambas cosas, y el Contrato se modificará según corresponda. El Proveedor deberá presentar la solicitud de ajuste conforme a lo establecido en esta cláusula dentro de los 28 (veintiocho) días contados a partir de la fecha en que reciba la solicitud de la orden de cambio del Comprador.

33.3 Los precios que cobrará el Proveedor por Servicios Conexos que pudieran ser necesarios, pero que no fueron incluidos en el Contrato, deberán convenirse previamente entre las partes y no excederán los precios que el Proveedor cobra habitualmente a terceros por servicios similares.

33.4 **Ingeniería de valor:** El Proveedor podrá preparar una propuesta de ingeniería de valor en cualquier momento durante la ejecución del Contrato, y correrá con los gastos realizados en tal preparación. La propuesta de ingeniería de valor deberá incluir, como mínimo, lo siguiente:

(a) los cambios propuestos y una descripción de la diferencia respecto de los requisitos contractuales existentes;

(b) un análisis exhaustivo de costos/beneficios de los cambios propuestos, incluidas una descripción y una estimación de los costos (entre ellos, los correspondientes al ciclo de vida útil) que el Comprador pueda sufragar durante la implementación de la propuesta de ingeniería de valor; y

(c) una descripción de los efectos del cambio en el rendimiento y la funcionalidad.

El Comprador podrá aceptar la propuesta de ingeniería de valor si en esta se demuestran beneficios que permitan:

(a) acelerar el período de entrega;

(b) reducir el Precio del Contrato o los costos del ciclo de vida útil para el Comprador;

(c) mejorar la calidad, eficiencia o sostenibilidad de los Bienes; o

(d) aportar cualquier otro beneficio al Comprador, sin poner en riesgo las funciones necesarias de las Instalaciones.

Si el Comprador aprueba la propuesta de ingeniería de valor y su implementación genera:

(a) una reducción en el Precio del Contrato; el monto que se ha de pagar al Proveedor será equivalente al porcentaje indicado **en las CEC** de la reducción del Precio del Contrato; o

(b) un aumento en el Precio del Contrato, pero conlleva una reducción de los costos de la vida útil debido a cualquiera de los beneficios descritos en los incisos (a) a (d) anteriores, el monto que se ha de pagar al Proveedor será equivalente al aumento total en el Precio del Contrato.

33.5 Con sujeción a lo anterior, no se introducirá ningún cambio o modificación al Contrato excepto mediante enmienda por escrito firmada por ambas partes.

34. Prórroga de los plazos

34.1 Si en cualquier momento durante la ejecución del Contrato el Proveedor o sus Subcontratistas encontrasen condiciones que impidiesen la entrega oportuna de los Bienes o la finalización de los Servicios Conexos de conformidad con la Cláusula 13 de las CGC, el Proveedor informará de inmediato y por escrito al Comprador sobre la demora, la posible duración y la causa. Tan pronto como sea posible después de recibir la comunicación del Proveedor, el Comprador evaluará la situación y, a su discreción, podrá prorrogar el plazo de cumplimiento del Proveedor. En tal caso, ambas Partes ratificarán la prórroga mediante una enmienda al Contrato.

34.2 Excepto en caso de Fuerza Mayor, como se dispone en la Cláusula 32 de las CGC, cualquier retraso en el cumplimiento de sus obligaciones de Entrega y Finalización expondrá al Proveedor a la imposición de liquidación por daños y perjuicios de conformidad con la Cláusula 26 de las CGC, a menos que se acuerde una prórroga en virtud de la Subcláusula 34.1 de las CGC.

35. Resolución

35.1 Resolución por incumplimiento

(a) El Comprador, sin perjuicio de otros recursos previstos para casos de incumplimiento del Contrato, podrá resolver el Contrato en su totalidad o en parte enviando una notificación de incumplimiento por escrito al Proveedor:

(i) si el Proveedor no entrega alguno o ninguno de los Bienes dentro del período establecido en el Contrato, o dentro de alguna prórroga otorgada por el Comprador conforme a lo establecido en la Cláusula 34 de las CGC;

(ii) si el Proveedor no cumple con cualquier otra obligación derivada del Contrato; o

(iii) si el Proveedor, a juicio del Comprador, durante el proceso de Licitación o de ejecución del Contrato, ha participado en actos de fraude y corrupción, según se define en el párrafo 2.2 (a) del Apéndice 1 de las CGC.

(b) En caso de que el Comprador rescinda el Contrato en su totalidad o en parte, de conformidad con lo dispuesto en la Cláusula 35.1 (a) de las CGC, podrá adquirir, en los términos y condiciones que considere apropiados, Bienes o Servicios Conexos similares a los no suministrados o no prestados, y el Proveedor deberá pagar al Comprador los costos adicionales resultantes de dicha adquisición. Sin embargo, el Proveedor seguirá cumpliendo las obligaciones derivadas de la parte del Contrato que no se hubiese rescindido.

35.2 Resolución por insolvencia.

(a) El Comprador podrá resolver el Contrato notificando de ello por escrito al Proveedor si este se declarase en quiebra o en estado de insolvencia. En tal caso, la resolución no conllevará indemnización alguna para el Proveedor, siempre que no perjudique ni afecte algún derecho de

acción o recurso que tenga o pudiera llegar a tener posteriormente hacia el Comprador.

35.3 Resolución por conveniencia.

(a) El Comprador, mediante comunicación enviada al Proveedor, podrá resolver el Contrato total o parcialmente, en cualquier momento, por razones de conveniencia. La comunicación de resolución deberá indicar que esta se debe a la conveniencia del Comprador, el alcance de la extinción de las responsabilidades del Proveedor en virtud del Contrato y la fecha de entrada en vigencia de dicha resolución.

(b) Los Bienes que ya estén fabricados y listos para embarcar dentro de los 28 (veintiocho) días siguientes a la fecha en que el Proveedor reciba la notificación de resolución del Comprador deberán ser aceptados por el Comprador de acuerdo con los términos y precios establecidos en el Contrato. En cuanto al resto de los Bienes, el Comprador podrá elegir entre las siguientes opciones:

(iv) que se complete alguna porción y se entregue de acuerdo con las condiciones y precios del Contrato; y/o

(v) que se cancele el resto y se pague al Proveedor una suma convenida por aquellos Bienes o Servicios Conexos que se hubiesen completados parcialmente y por los materiales y repuestos adquiridos previamente por el Proveedor.

36. Cesión

36.1 El Comprador y Proveedor se abstendrán de ceder total o parcialmente las obligaciones que hubiesen contraído en virtud del Contrato, salvo que cuenten con el consentimiento previo por escrito de la otra parte.

37. Restricciones a la exportación

37.1 No obstante cualquier obligación incluida en el Contrato de cumplir con todas las formalidades de exportación, cualquier restricción de exportación atribuible al Comprador, al País del Comprador o al uso de los productos/bienes, sistemas o servicios que se proveerán, que provenga de regulaciones comerciales de un país proveedor de los productos/bienes, sistemas o servicios, y que impida que el Proveedor cumpla con sus obligaciones contractuales, liberará al Proveedor de la obligación de proveer bienes o servicios. Lo anterior tendrá efecto siempre y cuando el Proveedor pueda demostrar, a satisfacción del Banco y el Comprador, que ha cumplido puntualmente con todas las

formalidades, tales como la solicitud de permisos, autorizaciones y licencias necesarias para la exportación de los productos/bienes, sistemas o servicios de acuerdo con los términos del Contrato. El Contrato se resolverá sobre esta base para conveniencia del Comprador conforme a lo estipulado en la Subcláusula 35.3.

APÉNDICE 1

Fraude y Corrupción

(El texto de este anexo no deberá modificarse)

1. Propósito

1.1 Las Directrices del Banco de Lucha Contra la Corrupción y este anexo se aplicarán a las adquisiciones en el marco de las operaciones de Financiamiento para Proyectos de Inversión del Banco.

2. Requisitos

2.1 El Banco exige que los Prestatarios (incluidos los beneficiarios del financiamiento del Banco), licitantes (postulantes / proponentes), consultores, contratistas y proveedores, todo subcontratista, subconsultor, prestadores de servicios o proveedores, todo agente (haya sido declarado o no), y todo miembro de su personal, observen las más elevadas normas éticas durante el proceso de adquisición, la selección y la ejecución de contratos financiados por el Banco, y se abstengan de prácticas fraudulentas y corruptas.

2.2 Con ese fin, el Banco:

a. Define de la siguiente manera, a los efectos de esta disposición, las expresiones que se indican a continuación:

i. Por “práctica corrupta” se entiende el ofrecimiento, entrega, aceptación o solicitud directa o indirecta de cualquier cosa de valor con el fin de influir indebidamente en el accionar de otra parte.

ii. Por “práctica fraudulenta” se entiende cualquier acto u omisión, incluida la tergiversación de información, con el que se engañe o se intente engañar en forma deliberada o imprudente a una parte con el fin de obtener un beneficio financiero o de otra índole, o para evadir una obligación.

iii. Por “práctica colusoria” se entiende todo arreglo entre dos o más partes realizado con la intención de alcanzar un propósito ilícito, como el de influir de forma indebida en el accionar de otra parte.

iv. Por “práctica coercitiva” se entiende el perjuicio o daño o la amenaza de causar perjuicio o daño directa o indirectamente a cualquiera de las partes o a sus bienes para influir de forma indebida en su accionar.

v. Por “práctica de obstrucción” se entiende:

(a) la destrucción, falsificación, alteración u ocultamiento deliberado de pruebas materiales referidas a una investigación o el acto de dar falsos testimonios a los investigadores para impedir materialmente que el Banco investigue denuncias de prácticas corruptas, fraudulentas, coercitivas o colusorias, o la amenaza, persecución o intimidación de otra parte para evitar que revele lo que conoce

sobre asuntos relacionados con una investigación o lleve a cabo la investigación, o

(b) los actos destinados a impedir materialmente que el Banco ejerza sus derechos de inspección y auditoría establecidos en el párrafo 2.2 e, que figura a continuación.

b. Rechazará toda propuesta de adjudicación si determina que la empresa o persona recomendada para la adjudicación, los miembros de su personal, sus agentes, subconsultores, subcontratistas, prestadores de servicios, proveedores o empleados han participado, directa o indirectamente, en prácticas corruptas, fraudulentas, colusorias, coercitivas u obstructivas para competir por el contrato en cuestión.

c. Además de utilizar los recursos legales establecidos en el convenio legal pertinente, podrá adoptar otras medidas adecuadas, entre ellas declarar que las adquisiciones están viciadas, si determina en cualquier momento que los representantes del prestatario o de un receptor de una parte de los fondos del préstamo participaron en prácticas corruptas, fraudulentas, colusorias, coercitivas u obstructivas durante el proceso de adquisición, o la selección o ejecución del contrato en cuestión, y que el prestatario no tomó medidas oportunas y adecuadas, satisfactorias para el Banco, para abordar dichas prácticas cuando estas ocurrieron, como informar en tiempo y forma a este último al tomar conocimiento de los hechos.

d. Podrá sancionar, conforme a lo establecido en las Directrices del Banco de Lucha Contra la Corrupción y a sus políticas y procedimientos de sanciones vigentes, a cualquier empresa o persona en forma indefinida o durante un período determinado, lo que incluye declarar a dicha empresa o persona inelegibles públicamente para: (i) obtener la adjudicación o recibir cualquier beneficio, ya sea financiero o de otra índole, de un contrato financiado por el Banco[1]; (ii) ser nominada[2]como subcontratista, consultor, fabricante o proveedor, o prestador de servicios de una firma que de lo contrario sería elegible a la cual se le haya adjudicado un contrato financiado por el Banco, y (iii) recibir los fondos de un préstamo del Banco o participar más activamente en la preparación o la ejecución de cualquier proyecto financiado por el Banco.

e. Exigirá que en los documentos de solicitud de ofertas/propuestas y en los contratos financiados con préstamos del Banco se incluya una cláusula en la que se exija que los licitantes (postulantes /proponentes), consultores, contratistas y proveedores, así como sus respectivos subcontratistas, subconsultores, prestadores de servicios,

[1] A fin de disipar toda duda al respecto, la inelegibilidad de una parte sancionada en relación con la adjudicación de un contrato implica, entre otras cosas, que la empresa o persona no podrá: (i) presentar una solicitud de precalificación, expresar interés en una consultoría, y participar en una licitación, ya sea directamente o en calidad de subcontratista nominado, consultor nominado, fabricante o proveedor nominado, o prestador de servicios nominado, con respecto a dicho contrato, ni (ii) firmar una enmienda mediante la cual se introduzca una modificación sustancial en cualquier contrato existente.

[2] Un subcontratista nominado, consultor nominado, fabricante o proveedor nominado, o prestador de servicios nominado (se utilizan diferentes nombres según el documento de licitación del que se trate) es aquel que: (i) ha sido incluido por el licitante en su solicitud de precalificación u oferta por aportar experiencia y conocimientos técnicos específicos y esenciales que le permiten al licitante cumplir con los requisitos de calificación para la oferta particular; o (ii) ha sido designado por el Prestatario.

proveedores, agentes y personal, permitan al Banco inspeccionar[3]todas las cuentas, registros y otros documentos referidos a la presentación de ofertas y la ejecución de contratos, y someterlos a la auditoría de profesionales nombrados por este.

[3] Las inspecciones que se llevan a cabo en este contexto suelen ser de carácter investigativo (es decir, forense). Consisten en actividades de constatación realizadas por el Banco o por personas nombradas por este para abordar asuntos específicos relativos a las investigaciones/auditorías, como determinar la veracidad de una denuncia de fraude y corrupción a través de los mecanismos adecuados. Dicha actividad incluye, entre otras cosas, acceder a la información y los registros financieros de una empresa o persona, examinarlos y hacer las copias que corresponda; acceder a cualquier otro tipo de documentos, datos o información (ya sea en formato impreso o electrónico) que se considere pertinente para la investigación/auditoría, examinarlos y hacer las copias que corresponda; entrevistar al personal y otras personas; realizar inspecciones físicas y visitas al emplazamiento, y someter la información a la verificación de terceros.

APÉNDICE 2

Declaración de Desempeño en materia de Explotación y Abuso Sexual (EAS) y/o Acoso Sexual (ASx) de los Subcontratistas

[La siguiente Tabla debe ser completada por cada Subcontratista propuesto por el Proveedor que no haya sido designado en el Contrato]

Nombre del Subcontratista: *[indicar el nombre completo]*
Fecha: *[insertar día, mes, año]*
No. y nombre del Contrato: *[insertar la referencia número y nombre]*
Página *[insertar número de página] de [insertar número total] páginas*

Declaración EAS y /o ASx
Nosotros: ☐ (a) no hemos sido objeto de descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS / ASx. ☐ (b) no estamos sujetos a descalificación por parte del Banco por incumplimiento de las obligaciones sobre EAS / ASx ☐ (c) hemos sido descalificados por el Banco por incumplimiento de las obligaciones sobre EAS/ASx, pero fuimos excluidos de las empresas descalificadas. Se ha dictado un laudo arbitral en el caso de descalificación a nuestro favor.
[Si (c) anterior es aplicable, adjunte evidencia de un laudo arbitral que revierta las conclusiones sobre los problemas subyacentes a la descalificación.]

Nombre del Subcontratista

Nombre de la persona debidamente autorizada para firmar a nombre del Subcontratista____

Cargo de la Persona que firma a nombre del Subcontratista_____

Firma de la persona designada arriba

Fecha de la firma _____ día de_____, _____

Firma del representante autorizado del Proveedor:

Firma: _____

Fecha de la firma _____ día de _____, _____

Sección IX. Condiciones Especiales del Contrato

Las siguientes Condiciones Especiales del Contrato (CEC) complementarán o enmendarán las Condiciones Generales del Contrato (CGC) y, en caso de conflicto, prevalecerán sobre ellas.

CGC 1.1 (i)	El País del Comprador es: Peru.
CGC 1.1 (j)	El comprador es: Programa Nacional de Telecomunicaciones - PRONATEL.
CGC 1.1 (o)	El destino final del emplazamiento del Proyecto es: Las instalaciones del Edificio de la Central 911, ubicado en la Avenida El Sol S/N, distrito de Chorrillos, provincia y departamento de Lima, donde se ejecutará de manera presencial el servicio objeto del Contrato. Para la implementación del Proyecto, la entrega de los equipos y accesorios previa a su instalación se realizará en el almacén que implemente el Proveedor dentro de las instalaciones de la Central 911, el cual deberá contar con las condiciones físicas, ambientales y de seguridad requeridas, previa coordinación con el Gerente de Proyecto asignados para el Contrato.
CGC 1.1 (p)	El término EAS/ASx se usa en el Contrato con el siguiente significado: • "**Explotación y Abuso Sexual**" **"(EAS)"** significa lo siguiente: La **Explotación Sexual** se define como cualquier abuso o intento de abuso a una posición vulnerable, abuso de poder o de confianza con fines sexuales, que incluyen, entre otros, el aprovechamiento monetario, social o político mediante la explotación sexual de otra persona. El **Abuso Sexual** se define como la amenaza o la intrusión física real de naturaleza sexual, ya sea por la fuerza o bajo condiciones desiguales o coercitivas; • **"Acoso Sexual" "ASx"** se define como avances sexuales indeseables, demanda de favores sexuales, y otras conducta física o verbal de una naturaleza sexual por el Personal del Proveedor con otros miembros del personal del Proveedor, subcontratistas o del personal del Comprador.
CGC 4.2 (a)	El significado de los términos comerciales será el establecido en los Incoterms.
CGC 4.2 (b)	La versión de la edición de los Incoterms será*:* 2020.
CGC 5.1	El idioma será: Español.

CGC 8.1	Para **notificaciones**, la dirección del Comprador será: Atención: UE 1720: Programa Nacional de Telecomunicaciones - PRONATEL. Atención: Gerente de Proyecto asignado al Contrato - (Proyecto 911). Domicilio postal: Av. Paseo de la República Nº 1645 - La Victoria - Lima - Perú. Piso/oficina: 17 Ciudad: Lima Código postal: 15034 País: Peru. Dirección de correo electrónico: crep911@pronatel.gob.pe
CEC 9.1	El derecho aplicable será el de: República del Perú.
CGC 10.2	Las controversias que surjan entre las Partes en relación con este Contrato, incluidas aquellas referidas a su interpretación, ejecución, incumplimiento, resolución, nulidad o validez, serán resueltas definitivamente mediante arbitraje, de conformidad con las siguientes disposiciones: (a) Contrato con Proveedor extranjero: Toda controversia, discrepancia o reclamación derivada de este Contrato o relacionada con él, incluyendo cualquier cuestión relativa a su existencia, validez, interpretación, ejecución, incumplimiento, resolución o terminación, será resuelta mediante arbitraje internacional administrado por el Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú (PUCP). El arbitraje se desarrollará de acuerdo con el Reglamento de Arbitraje de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) vigente a la fecha de inicio del arbitraje, complementado por las normas administrativas del Centro de Arbitraje antes señalado. 1. **Selección de árbitros** a) Cuando las Partes acuerden que la controversia versa principalmente sobre aspectos técnicos, podrán designar de común acuerdo un árbitro único. Si no alcanzan acuerdo dentro de los treinta (30) días calendario siguientes a la solicitud de arbitraje, cualquiera de las Partes podrá solicitar al Centro de Análisis y Resolución de Conflictos de la PUCP la designación del árbitro único.

	b) Cuando las Partes no acuerden que la controversia es de naturaleza técnica o cuando la complejidad del caso así lo requiera, el tribunal arbitral estará conformado por tres (3) árbitros. Cada Parte designará un árbitro y los dos árbitros así designados nombrarán al presidente del tribunal arbitral. Si cualquiera de las designaciones no se realiza dentro de los treinta (30) días calendario correspondientes, o si los árbitros designados no acuerdan el nombramiento del presidente dentro del plazo señalado, la designación pendiente será efectuada por el Centro de Análisis y Resolución de Conflictos de la PUCP. 2. **Reglas de procedimiento** Sin perjuicio de lo establecido en esta cláusula, el procedimiento arbitral se regirá por el Reglamento de Arbitraje CNUDMI vigente a la fecha de inicio del arbitraje y, de manera supletoria, por el Reglamento del Centro de Análisis y Resolución de Conflictos de la PUCP. 3. **Sustitución de árbitros** Si un árbitro renuncia, fallece, es recusado o se encuentra imposibilitado de ejercer sus funciones, será sustituido conforme al mismo procedimiento utilizado para su designación original. 4. **Sede, idioma y ley aplicable** La sede del arbitraje será la ciudad de Lima, Perú. El idioma del arbitraje será el español. El tribunal arbitral decidirá la controversia conforme a la ley sustantiva aplicable al Contrato. 5. **Carácter definitivo** El laudo arbitral será definitivo, vinculante para las Partes y ejecutable conforme a la legislación aplicable. (b) Contrato con Proveedor ciudadano del país del Comprador: Si el Proveedor es ciudadano del país del Comprador, toda controversia derivada o relacionada con este Contrato será resuelta mediante arbitraje institucional administrado por el Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú (PUCP), de conformidad con su Reglamento vigente al momento de la presentación de la solicitud de arbitraje. El tribunal arbitral estará integrado por un árbitro único o por tres árbitros, según corresponda de acuerdo con el Reglamento del Centro de Arbitraje. La sede del arbitraje será Lima, Perú, el idioma será el español y el laudo arbitral será definitivo y vinculante para las Partes.

CGC 13.1	Detalle de los documentos de embarque y otros documentos que deben ser proporcionados por el Proveedor, según corresponda al medio de transporte utilizado, los siguientes documentos: 1. **Factura comercial original** del Proveedor que describa los Bienes, cantidades, precio unitario y valor total del contrato. 2. **Lista de empaque (Packing List)** que identifique el contenido de cada bulto, peso bruto, peso neto y dimensiones. 3. **Documento de transporte**, según corresponda. 4. **Certificado de origen** de los Bienes emitido por la autoridad competente del país de origen, cuando sea aplicable. 5. **Documentos de despacho aduanero de importación**, incluyendo la declaración aduanera y evidencia del pago de derechos, impuestos y demás gravámenes aplicables, de conformidad con el Incoterm DDP, cuando sea aplicable. 6. **Certificados de calidad o conformidad del fabricante**, cuando sea aplicable. 7. **Manual de operación, mantenimiento y documentación técnica**, cuando sea aplicable. 8. **Certificado de garantía del fabricante o proveedor**. 9. **Acta o constancia de entrega en el lugar de destino**, firmada por el representante del Comprador o la entidad receptora.
CGC 14.10	**<u>Se agrega:</u>** El Proveedor deberá contar con normas de conducta aplicables a su personal y garantizar la sensibilización y capacitación correspondiente, a fin de que el personal encargado de la ejecución de los Servicios Relacionados, incluyendo cuando corresponda las actividades de **instalación, operación y/o mantenimiento del equipamiento ofimático y de redes LAN**, mantenga un ambiente de trabajo seguro, respetuoso y libre de cualquier forma de explotación, abuso o acoso sexual. En tal sentido, el personal del Proveedor deberá abstenerse de participar en las siguientes conductas: (i) **Cualquier forma de acoso sexual**, incluyendo insinuaciones sexuales no deseadas, solicitudes de favores sexuales, comentarios, gestos, conductas verbales o físicas de naturaleza sexual dirigidas al personal del Comprador, del Proveedor o de terceros vinculados con la ejecución del Contrato; (ii) **Cualquier forma de explotación sexual**, entendida como el abuso real o intento de abuso de una situación de vulnerabilidad, una relación de poder o una posición de confianza con fines sexuales, incluyendo, entre otros, la

	obtención de beneficios económicos, sociales o políticos derivados de la explotación sexual de otra persona; (iii) **Cualquier forma de abuso sexual**, entendido como la intrusión física real o amenaza de intrusión de naturaleza sexual, ya sea mediante el uso de la fuerza, coerción o bajo condiciones de desigualdad o vulnerabilidad; y (iv) **Cualquier actividad sexual con personas menores de dieciocho (18) años**, salvo cuando exista un matrimonio legalmente reconocido previo conforme a la normativa aplicable. **CGC 14.10.2** El Comprador podrá solicitar al Proveedor el retiro inmediato del sitio de ejecución del Contrato, o de cualquier otro lugar donde se desarrollen los Servicios Relacionados de **instalación, operación y/o mantenimiento del equipamiento ofimático y de redes LAN**, de cualquier miembro de su personal que incurra en conductas contrarias a las normas de conducta establecidas en la CGC 14.10.1. Ante dicha solicitud, y sin perjuicio de cualquier obligación adicional de reemplazo que establezca el Comprador, el Proveedor deberá retirar o disponer el retiro inmediato de dicha persona del lugar de ejecución de los Servicios Relacionados. En todos los casos, cuando corresponda, el Proveedor deberá designar oportunamente un reemplazo idóneo que cuente con competencias, experiencia y calificaciones equivalentes, garantizando la continuidad adecuada de la prestación de los Servicios Relacionados.
CGC 15.1	Los precios de los Bienes suministrados y los Servicios Conexos prestados no serán ajustables.
CGC 16.1	La forma y las condiciones de pago al Proveedor en virtud del Contrato serán las siguientes: El Proveedor deberá presentar la solicitud de pago acompañada del certificado de conformidad correspondiente emitido por el Comprador, que acredite que los bienes han sido recibidos y/o que los servicios contratados han sido prestados de conformidad con las condiciones del Contrato, a través de la Mesa de Partes de la UE 1720: Programa Nacional de Telecomunicaciones – PRONATEL, adjuntando obligatoriamente la documentación requerida. El pago se realizará dentro de los treinta (30) días siguientes a la presentación de la solicitud de pago acompañada de la totalidad de la documentación requerida. El incumplimiento o la presentación incompleta de la documentación suspenderá el trámite de pago hasta su total subsanación.

	El pago se realizará en la moneda de la oferta, de la siguiente manera: **(i)Al recibir los bienes:** El ochenta por ciento (80 %) del valor ofertado de los bienes efectivamente entregados y conformados en el lugar de destino final, contra la presentación de los documentos especificados en la Cláusula 13.1 de las CGC. Podrán efectuarse pagos parciales en función de las entregas efectivamente realizadas y conformadas, calculados proporcionalmente sobre el valor ofertado de los bienes correspondientes a cada entrega. En conjunto, dichos pagos no podrán exceder el ochenta por ciento (80 %) del valor total ofertado de los bienes. **(ii) Contra Aceptación Operativa de la solución:** El veinte por ciento (20 %) restante del valor total ofertado de los bienes será pagado una vez culminadas satisfactoriamente las actividades de instalación, configuración, integración, pruebas y comisionamiento, previa suscripción del Acta de Aceptación Operativa y emisión de la conformidad correspondiente por parte del Comprador. **(iii) Servicios conexos:** El cien por ciento (100 %) del valor ofertado de cada Servicio Conexo, conforme a la Lista de Precios que forma parte del Contrato, será pagado mediante cuatro (4) pagos trimestrales, cada uno equivalente al veinticinco por ciento (25 %) del valor ofertado del respectivo servicio, previa conformidad del Comprador respecto de las prestaciones ejecutadas durante cada trimestre. El período de doce (12) meses de prestación de los Servicios Conexos se computará a partir de la fecha establecida en el Acta de Aceptación Operativa.
CGC 16.5	El plazo de pago después del cual el Comprador deberá pagar intereses al Proveedor es de 30 días. La tasa de interés que se aplicará es la publicada en el Banco Central de Reserva del Perú.
CGC 18.1	Si se requiere una Garantía de Cumplimiento, esta deberá presentarse en la forma de una Garantía Bancaria. El monto de la Garantía Bancaria deberá ser equivalente al 10% del monto total del Contrato y deberá mantenerse vigente hasta la entrega y conformidad de los bienes suministrados, incluida su instalación. Una vez emitida la aceptación operativa de los bienes e iniciada la prestación de los servicios conexos, el monto de la Garantía de Cumplimiento se reducirá al 5% del valor del Contrato, manteniéndose vigente hasta el cumplimiento satisfactorio de dichos servicios.

CGC 18.3	Si se requiere una Garantía de Cumplimiento, esta deberá presentarse en la forma de: **Garantía Bancaria** en **la moneda del monto del contrato.** Esta garantía tendrá carácter irrevocable, solidaria, incondicional, sin beneficio de excusión, de realización automática y será emitida por un banco que se encuentre bajo la supervisión de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.
CGC 18.4	La liberación de la Garantía de Cumplimiento será previa solicitud por escrito, al cumplimiento de la entrega total de los bienes y servicios conexos materia del contrato.
CGC 23.2	El Proveedor será responsable de que el embalaje, rotulado, identificación y documentación de los Bienes sean adecuados y suficientes para garantizar su protección, conservación, manipulación, transporte, almacenamiento, identificación y entrega en el Lugar de Destino Final indicado en el Contrato. El embalaje deberá ser nuevo y apropiado para equipos de tecnologías de la información (TI), de conformidad con las buenas prácticas comerciales y las recomendaciones del fabricante, a fin de evitar daños, deterioro o pérdida durante el transporte y almacenamiento hasta su recepción final. Todos los bultos deberán estar debidamente rotulados e identificados de manera clara, legible e indeleble. El rotulado deberá incluir, como mínimo, la siguiente información: a) Nombre o razón social del Proveedor; b) Descripción de los Bienes; c) Cantidad contenida en cada bulto; d) Número de serie, cuando corresponda; e) Número del Contrato; f) Referencia al Proyecto 911; y g) Cualquier otra información necesaria para la correcta identificación y control de los Bienes. Asimismo, cada entrega deberá estar acompañada de la documentación correspondiente, incluyendo, según resulte aplicable, guía de remisión, lista de empaque (packing list), relación de números de serie, certificados, garantías,

	manuales y cualquier otro documento exigido en las Especificaciones Técnicas o en el Contrato. La Entidad Contratante verificará el cumplimiento de las presentes disposiciones durante la recepción de los Bienes. En caso de detectarse deficiencias en el embalaje, rotulado, identificación o documentación, la Entidad podrá formular las observaciones correspondientes y requerir al Proveedor su subsanación, sin costo adicional para la Entidad y sin perjuicio de las demás obligaciones y responsabilidades previstas en el Contrato.
CGC 24.1	La cobertura de seguro se ajustará a lo establecido en los Incoterms.
CGC 24.2	Se agrega: El Proveedor será responsable por la custodia, conservación y protección de los Bienes desde su entrega y hasta la emisión del Informe de Conformidad Final por parte del Comprador, asumiendo los riesgos de pérdida, daño o deterioro durante el transporte, almacenamiento, instalación, configuración, integración, pruebas y puesta en operación de la solución. El Proveedor deberá contar con los seguros que resulten necesarios para cubrir dichos riesgos durante la ejecución contractual, manteniéndolos vigentes hasta la emisión del Informe de Conformidad Final. Las primas, deducibles y demás costos asociados serán asumidos íntegramente por el Proveedor. Asimismo, el personal que participe en las actividades de instalación, configuración, integración y pruebas deberá contar con los seguros laborales exigibles conforme a la normativa aplicable.
CGC 25.1	La responsabilidad por el transporte de los Bienes se ajustará a lo establecido en los Incoterms.
CGC 25.2	Los servicios incidentales que deberá suministrar el Proveedor, incluidos en el precio del Contrato, comprenden como mínimo: a) La instalación, configuración, parametrización e implementación integral del equipamiento y servicios conexos objeto del Contrato. b) El suministro de toda herramienta, utilidad, licencia temporal o recurso técnico necesario para la correcta instalación, configuración, pruebas y operación inicial de la solución. c) La entrega de manuales técnicos y funcionales actualizados, en idioma español, incluyendo como mínimo: • Manual de instalación. • Manual de administración. • Manual de operación. • Manual de mantenimiento y soporte.

	• Documentación técnica de configuración y parametrización. d) La prestación de servicios de soporte técnico durante el período de garantía establecido en el Contrato, incluyendo mantenimiento correctivo, atención de incidencias y asistencia remota o presencial cuando sea requerida. e) La capacitación del personal designado por el Comprador en la administración, operación, mantenimiento funcional y uso del software implementado, tanto en las instalaciones del Comprador como mediante sesiones virtuales cuando corresponda. f) La asistencia técnica durante las pruebas de aceptación, puesta en producción y estabilización de la solución. Todos los costos asociados a los servicios incidentales descritos precedentemente se consideran incluidos en el precio total del Contrato y no generarán pagos adicionales para el Comprador.
CGC 26.1	Las inspecciones y pruebas del equipamiento y servicios conexos se realizarán por cuenta y costo del Proveedor e incluirán, como mínimo, las siguientes actividades: a. Revisión de la documentación técnica y funcional entregada por el Proveedor. b. Verificación de la correcta instalación, configuración e integración del equipamiento con la infraestructura tecnológica existente de la Central de Emergencia 911. c. Pruebas funcionales para verificar el cumplimiento de todos los requisitos técnicos y funcionales establecidos en las Especificaciones Técnicas. d. Pruebas de rendimiento, estabilidad y disponibilidad del sistema. e. Pruebas de seguridad y control de acceso, cuando correspondan. f. Pruebas de integración con sistemas internos y externos definidos en el alcance del proyecto. g. Pruebas de puesta en producción y estabilización operativa. El Proveedor deberá notificar al Comprador con una anticipación mínima de cinco (5) días hábiles respecto de la fecha programada para la ejecución de cualquier prueba formal de aceptación. El Proveedor presentará informes documentados de resultados de cada fase de pruebas, incluyendo incidencias detectadas, acciones correctivas implementadas y evidencias de cumplimiento.

	La aceptación final de la solución estará condicionada a la aprobación satisfactoria de todas las pruebas establecidas y a la subsanación de cualquier observación formulada por el Comprador.
CGC 26.2	Las inspecciones y pruebas se realizarán en: a) Las instalaciones de la Central de Emergencia 911, ubicadas en Av. El Sol S/N, distrito de Chorrillos, Lima, Perú. b) Las instalaciones del Proveedor, cuando se trate de pruebas preliminares, pruebas de fábrica o validaciones previas a la instalación, pudiendo el Comprador participar presencial o remotamente.
CGC 27.1	El valor de la liquidación por daños y perjuicios será: El valor de la liquidación por daños y perjuicios será de cero comas cinco por ciento (0,5 %) por cada semana o fracción de semana de retraso, calculado sobre el precio de los bienes no entregados o de los servicios conexos no prestados oportunamente, conforme al Contrato.
CGC 28.3	**a) <u>Período de validez de la Garantía</u>:** El período de validez de la Garantía será de **365 (trescientos sesenta y cinco) días calendario**, equivalentes a **doce (12) meses**, contados a partir de la **fecha establecida en el Acta firmada en la Aceptación Operativa** de la totalidad de los bienes, sistemas y componentes por parte del Comprador. Para fines de la Garantía, el (los) lugar(es) de destino final(es) será(n): **Las instalaciones de la Central de Emergencia 911, ubicadas en Av. El Sol S/N, distrito de Chorrillos, Lima, Perú**, donde los bienes serán instalados, integrados, probados y puestos en operación. **b) <u>Alcance de la garantía</u>:** El Proveedor garantiza que los bienes suministrados cumplirán con todas las especificaciones técnicas, funcionales, de desempeño, interoperabilidad y disponibilidad establecidas en el Contrato durante todo el período de garantía. **c) <u>Obligaciones del Proveedor</u>:** Si durante el período de garantía los bienes o cualquier parte de ellos no cumplen con las condiciones de funcionamiento, desempeño o calidad establecidas en el Contrato, el Proveedor deberá, a elección del Comprador: **(i) <u>Corrección sin costo</u>** Realizar, sin costo adicional para el Comprador, todas las reparaciones, ajustes, modificaciones o reemplazos necesarios para restablecer el cumplimiento de las garantías contractuales, incluyendo la repetición de pruebas conforme a la Cláusula 26.7 de las CGC.

	(ii) <u>Daños liquidados por incumplimiento de garantía</u> En caso de incumplimiento reiterado o imposibilidad de corrección dentro de un plazo razonable, el Proveedor deberá pagar daños liquidados al Comprador por incumplimiento de la garantía contractual. La cuantía de dichos daños liquidados será la conforme a la Cláusula 27.1 de las CGC y a lo previsto en los Documentos de Licitación. **(iii) <u>Alcance adicional:</u>** El Proveedor deberá cumplir con todas las garantías adicionales de funcionamiento, disponibilidad, compatibilidad e integración establecidas en el Contrato, las cuales se considerarán complementarias a la presente garantía. El incumplimiento de dichas garantías no exime al Proveedor de sus demás obligaciones contractuales ni limita la aplicación de las Cláusulas 27 y 35 de las CGC.
CGC 28.5, CGC 28.6	El plazo para reparar o reemplazar los bienes defectuosos será de cinco (5) días calendario contados a partir de la notificación efectuada por el Comprador. Durante el período de garantía, el Proveedor deberá cumplir con las condiciones de garantía y soporte establecidas en las Especificaciones Técnicas, incluyendo la prestación de soporte técnico 24 horas al día, 7 días a la semana (24x7) en sitio (on-site) y un tiempo máximo de respuesta de cuatro (4) horas. La reparación o reemplazo de los bienes defectuosos deberá realizarse sin costo alguno para el Comprador, incluyendo mano de obra, repuestos, licencias, transporte, instalación, configuración, pruebas y cualquier otro gasto necesario para restablecer las condiciones de funcionamiento previstas en el Contrato. Cuando la reparación definitiva no pueda completarse dentro del plazo establecido, el Proveedor deberá proporcionar temporalmente, sin costo adicional para el Comprador, equipos, componentes o soluciones de reemplazo de características técnicas iguales o superiores que permitan mantener la continuidad operativa de la Central de Emergencia 911 hasta la solución definitiva. Si el Proveedor no corrige los defectos o no reemplaza los bienes dentro del plazo señalado, el Comprador podrá adoptar las medidas necesarias para remediar la situación, directamente o mediante terceros, por cuenta y riesgo del Proveedor y sin perjuicio de cualquier otro derecho o recurso previsto en el Contrato.

CGC 33.4	**Ingeniería de valor** Si el Comprador aprueba la propuesta de ingeniería del valor, el monto que se pagará al Proveedor será equivalente al setenta por ciento (70 %) de la reducción en el precio del Contrato resultante de la implementación de dicha propuesta.

Sección X. Formularios del Contrato

Esta Sección contiene formularios que, una vez completados, formarán parte del Contrato. Los formularios para la Garantía de Cumplimiento y para la Garantía por Pago de Anticipo, cuando sean requeridas, deberán ser completados solamente por el Licitante seleccionado luego de la adjudicación del Contrato.

Índice de Formularios

Carta de Aceptación……..…….…….298
Convenio de Contrato…….……299
Garantía de Cumplimiento…….……301
Garantía Bancaria por Pago de Anticipo Garantía a demanda…….……303

Carta de Aceptación

[utilice papel con membrete del Comprador]

[Fecha]

Para:*[nombre y dirección del Proveedor]*

Asunto: ***Notificación de la Adjudicación del Contrato n.º:***

Por medio de la presente le hacemos saber que nuestra Agencia ha decidido aceptar su Oferta de fecha ***[indique fecha]*** para la ejecución de ***[indique el nombre del Contrato y el número de identificación, según se indica en las CEC]***, por el Precio del Contrato aceptado de ***[indique el precio del Contrato en números y letras y la moneda]***, con las correcciones y modificaciones realizadas según las Instrucciones a los Licitantes.

Se le solicita que presente (i) la Garantía de Cumplimiento dentro de un plazo de 28 días, de acuerdo con las Condiciones del Contrato; para ello, deberá utilizar el formulario de Garantía de Cumplimiento.

Firma de la persona autorizada:
Nombre y cargo del firmante:
Nombre de la Agencia:

Adjunto: Convenio de Contrato.

Convenio de Contrato

[El Licitante seleccionado completará este formulario de acuerdo con las instrucciones indicadas].

ESTE CONVENIO DE CONTRATO se celebra

el día *[indique **número**]* de *[indique **mes**]* de *[indique **año**]*

ENTRE

(1) *[Indique nombre completo del Comprador], [indique la descripción de la entidad jurídica, por ejemplo, agencia del Ministerio de ... del Gobierno de {indique el nombre del País del Comprador}, o sociedad constituida al amparo de las leyes de {indique el nombre del País del Comprador}]*, con sede principal en *[indique la dirección del Comprador]* (en adelante, el "Comprador"), y

(2) *[Indique el nombre del Proveedor]*, sociedad constituida al amparo de las leyes de *[indique el nombre del país del Proveedor]* con sede principal en *[indique la dirección del Proveedor]* (en adelante, el "Proveedor").

POR CUANTO el Comprador ha llamado a licitación respecto de ciertos Bienes y Servicios Conexos, a saber, *[indique una breve descripción de los Bienes y Servicios]*, y ha aceptado una Oferta del Proveedor para el suministro de dichos Bienes y Servicios.

El Comprador y el Proveedor acuerdan lo siguiente:

1. En este Convenio las palabras y expresiones tendrán el mismo significado que se les asigne en los respectivos documentos del Contrato a que se refieran.

2. Los siguientes documentos constituyen el Contrato entre el Comprador y el Proveedor, y serán leídos e interpretados como parte integral del Contrato. Este Convenio prevalecerá sobre los demás documentos del Contrato.

   (a) la Carta de Aceptación;

   (b) la Carta de la Oferta;

   (c) las enmiendas n.° _____ (si las hubiera);

   (d) las Condiciones Especiales del Contrato;

   (e) las Condiciones Generales del Contrato;

   (f) los requerimientos técnicos (incluyendo los Requisitos de los Bienes y Servicios Conexos y las Especificaciones Técnicas);

   (g) las listas completas (incluyendo las Listas de Precios);

(h) cualquier otro documento enumerado en las CGC como parte integrante del Contrato.

3. Como contraprestación por los pagos que el Comprador hará al Proveedor conforme a lo estipulado en este Contrato, el Proveedor se compromete a suministrar los Bienes y Servicios al Comprador y a subsanar los defectos de estos en total consonancia con las disposiciones del Contrato.

4. El Comprador se compromete a pagar al Proveedor, como contraprestación por el suministro de los Bienes y Servicios Conexos y la subsanación de sus defectos, el Precio del Contrato o las sumas que resulten pagaderas de conformidad con lo dispuesto en el Contrato en el plazo y en la forma prescriptos en este.

EN PRUEBA DE CONFORMIDAD, las Partes han suscripto el presente Convenio, de conformidad con el derecho vigente de *[indique el nombre de la ley del país que gobierna el Contrato]* en el día, mes y año antes indicados.

En representación del Comprador

Firma: *[firma]*
en calidad de *[indique el cargo u otra designación apropiada]*
en presencia de *[indique la identificación del testigo]*

En representación del Proveedor

Firma: *[firmas de los representantes autorizados del Proveedor]*
en calidad de *[indique el cargo u otra designación apropiada]*
en presencia de *[indique la identificación del testigo]*

Garantía de Cumplimiento

Opción 1: (Garantía bancaria)

[El banco, a solicitud del Licitante seleccionado, completará este formulario de acuerdo con las instrucciones indicadas].

[Membrete del Garante o código de identificación SWIFT].

Beneficiario: *[Indique el nombre y la dirección del Comprador].*

Fecha: *[Indique la fecha de la emisión].*

GARANTÍA DE CUMPLIMIENTO N.°: *[Indique número de referencia de la Garantía].*

Garante: *[Indique el nombre y la dirección del emisor de la garantía, a menos que esté indicado en el membrete].*

Se nos ha informado que *[indique el nombre del Proveedor, que, en el caso de APCA, será el de la APCA]* (en adelante, el "Solicitante") ha celebrado el Contrato n.° *[indique número de referencia del Contrato]*, de fecha *[indique fecha]*, con el Beneficiario, para el suministro de *[indique nombre del contrato y breve descripción de los Bienes y Servicios Conexos]* (en adelante, el "Contrato").

Además, entendemos que, de acuerdo con las condiciones del Contrato, se requiere una Garantía de Cumplimiento.

A solicitud del Solicitante, nosotros, en calidad de Garantes, por medio de la presente Garantía nos obligamos irrevocablemente a pagar al Beneficiario una suma (o sumas) que no exceda *[indique la(s) suma(s) en cifras y en letras]* (_____)[1]. Dichas sumas se pagarán en los tipos y las proporciones de monedas en las que se debe pagar el Precio del Contrato, cuando recibamos la demanda del Beneficiario, respaldada por la declaración del Beneficiario, ya sea en la misma demanda o en un documento aparte firmado para acompañar o identificar la demanda, en la que se indique que el Solicitante incumplió las obligaciones contraídas en el marco del Contrato, sin necesidad de que el Beneficiario tenga que probar o aducir causa o razón alguna de su demanda o la suma especificada en ella.

10*[indique el número]* de *[indique el mes]* de *[indique el año]*[2], y cualquier reclamación de pago al amparo de ella deberá ser recibida por nosotros en la oficina mencionada arriba a más tardar en esa fecha.

---

[1] *El Garante deberá especificar una suma que represente el porcentaje del monto aceptado del Contrato que se detalla en la Carta de Aceptación y que esté denominada ya sea en la(s) moneda(s) del Contrato o en una moneda de libre convertibilidad aceptable al Beneficiario.*

11Cámara de Comercio Internacional (CCI) relativas a las garantías contra primera solicitud, revisión de 2010, publicación n.° 758 de la CCI; queda excluida de la presente la declaración de respaldo del inciso (a) del artículo 15 de dichas reglas.

_____

[firma(s)]

Nota: El texto en cursiva (incluidas las notas de pie de página) se incluye al solo efecto de preparar el presente formulario y deberá eliminarse en la versión definitiva.

---

[2] *Consigne una fecha 28 días posteriores a la fecha prevista para la finalización, como se describe en la Cláusula 18.4 de las CGC. El Comprador deberá advertir que, en caso de prórroga del plazo para cumplimiento del Contrato, el Comprador deberá solicitar al Garante una extensión de esta Garantía. Dicha solicitud deberá formularse por escrito y presentarse antes de la fecha de vencimiento establecida en la Garantía. Al preparar esta Garantía, el Comprador podría considerar la posibilidad de agregar el siguiente texto al final del penúltimo párrafo del Formulario: "El Garante acepta una sola extensión de esta Garantía por un plazo no superior a [seis meses] [un año], en respuesta a una solicitud por escrito de dicha extensión formulada por el Beneficiario, la que nos será presentada antes del vencimiento de la Garantía".*

Garantía Bancaria por Pago de Anticipo
Garantía a demanda

[Membrete del Garante o código de identificación SWIFT].

Beneficiario: *[Indique el nombre y la dirección del Comprador].*

Fecha: *[Indique la fecha de la emisión].*

GARANTÍA POR PAGO DE ANTICIPO N.°: *[Indique número de referencia de la Garantía].*

Garante: *[Indique el nombre y la dirección del emisor de la garantía, a menos que esté indicado en el membrete].*

Se nos ha informado que *[indique el nombre del Proveedor, que, en el caso de APCA, será el de la APCA]* (en adelante, el "Solicitante") ha celebrado el Contrato n.° *[indique número de referencia del Contrato]*, de fecha *[indique fecha]* con el Beneficiario, para el suministro de *[indique nombre del contrato y breve descripción de los Bienes y Servicios Conexos]* (en adelante, el "Contrato").

Asimismo, entendemos que, de acuerdo con las condiciones del Contrato, se hará un anticipo por la suma de *[indique el monto en cifras]* (____) *[indique el monto en palabras]* contra una garantía por pago de anticipo.

A solicitud del Solicitante, nosotros, en calidad de Garantes, por medio de la presente Garantía nos obligamos irrevocablemente a pagar al Beneficiario una suma (o sumas) que no exceda *[indique la(s) suma(s) en cifras y en letras]* (_____)[1] al recibo en nuestras oficinas de la demanda conforme a los requisitos del Beneficiario, respaldada por una declaración del Beneficiario, ya sea en la demanda propiamente dicha o en un documento aparte firmado que acompañe o identifique la demanda, donde conste que el Solicitante:

(d) 12para la provisión de los Bienes, o

[1] *El Garante deberá especificar una suma que represente el monto del pago por anticipado que esté denominada ya sea en la(s) moneda(s) del pago por anticipado que se indica(n) en el Contrato o en una moneda de libre convertibilidad aceptable al Comprador.*

(e) no ha cumplido con el reembolso del pago por anticipo de acuerdo con las condiciones del Contrato, especificando el monto que el Solicitante no ha reembolsado.

En virtud de esta Garantía se podrá presentar un reclamo a partir del momento en que el Garante presente un certificado del banco del Beneficiario en el que se indique que el pago mencionado arriba se ha acreditado en la cuenta número *[indique número]* que el Solicitante mantiene en *[indique el nombre y la dirección del banco del Solicitante]*.

El monto máximo de esta garantía se reducirá gradualmente en la misma cantidad de reembolsos de pagos anticipados que realice el Solicitante conforme se indica en las copias de los estados o certificados de pago provisionales que se nos deberán presentar. Esta garantía vencerá, a más tardar, en el momento en que recibamos una copia del certificado provisional de pago en el que se indique que se ha certificado para pago el 90 % (noventa por ciento) del monto aceptado del Contrato, o bien el día _____ de _____, 20___ (lo que ocurra primero). En consecuencia, cualquier reclamo de pago realizado en virtud de esta garantía deberá recibirse en nuestra oficina a más tardar en la fecha señalada.

Esta garantía está sujeta a las Reglas Uniformes de la Cámara de Comercio Internacional relativas a las garantías contra primera solicitud, revisión de 2010, publicación n.° 758 de la CCI; queda excluida de la presente la declaración de respaldo del inciso (a) del artículo 15 de dichas reglas.

_____

[firma(s)]

Nota: El texto en cursiva (incluidas las notas de pie de página) se incluye al solo efecto de preparar el presente formulario y deberá eliminarse en la versión final.