



Ciudad Autónoma de Buenos Aires, 04 NOV. 2025

VISTO:

El artículo 137 de la Constitución de la Ciudad Autónoma de Buenos Aires, la Ley N° 3 y la Ley N° 2095 y sus modificatorias, las Disposiciones N° 29/22, N° 140/23, N° 71/24 y el expediente N° 470/25 de esta Defensoría del Pueblo;

Y CONSIDERANDO QUE:

El artículo 137 de la Constitución de la Ciudad Autónoma de Buenos Aires creó a la Defensoría del Pueblo como órgano unipersonal e independiente, con autonomía funcional y autarquía financiera, dotándola de personería jurídica con legitimación procesal;

La mencionada Ley N° 3 que reglamenta la conformación del organismo, otorga al Defensor del Pueblo, en su artículo 13, incisos n) y o), las atribuciones de dictar el reglamento interno, ejecutar su presupuesto y toda otra acción conducente al mejor ejercicio de sus funciones;

Mediante la Disposición N° 71/24 se aprobó la reglamentación de la Ley N° 2095 y sus modificatorias para ser aplicado en el ámbito de la Defensoría del Pueblo;

La Coordinación Operativa de Gestión Técnica de esta Defensoría, desempeña el rol de Unidad Operativa de Adquisiciones conforme la Ley N° 2095 y sus modificatorias y de acuerdo lo establecido por la Disposición N° 140/23;

Mediante la Disposición N° 71/2024, fue aprobado el Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios que realice la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires, publicado en el BOCBA N° 6884 del 30/05/24;

Mediante Memo N° 252468/25 la Dirección General de Tecnología solicitó la **"Infraestructura Tecnológica para la plataforma de ciberseguridad"**;

En razón de lo expuesto y habiéndose determinado, por parte de la Unidad Operativa de Adquisiciones la modalidad de contratación corresponde efectuar el llamado a **Licitación Pública**, de acuerdo a lo normado en el artículo 32 de la Ley 2095 y sus modificatorias, y aprobar el Pliego de Condiciones Particulares y Especificaciones Técnicas para la **"Infraestructura Tecnológica para la plataforma de ciberseguridad"** para la Defensoría del Pueblo;

La Conducción Ejecutiva de Asuntos Legales, en su carácter de Servicio Jurídico Permanente ha tomado la intervención que le corresponde en orden a sus competencias;

Por todo ello y en uso de las facultades que le confiere el artículo 13, inc. n) y o) de la Ley N° 3;

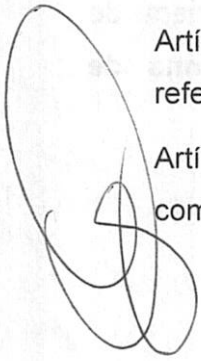
**LA DEFENSORA DEL PUEBLO
DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES
RESUELVE:**

Artículo 1º: Llamar a **Licitación Pública N° 17/2025** para la **"Infraestructura Tecnológica para la plataforma de ciberseguridad"** por un monto estimado de pesos: cuatrocientos ochenta y ocho millones cinco mil trescientos cuarenta y seis mil con 52/100 centavos (\$ 488.005.346,52.-).

Artículo 2º: Aprobar el Pliego de Bases y Condiciones Particulares de la **Licitación Pública** referida en el artículo precedente, que como **Anexo I** integra la presente Resolución.

Artículo 3º: Aprobar el Pliego de Especificaciones Técnicas de la **Licitación Pública** referida en el artículo precedente, que como **Anexo II** integra la presente Resolución.

Artículo 4º: Establecer el día **martes 25 de noviembre de 2025 a las 11:00 horas** como fecha para la apertura pública de ofertas.



Artículo 5º: Designar como integrantes titulares de la Comisión Evaluadora de Ofertas (C.E.O) en el marco de la presente Licitación: al Director Ejecutivo de la Conducción Ejecutiva Técnica y Administrativa: Sr. Dante Sironi; al Director General de Tecnología: Sr. Pablo Maccari y al Director de Operaciones de Tecnología Sr. Leandro Centurión.

Artículo 6º: Designar como integrantes suplentes de la Comisión Evaluadora de Ofertas (C.E.O) en el marco de la presente Licitación: al Subdirector de Conectividad y Redes, Sr. Mariano Talarico y al Director de Planeamiento Informático Sr. Mauro Müller.

Artículo 7º: Los integrantes de la Comisión Evaluadora de Ofertas quedan facultados para ejercer las funciones que se estipulan en los artículos 99, 100 y 101 de la Ley de Compras y Contrataciones Ley N°2.095 y sus modificatorias.

Artículo 8º: Dar intervención a la Coordinación Operativa de Gestión Técnica en su ámbito de competencia.

Artículo 9º: La erogación que demande la presente gestión será imputada en la correspondiente partida presupuestaria.

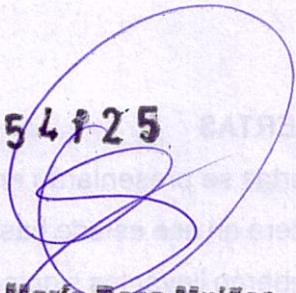
Artículo 10º: Los pliegos serán gratuitos.

Artículo 11º: Las publicaciones e invitaciones se realizarán de acuerdo a lo normado en los artículos 91 y 92 de la Ley N° 2095 y sus modificatorias.

Artículo 12º: Registrar, publicar en el Boletín Oficial por el término de tres (3) días, y en el sitio web de la Defensoría del Pueblo de la Ciudad de Buenos Aires.

vfm/ETU/COGT

RESOLUCIÓN INTERNA N° 254125



María Rosa Mulinos
*Defensora del Pueblo
de la Ciudad Autónoma
de Buenos Aires*

UNIDAD OPERATIVA DE ADQUISICIONES
COORDINACIÓN OPERATIVA DE GESTIÓN TÉCNICA

ANEXO I

RESOLUCIÓN INTERNA N°: 254125

PLIEGO DE BASES Y CONDICIONES PARTICULARES

LICITACIÓN PÚBLICA N° 17/2025

OBJETO DEL LLAMADO: "Infraestructura Tecnológica para la plataforma de ciberseguridad"

FECHA DE APERTURA: martes 25 de noviembre de 2025 a las 11:00 horas

1. RÉGIMEN DE CONTRATACIÓN

El presente llamado se sujeta al régimen establecido por el Art. 32 de la Ley 2095 y sus modificatorias, y su Reglamentación para esta Defensoría del Pueblo establecida por la Disposición N° 71/24

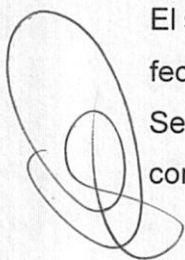
El mismo se regirá por la citada normativa, por las disposiciones del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios (Disposición N° 71/2024 disponible en la página web del organismo), y las contenidas en el presente Pliego de Bases y Condiciones Particulares.

2. FORMA DE COTIZAR

2.1. PRESENTACIÓN DE OFERTAS

En sobre cerrado. Las ofertas se presentarán en un solo sobre común, perfectamente cerrado, el cual permanecerá en ese estado hasta el día y hora fijados para la apertura. El sobre y la cotización deberán llevar los siguientes datos: N° de contratación, objeto, fecha y hora de apertura.

Se deberá indicar en la cotización N° de CUIT y N° de Ingresos Brutos correspondientes.





La oferta económica y toda la documentación deberá estar firmada en todas sus hojas por el oferente o su representante legal de puño y letra o mediante firma digital validada por certificadora oficial en los términos de la Ley N°25.506. La firma deberá encontrarse aclarada indicando el carácter del firmante. La oferta económica deberá presentarse por duplicado.

Toda la documentación presentada deberá estar debidamente foliada, en el extremo superior derecho, anverso y reverso con indicación de la cantidad de fojas presentadas (ejemplo: 1 de 10, 2 de 10, etc.).

2.2. MONEDA DE COTIZACIÓN

Pesos Argentinos.

2.3. CONDICIÓN FRENTE AL IVA

El precio contenido en la oferta económica deberá estar expresado en pesos argentinos, e incluir el monto correspondiente al Impuesto al Valor Agregado (I.V.A.).

A los efectos emergentes del Impuesto al Valor Agregado (I.V.A.), este Organismo reviste la condición de Exento; en consecuencia, en las propuestas económicas que el interesado presente junto a las ofertas no se deberá discriminar el importe correspondiente a la incidencia de este impuesto, debiendo incluirse el mismo en el precio cotizado, indicándose el porcentaje de este impuesto incluido. (27%, 21%, 10,5%, según corresponda).

El número de CUIT correspondiente a la Defensoría del Pueblo de la Ciudad de Buenos Aires es: 30-99927523-7.

2.4. DETALLE DE LA COTIZACIÓN

La oferta deberá especificar el precio unitario y cierto en números el que deberá responder estrictamente a la unidad de medida solicitada, el precio total del renglón en números y el total general de la oferta, en base a la alternativa de mayor valor, expresado en letras y números, determinados en la moneda de curso legal.

El importe total de cada renglón cotizado deberá presentarse con 2 (dos) dígitos decimales, en caso de cotizar con más dígitos decimales, se tomarán en cuenta los primeros dos, no realizándose redondeo alguno.

No se aceptarán ofertas que no contengan las condiciones detalladas en el precedente artículo 2.

3.FORMULACIÓN DE LA OFERTA

Las ofertas deberán cotizar la totalidad de los renglones solicitados. No se tendrán en cuenta cotizaciones parciales.

4.CONULTAS

Las consultas relacionadas con la presente contratación podrán realizarse ante esta Unidad Operativa de Adquisiciones hasta 72 (setenta y dos) horas previas a la fecha establecida para la apertura de las ofertas al siguiente mail: uoa@defensoria.org.ar

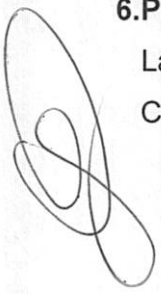
5.CIRCULARES Y NOTIFICACIONES

La dirección de correo electrónico consignada por el interesado al momento de la presentación de la oferta será registrada como la dirección donde se cursarán y serán válidas todas las circulares emitidas y demás comunicaciones que sea necesario remitir a los interesados.

En virtud de ello, la Orden de Compra, entre otras, será remitida al mencionado correo generando esta notificación fehaciente. **Si no existiera respuesta alguna del proveedor dentro de los 3 (tres) días hábiles de remitida la Orden, se considerará tácitamente perfeccionado el contrato.**

6.PRESENTACIÓN DE OFERTAS

Las ofertas deberán presentarse en la Subcoordinación Operativa de Compras y Contrataciones, sita en la sede de la Defensoría del Pueblo, Venezuela 538, primer





piso C.A.B.A., en el siguiente plazo y horario: de lunes a viernes de 11:00 a 16:00 horas, hasta la fecha y horario fijada para el Acto de Apertura.

7. ACTO DE APERTURA

En la Subcoordinación Operativa de Compras y Contrataciones, sita en la sede de la Defensoría del Pueblo, Venezuela 538, primer piso, C.A.B.A.

En la siguiente fecha y horario: **martes 25 de noviembre de 2025 a las 11:00 horas**

8. DOCUMENTACIÓN COMPLEMENTARIA PARA PRESENTAR CON LA OFERTA

Complementariamente a los instrumentos a presentar con la oferta de acuerdo a lo requerido en el Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios, los oferentes deberán integrar la siguiente documentación:

8.1 GARANTÍA DE OFERTA, de corresponder, según lo estipulado en el Art. 12 del presente Pliego.

8.2 DECLARACIÓN JURADA DE INTERESES PERSONAS HUMANAS – PERSONAS JURÍDICAS: de acuerdo al modelo previsto en el Anexo VII- VIII del Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios. (Descargar desde página web institucional) conforme personería jurídica del oferente.

8.3 DECLARACIÓN JURADA DE APTITUD PARA CONTRATAR conforme Art. 89 de la Ley N° 2095 y sus modificatorias, de acuerdo al modelo previsto en el Anexo III del Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios. (Descargar desde página web institucional)

8.4 CARTA DE PRESENTACIÓN, indicando toda la documentación presentada en la oferta, conforme Anexo IV del Pliego Único de Bases y Condiciones Generales para

la contratación de bienes y servicios. (Descargar desde página web institucional)

8.5 DECLARACIÓN DE LIBRE DEUDA PREVISIONAL, conforme Anexo V del Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios. (Descargar desde página web institucional)

8.6 DECLARACIÓN JURADA LEY N° 778, conforme Anexo VI del Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios. (Descargar desde página web institucional)

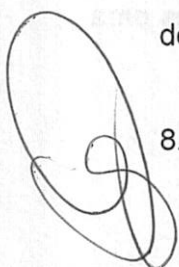
El Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios y los anexos completos que constituyen declaraciones juradas que deben ser parte de la oferta para la presente contratación se encuentran publicados en la página web del organismo para su descarga: <https://defensoria.org.ar/compras-y-contrataciones/>

8.7 CONSTANCIA DE INSCRIPCIÓN/OPCIÓN EN ARCA, vigente al momento de la presentación de ofertas.

8.8 FORMULARIO DE INSCRIPCIÓN EN EL IMPUESTO A LOS INGRESOS BRUTOS, contribuyentes locales (inscripción en la Dirección General de Rentas – AGIP) O Inscripción en el Régimen de Convenio Multilateral (CM01), según corresponda.

8.9 ACREDITACIÓN DE LA PERSONERÍA O CAPACIDAD DEL FIRMANTE DE LA OFERTA, conforme personería jurídica; Personas Jurídicas: copia del estatuto, acta de designación, etc. según tipo societario. Personas Humanas: copia del DNI.

8.10 PRESENTACIÓN DEL PRESENTE PLIEGO DE BASES Y CONDICIONES





PARTICULARES Y ESPECIFICACIONES TÉCNICAS FIRMADO EN TODAS LAS HOJAS DECLARANDO ACEPTACIÓN DE CONDICIONES.

8.11 PRESENTACIÓN DE COMPROBANTE DE C.B.U (Clave Bancaria Única), expedido por entidad bancaria.

8.12 PRESENTACIÓN DE EXENCIONES IMPOSITIVAS, de corresponder.

9. RIUPP - Registro Informatizado Único y Permanente de Proveedores

La Unidad Operativa de Adquisiciones consulta on-line el estado registral de los proveedores en el Registro.

El oferente deberá haber iniciado el trámite de inscripción previo al momento de la apertura de las ofertas, caso contrario la oferta será desestimada.

Es condición para la preadjudicación y adjudicación que el proveedor se encuentre en estado inscripto en el RIUPP y con la documentación respaldatoria actualizada. Cuando se tratare de licitaciones o concursos de etapa múltiple, el proveedor debe estar inscripto en forma previa a la preselección y adjudicación.

Los proveedores deben mantener la documentación, rubros, y clases ofrecidos actualizados, cumplimentando el trámite de actualización.

En caso de detectar un estado registral desactualizado al momento de la adjudicación esta Defensoría le otorgará al proveedor un plazo de 10 (diez) días hábiles para regularizar tal situación, a los fines de la adjudicación. Este plazo podrá prorrogarse por única vez por un mismo periodo en los casos que estén debidamente fundada las razones que lo ameriten y en los casos en que se tratare de un único oferente.

10.MANTENIMIENTO DE OFERTAS

Los oferentes deberán mantener las ofertas por el término de 30 (treinta) días hábiles contados a partir de la fecha del acto de apertura.

Si el oferente no manifestara en forma fehaciente su voluntad de no renovar la oferta

con una antelación mínima de 10 (diez) días al vencimiento del plazo, aquella se considerará prorrogada automáticamente por un lapso igual al inicial.

11.SUBSANACIÓN DE DEFICIENCIAS

A fin de subsanar omisiones o deficiencias en las ofertas presentadas, esta Unidad Operativa de Adquisiciones se reserva el derecho a requerir con posterioridad a la apertura, toda documentación que no fuera presentada en la oferta y/o aquella que considere necesaria.

Dicha solicitud deberá ser respondida por los oferentes dentro de las 72 (setenta y dos) horas de solicitada. **Bajo apercibimiento de proceder a desestimar la oferta en caso de incumplimiento.**

La misma será solicitada al mail declarado en la DDJJ solicitada en el punto 8.4 del presente pliego.

12.GARANTÍA DE OFERTA Y CUMPLIMIENTO DE CONTRATO

Garantía de impugnación al Pliego de Bases y Condiciones:

La integración de esta garantía deberá realizarse dentro del plazo establecido para realizar las impugnaciones conforme lo establecido en el Art. 9° del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios. La falta de su integración dará lugar a la desestimación sin más trámite. El monto de esta corresponderá al 1% del presupuesto oficial o monto estimado de la compra.

Garantía de Mantenimiento de Oferta: Los oferentes deberán constituir una garantía de mantenimiento de oferta incondicional e irrevocable a favor de la Defensoría del Pueblo de la Ciudad de Buenos Aires, por una suma equivalente al 5 % del valor de la oferta presentada.

Si la oferta fuese con alternativa, el oferente deberá calcularla sobre el mayor valor cotizado. Dicha garantía deberá ser mantenida por los oferentes hasta perfeccionamiento de la Orden de Compra y será constituida a través de póliza de



seguro de caución emitida por una compañía aseguradora local y a satisfacción de la Defensoría del Pueblo de la Ciudad de Buenos Aires.

En el caso de existir impugnación de la pre adjudicación, deberá presentar garantía del 5 % del monto de la oferta del renglón o renglones impugnados.

Garantía de cumplimiento del contrato: El adjudicatario deberá presentar en los términos del Artículo 107 de la Ley 2095 y sus modificatorias, de un 10% sobre el valor total de la adjudicación. La misma deberá constituirse dentro de los 5 (cinco) días del perfeccionamiento de la Orden de Compra de acuerdo a lo establecido en el Artículo 9° del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios. De acuerdo al Artículo 10°: "EXENCIÓN DE PRESENTAR GARANTÍAS" del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios.

Nota: De acuerdo al Artículo 10°: "EXENCIÓN DE PRESENTAR GARANTÍAS" del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios:

"No es necesario constituir la garantía de mantenimiento de oferta ni de cumplimiento del contrato, cuando el monto de la oferta y del contrato, respectivamente, no supere el límite de las 100.000 (cien mil) Unidades de Compra. El monto de cada unidad de compra para el ejercicio 2025 es de pesos: trescientos setenta con 00/100 centavos (\$ 370.00.-). Por lo tanto, las ofertas inferiores a pesos: treinta y siete millones con 00/10 centavos (\$ 37.000.000,00.-) quedan eximidas de la presentación de las garantías nombradas precedentemente"

La excepción a la que hace referencia esta nota, aplica a la Garantía de Mantenimiento de Oferta y a la Garantía de Cumplimiento del Contrato.

13.CRITERIO DE EVALUACIÓN DE OFERTAS

La etapa de evaluación de las ofertas es confidencial, por lo cual durante esta etapa no se concederá la vista del expediente.

De conformidad con el Art. 102° de la Ley N° 2095 y sus modificatorias, la adjudicación se realiza a favor de la oferta más conveniente, teniendo en cuenta para ello el precio, la calidad, la idoneidad del oferente, los costos asociados de uso y mantenimiento presentes y futuros y demás condiciones de la oferta.

La evaluación de las ofertas se realizará conforme a la siguiente **matriz de evaluación objetiva**, que ponderará los principales criterios definidos en el presente Pliego.

El puntaje final de cada oferta será el resultado de la suma de los puntajes obtenidos en cada criterio evaluado, aplicando la siguiente fórmula general:

$$\text{Puntaje Final} = \Sigma (\text{Puntaje obtenido por criterio} \times \text{Ponderación asignada})$$

La Comisión Evaluadora de Ofertas recomendará la adjudicación a la oferta que alcance el mayor puntaje total, siempre que cumpla con las condiciones técnicas mínimas establecidas en el Pliego.

Criterio de evaluación	Descripción	Puntaje Máx.	Método de puntuación	Ponderación (%)
Precio	Comparación con la oferta más baja	35 pts	Oferta más baja = 35 pts. Las demás: (Precio más bajo / Precio oferta) × 35	35%
Cumplimiento técnico mínimo	Acredita cumplimiento de las especificaciones obligatorias del pliego	20 pts	Evaluado con checklist técnico. Cumple = 20 pts / No cumple = EXCLUIDO	20%
Valor agregado técnico	Características adicionales: interoperabilidad, escalabilidad, seguridad, certificaciones	10 pts	Evaluado con checklist técnico. Cumple totalmente = 10 pts / Cumple parcialmente = 5 pts / No cumple = EXCLUIDO	10%
Plan de Trabajo e implementación	Calidad del Plan de Trabajo, tiempos de implementación	10 pts	Cumple Satisfactoriamente = 10 pts, Cumple = 5 pts, No cumple = EXCLUIDO	10%
Capacitación y transferencia de conocimiento	Entrenamiento al personal interno. Documentación e instructivos.	5 pts	Programa Capacitación integral Cumple Satisfactoriamente = 5 pts / Cumple = 3 pts / no incluida = 0	5%



Cv y Certificaciones del personal.	Experiencia del equipo de trabajo, certificaciones	10 pts	Con antecedentes y certificaciones = 10 pts / sin antecedentes = EXCLUIDO	10%
Experiencia y antecedentes	Proyectos similares acreditados	10 pts	> 5 antecedentes verificables = 10 pts / hasta 5 antecedentes = 2 pts / ninguno = EXCLUIDO	10%

14.VISTA DE EXPEDIENTE

La solicitud deberá ser realizada por el oferente, mediante nota ingresada por Mesa de Entrada dentro del período de 3 (tres) días hábiles administrativos, luego de la publicación en Boletín Oficial y el sitio web de esta Defensoría del Dictamen de la Comisión Evaluadora de Ofertas, de acuerdo a la normativa vigente.

15.CAUSALES DE RECHAZO DE LA OFERTA

Se procederá al rechazo de la oferta en los casos en los cuales corresponda la constitución de garantía y la empresa oferente no la presentará (conforme Art. 9º del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios y Art. 98 Ley 2095 y sus modificatorias).

En concordancia con lo establecido precedentemente, se procederá también al rechazo de las ofertas cuando las mismas incurrieren en alguno de los siguientes supuestos:

- a). Si el original no estuviera firmado por el oferente o su representante legal.
- b). Si estuviera escrita con lápiz.
- c). Si contuviera condicionamientos.
- d). Si tuvieran raspaduras, enmiendas o interlíneas en el precio, cantidad, plazo de entrega o alguna otra parte que hiciere a la esencia del contrato y no estuvieren debidamente salvadas.
- e). Si contuviera cláusulas en contraposición con las normas que rigen la contratación.
- g). Cuando el oferente no realizara la correspondiente "Visita de Obra".

16. ADJUDICACIÓN

La adjudicación se realizará a favor de la oferta más conveniente, de manera global, teniendo en cuenta para ello el precio, la calidad, la idoneidad del oferente, los costos asociados de uso y mantenimiento presentes y futuros y demás condiciones de la oferta, habiendo cumplido con las cláusulas de los pliegos y los requisitos técnicos.

17. VISITA DE OBRA

La empresa oferente deberá efectuar la visita en los edificios de esta Defensoría del Pueblo que indique la Dirección General de Tecnología.

La visita podrá efectuarse en día y horario combinado con una antelación no inferior a las 24 (veinticuatro) horas por vía telefónica con: Subcoordinación Operativa de Compras y Contrataciones de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires. Tel. de Contacto: 11 3209-0791 u 11 3628-2566.

18. SEGUROS

Los seguros deberán contratarse en Compañías o Entidades Aseguradoras, con domicilio en la Ciudad Autónoma de Buenos Aires, y que resulten aptas para la prestación enunciada a juicio exclusivo de la DPCABA, e incluirá al mismo como cotitular y/o beneficiario, según corresponda.

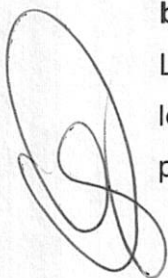
En cualquier momento la DPCABA podrá requerir la sustitución de la entidad bancaria o de la compañía aseguradora si a su solo juicio las mismas no ofrecen suficiente garantía de solvencia y seriedad.

a) Exigencias de las pólizas sin restricciones

En caso que las primas sean abonadas en cuotas, las respectivas pólizas no deberán tener cláusulas restrictivas alguna, de existir incumplimiento en el pago de las mismas.

b) Accidentes de trabajo

La firma adjudicataria será responsable de su personal por accidentes de trabajo, para lo cual deberá contratar un seguro que cubra la totalidad de las obligaciones fijadas por la Ley sobre Riesgos de trabajo N° 24.557 y sus Decretos Reglamentarios. El





seguro deberá cubrir los riesgos y accidentes de trabajo y/o enfermedades profesionales e inculpables, amparando las indemnizaciones por incapacidad permanente, parcial y absoluta, incapacidad temporaria y/o muerte, accidente "in-itinere" y prestación médico-farmacéutica, por el monto máximo que fijare la legislación vigente.

Además, la firma adjudicataria deberá presentar ante la DPCABA "Declaración Jurada", donde conste que todo el personal afectado a la prestación se encuentra cubierto por este seguro, indicando el número de Póliza correspondiente y el nombre de la compañía Aseguradora. Por lo tanto, en cada oportunidad que se produzca alguna modificación en la dotación destacada, deberá comunicarse dentro de las 72 (setenta y dos) horas de producida la misma.

c) Responsabilidad Civil

El adjudicatario deberá contratar un seguro que cubre expresamente la actividad a realizar, POR HECHO Y POR PERSONA, que cubra los riesgos de responsabilidad civil, por los daños que, como consecuencia de la prestación del servicio que se contrata, se ocasionen a personas, cosas y/o bienes de terceros y/o de la DPCABA.- Dicha póliza deberá ser endosada a favor de la DPCABA.

En caso que el monto del mismo no alcanzare a cubrir los daños provocados, la diferencia resultante correrá por parte del adjudicatario.

19. DEPENDENCIA LABORAL

Todo el personal afectado al servicio estará bajo exclusivo cargo de la adjudicataria, no teniendo en consecuencia relación de dependencia alguna con la DPCABA, la que no asume por lo tanto ninguna responsabilidad ante cualquier conflicto o litigio que eventualmente se genere por cuestiones de índole laboral entre la adjudicataria y su personal.

Cada trabajador será notificado de esta situación y suscribirá una declaración jurada, reconociendo que la única relación laboral existente es la que lo vincula con la adjudicataria.

Estas declaraciones juradas deberán ser entregadas a la Dirección General de Tecnología junto con las nóminas requeridas para ser incorporadas al expediente respectivo.

Asimismo, la adjudicataria será responsable del cumplimiento de las leyes y normas sanitarias que sean exigibles por la característica de la actividad (Libretas Sanitarias actualizadas, exámenes físicos, etc.).

La adjudicataria deberá cumplir estrictamente con todas las obligaciones que le competen en materia previsional, tributaria o fiscal y de empleo, de acuerdo con las exigencias legales vigentes o las que se dicten en el futuro.

En cualquier momento durante la ejecución del contrato, la DPCABA podrá requerir los comprobantes que acrediten el cumplimiento de dichas obligaciones. La adjudicataria será responsable del cumplimiento de sus obligaciones impositivas.

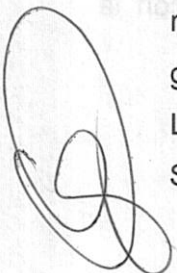
Todos los impuestos que graven la actividad de la adjudicataria deberán estar incluidos en el precio cotizado.

La adjudicataria queda comprometida a mantener indemne a la DPCABA, de cualquier suma que deba abonar, derivada de las obligaciones laborales y de la seguridad social relacionadas con su personal y/o subcontratista que tenga o pudiera tener a su cargo o que contrate con la modalidad laboral que dispusiera, o preste servicios en cumplimiento del objeto de la contratación.

Asimismo, La adjudicataria asume en forma exclusiva toda responsabilidad civil derivada de la prestación del servicio comprometiéndose a mantener indemne a la DPCABA respecto de cualquier reclamo originado en hechos ocurridos en ocasión de la prestación del servicio.

La adjudicataria se compromete a notificar de forma inmediata y en un plazo no mayor a los 3 (tres) días hábiles administrativos de haber tomado conocimiento de cualquier reclamación, acción o procedimiento de los que tengan conocimiento y que puedan generar cualquier tipo de responsabilidad respecto de la otra parte.

La adjudicataria se obliga a cumplir acabadamente con todas las normas de Seguridad, Salubridad e Higiene y Protección del Medio Ambiente y con cualquier otra norma





aplicable a su actividad y a los Servicios a nivel nacional, provincial y municipal, durante toda la vigencia de la relación contractual. La adjudicataria será la única responsable por los accidentes y/o infracciones que pudieran ocurrir y/o cometerse durante o con motivo de la prestación de los Servicios.

20. CLÁUSULA DE INDEMNIDAD

El adjudicatario se compromete y acuerda en forma irrevocable mantener indemne a la DPCABA por cualquier reclamo, acción judicial, demanda, daño o responsabilidad de cualquier tipo o naturaleza que sea entablada por cualquier persona pública o privada, física o jurídica, o dependientes del adjudicatario, cualquiera fuera la causa del reclamo, responsabilidad que se mantendrá aún terminado el contrato por cualquier causa. La responsabilidad se extenderá a indemnización, gastos y costas, sin que la enunciación sea limitativa. En estos casos la DPCABA queda facultada para afectar cualquier suma que por cualquier concepto la DPCABA adeudara al adjudicatario sin que ello limite la responsabilidad de este último.

21. RESPONSABILIDAD DE LA ADJUDICATARIA POR ACTOS DE SU PERSONAL

La adjudicataria se responsabiliza por toda rotura, deterioro o desaparición de elementos personales, artefactos, equipos, muebles, sanitarios, cortinados, vidrios, etc. Comprobado fehacientemente que alguno de estos elementos o bienes fue afectado durante la realización de la prestación, queda a cargo de la adjudicataria la reparación o reposición inmediata de los mismos, a satisfacción de la DPCABA.

Si intimada, la contratista dentro del plazo de 7 (siete) días corridos, no cumple con la reparación o reposición, la DPCABA, sin más trámite, dispondrá su reparación o reposición en forma directa con cargo a la adjudicataria y por el monto que resulte.

22. PENALIDADES

El incumplimiento de las condiciones de tiempo, modo y lugar de cualquiera de las obligaciones asumidas por la contratista en virtud del plexo jurídico aplicable a la

contratación que se celebra, genera la mora automática sin necesidad de interpelación administrativo ni judicial, siendo, asimismo, pasible de ser penalizado y/o sancionado conforme regulación y atribuciones contempladas en la Ley 2095, Artículos 117 y 129 y sus modificatorias, su Reglamentación, y las previsiones de este pliego.

La penalidad o la sanción aplicable lo será sin perjuicio del derecho que le corresponde a la DPCABA por los daños y perjuicios que eventualmente se ocasionen.

A los efectos de la aplicación y graduación de las penalidades previstas en la Ley 2095, sus modificatorias y su reglamentación, el órgano competente debe considerar las circunstancias fácticas del caso, el incumplimiento detectado, su gravedad, el eventual daño causado, así como la aplicación de penalidades y/o sanciones previas.

23.CONTINUIDAD DE LOS SERVICIOS

En caso de producirse una interrupción total o parcial del servicio, la DPCABA podrá efectuarlo directamente por sí o por terceros, a fin de mantener su continuidad, por cuenta y cargo del adjudicatario.

24.PLAZO Y FORMA DE PAGO

Para los renglones 1,2,3,4,5,6,7:

Contra entrega, Se realizará el pago por renglón contra la presentación de la factura y el PRD emitido por el área requirente, que acredite la recepción conforme del bien. Los pagos se efectuarán dentro de los 20 (veinte) días hábiles posteriores de recibida la factura y el PRD en la Coordinación Operativa de Gestión Económica y Financiera.

Renglones 8,9,10,11,12:

Finalizada la implementación del Renglón, Se realizará el pago por renglón contra la presentación de la factura y el PRD emitido por el área requirente, que acredite la recepción conforme del bien.

Los pagos se efectuarán dentro de los 20 (veinte) días hábiles posteriores de recibida la factura y el PRD en la Coordinación Operativa de Gestión Económica y Financiera.

El/Los pago/s serán efectuado/s mediante transferencia bancaria al C.B.U. declarado





por el proveedor de acuerdo al artículo 8.11 del presente pliego.

Excepcionalmente, el proveedor podrá solicitar expresamente a través de una nota, el pago mediante la emisión de cheque bancario, detallando los datos que correspondan al efecto.

25. LUGAR Y FORMA DE ENTREGA/ PRESTACIÓN

La prestación/entrega se realizará bajo la coordinación y supervisión de Dirección General de Tecnología de esta Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires.

26. PLAZO DE ENTREGA /PRESTACIÓN DE SERVICIO

La prestación/entrega se realizará bajo la coordinación y supervisión de la Dirección General de Tecnología Tel de Contacto: 4338-4900 interno 3794, dentro de los 30 (treinta) días hábiles administrativos de la fecha de emisión de la Orden de Compra. El proveedor deberá garantizar contar con capacidad técnica y operativa para cumplir con la entrega en el tiempo y la forma en que sean requeridos.

La DPCABA, podrá solicitar una prórroga contractual en las mismas condiciones que las establecidas en el contrato original, por un plazo igual o menor del contrato inicial, no pudiendo el plazo de la prórroga superar el plazo de vigencia original del contrato

27. ORDEN DE COMPRA – CONDICIONES PARA LA EMISIÓN

Previo a la emisión de la Orden de Compra el organismo procederá a solicitar información a la Agencia de Recaudación y Control Aduanero - ARCA a los efectos de verificar la habilidad para contratar de la firma adjudicada quien no deberá contar con incumplimientos tributarios y/o previsionales de acuerdo a la normativa en vigencia (RG 4164/2017 AFIP). Ante la existencia de incumplimiento, esta Defensoría le otorgará al proveedor un plazo de 10 (diez) días hábiles para regularizar tal situación, a los fines de la emisión de la orden de compra. Este plazo podrá prorrogarse por única vez por un mismo periodo en los casos que estén debidamente fundada las

razones que lo ameriten y en los casos en que se tratare de un único oferente.

28. RECEPCIÓN DEFINITIVA

La recepción y conformidad definitiva de los bienes entregados y/o la certificación de la prestación de un servicio, será efectuada por la Dirección General de Tecnología. A los efectos de la recepción y conformidad técnica, deberá procederse a la confrontación de la prestación con las especificaciones del pedido que surgen de la Orden de Compra.

En consecuencia, se confeccionará un Parte de Recepción Definitiva el cual será suscripto por el o los responsables de la recepción, dando conformidad a la entrega y/o prestación. Dicha conformidad debe ser acordada dentro de un plazo de 8 (ocho) días corridos de la entrega o finalización de la prestación.

29. CLÁUSULA DE RESCISIÓN

La DPCABA se reserva el derecho a rescindir o disminuir el contrato que origine la presente contratación, por razones presupuestarias, traslados, modificación y /o baja de sedes, etc., sin asistírle derecho alguno al adjudicatario sobre compensaciones, gastos administrativos, constitución de las garantías, lucro cesante e indemnizaciones, etc. Para ejercer este derecho el organismo contratante, efectuará la respectiva comunicación con la anticipación de 30 (treinta) días corridos.

Asimismo, la DPCABA se reserva el derecho de rescindir el contrato que origine la presente contratación para el caso que el futuro adjudicatario no cumpla con las exigencias establecidas en el Pliego de Bases y Condiciones Particulares y Especificaciones Técnicas.



María Rosa Muñoz
Defensora del Pueblo
de la Ciudad Autónoma
de Buenos Aires



UNIDAD OPERATIVA DE ADQUISICIONES

COORDINACIÓN OPERATIVA DE GESTIÓN TÉCNICA

ANEXO II

RESOLUCIÓN INTERNA N°: 254125

PLIEGO DE ESPECIFICACIONES TÉCNICAS

LICITACIÓN PÚBLICA N° 17/2025

OBJETO DEL LLAMADO: "Infraestructura Tecnológica para la plataforma de ciberseguridad"

FECHA DE APERTURA: martes 25 de noviembre de 2025 a las 11:00 horas

Renglón	Descripción	Cantidad
1	Equipos de Firewall para centro de datos (Borde)	2
2	Equipos de Firewall para sucursales (Borde)	5
3	Switch Core de Capa 3	2
4	Switch de distribución	5
5	Switch de acceso de Capa 2	14
6	Switch de acceso de Capa 2 con POE	14
7	Módulo transceptor Óptico	120
8	Plataforma de administración y analíticas	1
9	Cableado back bone de fibra óptica	50
10	Pacheras inteligentes	35
11	Servicios de instalación y puesta en marcha	1
12	Servicio de capacitación y Skill Transfer	1

La presente contratación se refiere a la Plataforma unificada de seguridad Fortinet Security Fabric o equivalente

1. MARCA

Es imprescindible que se consigne la marca de los productos ofertados, o indicar si son de su

fabricación y/o fraccionamiento. Cuando las especificaciones se mencione tipo de marca, lo es al solo efecto de señalar las características generales del artículo solicitado sin que aquello implique que el proponente no pueda ofrecer artículos similares, de otras marcas, pero asimismo deberá especificar lo que ofrece.

De cotizar marcas distintas a las solicitadas los oferentes deberán presentar una muestra de lo ofertado a los efectos de apreciar calidad e indicar en su oferta concretamente la marca ofrecida. La muestra se entregará en el servicio solicitante, pudiendo hacerlo hasta el momento de la apertura; estando el oferente obligado a incluir dentro del sobre de oferta el remito de entrega de la misma. Requisito que de omitirse no configurará el descarte de la propuesta, siempre y cuando se encuentre debidamente acreditado en la planilla del sector interviniente la recepción de muestras.

En caso que el oferente no haya identificado el producto con una marca determinada, o no hubiera indicado si son de su fabricación y / o fraccionamiento, la respectiva oferta será descartada, a excepción de aquellos elementos que por su naturaleza no lleven marca. Pudiendo establecerse su calidad a través de las especificaciones y / o muestras en caso de ser requeridas.

2. CATALOGO Y/O FOLLETERIA

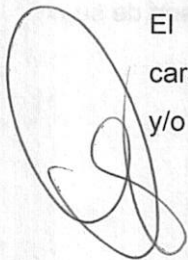
Los oferentes deberán presentar un catálogo y/o folletería de lo ofertado a los efectos de apreciar calidad. Deberán adjuntarse folletos y catálogos ilustrativos de los bienes requeridos en idioma castellano y/o fotografías de los elementos cotizados, como así también ampliación de las especificaciones técnicas o cualquier otro elemento informativo que se considere de interés u que permita una mejor evaluación de los bienes cotizados.

3. GARANTÍA DE LAS UNIDADES

Los productos deberán tener como mínimo tres (3) años de garantía y deberán ser entregados ya armados o bien incluir el servicio de armado al momento de la entrega.

4. ALTERNATIVA

El Organismo Licitante se reserva el derecho de considerar ofertas alternativas, de características distintas a lo indicado en el Pliego de Bases y Condiciones, incluidos envases, y/o presentaciones de contenidos diferentes a los solicitados. En el caso de ofrecer distintas





marcas comerciales para un mismo renglón deberán ser presentadas por separado como ofertas alternativas, de lo contrario no serán consideradas ofertas válidas. Deberán los proveedores especificar dicha característica en su oferta. Las ofertas alternativas serán consideradas sin vulnerar el principio de igualdad que rige a la Administración Pública, esto es, que no pueden variar la sustancia de lo requerido.

5. ESPECIFICACIONES TÉCNICAS.

OBJETO DEL LLAMADO: Adquisición de equipamiento de infraestructura de red (firewalls, switches de acceso, distribución y core), módulos transceptores ópticos, teléfonos IP y puntos de acceso Wi-Fi, con servicios de soporte y garantía asociados. La presente contratación se refiere a la Plataforma unificada de seguridad Fortinet Security Fabric o equivalente

6. OBJETO GENERAL

El presente pliego tiene como objeto definir los lineamientos, características funcionales y requisitos técnicos mínimos para la adquisición de equipos de infraestructura de red que incluyen firewalls de borde, switches de acceso, distribución y core, así como teléfonos IP y puntos de acceso Wi-Fi. Esta adquisición es fundamental para la renovación y ampliación de la infraestructura de red de la Defensoría del Pueblo de la C.A.B.A., buscando mejorar el rendimiento, la fiabilidad, la escalabilidad y la seguridad ante el fin de vida útil de equipos actuales y la necesidad de incorporar nuevas sedes.

7. ESPECIFICACIONES TÉCNICAS

Renglón N° 1.- EQUIPOS DE NEXT GEN FIREWALL PARA CENTRO DE DATOS

Cantidad: 2 (dos).

Interfaces

- 2.1.1. Al menos 8 (ocho) interfaces de 1GE RJ45.
- 2.1.2. Al menos 8 (ocho) interfaces de 1/ 2.5/5 GE RJ45.
- 2.1.3. Al menos 8 (ocho) interfaces de 1/10GE SFP+
- 2.1.4. Al menos 4 (cuatro) interfaces de 1GE SFP.
- 2.1.5. Al menos una interface de administración de 1GE RJ45

2.1.6. Al menos una interface de HA (alta disponibilidad) de 1GE RJ45

Performance y dimensionamiento

2.1.7. Cada equipamiento deberá poder conmutar al menos, 39 Gbps de tráfico del tipo IPv4 con paquetes de un tamaño de 1518 bytes y políticas de firewall activas.

2.1.8. Cada equipo deberá poder tener un performance de 9 Gbps a nivel de IPS.

2.1.9. Cada equipamiento deberá poder establecer al menos 400.000 nuevas sesiones TCP por segundo.

2.1.10. Cada equipamiento deberá poder mantener al menos 11.000.000 de sesiones activas establecidas (sesiones concurrentes).

2.1.11. Cada equipamiento deberá poder establecer y mantener al menos 2.000 túneles IPsec.

Características Generales

2.1.12. La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.;

2.1.13. Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;

2.1.14. Las funcionalidades de protección de red que conforman la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;

2.1.15. La solución debe estar optimizada para análisis de contenido de aplicaciones en capa 7;

2.1.16. Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19", incluyendo un rail kit (si sea necesario) y los cables de alimentación;

2.1.17. La gestión de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;

2.1.18. Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;

2.1.19. Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;



- 2.1.20. Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
- 2.1.21. Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
- 2.1.22. Los dispositivos de protección de red deben soportar DHCP Relay;
- 2.1.23. Los dispositivos de protección de red deben soportar DHCP Server;
- 2.1.24. Los dispositivos de protección de red deben soportar sFlow;
- 2.1.25. Los dispositivos de protección de red deben soportar Jumbo Frames;
- 2.1.26. Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
- 2.1.27. Debe ser compatible con NAT dinámica (varios-a-1);
- 2.1.28. Debe ser compatible con NAT dinámica (muchos-a-muchos);
- 2.1.29. Debe soportar NAT estática (1-a-1);
- 2.1.30. Debe admitir NAT estática (muchos-a-muchos);
- 2.1.31. Debe ser compatible con NAT estático bidireccional 1-a-1;
- 2.1.32. Debe ser compatible con la traducción de puertos (PAT);
- 2.1.33. Debe ser compatible con NAT Origen;
- 2.1.34. Debe ser compatible con NAT de destino;
- 2.1.35. Debe soportar NAT de origen y NAT de destino de forma simultánea;
- 2.1.36. Debe soportar NAT de origen y NAT de destino en la misma política
- 2.1.37. Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
- 2.1.38. Debe ser compatible con NAT64 y NAT46;
- 2.1.39. Debe implementar el protocolo ECMP;
- 2.1.40. Debe soportar SD-WAN de forma nativa
- 2.1.41. Debe soportar el balanceo de enlace hash por IP de origen;
- 2.1.42. Debe soportar el balanceo de enlace por hash de IP de origen y destino;
- 2.1.43. Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe

ser compatible con el balanceo en al menos tres enlaces;

2.1.44. Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;

2.1.45. Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;

2.1.46. Enviar logs a sistemas de gestión externos simultáneamente;

2.1.47. Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;

2.1.48. Debe soportar protección contra la suplantación de identidad (anti-spoofing);

2.1.49. Implementar la optimización del tráfico entre dos dispositivos;

2.1.50. Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);

2.1.51. Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);

2.1.52. Soportar OSPF graceful restart;

2.1.53. Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;

2.1.54. Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;

2.1.55. Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;

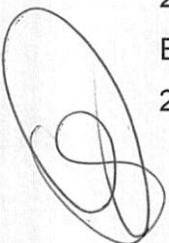
2.1.56. Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;

2.1.57. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo:
En modo transparente;

2.1.58. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo:
En capa 3;

2.1.59. Soportar configuración de alta disponibilidad activo / pasivo y activo / activo:
En la capa 3 y con al menos 3 dispositivos en el cluster;

2.1.60. La configuración de alta disponibilidad debe sincronizar:





- Sesiones;
- Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
- Las asociaciones de seguridad VPN;
- Tablas FIB;

2.1.61. En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;

2.1.62. Debe soportar la creación de sistemas virtuales en el mismo equipo;

2.1.63. Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;

2.1.64. Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;

2.1.65. La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;

2.1.66. Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);

2.1.67. Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;

2.1.68. El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;

2.1.69. Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;

2.1.70. La consola de administración debe soportar como mínimo, Inglés y Español.

2.1.71. La consola debe soportar la administración de switches y puntos de acceso inalámbricos para mejorar el nivel de seguridad.

2.1.72. La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.

Control por Política de Firewall

2.1.73. Debe soportar controles de zona de seguridad;

2.1.74. Debe contar con políticas de control por puerto y protocolo;

2.1.75. Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;

2.1.76. Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;

2.1.77. Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;

2.1.78. Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;

2.1.79. Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.

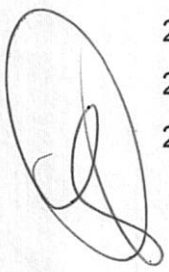
2.1.80. Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);

2.1.81. Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes

2.1.82. Debe soportar el protocolo estándar de la industria VXLAN;

2.1.83. La solución debe permitir la implementación sin asistencia de SD-WAN

2.1.84. En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas,





IPSEC VPN;

2.1.85. La solución debe soportar la integración nativa con solución de Sandboxing, protección de correo electrónico, cache y Web application firewall.

Control de Aplicación

2.1.86. Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;

2.1.87. Detección de aplicaciones en categorías, como, por ejemplo, tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;

2.1.88. Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, x, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, google chat, whatsapp, 4shared, dropbox, Google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

2.1.89. Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y

controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;

2.1.90. Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;

2.1.91. Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;

2.1.92. Actualización de la base de firmas de la aplicación de forma automática;

2.1.93. Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;

2.1.94. Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;



2.1.95. Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;

2.1.96. El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;

2.1.97. Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;

2.1.98. Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;

2.1.99. Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Google Chat el chat, pero impedir la llamada de video;

2.1.100. Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;

2.1.101. Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);

2.1.102. Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;

2.1.103. Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;

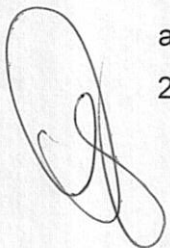
2.1.104. Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Prevención de Amenazas

2.1.105. Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;

2.1.106. Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);

2.1.107. Las características de IPS y antivirus deben funcionar de forma permanente,





pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;

2.1.108. Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;

2.1.109. Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;

2.1.110. Deber permitir el bloqueo de vulnerabilidades y exploits conocidos

2.1.111. Debe incluir la protección contra ataques de denegación de servicio;

2.1.112. Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;

2.1.113. Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;

2.1.114. Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;

2.1.115. Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP;

2.1.116. Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);

2.1.117. Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc;

2.1.118. Detectar y bloquear los escaneos de puertos de origen;

2.1.119. Bloquear ataques realizados por gusanos (worms) conocidos;

2.1.120. Contar con firmas específicas para la mitigación de ataques DoS y DDoS;

2.1.121. Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);

2.1.122. Debe poder crear firmas personalizadas en la interfaz gráfica del producto;

2.1.123. Identificar y bloquear la comunicación con redes de bots;

2.1.124. Registrar en la consola de supervisión la siguiente información sobre

amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;

2.1.125. Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;

2.1.126. Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;

2.1.127. Los eventos deben identificar el país que origino la amenaza;

2.1.128. Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);

2.1.129. Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;

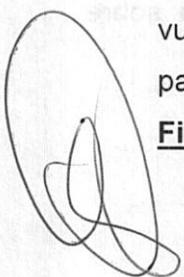
2.1.130. Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;

2.1.131. En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;

2.1.132. Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);

2.1.133. Debe soportar virtual Patching para bloquear la explotación de vulnerabilidades conocidas en sistemas y aplicaciones, sin la necesidad de instalar un parche de software convencional y formal,

Filtrado de URL



2.1.134. Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;

2.1.135. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios;

2.1.136. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;

2.1.137. Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios;

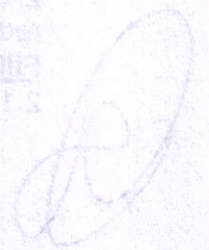
2.1.138. Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios;

2.1.139. Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autenticación residente en el equipo de seguridad (portal cautivo);

2.1.140. Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;

2.1.141. Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;

2.1.142. Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;



2.1.143. Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;

QoS Traffic Shaping

2.1.144. Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;

2.1.145. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;

2.1.146. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;

2.1.147. Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;

2.1.148. Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;

2.1.149. Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;

2.1.150. En QoS debe permitir la definición de tráfico con ancho de banda garantizado;

2.1.151. En QoS debe permitir la definición de tráfico con máximo ancho de banda;

2.1.152. En QoS debe permitir la definición de colas de prioridad;

2.1.153. Soportar marcación de paquetes DiffServ, incluso por aplicación;

2.1.154. Soportar la modificación de los valores de DSCP para Diffserv;

2.1.155. Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);

2.1.156. Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

Filtro de Datos

2.1.157. Debe permitir la creación de filtros para archivos y datos predefinidos;





2.1.158. Los archivos deben ser identificados por tamaño y tipo;

2.1.159. Debe permitir identificar y -opcionalmente- prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;

2.1.160. Debe soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;

2.1.161. Debe soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;

2.1.162. Debe permitir identificar y -opcionalmente- prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;

Geolocalización

2.1.163. Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países;

2.1.164. Debe permitir la visualización de los países de origen y destino en los registros de acceso;

2.1.165. Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

VPN

2.1.166. Soporte VPN de sitio-a-sitio y cliente-a-sitio;

2.1.167. Soportar VPN IPSec;

2.1.168. La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512

2.1.169. La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;

2.1.170. La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);

2.1.171. La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);

2.1.172. Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

2.1.173. Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;

2.1.174. Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;

2.1.175. Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;

2.1.176. Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;

2.1.177. Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;

2.1.178. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;

2.1.179. Deberá mantener una conexión segura con el portal durante la sesión;

2.1.180. El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

Wireless Controller

2.1.181. Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);

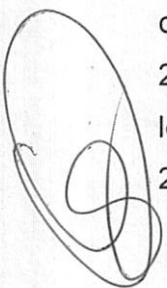
2.1.182. Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;

2.1.183. Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac / ax y que transmitan tráfico IPv4 e IPv6 a través del controlador.

2.1.184. La solución debe ser capaz de administrar puntos de acceso de tipo indoor outdoor;

2.1.185. El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;

2.1.186. La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en





los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario;

2.1.187. Debe permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points;

2.1.188. El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tunelados hasta el controlador inalámbrico;

2.1.189. Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;

2.1.190. Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico;

2.1.191. Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPAWPA2-Personal (PSK), en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;

2.1.192. La solución debe permitir definir qué redes serán tuneladas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso;

2.1.193. La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tunelados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso;

2.1.194. La solución debe implementar recursos que posibiliten la identificación de

interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz , 5GHz y 6GHz;

2.1.195. La solución debe detectar Receiver Start of Packet (RX-SOP) en paquetes inalámbricos y ser capaz de omitir aquellos que están por debajo de determinado umbral especificado en dBm;

2.1.196. La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso;

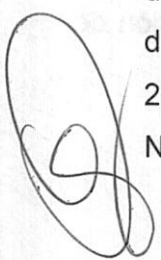
2.1.197. La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y basada en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados;

2.1.198. La solución debe identificar automáticamente puntos de acceso intrusos que estén conectados a la red de cable (LAN). La solución debe ser capaz de identificar el punto de acceso intruso incluso cuando el MAC Address de la interfaz LAN es ligeramente diferente (adyacente) del MAC Address de la interfaz WLAN;

2.1.199. La solución debe detectar los puntos de acceso no autorizados y / o intrusos a través de radios dedicados a la función de análisis o a través de Off-channel / Background scanning. Cuando se realiza a través de Off-channel / Background scanning, la solución debe ser capaz de identificar el uso del punto de acceso para, en caso necesario, retrasar el análisis y de esta forma no perjudicar a los clientes conectados;

2.1.200. La solución debe permitir la configuración individual de las radios del punto de acceso para que operen en el modo monitor, o sea, con función dedicada para detectar amenazas en la red inalámbrica y con ello permitir mayor flexibilidad en el diseño de la red;

2.1.201. La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y





sincronizar la configuración del principal, además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener función de primario de forma temporal;

2.1.202. La solución debe permitir el agrupamiento de VLANs para que se distribuyan múltiples subredes en un determinado SSID, reduciendo así el broadcast y aumentando la disponibilidad de direcciones IP;

2.1.203. La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado;

2.1.204. La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios;

2.1.205. Debe permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;

2.1.206. La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;

2.1.207. La solución debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia;

2.1.208. La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectado mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;

2.1.209. La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica;

2.1.210. La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado;

2.1.211. La solución debe implementar técnicas de Call Admission Control para limitar el número de llamadas simultáneas;

2.1.212. La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica e informar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado, Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación;

2.1.213. Para garantizar una mejor distribución de dispositivos entre las frecuencias disponibles y mejorar la utilización de la radiofrecuencia, la solución debe ser capaz de distribuir automáticamente los dispositivos de banda dual para que se conecten primariamente a 5GHz a través del recurso conocido como Band Steering;

2.1.214. La solución debe permitir la configuración de los data rates que se activarán en la herramienta y las que se deshabilitar para las frecuencias de 2.4, 5GHz y 6GHz y los estándares 802.11a / b / g / n / ac / ax;

2.1.215. La solución debe tener capacidad capaz de convertir paquetes Multicast en paquetes Unicast cuando se reenvían a los dispositivos que están conectados a la infraestructura inalámbrica, mejorando así el consumo de Airtime;

2.1.216. La solución debe soportar la característica que ignore Probe Requests de clientes que tienen una señal débil o distante. Debe permitir definir el umbral para que los Probe Requests sean ignorados;

2.1.217. La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz;

2.1.218. La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;

2.1.219. La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio direcciones de origen y destino (IPv4 e IPv6), puertos y protocolos;



2.1.220. La solución debe implementar la función de web filtering para controlar los sitios que se accede a la red inalámbrica. Debe poseer una base de conocimiento para categorizar los sitios y permitir configurar qué categorías de sitios serán permitidos y bloqueados para cada perfil de usuario y SSID;

2.1.221. La solución debe tener capacidad de reconocimiento de aplicaciones a través de la técnica de DPI (Deep Packet Inspection) que permita al administrador de la red monitorear el perfil de acceso de los usuarios e implementar políticas de control. Debe permitir el funcionamiento de esta característica y la actualización periódica de la base de aplicaciones durante todo el período de garantía de la solución; 2.1.222. La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil y quinientas) aplicaciones;

2.1.223. La solución debe permitir la creación de reglas para el bloqueo y el límite de banda (en Mbps, Kbps o Bps) para las aplicaciones reconocidas a través de la técnica de DPI;

2.1.224. La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;

2.1.225. "La solución debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica. Al menos los siguientes ataques deben ser identificados:

- Ataques de flood contra el protocolo EAPOL (EAPOL Flooding);
- Los siguientes ataques de denegación de servicio: Association Flood, Authentication Flood, Broadcast Deauthentication y Spoofed Deauthentication;
- ASLEAP;
- Null Probe Response / Null SSID Probe Response;
- Long Duration;
- Ataques contra Wireless Bridges;
- Weak WEP;
- Invalid MAC OUI."



2.1.226. La solución debe implementar mecanismos de protección para mitigar ataques a la infraestructura inalámbrica. Al menos ataques de denegación de servicio deben ser mitigados por la infraestructura a través del envío de paquetes de autenticación.

2.1.227. La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;

2.1.228. La solución debe monitorear y clasificar el riesgo de las aplicaciones accedidas por los clientes inalámbricos;

2.1.229. Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;

2.1.230. Debe implementar la autenticación administrativa a través del protocolo RADIUS;

2.1.231. En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);

2.1.232. En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;

2.1.233. La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;

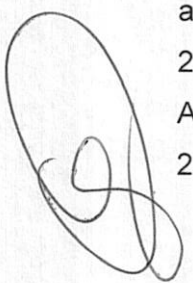
2.1.234. Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada;

2.1.235. La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS;

2.1.236. La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X;

2.1.237. La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;

2.1.238. La solución debe implementar la característica de autenticación de los





usuarios a través de la página web HTTPS, también conocido como Captive Portal. La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red;

2.1.239. La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico;

2.1.240. La solución debe permitir la personalización de la página de autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes;

2.1.241. La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;

2.1.242. La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;

2.1.243. La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada;

2.1.244. La solución debe garantizar que los usuarios se autenticquen en el portal cautivo que utilice la dirección IPv6;

2.1.245. La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución;

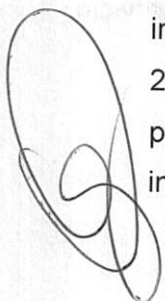
2.1.246. Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;

2.1.247. La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;

2.1.248. La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;

2.1.249. La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible;

- 2.1.250. La solución debe permitir la configuración de redes Mesh entre los puntos de acceso administrados por ella;
- 2.1.251. La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;
- 2.1.252. La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;
- 2.1.253. La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;
- 2.1.254. La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps;
- 2.1.255. La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;
- 2.1.256. La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);
- 2.1.257. La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato .pcap;
- 2.1.258. La solución debe permitir la adición de planta baja del pavimento para ilustrar gráficamente la posición geográfica y el estado de operación de los puntos de acceso administrados por ella. Debe permitir la adición de plantas bajas en los siguientes formatos: JPEG, PNG, GIF o CAD;
- 2.1.259. La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos;
- 2.1.260. La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;
- 2.1.261. La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;
- 2.1.262. La solución debe permitir la identificación del firmware utilizado por cada punto de acceso administrado y permitir la actualización individualizada a través de interfaz gráfica;





- 2.1.263. La solución debe tener herramientas de diagnóstico y depuración;
- 2.1.264. La solución debe soportar la comunicación con elementos externos a través de las API;
- 2.1.265. La solución deberá ser compatible y administrar los puntos de acceso de este proceso;
- 2.1.266. Los firewalls de nueva generación deben contar con fuentes AC 220V, 50Hz y cables de energía norma IRAM
- 2.1.267. Los firewalls deben estar en alta disponibilidad y ambos contar con fuentes de alimentación redundantes.

Licenciamiento

- 2.1.268. La totalidad de los equipos deben contar con la licencia de seguridad y soporte que contemple las siguientes funcionalidades: IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service.
- 2.1.269. Los equipos deben contar con licencia y soporte a 3 años.
- 2.1.270. La licencia debe incluir soporte de ticket por mail y/o teléfono en español, además de RMA en caso de contar con alguna falla

Ren glón N.º 2.- EQUIPOS DE NEXT GEN FIREWALL PARA CENTRO DE DATOS

Cantidad: 5 (cinco)

Interfaces

- 2.2.1. Al menos 16 (dieciséis) interfaces de 1GE RJ45.
- 2.2.2. Al menos 4 (cuatro) interfaces de 1/10GE SFP+
- 2.2.3. Al menos 8 (ocho) interfaces de 1GE SFP.
- 2.2.4. Al menos una interface de administración de 1GE RJ45
- 2.2.5. Al menos una interface de HA (alta disponibilidad) de 1GE RJ45

Performance y dimensionamiento

- 2.2.6. Cada equipamiento deberá poder conmutar al menos, 39 Gbps de tráfico del tipo IPv4 con paquetes de un tamaño de 1518 bytes y políticas de firewall activas.
- 2.2.7. Cada equipo deberá poder tener un performance de 5.3 Gbps a nivel de IPS

2.2.8. Cada equipamiento deberá poder establecer al menos 140.000 nuevas sesiones TCP por segundo.

2.2.9. Cada equipamiento deberá poder mantener al menos 3.000.000 de sesiones activas establecidas (sesiones concurrentes).

2.2.10. Cada equipamiento deberá poder establecer y mantener al menos 2.000 túneles IPSec.

Características Generales

2.2.11. La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.;

2.2.12. Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;

2.2.13. Las funcionalidades de protección de red que conforman la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;

2.2.14. La solución debe estar optimizada para análisis de contenido de aplicaciones en capa 7;

2.2.15. Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19", incluyendo un rail kit (si sea necesario) y los cables de alimentación;

2.2.16. La gestión de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;

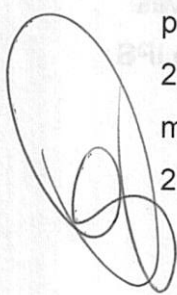
2.2.17. Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;

2.2.18. Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;

2.2.19. Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;

2.2.20. Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);

2.2.21. Los dispositivos de protección de red deben soportar DHCP Relay;





- 2.2.22. Los dispositivos de protección de red deben soportar DHCP Server;
- 2.2.23. Los dispositivos de protección de red deben soportar sFlow;
- 2.2.24. Los dispositivos de protección de red deben soportar Jumbo Frames;
- 2.2.25. Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
- 2.2.26. Debe ser compatible con NAT dinámica (varios-a-1);
- 2.2.27. Debe ser compatible con NAT dinámica (muchos-a-muchos);
- 2.2.28. Debe soportar NAT estática (1-a-1);
- 2.2.29. Debe admitir NAT estática (muchos-a-muchos);
- 2.2.30. Debe ser compatible con NAT estático bidireccional 1-a-1;
- 2.2.31. Debe ser compatible con la traducción de puertos (PAT);
- 2.2.32. Debe ser compatible con NAT Origen;
- 2.2.33. Debe ser compatible con NAT de destino;
- 2.2.34. Debe soportar NAT de origen y NAT de destino de forma simultánea;
- 2.2.35. Debe soportar NAT de origen y NAT de destino en la misma política
- 2.2.36. Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
- 2.2.37. Debe ser compatible con NAT64 y NAT46;
- 2.2.38. Debe implementar el protocolo ECMP;
- 2.2.39. Debe soportar SD-WAN de forma nativa
- 2.2.40. Debe soportar el balanceo de enlace hash por IP de origen;
- 2.2.41. Debe soportar el balanceo de enlace por hash de IP de origen y destino;
- 2.2.42. Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;
- 2.2.43. Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
- 2.2.44. Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles

establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;

2.2.45. Enviar logs a sistemas de gestión externos simultáneamente;

2.2.46. Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;

2.2.47. Debe soportar protección contra la suplantación de identidad (anti-spoofing);

2.2.48. Implementar la optimización del tráfico entre dos dispositivos;

2.2.49. Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);

2.2.50. Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);

2.2.51. Soportar OSPF graceful restart;

2.2.52. Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;

2.2.53. Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;

2.2.54. Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;

2.2.55. Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;

2.2.56. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;

2.2.57. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;

2.2.58. Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;

2.2.59. La configuración de alta disponibilidad debe sincronizar:

- Sesiones;
- Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
- Las asociaciones de seguridad VPN;
- Tablas FIB;





- 2.2.60. En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
- 2.2.61. Debe soportar la creación de sistemas virtuales en el mismo equipo;
- 2.2.62. Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;
- 2.2.63. Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;
- 2.2.64. La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
- 2.2.65. Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);
- 2.2.66. Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;
- 2.2.67. El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;
- 2.2.68. Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;
- 2.2.69. La consola de administración debe soportar como mínimo, Inglés y Español.
- 2.2.70. La consola debe soportar la administración de switches y puntos de acceso inalámbricos para mejorar el nivel de seguridad
- 2.2.71. La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.

Control por Política de Firewall

- 2.2.72. Debe soportar controles de zona de seguridad;
- 2.2.73. Debe contar con políticas de control por puerto y protocolo;
- 2.2.74. Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
- 2.2.75. Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
- 2.2.76. Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
- 2.2.77. Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- 2.2.78. Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
- 2.2.79. Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- 2.2.80. Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes
- 2.2.81. Debe soportar el protocolo estándar de la industria VXLAN;
- 2.2.82. La solución debe permitir la implementación sin asistencia de SD-WAN
- 2.2.83. En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
- 2.2.84. La solución debe soportar la integración nativa con solución de Sandboxing, protección de correo electrónico, cache y Web application firewall.

Control de Aplicación

- 2.2.85. Los dispositivos de protección de red deben tener la capacidad de reconocer



las aplicaciones, independientemente del puerto y protocolo;

2.2.86. Detección de aplicaciones en categorías, como por ejemplo, tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;

2.2.87. Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, x, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, google chat, whatsapp, 4shared, dropbox, Google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

2.2.88. Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;

2.2.89. Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;

2.2.90. Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;

2.2.91. Actualización de la base de firmas de la aplicación de forma automática;

2.2.92. Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;

2.2.93. Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;

2.2.94. Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;

2.2.95. El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;

2.2.96. Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc)

permitiendo granularidad de control/reglas para el mismo;

2.2.97. Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;

2.2.98. Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Google Chat el chat, pero impedir la llamada de video;

2.2.99. Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;

2.2.100. Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);

2.2.101. Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;

2.2.102. Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;

2.2.103. Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Prevención de Amenazas

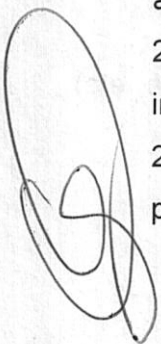
2.2.104. Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;

2.2.105. Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);

2.2.106. Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;

2.2.107. Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;

2.2.108. Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de





origen, dirección de destino, servicio y la combinación de todos estos elementos;

2.2.109. Deber permitir el bloqueo de vulnerabilidades y exploits conocidos

2.2.110. Debe incluir la protección contra ataques de denegación de servicio;

2.2.111. Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;

2.2.112. Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;

2.2.113. Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;

2.2.114. Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP;

2.2.115. Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);

2.2.116. Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones

(flood) de SYN, ICMP, UDP, etc;

2.2.117. Detectar y bloquear los escaneos de puertos de origen;

2.2.118. Bloquear ataques realizados por gusanos (worms) conocidos;

2.2.119. Contar con firmas específicas para la mitigación de ataques DoS y DDoS;

2.2.120. Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);

2.2.121. Debe poder crear firmas personalizadas en la interfaz gráfica del producto;

2.2.122. Identificar y bloquear la comunicación con redes de bots;

2.2.123. Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;

2.2.124. Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;

2.2.125. Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;

2.2.126. Los eventos deben identificar el país que origino la amenaza;

2.2.127. Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);

2.2.128. Tener protección contra descargas involuntarias mediante archivos ejecutables

maliciosos y HTTP;

2.2.129. Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;

2.2.130. En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;

2.2.131. Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);

2.2.132. Debe soportar virtual Patching para bloquear la explotación de vulnerabilidades conocidas en sistemas y aplicaciones, sin la necesidad de instalar un parche de software convencional y formal.

Filtrado de URL

2.2.133. Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;



2.2.134. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios;

2.2.135. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;

2.2.136. Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios;

2.2.137. Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios;

2.2.138. Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autenticación residente en el equipo de seguridad (portal cautivo);

2.2.139. Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;

2.2.140. Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;

2.2.141. Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;

2.2.142. Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;

QoS Traffic Shaping

2.2.143. Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser

excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;

2.2.144. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;

2.2.145. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;

2.2.146. Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;

2.2.147. Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;

2.2.148. Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;

2.2.149. En QoS debe permitir la definición de tráfico con ancho de banda garantizado;

2.2.150. En QoS debe permitir la definición de tráfico con máximo ancho de banda;

2.2.151. En QoS debe permitir la definición de colas de prioridad;

2.2.152. Soportar marcación de paquetes DiffServ, incluso por aplicación;

2.2.153. Soportar la modificación de los valores de DSCP para Diffserv;

2.2.154. Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);

2.2.155. Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes; Filtro de Datos

2.2.156. Debe permitir la creación de filtros para archivos y datos predefinidos;

2.2.157. Los archivos deben ser identificados por tamaño y tipo;

2.2.158. Debe permitir identificar y -opcionalmente- prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;

2.2.159. Debe soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;



2.2.160. Debe soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;

2.2.161. Debe permitir identificar y -opcionalmente- prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;

Geolocalización

2.2.162. Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países;

2.2.163. Debe permitir la visualización de los países de origen y destino en los registros de acceso;

2.2.164. Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

VPN

2.2.165. Soporte VPN de sitio-a-sitio y cliente-a-sitio;

2.2.166. Soportar VPN IPSec;

2.2.167. La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512

2.2.168. La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;

2.2.169. La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);

2.2.170. La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);

2.2.171. Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

2.2.172. Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;

2.2.173. Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;

2.2.174. Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el



túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;

2.2.175. Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;

2.2.176. Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;

2.2.177. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;

2.2.178. Deberá mantener una conexión segura con el portal durante la sesión;

2.2.179. El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

Wireless Controller

2.2.180. Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);

2.2.181. Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;

2.2.182. Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac / ax y que transmitan tráfico IPv4 e IPv6 a través del controlador;

2.2.183. La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;

2.2.184. El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;

2.2.185. La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario;

2.2.186. Debe permitir programar día y hora en que ocurrirá la optimización del



aprovisionamiento automático de canales en los Access Points;

2.2.187. El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tunelados hasta el controlador inalámbrico;

2.2.188. Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;

2.2.189. Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico;

2.2.190. Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPAWPA2-Personal (PSK), en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;

2.2.191. La solución debe permitir definir qué redes serán tuneladas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso;

2.2.192. La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tunelados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso;

2.2.193. La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz, 5GHz y 6GHz;

2.2.194. La solución debe detectar Receiver Start of Packet (RX-SOP) en paquetes inalámbricos y ser capaz de omitir aquellos que están por debajo de determinado

umbral especificado en dBm;

2.2.195. La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso;

2.2.196. La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y basada en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados;

2.2.197. La solución debe identificar automáticamente puntos de acceso intrusos que estén conectados a la red de cable (LAN). La solución debe ser capaz de identificar el punto de acceso intruso incluso cuando el MAC Address de la interfaz LAN es ligeramente diferente (adyacente) del MAC Address de la interfaz WLAN;

2.2.198. La solución debe detectar los puntos de acceso no autorizados y / o intrusos a través de radios dedicados a la función de análisis o a través de Off-channel / Background scanning. Cuando se realiza a través de Off-channel / Background scanning, la solución debe ser capaz de identificar el uso del punto de acceso para, en caso necesario, retrasar el análisis y de esta forma no perjudicar a los clientes conectados;

2.2.199. La solución debe permitir la configuración individual de los radios del punto de acceso para que operen en el modo monitor, o sea, con función dedicada para detectar amenazas en la red inalámbrica y con ello permitir mayor flexibilidad en el diseño de la red;

2.2.200. La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y sincronizar la configuración del principal, además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener



función de primario de forma temporal;

2.2.201. La solución debe permitir el agrupamiento de VLANs para que se distribuyan múltiples subredes en un determinado SSID, reduciendo así el broadcast y aumentando la disponibilidad de direcciones IP;

2.2.202. La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado;

2.2.203. La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios;

2.2.204. Debe permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;

2.2.205. La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;

2.2.206. La solución debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia;

2.2.207. La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectado mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;

2.2.208. La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica;

2.2.209. La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado;

2.2.210. La solución debe implementar técnicas de Call Admission Control para limitar el número de llamadas simultáneas;

2.2.211. La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica e informar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado, Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación;

2.2.212. Para garantizar una mejor distribución de dispositivos entre las frecuencias disponibles y mejorar la utilización de la radiofrecuencia, la solución debe ser capaz de distribuir automáticamente los dispositivos de banda dual para que se conecten primariamente a 5GHz a través del recurso conocido como Band Steering;

2.2.213. La solución debe permitir la configuración de los data rates que se activarán en la herramienta y las que se deshabilitar para las frecuencias de 2.4, 5GHz y 6GHz y los estándares 802.11a / b / g / n / ac / ax;

2.2.214. La solución debe tener capacidad capaz de convertir paquetes Multicast en paquetes Unicast cuando se reenvían a los dispositivos que están conectados a la infraestructura inalámbrica, mejorando así el consumo de Airtime;

2.2.215. La solución debe soportar la característica que ignore Probe Requests de clientes que tienen una señal débil o distante. Debe permitir definir el umbral para que los Probe Requests sean ignorados;

2.2.216. La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz;

2.2.217. La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;

2.2.218. La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio direcciones de origen y destino (IPv4 e IPv6), puertos y protocolos;

2.2.219. La solución debe implementar la función de web filtering para controlar los



sitios que se accede a la red inalámbrica. Debe poseer una base de conocimiento para categorizar los sitios y permitir configurar qué categorías de sitios serán permitidos y bloqueados para cada perfil de usuario y SSID;

2.2.220. La solución debe tener capacidad de reconocimiento de aplicaciones a través de la técnica de DPI (Deep Packet Inspection) que permita al administrador de la red monitorear el perfil de acceso de los usuarios e implementar políticas de control. Debe permitir el funcionamiento de esta característica y la actualización periódica de la base de aplicaciones durante todo el período de garantía de la solución;

2.2.221. La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil y quinientas) aplicaciones;

2.2.222. La solución debe permitir la creación de reglas para el bloqueo y el límite de banda (en Mbps, Kbps o Bps) para las aplicaciones reconocidas a través de la técnica de DPI;

2.2.223. La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS; 2.2.224. "La solución debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica. Al menos los siguientes ataques deben ser identificados:

- Ataques de flood contra el protocolo EAPOL (EAPOL Flooding);
- Los siguientes ataques de denegación de servicio: Association Flood, Authentication Flood, Broadcast Deauthentication y Spoofed Deauthentication;
- ASLEAP;
- Null Probe Response / Null SSID Probe Response;
- Long Duration;
- Ataques contra Wireless Bridges;
- Weak WEP;
- Invalid MAC OUI."

2.2.225. La solución debe implementar mecanismos de protección para mitigar ataques a la infraestructura inalámbrica. Al menos ataques de denegación de servicio

deben ser mitigados por la infraestructura a través del envío de paquetes de autenticación.

2.2.226. La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;

2.2.227. La solución debe monitorear y clasificar el riesgo de las aplicaciones accedidas por los clientes inalámbricos;

2.2.228. Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;

2.2.229. Debe implementar la autenticación administrativa a través del protocolo RADIUS;

2.2.230. En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);

2.2.231. En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;

2.2.232. La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;

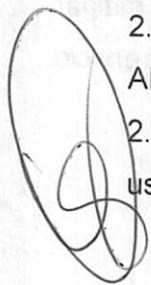
2.2.233. Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada;

2.2.234. La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS;

2.2.235. La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X;

2.2.236. La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;

2.2.237. La solución debe implementar la característica de autenticación de los usuarios a través de la página web HTTPS, también conocido como Captive Portal.





La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red;

2.2.238. La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico;

2.2.239. La solución debe permitir la personalización de la página de autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes;

2.2.240. La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;

2.2.241. La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;

2.2.242. La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada;

2.2.243. La solución debe garantizar que los usuarios se autenticuen en el portal cautivo que utilice la dirección IPv6;

2.2.244. La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución;

2.2.245. Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;

2.2.246. La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;

2.2.247. La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;

2.2.248. La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible;



2.2.249. La solución debe permitir la configuración de redes Mesh entre los puntos de acceso

administrados por ella;

2.2.250. La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;

2.2.251. La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;

2.2.252. La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;

2.2.253. La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps;

2.2.254. La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;

2.2.255. La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);

2.2.256. La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato .pcap;

2.2.257. La solución debe permitir la adición de planta baja del pavimento para ilustrar gráficamente la posición geográfica y el estado de operación de los puntos de acceso administrados por ella. Debe permitir la adición de plantas bajas en los siguientes formatos: JPEG, PNG, GIF o CAD;

2.2.258. La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos;

2.2.259. La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;

2.2.260. La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;

2.2.261. La solución debe permitir la identificación del firmware utilizado por cada



punto de acceso administrado y permitir la actualización individualizada a través de interfaz gráfica;

2.2.262. La solución debe tener herramientas de diagnóstico y depuración;

2.2.263. La solución debe soportar la comunicación con elementos externos a través de las API;

2.2.264. La solución deberá ser compatible y administrar los puntos de acceso de este proceso;

2.2.265. Los firewalls de nueva generación deben contar con fuentes AC 220V, 50Hz y cables de energía norma IRAM

2.2.266. Los firewalls deben estar en alta disponibilidad y ambos contar con fuentes de alimentación redundantes.

Licenciamiento

2.2.267. La totalidad de los equipos deben contar con la licencia de seguridad y soporte que contemple las siguientes funcionalidades: IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service.

2.2.268. Los equipos deben contar con licencia y soporte a 3 años.

2.2.269. La licencia debe incluir soporte de ticket por mail y/o teléfono en español, además de RMA en caso de contar con alguna falla.

Ren glón N.º 3.- SWITCH CORE DE CAPA 3

Cantidad: 2 (dos).

Características del equipamiento

2.3.1. Al menos 24 (veinticuatro) interfaces de 24x 10G/1G SFP+/SFP.

2.3.2. Al menos 2 (dos) interfaces de 100G/40G QSFP28/QSFP+.

2.3.3. Al menos una interface de administración de 1GE RJ45

2.3.4. Deberá soportar al menos una capacidad de switching de 880 Gbps (en Duplex)

2.3.5. Deberá soportar al menos 1309 Mpps de paquetes por segundo (Duplex 64 bytes) **Administración General**

2.3.6. El switch deberá poder ser administrado por una consola de gestión centralizada

para la configuración de ruteo en capa 3, si aplicara la funcionalidad, ruteo basado en políticas y VLANs

2.3.7. Se podrán administrar todos los switches core desde la consola central indicada en el renglón 1 o 2.

2.3.8. El switch deberá poder aceptar actualizaciones de firmware

2.3.9. El switch deberá poder actualizarse automáticamente a la versión de firmware especificada previamente al conectarse a la consola de administración centralizada

2.3.10. Deberá soportar REST API

2.3.11. Deberá soportar detección y notificación de conflictos de direcciones IP

2.3.12. Deberá soportar administración en la nube

2.3.13. Con la consola de administración centralizada deberá poder crear listas negras y blancas

2.3.14. Con la consola de administración centralizada deberá poder crear políticas de control de acceso (NAC) para usuarios y dispositivos sin necesidad de licencia adicional

2.3.15. Con la consola de administración centralizada deberá soportar una vista completa de toda la solución de switches.

2.3.16. Con la consola de administración centralizada se deberá soportar la identificación dinámica de los tipos y familias de dispositivos conectados a los switches incluyendo, más no limitado a: teléfono, laptop, computadora, entre otros.

2.3.17. Con la consola de administración centralizada deberá poder implementar la función de Firewall, Antivirus, Control de Aplicaciones, Filtrado de Navegación Web (HTTP/HTTPS/Video/DNS), Filtrado de Archivos, IPS, Anti-Botnet, Filtrado de Anti-Spam e Inspección SSL.

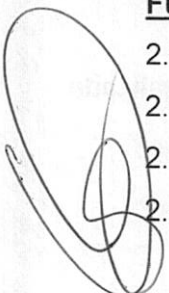
Funcionalidades de Capa 2 y Capa 3

2.3.18. Deberá soportar administración por IPv4 e IPv6

2.3.19. Deberá soportar Telnet / SSH para acceso a la consola

2.3.20. Deberá soportar HTTP / HTTPS

2.3.21. Deberá soportar SNMP v1/v2c/v3





- 2.3.22. Deberá soportar SNTP
- 2.3.23. Deberá contar con una línea de comandos estándar y con interface para configurar via Web
- 2.3.24. Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI
- 2.3.25. Deberá soportar HTTP REST APIs para Configuración y monitoreo
- 2.3.26. Deberá soportar Link Aggregation estático
- 2.3.27. Deberá soportar LACP
- 2.3.28. Deberá soportar Spanning Tree
- 2.3.29. Deberá soportar DHCP Snooping
- 2.3.30. Deberá soportar Jumbo Frames
- 2.3.31. Deberá soportar Auto-negociación para la velocidad de los puertos y para Duplex
- 2.3.32. Deberá soportar el estándar IEEE 802.1D MAC Bridging/STP
- 2.3.33. Deberá soportar el estándar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- 2.3.34. Deberá soportar el estándar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- 2.3.35. Deberá soportar la funcionalidad STP Root Guard
- 2.3.36. Deberá soportar STP BPDU Guard
- 2.3.37. Deberá soportar Edge Port / Port Fast
- 2.3.38. Deberá soportar el estándar IEEE 802.1Q VLAN Tagging
- 2.3.39. Deberá soportar Private VLAN
- 2.3.40. Deberá soportar el estándar IEEE 802.3ad Link Aggregation con LACP
- 2.3.41. Deberá poder balancear tráfico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
- 2.3.42. Deberá soportar el estándar IEEE 802.1AX Link Aggregation
- 2.3.43. Deberá soportar instancias de Spanning Tree (MSTP/CST)
- 2.3.44. Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure
- 2.3.45. Deberá soportar el estándar IEEE 802.3 10Base-T

- 2.3.46. Deberá soportar el estándar IEEE 802.3u 100Base-TX
- 2.3.47. Deberá soportar el estándar IEEE 802.3z 1000Base-SX/LX
- 2.3.48. Deberá soportar el estándar IEEE 802.3ab 1000Base-T
- 2.3.49. Deberá soportar el estándar IEEE 802.3ae 10 Gigabit Ethernet
- 2.3.50. Deberá soportar el estándar IEEE 802.3 CSMA/CD como método de acceso y las especificaciones de la capa física
- 2.3.51. Deberá contar con la funcionalidad de Control de Tormentas (Storm Control)
- 2.3.52. Deberá soportar la creación de VLANs por MAC, IP y Ethertype-based
- 2.3.53. Deberá soportar la funcionalidad de Virtual-Wire
- 2.3.54. Deberá soportar Time-Domain Reflectometer (TDR)
- 2.3.55. Deberá soportar 4094 VLANs simultáneas
- 2.3.56. Deberá soportar IGMP Snooping
- 2.3.57. Deberá soportar IGMP proxy y querier
- 2.3.58. Deberá soportar emergency location identifier numbers (ELINs) en LLDP-MED
- 2.3.59. Deberá permitir la negociación de POE en LLDP-MED
- 2.3.60. Deberá permitir limitar la cantidad de MACs aprendidas por puerto
- 2.3.61. Deberá permitir un mínimo de 15 instancias de MSTP
- 2.3.62. Deberá permitir controlar tormentas de broadcast independientemente en cada puerto
- 2.3.63. Deberá soportar un mecanismo de detección y prevención de loops
- 2.3.64. Deberá soportar VLAN Stacking (QinQ)
- 2.3.65. Deberá soportar SPAN
- 2.3.66. Deberá soportar RSPAN y ERSPAN
- 2.3.67. Deberá soportar ruteo estático
- 2.3.68. Deberá soportar RIP v2
- 2.3.69. Deberá soportar OSPF v2
- 2.3.70. Deberá soportar VRRP
- 2.3.71. Deberá soportar IS-IS
- 2.3.72. Deberá soportar BGP



- 2.3.73. Deberá soportar protocolos de ruteo multicast
- 2.3.74. Deberá soportar Equal Cost Multipath Routing (ECMP)
- 2.3.75. Deberá soportar Bidirectional Forwarding Detection (BFD)
- 2.3.76. Deberá soportar DHCP Relay
- 2.3.77. Deberá soportar DHCP Server
- 2.3.78. Deberá soportar MC-LAG (multi- chassis link agragation)

RFC Compliance.

- 2.3.79. Deberá soportar el RFC 2571 Architecture for Describing SNMP
- 2.3.80. Deberá soportar el RFC 854 Telnet Server
- 2.3.81. Deberá soportar el RFC 2865 RADIUS
- 2.3.82. Deberá soportar el RFC 1643 Ethernet-like Interface MIB
- 2.3.83. Deberá soportar el RFC 1213 MIB-II
- 2.3.84. Deberá soportar el RFC 1354 IP Forwarding Table MIB
- 2.3.85. Deberá soportar el RFC 2572 SNMP Message Processing and Dispatching
- 2.3.86. Deberá soportar el RFC 1573 SNMP MIB II
- 2.3.87. Deberá soportar el RFC 1157 SNMPv1/v2c
- 2.3.88. Deberá soportar el RFC 2030 SNTTP

Seguridad y Visibilidad

- 2.3.89. Deberá soportar Port Mirroring
- 2.3.90. Deberá soportar Admin Authentication Via RFC 2865 RADIUS
- 2.3.91. Deberá soportar el estándar IEEE 802.1x authentication Port-based
- 2.3.92. Deberá soportar el estándar IEEE 802.1x Authentication MAC-based
- 2.3.93. Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN
- 2.3.94. Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB)
- 2.3.95. Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment
- 2.3.96. Deberá soportar Radius CoA (Change of Authority)
- 2.3.97. Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
- 2.3.98. Deberá soportar el estándar IEEE 802.1ab LLDP-MED

- 2.3.99. Deberá soportar Radius Accounting
- 2.3.100. Deberá soportar EAP-passthrough
- 2.3.101. Deberá soportar detección de dispositivos
- 2.3.102. Deberá soportar MAC-IP binding
- 2.3.103. Deberá soportar sFlow
- 2.3.104. Deberá soportar Flow Export
- 2.3.105. Deberá soportar ACLs
- 2.3.106. Deberá soportar múltiples ACLs de ingreso
- 2.3.107. Deberá soportar scheduling de ACLs
- 2.3.108. Deberá soportar DHCP Snooping
- 2.3.109. Deberá soportar listas de servidores DHCP permitidos
- 2.3.110. Deberá soportar bloqueo de DHCP
- 2.3.111. Deberá permitir Dynamic ARP Inspection (DAI)
- 2.3.112. Deberá permitir Access VLANs
- 2.3.113. Deberá permitir tagging de tráfico con VLAN ID mediante ACLs

Varios

- 2.3.114. Deberá soportar Syslog
- 2.3.115. Debe contar con un sensor de temperatura interno
- 2.3.116. Debe permitir monitorear la temperatura del dispositivo
- 2.3.117. Debe soportar QSFP+ low-power mode
- 2.3.118. Debe soportar Energy-Efficient Ethernet (EEE)

Soporte

- 2.3.119. La totalidad de los equipamientos Switches de Red deberán contar con un soporte con cobertura por RMA, actualización de Firmware y soporte técnico por un período de 3 años.
- 2.3.120. El soporte de ticket por mail y/o teléfono en español, además de RMA en caso de contar con alguna falla.

Renglón N.º 4.- SWITCH DE DISTRIBUCIÓN



Cantidad: 5 (cinco)

Interfaces

2.4.1. Al menos 24 (veinticuatro) interfaces de 2.5G/1G/100M/10M RJ45

2.4.2. Al menos 6 (seis) interfaces de 1G/10GE SFP+Performance y dimensionamiento

2.4.3. Cada equipamiento deberá poder conmutar al menos, 240 Gbps de tráfico.

2.4.4. Cada equipamiento deberá poder conmutar al menos 355 Mpps paquetes por segundo.

2.4.5. Cada equipamiento deberá poder almacenar por lo menos 32.000 Mac Address.

2.4.6. Cada equipo deberá entregar al menos 780W de PoE

Características generales

2.4.7. Deberá soportar priorización de tráfico basada en 802.1p

2.4.8. Deberá soportar priorización de tráfico basada en IP TOS/DSCP

2.4.9. Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP

2.4.10. Los equipamientos deben contar con fuentes AC 220V, 50Hz y cables de energía norma IRAM

2.4.11. Los equipamientos deben permitir el rackeo en racks standard de 19 pulgadas mediante.

2.4.12. Soporte para Jumbo Frames.

2.4.13. Control de flujo conforme a IEEE 802.3x.

2.4.14. Prevención de tormentas de broadcast.

2.4.15. Autenticación de red 802.1X.

2.4.16. Soporte para inspección ARP dinámica (DAI).

2.4.17. Inspección de DHCP snooping.

2.4.18. Soporte para STP, RSTP y MSTP.

2.4.19. Funciones de protección como BPDU Guard y Root Guard.

2.4.20. Control de acceso basado en listas (ACL).

2.4.21. Aislamiento de puertos para seguridad adicional.

Administración y Monitoreo

2.4.22. Interfaces de gestión: Web (HTTP/HTTPS), CLI, SNMP v1/v2c/v3, SSH, Telnet.

2.4.23. Soporte para LLDP y LLDP-MED.

2.4.24. Sincronización horaria mediante SNTP.

2.4.25. Transferencia de archivos vía TFTP.

2.4.26. Posibilidad de gestión remota y centralizada.

2.4.27. Se podrán administrar todos los switches desde la consola central indicada en el renglón 1 o 2.

Calidad de Servicio (QoS)

2.4.28. Priorización de tráfico crítica (voz, video).

2.4.29. Clasificación y limitación del tráfico por puerto o VLAN.

2.4.30. Soporte para colas de prioridad y shaping.

Control de Acceso

2.4.31. Desde la consola de gestión centralizada (renglón 1 o 2) deberá poder controlar el acceso y asignación de vlan de forma dinámica y automática por MAC, Sistema Operativo, Vendor y Familia al menos.

Soporte

2.4.32. La totalidad de los equipamientos Switches de Red deberán contar con un soporte con cobertura por RMA, actualización de Firmware y soporte técnico por un período de 3 años.

2.4.33. El soporte de ticket por mail y/o teléfono en español, además de RMA en caso de contar con alguna falla.

Renglón N.º 5.- SWITCH DE ACCESO DE CAPA 2 CON POE+

Cantidad: 14 (catorce)

Interfaces

2.5.1. Al menos 48 (cuarenta y ocho) interfaces de 1GE RJ45

2.5.2. Al menos 4 (cuatro) interfaces de 10GE SFP+

2.5.3. Al menos 1 (un) interfaz de consola RJ45

2.5.4. Debe soportar PoE (802.3 bt y af/at) con una capacidad de 740W



Performance y dimensionamiento

- 2.5.5. Cada equipamiento deberá poder conmutar al menos, 170 Gbps de tráfico.
- 2.5.6. Cada equipamiento deberá poder conmutar al menos 250 Mpps de 64Bytes.
- 2.5.7. Cada equipamiento deberá poder almacenar por lo menos 30.000 Mac Address.
- 2.5.8. Capacidad total de energizar puertos de red PoE de 780 W

Características generales

- 2.5.9. Deberá soportar priorización de tráfico basada en 802.1p
- 2.5.10. Deberá soportar priorización de tráfico basada en IP TOS/DSCP
- 2.5.11. Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP
- 2.5.12. Los equipamientos deben contar con fuentes AC 220V, 50Hz y cables de energía norma IRAM
- 2.5.13. Los equipamientos deben permitir el rackeo en racks standard de 19 pulgadas mediante.
- 2.5.14. Soporte para Jumbo Frames.
- 2.5.15. Control de flujo conforme a IEEE 802.3x.
- 2.5.16. Prevención de tormentas de broadcast.
- 2.5.17. Autenticación de red 802.1X.
- 2.5.18. Soporte para inspección ARP dinámica (DAI).
- 2.5.19. Inspección de DHCP snooping.
- 2.5.20. Soporte para STP, RSTP y MSTP.
- 2.5.21. Funciones de protección como BPDU Guard y Root Guard.
- 2.5.22. Control de acceso basado en listas (ACL).
- 2.5.23. Aislamiento de puertos para seguridad adicional.

Administración y Monitoreo

- 2.5.24. Interfaces de gestión: Web (HTTP/HTTPS), CLI, SNMP v1/v2c/v3, SSH, Telnet.
- 2.5.25. Soporte para LLDP y LLDP-MED.
- 2.5.26. Sincronización horaria mediante SNTP.
- 2.5.27. Transferencia de archivos vía TFTP.
- 2.5.28. Posibilidad de gestión remota y centralizada (desde centro de datos o sucursal)

–renglón 1 o 2).

Calidad de Servicio (QoS)

2.5.29. Priorización de tráfico crítica (voz, video).

2.5.30. Clasificación y limitación del tráfico por puerto o VLAN.

2.5.31. Soporte para colas de prioridad y shaping.

Control de Acceso

2.5.32. Desde la consola de gestión centralizada (renglón 1 o 2) deberá poder controlar el acceso y asignación de vlan de forma dinámica y automática por MAC, Sistema Operativo, Vendor y Familia al menos.

Soporte

2.5.33. La totalidad de los equipamientos Switches de Red deberán contar con un soporte con cobertura por RMA, actualización de Firmware y soporte técnico por un período de 3 años.

2.5.34. El soporte de ticket por mail y/o teléfono en español, además de RMA en caso de contar con alguna falla.

Renglón N.º 6.- SWITCH DE ACCESO DE CAPA 2

Cantidad: 14 (catorce)

Interfaces

2.6.1. Al menos 48 (cuarenta y ocho) interfaces de 1GE RJ45

2.6.2. Al menos 4 (cuatro) interfaces de 10 GE SFP+

2.6.3. Al menos 1 (un) interfaz de consola RJ45

Performance y dimensionamiento

2.6.4. Cada equipamiento deberá poder conmutar al menos, 170 Gbps de tráfico.

2.6.5. Cada equipamiento deberá poder conmutar al menos 260 Mpps de paquetes por segundo.

2.6.6. Cada equipamiento deberá poder almacenar por lo menos 32.000 Mac Address.

Características generales

2.6.7. Soporte para Jumbo Frames.



- 2.6.8. Control de flujo conforme a IEEE 802.3x.
- 2.6.9. Prevención de tormentas de broadcast.
- 2.6.10. Autenticación de red 802.1X.
- 2.6.11. Soporte para inspección ARP dinámica (DAI).
- 2.6.12. Inspección de DHCP snooping.
- 2.6.13. Soporte para STP, RSTP y MSTP.
- 2.6.14. Funciones de protección como BPDU Guard y Root Guard.
- 2.6.15. Control de acceso basado en listas (ACL).
- 2.6.16. Aislamiento de puertos para seguridad adicional.

Administración y Monitoreo

- 2.6.17. Interfaces de gestión: Web (HTTP/HTTPS), CLI, SNMP v1/v2c/v3, SSH, Telnet.
- 2.6.18. Soporte para LLDP y LLDP-MED.
- 2.6.19. Sincronización horaria mediante SNTP.
- 2.6.20. Transferencia de archivos vía TFTP.
- 2.6.21. Posibilidad de gestión remota y centralizada (desde centro de datos o sucursal – renglón 1 o 2).

Calidad de Servicio (QoS)

- 2.6.22. Priorización de tráfico crítica (voz, video).
- 2.6.23. Clasificación y limitación del tráfico por puerto o VLAN.
- 2.6.24. Soporte para colas de prioridad y shaping.

Control de Acceso

- 2.6.25. Desde la consola de gestión centralizada (renglón 1 o 2) deberá poder controlar el acceso y asignación de vlan de forma dinámica y automática por MAC, Sistema Operativo, Vendor y Familia al menos.

Soporte

- 2.6.26. La totalidad de los equipamientos Switches de Red deberán contar con un soporte con cobertura por RMA, actualización de Firmware y soporte técnico por un periodo de 3 años.
- 2.6.27. El soporte de ticket por mail y/o teléfono en español, además de RMA en caso

de contar con alguna falla.

Renglón N.º 7.- MÓDULO TRANSCEPTOR ÓPTICO

Cantidad: 120 (Ciento veinte)

Especificaciones

- 2.7.1. Tipo: Fibra Multimodo 850nm
- 2.7.2. Velocidad: 10GE SFP+
- 2.7.3. Alcance máx: 300 metros
- 2.7.4. Tipo de Conector: LLC
- 2.7.5. Deben ser de la misma marca de los Firewall Perimetral (renglón 1 y 2)

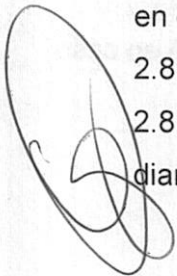
Renglón N.º 8.- PLATAFORMA DE ADMINISTRACIÓN Y ANALÍTICAS

Se deberán proveer dos soluciones separadas en modalidad VM (virtual Machine). Una para la gestión de reportes y troubleshooting centralizada y la otra, para la administración centrales de los Next Gen Firewalls

Plataforma de gestión analítica

Especificaciones

- 2.8.1. La solución debe ser del tipo Virtual Appliance para implementarse on premise.
- 2.8.2. La solución no debe tener restricciones en la capacidad de almacenamiento en disco.
- 2.8.3. La solución no debe tener restricciones en la cantidad de storage asignado.
- 2.8.4. Debe recibir y procesar logs de todos los Next Generation Firewall y SDWAN indicados en los ítems anteriores del presente pliego.
- 2.8.5. La solución debe presentar un esquema de licenciamiento por suscripción por 3 años que incluya el soporte de la solución y, además, de ticket por mail y/o teléfono en español, además de RMA en caso de contar con alguna falla.
- 2.8.6. Se debe licenciar la cantidad de GB por día de logs que puede recibir la solución.
- 2.8.7. La solución debe tener capacidad de recibir y procesar al menos 10 GB de logs diarios.





- 2.8.8. La suscripción debe incluir análisis de Indicadores de Compromisos, con inteligencia provista y actualizada periódicamente por el fabricante.
- 2.8.9. La suscripción debe incluir un dashboard de SoC donde se permitan realizar tareas automatizadas a partir de diversos inputs preconfigurados.
- 2.8.10. La integración con los Firewall de nueva generación (renglón 1 y 2) debe permitir generar de forma automática una topología física y lógica de las conexiones principales.
- 2.8.11. La solución debe incluir un Asistente de IA (inteligencia Artificial) del mismo fabricante para responder preguntas y obtener ayuda con las configuraciones utilizando un lenguaje natural.
- 2.8.12. Requisitos de funcionalidad
- 2.8.13. La solución debe permitir la virtualización en los siguientes hipervisores: VMware ESX/ESXi
- 2.8.14. Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+ y KVM sobre RedHat 6.5+.
- 2.8.15. La solución no debe tener limitaciones en cuanto a la asignación de vCPU.
- 2.8.16. La solución no debe tener limitaciones en cuanto a la asignación de memoria.
- 2.8.17. Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución.
- 2.8.18. Contar con comunicación cifrada y autenticación con usuario y contraseña para su administración, tanto en interface gráfica (GUI) como vía línea de comandos.
- 2.8.19. Permitir acceso simultáneo de administración, así como permitir crear por lo menos
- 2 (dos) perfiles para administración y monitoreo.
- 2.8.20. Soporte SNMP versión 2 y 3.
- 2.8.21. Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH.
- 2.8.22. Debe permitir la autenticación de usuarios de acceso a la plataforma vía LDAP.
- 2.8.23. Debe permitir la autenticación de usuarios de acceso a la plataforma vía

Radius.

2.8.24. Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos.

2.8.25. Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.

2.8.26. Generación de informes en tiempo real de tráfico, en formato de gráfica de tabla.

2.8.27. Definición de perfiles de acceso a consola con permiso granulares, tales como : acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.

2.8.28. Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.

2.8.29. Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado.

2.8.30. Contar con mecanismos de borrado automático de logs antiguos.

2.8.31. Permitir la importación y exportación de reportes.

2.8.32. Debe contar con la capacidad de crear informes en formato HTML.

2.8.33. Debe contar con la capacidad de crear informes en formato PDF.

2.8.34. Debe contar con la capacidad de crear informes en formato XML.

2.8.35. Debe contar con la capacidad de crear informes en formato CSV.

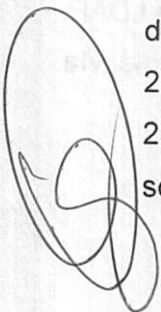
2.8.36. Debe permitir exportar los logs en formato CSV.

2.8.37. Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.

2.8.38. Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.

2.8.39. La solución debe contar con reportes predefinidos.

2.8.40. Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución.





- 2.8.41. Debe ser posible la duplicación de reportes existentes para su posterior edición.
- 2.8.42. Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
- 2.8.43. Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
- 2.8.44. Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
- 2.8.45. Debe tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas.
- 2.8.46. Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
- 2.8.47. Debe tener la capacidad de generar y enviar reportes periódicos automáticamente.
- 2.8.48. Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
- 2.8.49. Permitir el envío por email de manera automática de reportes.
- 2.8.50. Debe permitir que el reporte a enviar por email sea al destinatario específico.
- 2.8.51. Permitir la programación de reportes, conforme a un calendario definido por el administrador.
- 2.8.52. Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
- 2.8.53. Debe permitir el uso de filtros en los reportes.
- 2.8.54. Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
- 2.8.55. Permitir especificar el idioma de los reportes creados.
- 2.8.56. Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
- 2.8.57. Debe permitir el envío automático de reportes a un servidor externo SFTP o

FTP.

2.8.58. Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.

2.8.59. Debe tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.

2.8.60. Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.

2.8.61. La solución debe ser capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.

2.8.62. Debe ser posible debe poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.

2.8.63. Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.

2.8.64. Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.

2.8.65. Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos

2.8.66. Debe permitir visualizar en tiempo real los logs recibidos.

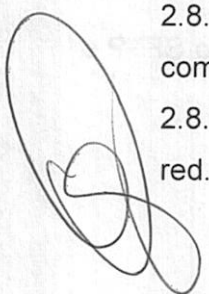
2.8.67. Debe permitir el reenvío de logs en formato syslog.

2.8.68. Debe permitir el reenvío de logs en formato CEF (Common Event Format).

2.8.69. Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para la red.

2.8.70. Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en la red.

2.8.71. Debe incluir dashboard para operaciones SOC que monitorea el tráfico en la red.



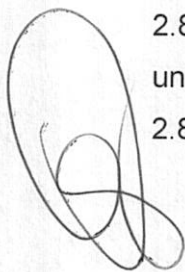
- 2.8.72. Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en la red.
- 2.8.73. Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en la red (sandboxing).
- 2.8.74. Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en la red.
- 2.8.75. Debe incluir dashboard para operaciones SOC que monitorea actividad VPN en la red.
- 2.8.76. Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso Wifi y SSIDs
- 2.8.77. Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria).
- 2.8.78. Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC.
- 2.8.79. Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3.
- 2.8.80. Debe permitir generar alertas de eventos a partir de logs recibidos.
- 2.8.81. Debe permitir crear incidentes a partir de alertas de eventos para endpoint.
- 2.8.82. Debe permitir la integración al sistema de tickets ServiceNow.
- 2.8.83. Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
- 2.8.84. Debe soportar el estándar SAML para autenticación de usuarios administradores.
- 2.8.85. Reportes de Firewall
- 2.8.86. Debe contar con reporte de cumplimiento de PCI DSS
- 2.8.87. Debe contar con reporte de utilización de aplicaciones SaaS
- 2.8.88. Debe contar con reporte de prevención de pérdida de datos (DLP)

- 2.8.89. Debe contar con reporte de VPN
- 2.8.90. Debe contar con reporte de Sistema de prevención de intrusos (IPS)
- 2.8.91. Debe contar con reporte de reputación de cliente
- 2.8.92. Debe contar con reporte de análisis de seguridad de usuario
- 2.8.93. Debe contar con reporte de análisis de amenaza cibernética
- 2.8.94. Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad
- 2.8.95. Debe contar con reporte de tráfico DNS
- 2.8.96. Debe contar con reporte tráfico de correo electrónico
- 2.8.97. Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red
- 2.8.98. Debe contar con reporte de Top 10 de Websites utilizadas en la red
- 2.8.99. Debe contar con reporte de uso de redes sociales

Plataforma de Administración Central

Especificaciones

- 2.8.100. La solución debe ser del tipo Virtual Appliance para implementarse on premise.
- 2.8.101. La solución debe incluir licencias para gestionar hasta 10 Firewalls de Nueva generación (renglón 1 y 2).
- 2.8.102. La solución debe presentar un esquema de licencia por suscripción por 3 años con soporte de la marca en español.
- 2.8.103. Debe gestionar de forma centralizada todos los Firewall de nueva generación solicitados en este documento.
- 2.8.104. Debe soportar al menos 4 vCPU y no debe tener una restricción máxima a asignar.
- 2.8.105. La solución debe permitir hasta 12 Network Interface
- 2.8.106. La solución no debe tener límite de memoria RAM a asignar.
- 2.8.107. La solución debe contar con plantillas de configuración de SD-WAN para unificar configuraciones en los Firewall de nueva generación (renglón 1 y 2).
- 2.8.108. La solución deberá tener la posibilidad de administrar los switches (renglón





3, 4, 5 y 6).

2.8.109. La solución debe incluir un Asistente de IA (inteligencia Artificial) del mismo fabricante para responder preguntas y obtener ayuda con las configuraciones utilizando un lenguaje natural.

2.8.110. Debe tener la capacidad de integrarse con la solución de análisis de logs (ítem 8.1) de forma nativa para permitir una mejor gestión y análisis de la seguridad de dispositivos Firewalls.

CARACTERÍSTICAS GENERALES

2.8.111. Creación, almacenamiento e implementación automatizada de configuraciones de dispositivos.

2.8.112. Permitir tener un solo repositorio de almacenamiento centralizado y administración de configuraciones, para simplificar las tareas de administración de una gran cantidad de dispositivos de seguridad con protección completa de contenido.

2.8.113. Las comunicaciones entre la consola de administración y los dispositivos administrados deben ser cifradas (Encriptadas)

2.8.114. La interface de administración es basada en Web Seguro (HTTPS)

2.8.115. Para un eficiente almacenamiento de las configuraciones, debe incluirse una base de datos relacional integrada compatible con la solución.

2.8.116. Administración basada en roles para permitir a los administradores delegar los derechos a dispositivos específicos con los privilegios adecuados de lectura/escritura.

2.8.117. Configuración basada en scripts para una mejor flexibilidad y control. Esta funcionalidad permite la automatización de tareas operativas, cuya implementación puede ser de forma masiva, con tiempos de aplicación mínimos a los dispositivos administrados

2.8.118. Se debe poder realizar automatización calendarizada de respaldos de la configuración y las bitácoras.

2.8.119. Se debe poder realizar operaciones sobre grupos de dispositivos, y añadir/cambiar/borrar dispositivos de esos grupos.

2.8.120. Permitir el hospedaje local de actualizaciones de firmas de AV / IPS y filtrado de contenido web y Antispam, de los firewalls de nueva generación. Esto permite el almacenamiento de forma local de las bases de datos de protección AV e IPS, además de Filtrado de Contenido y Anti-SPAM, con la finalidad de disminuir el tráfico de consultas de actualizaciones a Internet a lo mínimo, evitando el consumo innecesario de ancho de banda, permitiendo la utilización de este para los fines requeridos por los usuarios de red.

2.8.121. Capacidad de crear, exportar y almacenar versiones de configuración de los dispositivos administrados, antes de aplicar cambios a un dispositivo. De esta forma, se disminuye la posibilidad de cometer un error no intencional al modificar una política y permite regresar a una configuración en un estado operacional después de haber aplicado una implementación con resultados no esperados.

2.8.122. Capacidad de ejecución de scripts para automatización en el aprovisionamiento de dispositivos, políticas, etc.

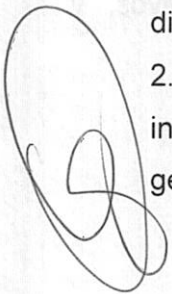
2.8.123. La solución deberá proveer opciones de integración mediante APIs (XML, JSON) para la definición y personalización de entornos anexos.

2.8.124. Posibilidad de administrar el firmware de los dispositivos de seguridad, permitiendo programar y aplicar actualizaciones de sistema operativo de forma desatendida a un equipo o grupo de equipos administrados por la consola, reduciendo tiempos de operación y administración del personal que administra los equipos de seguridad.

2.8.125. La consola de administración permite configuración en Alta Disponibilidad, de tal forma que en caso de falla pueda existir otro equipo en línea que tome las tareas del equipo dañado con una pérdida mínima en la disponibilidad del servicio.

2.8.126. Capacidad de creación y aplicación de configuraciones de VPN entre los dispositivos de seguridad administrados en esquema de comunidades

2.8.127. Cuando se requiera, deberá poder gestionar de forma independiente o integrada puntos de accesos inalámbricos asociados a los firewalls de nueva generación.





Monitoreo y Reportería

2.8.128. Deberá incluir un subsistema de Monitoreo en Tiempo-Real. Esto permite al equipo de monitoreo y administración obtener el estado actual de la infraestructura de dispositivos administrados, y permitir actuar proactivamente a un evento de seguridad y operación de los dispositivos de seguridad administrados.

2.8.129. Deberá incluir un sistema de reportaría integrado con al menos los siguientes reportes predeterminados:

- Logins y eventos de administración
- Anchos de Banda y aplicaciones
- Reputación de clientes
- Reportes por usuario
- VPN
- Redes inalámbricas
- IPS
- Amenazas

2.8.130. Deberá incluir un completo sistema de reportes personalizables pudiendo realizar consultas complejas a la base de datos de registro de logs.

2.8.131. Subsistema de monitoreo especial para los túneles de VPN de tal forma que el área de operación puede monitorear desde una sola pantalla el estado de todos los túneles de VPN establecidos, administrados y operados desde la consola de administración.

2.8.132. Deberá soportar automatización y calendarización en la ejecución de reportes.

2.8.133. Deberá contar con un panel de monitoreo en tiempo real para las siguientes opciones:

- Orígenes
- Aplicaciones
- Destinos
- Sitios Web
- Amenazas

- Eventos de sistema
- VPN (SSL / IPSEC)

Renglón N.º 9.- RED TRONCAL DE FIBRA ÓPTICA

Cables de Fibra Óptica. Cantidad: 50 (Cincuenta)

En cada uno de los edificios en los que se renueva el equipamiento de networking, se implementará a nuevo el cableado de backbone o cableado principal.

Estos cableados permitirán la interconexión del equipamiento nuevo que se provee.

Se debe incluir la provisión de materiales, y mano de obra especializada,

Diseñado en topología estrella, permitirá el vínculo de comunicaciones entre el MDF o sala de equipos principal de cada sede y cada uno de los IDFs o centros de cableado intermedios que se generan o existen en los distintos edificios.

Los cableados de backbone serán utilizados como soporte físico para implementar una red de datos multiservicios con capacidad de implementar 10 Gigabit Ethernet en vínculos de 300 m, en conjunto con el equipamiento de networking.

Listado de vínculos por edificios

El listado de vínculos a ejecutar se muestra a continuación



María Rosa Mulinos
Defensora del Pueblo
de la Ciudad Autónoma
de Buenos Aires



ID	ORIGEN	DESTINO	CABLE
VZ842 P1 • SW1 • SW2	MDF VZ842	• P1 SW1 • P1 SW2	FO MM OM4 12 H
VZ842 P2 • SW1 • SW2	MDF VZ842	• P2 SW1 • P2 SW2	FO MM OM4 12 H
VZ842 P3 SW1	MDF VZ842	P3 SW1	FO MM OM4 12 H
VZ842 P4 SW1	MDF VZ842	P4 SW1	FO MM OM4 12 H
VZ842 P5 SW1	MDF VZ842	P5 SW1	FO MM OM4 12 H
VZ842 P2 SWDC1	MDF VZ842	P2 SWDC1	FO MM OM4 12 H
VZ842 P2 SWDC2	MDF VZ842	P2 SWDC2	FO MM OM4 12 H
BOL501 P1 • SW1 • SW2 • SW3	MDF BOL501	• P1 SW1 • P1 SW1 • P1 SW3	FO MM OM4 12 H
BOL501 P2 • SW1 • SW2 • SW3 • SW4	MDF BOL501	• P2 SW1 • P2 SW2 • P2 SW3 • P2 SW4	FO MM OM4 12 H
BOL501 EP • SW1 • SW2	MDF BOL501	• EP SW1 • EP SW2	FO MM OM4 12 H
BOL501 PB • SW1 • SW2 • SW3	MDF BOL501	• PB SW1 • PB SW2 • PB SW3	FO MM OM4 12 H
BOL501 SS • SW1 • SW2 • SW3	MDF BOL501	• SS SW1 • SS SW2 • SS SW3	FO MM OM4 12 H
BEL588 P2 SW1	MDF BEL588	P2 SW1	FO MM OM4 06 H

ID	ORIGEN	DESTINO	CABLE
BEL570 PB SW1	MDF BEL570	PB SW1	FO MM OM4 06 H
BEL570 P2 SW1	MDF BEL570	P2 SW1	FO MM OM4 06 H
CHI700 P2 SW1	MDF CHI700	P2 SW1	FO MM OM4 06 H
BEL673 PB • SW1 • SW2	MDF BEL673	• PB SW1 • PB SW1	FO MM OM4 06 H
BEL673 EP • SW1 • SW2	MDF BEL673	• EP SW1 • EP SW2	FO MM OM4 06 H
BEL673 P1 • SW1 • SW2	MDF BEL673	• P1 SW1 • P1 SW2	FO MM OM4 06 H
PCOL PB SW1	MDF PCOL	PB SW1	FO MM OM4 06 H
PCOL P1 SW1	MDF PCOL	P1 SW1	FO MM OM4 06 H
PCOL P2 SW1	MDF PCOL	P2 SW1	FO MM OM4 06 H
PCOL P3 SW1	MDF PCOL	P3 SW1	FO MM OM4 06 H
PCOL P4 SW1	MDF PCOL	P4 SW1	FO MM OM4 06 H
PCOL P5 SW1	MDF PCOL	P5 SW1	FO MM OM4 06 H
PCOL P6 SW1	MDF PCOL	P6 SW1	FO MM OM4 06 H

Cableado

Parea la ejecución de la totalidad de los vínculos se utilizarán los siguientes materiales, todos del mismo fabricante y diseñados para el fin que se solicitan y certificados para el cumplimiento de las normas exigidas en el presente.

Cable de fibra óptica

2.9.1. Sera cable de fibra para interiores y exteriores, fabricado para distribución vertical, de baja emisión de humo y cero halógenos, unidad única de 6 o 12 fibras, sin

gel, multimodo OM4.

2.9.2. Poseerá marcado de cubierta en metros o pies, color de cubierta negro, clasificación de llama DCA

2.9.3. Especificaciones mecánicas

2.9.4. Radio de curvatura mínimo con carga: 83 mm.

2.9.5. Radio de curvatura mínimo sin carga: 55 mm

2.9.6. Carga de tracción máxima a largo plazo: 400 N

2.9.7. Carga de tracción máxima a corto plazo: 1335 N

2.9.8. Compresión: 10 N/mm. Método de ensayo de compresión: FOTP-41 | IEC 60794-1 E3

2.9.9. Flexión: 100 ciclos. Método de ensayo de flexión: FOTP-104 | IEC 60794-1 E6

2.9.10. Impacto: 2,94 N-m. Método de ensayo de impacto: FOTP-25 | IEC 60794-1 E4

2.9.11. Giro de 10 ciclos. Método de ensayo de giro FOTP-85 | IEC 60794-1 E7

2.9.12. Elevación vertical máxima de 500 m

Cajas de distribución de fibras ópticas

2.9.13. Los cables de fibra óptica se terminarán, en ambos extremos, en cajas de distribución de fibras ópticas, u ODF por sus siglas en ingles.

2.9.14. Estos ODFs de 19" serán específicamente diseñadas y fabricadas para este fin y provistas con todos los accesorios necesarios.

Bandeja de empalme

2.9.15. Permitirán alojar, acomodar y proteger los empalmes que se ejecutan para unir el cable de fibra óptica y las extensiones conectorizadas o pigtails necesarios

2.9.16. Será una bandeja con capacidad mínima de 24 empalmes.

2.9.17. Extensiones preconectorizadas o pigtails

2.9.18. Para terminar los vínculos de fibra óptica en ambos extremos se proveerán las extensiones ópticas preconectorizadas, ejecutadas y probadas en fábrica.

2.9.19. Serán construidas con cable MM OM4 conectores LC/UPC en un extremo.

2.9.20. Adicionalmente se proveerán para la instalación del extremo conectorizado en la caja, los acopladores y los paneles LX necesarios para conformar las salidas de la

caja de fibra.

2.9.21. Para la interconexión a los equipos de red se proveerán, por cada vínculo, un juego de dos patchcords de fibra, preconectorizados de a pares también de fibra óptica MM OM4 y conectores LC/UPC

2.9.22. Todos los tendidos respetarán rigurosamente el radio mínimo de curvatura especificado por el fabricante de la fibra, debiendo cumplir como mínimo con lo establecido por la norma EIA/TIA 568B.3, esto es radio de curvatura mínimo de 25 mm para tendidos no tensionados y de 50 mm para tendidos bajo tensiones de hasta 220 N.

2.9.23. Los recorridos, serán indicados durante la visita obra

2.9.24. Se utilizarán las canalizaciones implementadas para corrientes débiles en el interior de los edificios.

2.9.25. Todos los cables serán rotulados en cada caja de pase del sistema de canalización y a la llegada a la caja de cada extremo.

Renglón N.º 10.- PACHERAS INTELIGENTES

Cables de Fibra Óptica. Cantidad: 35 (Treinta y Cinco)

Provisión e Instalación de paneles de cableado inteligentes

2.10.1. En la totalidad de los centros de cableado que se intervienen para el cableado del backbone de fibra óptica se proveerán nuevos paneles de interconexión o patch panels que sustituyen a los existentes.

2.10.2. Estos paneles permitirán implementar a futuro la gestión automatizada de la infraestructura (AIM) que combina hardware inteligente con software para proporcionar visibilidad y control en tiempo real sobre la capa física de una red.

2.10.3. Estarán equipados con sensores que detectan y registran automáticamente cada conexión, desconexión y movimiento de los cables de conexión, proporcionando una visibilidad en tiempo real de la conectividad física.

Para la implementación del sistema se deberá agregar a futuro además de los paneles los siguientes componentes no incluidos



2.10.4. Controladores imVision: Los controladores se conectarán a los paneles iPatch y recopilan los datos de conectividad. Deberán tener una interfaz de pantalla táctil para simplificar el acceso a las funciones del sistema y guiar a los técnicos en las tareas de conexión.

2.10.5. Software de gestión del sistema (imVision System Manager): El software basado en la web deberá procesar la información de los controladores y proporcionar un mapa completo y visual de la red. Permitirá a esta DPCABA:

- Documentar automáticamente la infraestructura de cableado.
- Generar órdenes de trabajo electrónicas y guiar a los técnicos paso a paso para realizar cambios.
- Identificar dispositivos y su ubicación física en la red.
- Monitorizar y rastrear todos los cambios en las conexiones físicas en tiempo real.

Renglón N.º 11.- SERVICIOS DE INSTALACIÓN Y PUESTA EN MARCHA

El proveedor será responsable de la Instalación y Puesta en marcha de todo el equipamiento teniendo en cuenta la configuración a la nueva plataforma.

2.11.1. Montaje físico de los equipos

2.11.2. Configuración y puesta en marcha del sistema

2.11.3. Migración de configuración actual al nuevo equipamiento respetando las políticas actuales y de la Red LAN y WAN.

2.11.4. Documentación técnica del trabajo realizado

Renglón N.º 12.- SERVICIOS DE CAPACITACIÓN Y TRANSFERENCIA DE CONOCIMIENTO

2.12.1. Se deberá proveer una capacitación de al menos 20 horas provista de manera presencial en las oficinas del organismo en horario de lunes a viernes de 9 a 17hs.

2.12.2. La capacitación debe ser oficial del proveedor de los equipos con participación de los técnicos responsables de la instalación y puesta en marcha si fuera necesario.

2.12.3. Los asistentes deberán recibir documentación en modalidad impresa o digital.

2.12.4. Una vez finalizado el curso, el adjudicatario entregará al cursante un certificado de asistencia que así lo acredite.

2.12.5. La capacitación debe contemplar un mínimo de CINCO (5) personas

2.12.6. El contenido del curso deberá estar orientado a capacitar a trabajadores del organismo en la operación de los equipos que componen el sistema de respaldo de energía, potencias disponibles, sincronismo, conmutación automática y resolución de problemas comunes en casos de emergencia.

8. IDENTIFICACIÓN

Todos los vínculos serán identificados con indicación de número único de vínculo, origen y destino.

Una vez finalizadas las tareas, el sistema de identificación se documentará junto con el resto de la información.

9. DOCUMENTACIÓN

Una vez finalizados los trabajos, se procederá a la entrega de los siguientes documentos:

- Plano de planta y esquema de cableado vertical con indicación de canalizaciones, cables y centros de cableado (IDFs y MDFs)
- Planilla de vínculos ejecutados
- Informe de certificación de los tendidos de fibra óptica (FO)

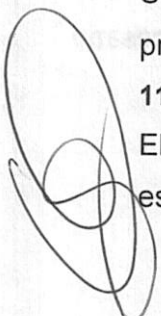
10. CONOCIMIENTO DE LOS LUGARES

Cada OFERENTE deberá realizar, previo a la presentación de su oferta, una visita a las dependencias de esta DPCABA, tomando debida nota las condiciones físicas y espaciales en las que debe implementar la solución.

Se deberá solicitar la correspondiente constancia de visita, la cual deberá ser presentada junto con la propuesta.

11. CALIDAD DE LOS TRABAJOS

El sistema por implementar cumplirá con las últimas versiones de las siguientes especificaciones:





- EIA/TIA 568: Cableado de telecomunicaciones en edificios comerciales.
- EIA/TIA 569: Trayectorias y espacios para telecomunicaciones en edificios comerciales.
- EIA/TIA 606: Estándar para la administración de infraestructura de telecomunicaciones en edificios comerciales.
- EIA/TIA 607: Requerimientos de puesta a tierra para telecomunicaciones.

Adicionalmente, se tendrán en cuenta las mejores prácticas y recomendaciones de los fabricantes.

Todos los componentes del cableado serán de una misma marca y fabricante a saber:

- Patch cords de fibra óptica
- Distribuidores de fibra óptica
- Fibra óptica
- Todo componente de cableado de fibra para backbone (conectores de FO, cajas de empalme de fibra y acopladores).

12. OFERENTES

Los OFERENTES deberán acreditar, mediante documento escrito, el cumplir con todos y cada uno de los antecedentes y otros requerimientos exigidos, los cuales deberán ser presentados junto con la propuesta técnica.

También, junto a la propuesta, el OFERENTE debe incluir una descripción técnica de la solución

Antecedentes

El oferente deberá acreditar el haber llevado a cabo al menos 5 (cinco) proyectos en los últimos 2 (dos) años de similar envergadura con provisión, instalación y puesta en marcha de equipos de networking de características similares a los solicitados e instalaciones de similar envergadura y complejidad

Los antecedentes presentados deberán haber sido llevados a cabo directamente entre el OFERENTE y el cliente final.

Los antecedentes mencionados serán parte integrante de la documentación a presentar al momento de la oferta.

Certificación

El oferente deberá ser Partner/socio de negocios de las marcas ofrecidas, debiendo presentar datos de sus correspondientes membresías, de forma tal que esto pueda ser corroborada directamente con el fabricante correspondiente.

13. CONDICIONES GENERALES DE LA CONTRATACIÓN

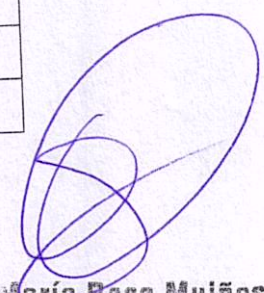
- La empresa oferente deberá presentar ante esta DPCABA carta de los fabricantes utilizados en la presente oferta donde exprese que está autorizado a comercializar, instalar y activar a las garantías de los productos ofrecidos.
- El oferente deberá poseer la certificación de partnership más alto con cada uno de los fabricantes de los productos ofrecidos con el objetivo de garantizar el correcto funcionamiento de la solución.
- El oferente deberá demostrar como mínimo cinco implementaciones comprobables de similares características.
- Los técnicos responsables de la configuración y puesta en marcha de las soluciones deberán estar certificados en las tecnologías utilizadas, para esto deberán presentar los CVs junto con los certificados vigentes correspondientes.
- El proveedor deberá proveer el CV de un Project Manager que sea responsable del proyecto.
- Se deberá realizar visita de obra para poder comprender todas las necesidades del proyecto.





**14. PRECIOS UNITARIOS DE REFERENCIA ESTIMADOS POR EL ÁREA TÉCNICA
REQUIRENTE**

REGLÓN N°	PRECIO UNITARIO ESTIMADO
1	\$ 34.647.738,42
2	\$ 14.910.884,79
3	\$ 29.069.624,56
4	\$ 4.111.068,21
5	\$ 5.218.741,08
6	\$ 2.544.225,90
7	\$ 198.588,30
8	\$ 12.200.402,12
9	\$ 853.776,00
10	\$ 1.138.368,00
11	\$ 36.048.320,00
12	\$ 2.168.320,00



María Rosa Muñoz
Defensora del Pueblo
de la Ciudad Autónoma
de Buenos Aires

