Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

GOBIERNO DEL ESTADO DE JALISCO

Poder Ejecutivo
Secretaría de Administración

DIRECCIÓN DEL COMITÉ DE ADQUISICIONES Y ENAJENACIONES

“BASES”

Licitación Pública Local
LPL297/2022 Con Concurrencia del Comité

“ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ”

De conformidad con lo previsto por el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, el artículo 19, apartado 1,fracción XI de la Ley Orgánica del Poder Ejecutivo del Estado de Jalisco, así como lo señalado por el artículo 1, 2 fracción IX, 3 fracción XXXI, XXXVI y LIX, 9, fracción II, 20, fracción I y 21 del Reglamento interno de la Secretaría de Administración, artículos 1, 2, 3, 4, 5, 23, 24, 31, 34, 35, 47, 55, apartado 1, fracción II,, 59, 63, 69, 72, y demás relativos de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios, y los artículos 1, 3, 4 y demás aplicables de su Reglamento; la Secretaría de Administración del Poder Ejecutivo del Estado, en coordinación con su Dirección General de Abastecimientos, constituidas en Unidad Centralizada de Compras, ubicadas en Prolongación Avenida Alcalde número 1221, Colonia Miraflores, Zona Centro, C.P. 44270, en la ciudad de Guadalajara, Jalisco; CONVOCA a las personas físicas y/o jurídicas interesadas en participar en el procedimiento de contratación mediante **Licitación Pública Local LPL297/2022 con Concurrencia del Comité para la "ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"**, en lo subsecuente "Procedimiento de Adquisición", derivado de las solicitud 35-107-2022; las cuales se llevará a cabo con Recursos FF, 15 recursos federales;SFF, Fondos de participaciones no condicionadas; capitulo 5000, partida 5971, 5911 (según corresponda) del Ejercicio 2022. Los pagos que se tengan que efectuar con cargo a estos ejercicios presupuestales futuros, estarán sujetos a la aprobación del presupuesto correspondiente y de conformidad a lo establecido en las siguientes:

B A S E S

Para los fines de estas **"BASES"**, se entenderá por:

"APORTACIÓN CINCO AL MILLAR"	Retención del monto total de los contratos de bienes y servicios antes de I.V.A., que será aportado al Fondo Impulso Jalisco, equivalente al 0.5 punto cinco por ciento del valor asignado, previa declaración de voluntad suscrita por el aportante.
"BASES"	Requisitos y condiciones de participación en que se desarrollará el procedimiento de adquisiciones o enajenación
"COMITÉ"	Comité de Adquisiciones de la Administración Pública Centralizada del Poder Ejecutivo del Estado de Jalisco
"CONTRATACIONES ABIERTAS"	La divulgación y uso de información abierta, accesible y oportuna sobre contrataciones del gobierno, para lograr que los ciudadanos y las empresas puedan participar.
"CONTRATO"	Instrumento Jurídico mediante el cual las partes se comprometen recíprocamente a respetar y cumplir la voluntad expresa de las mismas.
"CONVOCANTE"	El ente público que, a través del área requirente y la unidad centralizada de compras, tramita los procedimientos de adquisición y enajenación de bienes en los términos de la **"LEY"**.
"CONVOCATORIA"	Es el llamado a los interesados a participar en determinado procedimiento de adquisiciones o enajenación.
"DEPENDENCIA REQUIRENTE"	**SECRETARIA DE ADMINISTRACION**
"DIRECCIÓN GENERAL"	Dirección General de Abastecimientos.

“DIRECCIÓN”	Dirección de Comité de Adquisiciones y Enajenaciones de la Secretaría Administración
“DOMICILIO”	Dentro de las instalaciones de la Secretaría de Administración, inmueble ubicado en Prolongación Avenida Alcalde No. 1221, Col. Miraflores, Guadalajara, Jalisco, (ingreso opcional por puerta posterior de Av. Magisterio s/n)
“EMPRESA PRO INTEGRIDAD”	Aquella que adopte políticas de integridad empresarial y esté debidamente registrada, ante las autoridades correspondientes.
“FALLO” o “RESOLUCIÓN”	Documento emitido por el Comité mediante el cual, una vez realizados los análisis correspondientes respecto de las propuestas presentadas, se establece el o los licitantes adjudicados de cada procedimiento
“FONDO”	Fondo Impulso Jalisco FIMJA
“I.V.A.”	Impuesto al Valor Agregado.
“LEY”	Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
“ÓRGANO DE CONTROL”	La Contraloría del Estado.
“ÓRGANO INTERNO DE CONTROL”	Órgano interno de Control de la Secretaría de Administración.
“PARTICIPANTE” o “LICITANTE”	Persona Física o Jurídica que se registra y, participa en cualquiera de las etapas del procedimiento de adquisición, que de manera primordial presenta propuesta o proposición.
“PROCEDIMIENTO DE ADQUISICIÓN”	Licitación Pública Local , LPL297/2022 con Concurrencia del Comité para la **“ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ”**
“PROPUESTA” o “PROPOSICIÓN”	La propuesta técnica y económica que presenten los **“PARTICIPANTES”**
SOBRE	Se refiere al sobre, caja o paquete, en su caso, cerrado de manera que no se pueda modificar su contenido y que contiene la propuesta o proposición del participante en cuyo interior se presenta la propuesta técnica y/o económica.
“PROVEEDOR” o “CONTRATISTA”	**“PARTICIPANTE”** Adjudicado o que cuenta con registro vigente en el RUPC
“REGLAMENTO”	Reglamento de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
“RUPC”	Registro Estatal Único de Proveedores y Contratistas del Estado de Jalisco.
“SECG”	Sistema Electrónico de Compras Gubernamentales. Ubicado en el portal https://encompras.jalisco.gob.mx/SJ3Kweb/secure/
“SECRETARÍA”	Secretaría de Administración.
“UNIDAD CENTRALIZADA DE COMPRAS”	La unidad administrativa responsable de las adquisiciones, enajenaciones o arrendamientos de bienes y la contratación de los servicios de los entes públicos.
“VENTANILLA ÚNICA DE PROVEEDORES”	Ventanilla ubicada dentro del domicilio, en donde los proveedores podrán entregar y recibir documentos, solicitar informes o realizar trámites.

“DESECHAMIENTO”	Al acto mediante el cual el Comité Determina que una propuesta no es susceptible de ser adjudicada en virtud de no cumplir con los requerimientos técnicos o administrativos.
“GRUPO/PAQUETE”	Al formado por dos o más sub-partidas/progresivos en el procedimiento de licitación.
“PARTIDA/SUB-PARTIDA”	Cada uno de los elementos que integran el/los bien(es)/servicio a adquirir.
“ALTERACIÓN DE DOCUMENTO”	Aquel documento que presenta signos o datos de que ha sido variado, modificado o alterado su contenido primigenio.
“REQUISITOS DE PARTICIPACIÓN”	Son aquellos requisitos legales y administrativos que el participante debe de cumplir con la finalidad de que sea analizada su propuesta o proposición.
“REQUISITOS DE ADJUDICACIÓN”	Se refiere a los requisitos técnicos y económicos que el participante debe de cumplir con la finalidad que la convocante determine emitir el fallo a su favor.
“FIRMA AUTÓGRAFA”	Aquella estampada de puño y letra por parte del participante, su apoderado o representante legal.
“COMPRADOR”	Al servidor público encargado de tramitar el procedimiento de licitación adscrito a la Dirección General de Abastecimientos de la Secretaría de Administración.
“DICTAMEN TÉCNICO”	Análisis elaborado por el área requirente mediante el cual, se lleva a cabo la evaluación de los aspectos técnicos y demás características del bien o servicio ofertado por los participantes plasmados en la propuesta técnica.

CALENDARIO DE ACTIVIDADES
(ACTOS)

A C T O	PERÍODO O DÍA	HORA	LUGAR
Publicación de **"CONVOCATORIA"** y **"BASES"**	21 de OCTUBRE del 2022	A partir de las 15:00 horas	Portal de Compras Jalisco y/o el SECG.
Visita de Campo	N/A	N/A	N/A
Entrega de Muestras	N/A	N/A	N/A
Recepción de preguntas	24 de OCTUBRE del 2022	Hasta las 11:00 horas	De manera física en la Dirección del Comité de Adquisiciones, ubicado en el **"DOMICILIO"**
Registro para el Acto de Junta Aclaratoria	26 de OCTUBRE del 2022	De las 10:00 a las 10:29 horas	En el "**DOMICILIO"**.
Acto de Junta Aclaratoria	26 de OCTUBRE del 2022	A partir de las 10:30 horas	En el "**DOMICILIO"**.
Registro para la Presentación de Propuestas.	31 de OCTUBRE del 2022	De las 15:15 a las 15:45 horas	En el Aula 4 del Centro de Capacitación para el Servidor Pública, Ubicado en Av. Prolongación Alcalde #1855, en el Edificio del Archivo Histórico.
Presentación y Apertura de propuestas.	31 de OCTUBRE del 2022	A partir de las 16:00 horas	En el Aula 4 del Centro de Capacitación para el Servidor Pública, Ubicado en Av. Prolongación Alcalde #1855, en el Edificio del Archivo Histórico.
"FALLO" O "RESOLUCIÓN" de la convocatoria.	Dentro de los 20 días naturales siguientes a la fecha de presentación y apertura de propuestas, conforme al artículo 65 fracción III de la LEY.		A través del "**SECG"** o correo electrónico.

1. ESPECIFICACIONES.

El objeto del presente procedimiento es la contratación para la **"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"** conforme a las características señaladas en el **ANEXO 1** (Carta de Requerimientos Técnicos), de las presentes **"BASES"**, dichas especificaciones y características técnicas se consideran mínimas y con la más óptima calidad, por lo que los **"PARTICIPANTES"** podrán proponer bienes y/o servicios con especificaciones y características superiores, si así, lo consideran conveniente. Las propuestas deberán ser entregadas de manera **presencial** de acuerdo al calendario de actividades en el domicilio citado en la convocatoria.

2. PLAZO, LUGAR Y CONDICIONES DE ENTREGA.

La entrega de los servicios/bienes, objeto de este **"PROCEDIMIENTO DE ADQUISICIÓN"** deberá ser de acuerdo a lo establecido en el Anexo 1 de las presentes **"BASES"**, y de conformidad con las características y especificaciones que se establecerán en el **"CONTRATO"**. Las obligaciones correrán a partir de la notificación de la **"RESOLUCIÓN"** y bajo la estricta responsabilidad del **"PROVEEDOR"**, quien se asegurará de su adecuada transportación o prestación del servicio, hasta su correcta recepción a entera satisfacción de la "**DEPENDENCIA REQUIRENTE"**.

Se considerará que el **"PROVEEDOR"** ha entregado los servicios o bienes, objeto de este **"PROCEDIMIENTO DE ADQUISICIÓN"**, una vez que en la factura y/o en la Orden de Compra correspondiente, se plasme el sello y firma del personal técnico responsable de la "**DEPENDENCIA REQUIRENTE"** y se recabe el oficio de recepción de los bienes/servicios a entera satisfacción por parte del personal técnico responsable.

3. PAGO.

El pago se efectuará una vez que sea realizada la entrega parcial y/o total de los bienes/servicios conforme a lo establecido en el numeral 2 de las presentes **"BASES"**, y dentro de los 30 días naturales posteriores a la recepción de la documentación correspondiente, en la **"DEPENDENCIA REQUIRENTE",** de conformidad con los lineamientos de la Secretaría de la Hacienda Pública y/o **"DEPENDENCIA REQUIRENTE" (según corresponda).**

Documentos para pago de anticipo (cuando aplique)

- **a.** Original y copia del comprobante fiscal respectivo expedido a favor de la Secretaría de la Hacienda Pública, cuyo domicilio es en la calle Pedro Moreno No. 281, Guadalajara Centro, Guadalajara, Jalisco, C.P. 44100, y su R.F.C. es SPC130227L99, validado por la **"DEPENDENCIA REQUIRENTE"** y/o **"SECRETARÍA"**.
- **b.** Impresión de la verificación del CFDI de la página del Sistema de Administración Tributaria.
- **c.** Copia del Acta de "**RESOLUCIÓN"** o "**FALLO"**.
- **d.** Original del **"CONTRATO"**.
- **e.** Original de la póliza de fianza de anticipo a la que se hace referencia el numeral 20 de las presentes **"BASES",** expedida por una institución mexicana legalmente autorizada a nombre de la Secretaría de la Hacienda Pública, con domicilio en la calle Pedro Moreno No. 281, Colonia Centro, en el municipio de Guadalajara, Jalisco, C.P. 44100, R.F.C. SPC130227L99.
- **f.** Copia de la Declaración de aportación del 5 al millar para el Fondo Impulso Jalisco (Anexo 7 de las **"BASES"**) en la cual el "PROVEEDOR" declara su voluntad de si o no realizar la retención del 5 al millar del monto total del contrato antes del I.V.A., para su entero al Fondo Impulso Jalisco.

Documentos para pago parcial o final (cuando aplique)

a. Original del CFDI y XML, a nombre de la Secretaría de la Hacienda Pública, con domicilio en la calle Pedro Moreno No. 281, Colonia Centro, en el municipio de Guadalajara, Jalisco, C.P. 44100, R.F.C. SPC130227L99, validada por la **Dependencia y/o Entidad** requirente;

b. Impresión de la verificación del CFDI de la página del Sistema de Administración Tributaria.

c. Copia del Acta de "**RESOLUCIÓN"** o "**FALLO (solo se requiere para el primer trámite de pago)"**.

d. 1 copia del **"CONTRATO (solo se requiere para el primer trámite de pago)"**

e. "Orden de Reparación y Mantenimiento y Carta de Entera Satisfacción" en original;

f. 1 copia de la garantía de cumplimiento de **"CONTRATO"** a nombre de la Secretaría de la Hacienda Pública, con domicilio en la calle Pedro Moreno No. 281, Colonia Centro, en el municipio de Guadalajara, Jalisco, C.P. 44100, R.F.C. SPC130227L99, en caso de corresponder a la que hará referencia el contrato que en su momento suscriba(n) el o los proveedores participantes adjudicados (solo se requiere para el primer trámite de pago).

g. Copia de la Declaración de aportación del 5 al millar para el Fondo Impulso Jalisco (Anexo 7 de las **"BASES"**) en la cual el **"PROVEEDOR"** declara su voluntad de si o no realizar la retención del 5 al millar del monto total del contrato antes del IVA, para su entero al Fondo Impulso Jalisco. (solo se requiere para el primer trámite de pago).

De ser el caso, de acuerdo con los artículos 76 y 77 de la Ley del Presupuesto, Contabilidad y Gasto Público del Estado de Jalisco, los pagos que se tengan que efectuar con cargo a ejercicios presupuestales futuros, estarán sujetos a la aprobación del presupuesto correspondiente.

En caso de que las facturas entregadas para su pago presenten errores o deficiencias, la "**DEPENDENCIA REQUIRENTE"** y/o "**SECRETARÍA"**, dentro de los tres días hábiles siguientes al de su recepción, indicará al **"PROVEEDOR"** las deficiencias que deberá corregir. El periodo que transcurra a partir de la indicación de las deficiencias y hasta que el **"PROVEEDOR"** presente las correcciones no se computará para efectos del plazo del pago estipulado.

El pago de los bienes / servicios quedará condicionado proporcionalmente al pago que el **"PROVEEDOR"** deba efectuar, en su caso, por concepto de penas convencionales. Lo anterior, sin perjuicio de que la Secretaría de la Hacienda Pública y/o **"DEPENDENCIA REQUIRENTE**, pueda proceder al cobro de las penas convencionales previo al pago correspondiente conforme a lo estipulado en el **"CONTRATO"**.

Es requisito indispensable para el pago, que el **"PROVEEDOR"** realice la entrega de la garantía de cumplimiento del **"CONTRATO"** de los bienes / servicios adjudicados en el supuesto de proceder.

3.1. Vigencia de precios.

La proposición presentada por los "**LICITANTES"**, será bajo la condición de **precios fijos** hasta la total prestación de los servicios. Al presentar su propuesta en la presente Licitación, los **"PARTICIPANTES"** dan por aceptada esta condición.

Si con posterioridad a la adjudicación del presente proceso se presentan circunstancias económicas de tipo general ajenas a la responsabilidad de las partes, que provoquen directamente un aumento o reducción en los precios, se procederá de acuerdo con lo establecido en el artículo 75 de la Ley.

(para casos específicos y justificados que no sean por circunstancias económica de tipo general en este apartado debe señalarse la fórmula para los incrementos o decrementos).

3.2. Impuestos y derechos

La **"SECRETARÍA"** de Administración, aceptará cubrir los impuestos que le correspondan, siempre y cuando se presenten desglosados en las **"PROPUESTAS"** y en las facturas.

4. OBLIGACIONES DE LOS "PARTICIPANTES".

a. Contar con la capacidad administrativa, fiscal, financiera, legal, técnica y profesional para atender el requerimiento en las condiciones solicitadas.

b. Presentar al momento del Registro para el Acto de Presentación y Apertura de Propuestas, el **Manifiesto de Personalidad** anexo a estas **"BASES"**, con firma autógrafa, así como la **copia de la Identificación Oficial Vigente** de la persona que vaya a realizar la entrega del sobre cerrado. El incumplimiento será causal para no recepcionar el sobre de la propuesta.

c. Presentar todos los documentos y anexos solicitados en el numeral 9 de las presentes **"BASES"**, ya que son parte integral de la propuesta, para todos los efectos legales a que haya lugar, a excepción de los documentos opcionales.

d. En caso de resultar adjudicado, si el "**PARTICIPANTE"** se encontrara **dado de baja o no registrado** en el **"RUPC",** como lo establece el Capítulo III, de la **"LEY"**, deberá realizar su alta antes de la firma del respectivo contrato dentro de los plazos y términos previstos en el "REGLAMENTO",, este requisito es factor indispensable para la elaboración de la orden de compra y celebración del **"CONTRATO"**. La Dirección de Padrón de Proveedores determinará si su giro está incluido en el ramo de bienes o servicios que participa. En caso de no cumplir con lo anterior, no podrá celebrarse **"CONTRATO"** alguno, por lo que, no se celebrará **"CONTRATO"** con dicho participante y de resultar conveniente, se celebrará con el segundo lugar o se iniciará un nuevo **"PROCEDIMIENTO DE ADQUISICIÓN"**.

Para efectos de inscripción o actualización del registro, los interesados deberán cumplir con los requisitos señalados en el artículo 20 de la **"LEY"**, así como los referidos en los artículos 20, 21 y 22 de su "**REGLAMENTO"**; para ello deberán de acudir a la Dirección de Padrón de Proveedores, en el "**DOMICILIO"**.

e. En caso de resultar adjudicado, deberá de suscribir el **"CONTRATO"** en los formatos, términos y condiciones que la Dirección General Jurídica de la **"SECRETARÍA"** establezca, mismo que atenderá en todo momento a las presentes **"BASES"**, el Anexo 1, junta aclaratoria y la propuesta del adjudicado.

f. Conservar y mantener en forma confidencial toda información que llegara a su conocimiento necesaria para la elaboración y presentación de sus propuestas, con motivo de esta licitación, sea cual fuere su naturaleza o destino, obligándose por tanto, a abstenerse de comunicarla, divulgarla o utilizarla para sí o en beneficio de terceros, fuese o no con propósito de lucro, o cualquier otra información que se proporcione en forma verbal o por escrito, excepto por requerimiento de Autoridad del orden Judicial o Administrativo competente.

La contravención a lo dispuesto, generará la obligación a cargo del participante que la incumpla, de indemnizar a la dependencia requirente y/o de la "SECRETARÍA", por los daños y perjuicios causados con motivo del incumplimiento.

5. JUNTA ACLARATORIA.

Los "**LICITANTES"** que estén interesados en participar en el procedimiento deberán de presentar sus dudas o solicitudes de aclaración en la "**DIRECCIÓN"**, en el "**DOMICILIO"**, de manera física y firmada por el representante legal del "**PARTICIPANTE"**, **de conformidad al anexo de Solicitud de Aclaraciones** y de manera digital **en formato Word**; de conformidad con los artículos 62 apartado 4, 63 y 70 de la **"LEY"**, 63,

64 y 65 de su "**REGLAMENTO"**. La recepción de preguntas se llevará a cabo el día, hora y domicilio conforme al calendario previsto en la convocatoria.

Las solicitudes de aclaración deberán plantearse de manera clara y concisa, además de estar directamente vinculadas con los puntos contenidos en la convocatoria, sus **"BASES"** y su **ANEXO 1** (Carta de Requerimientos Técnicos), indicando el numeral o punto específico con el cual se relaciona. Las solicitudes que no cumplan con los requisitos señalados, podrán ser desechadas por la **"CONVOCANTE"**.

Serán atendidas únicamente las solicitudes de aclaración que se hayan recibido en el tiempo y forma establecidos, sin embargo, en el acto de junta de aclaraciones, los asistentes podrán formular cuestionamientos que no hayan sido plasmados en el documento entregado de forma previa, sin embargo, la **"CONVOCANTE"** no tendrá obligación de dar respuesta a éstos en el acta correspondiente, a no ser que, a su juicio, las respuestas otorgadas sean de trascendencia para la convocatoria y sus anexos.

El registro para asistir al acto de junta aclaratoria **se llevará a cabo el día, hora y domicilio conforme al calendario previsto en la** convocatoria.

El acto de Junta de Aclaraciones se llevará a**cabo el día, hora y domicilio conforme al calendario previsto en la** convocatoria, donde se dará respuesta a las preguntas recibidas.

Las aclaraciones o la ausencia de ellas y los acuerdos tomados en el acto serán plasmadas en el **Acta de la Junta de Aclaraciones**, la cual formará parte integral de la presente convocatoria para los efectos legales a los que haya lugar.

El acta de la junta de aclaraciones será publicada en el "SECG" y/o en los tableros o estrados destinados para tal efecto por la dirección.

La asistencia de los licitantes o sus representantes legales a la junta aclaratoria y/o visita en sitio, será bajo su estricta responsabilidad con carácter de **obligatoria**, de conformidad con el articulo 62 numeral 4 de la **"LEY".** El hecho de que el licitante no se presente a la junta de aclaraciones y/o visita en sitio, será motivo de suficiente para que no se tome en consideración su propuesta, con fundamento en el artículo 65 del **"REGLAMENTO"**.

6. VISITA DE CAMPO.

No aplica.

7. CARACTERÍSTICAS DE LA PROPUESTA.

De conformidad con los artículos 64 y 65 de la "**LEY"**, el "**PARTICIPANTE"** deberá presentar su propuesta técnica y económica mecanografiada o impresa, debidamente firmada, dirigida a la "**DIRECCIÓN GENERAL**" en la que debe constar el desglose de cada uno de los bienes/servicios que está ofertando y que la **"CONVOCANTE"** solicita adquirir.

a. Todas y cada una de las hojas de la propuesta elaborada por el "**PARTICIPANTE"**, deberán presentarse firmadas de forma autógrafa por el titular, representante legal o apoderado legal, en su caso.

b. Todos los documentos que integren la propuesta deberán presentarse, dentro de un sobre cerrado el cual deberá contener en su portada la fecha, nombre del participante (Razón Social) y número del **"PROCEDIMIENTO DE ADQUISICIÓN". La no observancia de este inciso podrá ser motivo suficiente para desechar la propuesta.**

c. Los documentos no deberán estar alterados, tachados y/o enmendados.

d. No se aceptarán opciones, el "**PARTICIPANTE"** deberá presentar **una sola propuesta**.

e. La propuesta deberá presentarse en los términos de los formatos establecidos en los anexos 2 (Propuesta Técnica) y 3 (Propuesta Económica).

f. El **"PARTICIPANTE"** deberá presentar de manera obligatoria, en los términos del formato establecido como Anexo 7 (Declaración de aportación cinco al millar para el Fondo Impulso Jalisco), su aceptación o no aceptación para la aportación cinco al millar del monto total adjudicado antes de I.V.A. para el Fondo.

g. La propuesta deberá estar dirigida a la "**DIRECCIÓN GENERAL"** y realizarse con estricto apego a las necesidades planteadas por la **"CONVOCANTE"** en las presentes **"BASES"**, de acuerdo al servicio y especificaciones requeridas en el Anexo 1(Carta de Requerimientos Técnicos).

h. La oferta se presentará en moneda nacional con los precios unitarios, I.V.A. y demás impuestos que en su caso correspondan desglosados. La propuesta económica deberá considerar para los cálculos aritméticos **únicamente dos decimales.**

i. La propuesta deberá incluir todos los costos involucrados, por lo que **no se aceptará ningún costo extra o precios condicionados**.

j. El participante en su propuesta podrá ofertar características superiores a los solicitados, lo cual deberá sustentarse documentalmente y deberá ser corroborado por el área requirente en su dictamen técnico.

k. Toda la documentación elaborada por el "**PARTICIPANTE"**, deberá redactarse en español. Únicamente podrán presentarse certificaciones, folletos, catálogos y/o cualquier tipo de documento informativo en el idioma original, adjuntando traducción simple al español.

La falta de alguna de estas características será causal desechamiento de la "PROPUESTA" del "PROVEEDOR".

7.1. Características adicionales de las propuestas.

a. Para facilitar en el acto de apertura la revisión de los documentos requeridos, se sugiere que éstos sean integrados en una carpeta conteniendo:

- Índice que haga referencia al número de hojas y orden de los documentos.
- Hojas simples de color que separen cada sección de la propuesta en la que se mencione de qué sección se trata.
- Los documentos originales que se exhiban con carácter devolutivo y por lo tanto no deban perforarse, presentarse dentro de micas. El no presentarlos dentro de la mica, exime de responsabilidad a la Unidad Centralizada de Compras de ser firmados y/o foliados.
- Sin grapas ni broches Baco.

La falta de alguna de las características adicionales de la propuesta, no será causal de desechamiento de la "PROPUESTA" del "PARTICIPANTE".

7.2. Estratificación

En los términos de lo previsto por el apartado 1 del Artículo 68 de la "**LEY",** con el objeto de fomentar la participación de las micro, pequeñas y medianas empresas en los procedimientos de adquisición y arrendamiento de bienes muebles, así como la contratación de servicios que realicen las dependencias y entidades de la Administración Pública Estatal, se deberá considerar el rango del **"PARTICIPANTE"** atendiendo a lo siguiente:

Criterios de Estratificación de las Micro, Pequeñas y Medianas Empresas o Personas físicas				
Tamaño	**Sector**	Rango de Número de Trabajadores (Empleados Registrados ante el IMSS y Personas Subcontratadas)	Rango de Monto de Ventas Anuales (mdp)	Tope Máximo Combinado*
Micro	**Todas**	Desde 01 Hasta 10	Hasta $4	4.6
Pequeña	**Comercio**	Desde 11 Hasta 30	Desde $4.01 Hasta $100	93
	Industria y Servicios	Desde 11 Hasta 50		95
Mediana	**Comercio**	Desde 31 Hasta 100	Desde 100.01 Hasta $250	235
	Servicios	Desde 51 Hasta 100		
	Industria	Desde 51 Hasta 250		250
***Tope Máximo Combinado = (Trabajadores) X 10% + (Ventas Anuales) X 90%**				

8. MUESTRAS FÍSICAS. – NO APLICA

9. PRESENTACIÓN DE PROPUESTAS.

9.1. Presentación y apertura de propuestas técnicas y económicas.

Con concurrencia del "COMITÉ". Este acto se llevará a cabo el día, hora conforme al calendario previsto en la convocatoria**,** en el **Aula 4 del Centro de Capacitación para el Servidor Pública, Ubicado en Av. Prolongación Alcalde #1855, en el Edificio del Archivo Histórico.**

Los **"PARTICIPANTES"** que concurran al acto, deberán firmar de manera obligatoria, un registro para dejar constancia de su asistencia y poder presentar propuesta, el cual iniciará en punto de las **15:15 horas** y cerrará a las **15:45 horas** del día de la presentación y apertura de propuestas y en el cual **deberán anotar su nombre completo, número de su Identificación Oficial vigente, Razón Social de la empresa y hora de registro.**

Los **"PARTICIPANTES"** que concurran al acto, deberán entregar con firma autógrafa el "**Manifiesto de Personalidad**" anexo a estas **"BASES" junto a una copia de su Identificación Oficial Vigente**. El incumplimiento será causal para no recepcionar el sobre de la propuesta.

Cualquier **"PROVEEDOR"** que no se haya registrado en tiempo y forma, será causal suficiente para que no le sea recepcionada su propuesta.

EL SOBRE DE LA PROPUESTA TÉCNICA y ECONÓMICA deberá contener lo siguiente:

a. **Anexo 2** (Propuesta Técnica) más documentos solicitados en el anexo 1.
b. **Anexo 3** (Propuesta económica).
c. **Anexo 4** (Carta de Proposición).
d. **Anexo 5** (Acreditación) o documentos que lo acredite.
e. **Anexo 6** (Declaración de Integridad y NO COLUSIÓN de proveedores).
f. **Anexo 7** (Declaración de aportación cinco al millar para el fondo impulso Jalisco).
g. **Anexo 8** (**Manifiesto de Opinión Positiva de Cumplimiento de Obligaciones Fiscales y Constancia impresa)**. De acuerdo al numeral 25 de las presentes **"BASES"**.
h. **Anexo 9** (**Manifiesto de Opinión de Cumplimiento de Obligaciones en Materia de Seguridad Social y Constancia) .**
i. **Anexo 10** (Identificación Oficial Vigente).
j. **Anexo 11** Manifestación de estar al corriente en Obligaciones Patronales y Tributarias.
k. **Anexo 12** (Estratificación)

La falta de cualquiera de los anexos anteriores descritos y/o los documentos que deban contener será motivo de desechamiento de la "PROPUESTA" del "PARTICIPANTE".

Dos o más personas podrán presentar conjuntamente una proposición sin necesidad de constituir una sociedad, o una nueva sociedad en caso de personas jurídicas; para tales efectos, en la proposición y en el **"CONTRATO"** se establecerán con precisión las obligaciones de cada una de ellas, así como la manera en que se exigiría su cumplimiento. En este supuesto la proposición deberá ser firmada por el representante común que para ese acto haya sido designado por el grupo de personas; esto último en apego al artículo 64 apartado 3 de la **"LEY"** y 79 de su **"REGLAMENTO"**.

De conformidad con el artículo 79 del **"REGLAMENTO"** de la **"LEY"**, a la proposición conjunta deberá de adjuntarse un documento que cumpla con lo siguiente:

- Deberá estar firmado por la totalidad de los asociados o sus representantes legales.
- Deberá plasmarse claramente los compromisos que cada uno de los asociados asumirá en caso de resultar adjudicados.
- Deberá plasmarse expresamente que la totalidad de los asociados se constituyen en obligados solidarios entre sí.
- Deberá indicarse claramente a cargo de qué "**PARTICIPANTE"** correrá la obligación de presentar la garantía, en caso de que no sea posible que se presente de manera conjunta.
- Deberá señalarse el representante común para efectos de las notificaciones.

En caso de no presentarse la documentación antes señalada no se considerará que constituye una propuesta conjunta.

9.1.1. Este acto se llevará de la siguiente manera:

a. A este acto deberá asistir el participante por sí mismo o mediante representante legal y/o apoderado de la empresa y presentar con firma autógrafa el "Manifiesto de Personalidad" anexo a estas **"BASES"**, así como una copia de su Identificación Oficial vigente (pasaporte, credencial para votar con fotografía, cédula profesional o cartilla del servicio militar);

b. Los **"PARTICIPANTES"** que concurran al acto firmarán un registro para dejar constancia de su asistencia.

c. Los **"PARTICIPANTES"** registrados entregarán su propuesta en sobre cerrado; este acto se llevará en acompañamiento del Órgano Interno de Control y/o la Contraloría del Estado.

d. Se procederá a la apertura del sobre con las "**PROPUESTAS"**, verificando la documentación solicitada en el numeral 9 de las presentes **"BASES"**, sin que ello implique la evaluación de su contenido;

e. Un miembro del **"COMITÉ**" dará lectura al total de su oferta económica I.V.A. incluido;

f. Cuando menos dos de los integrantes del **"COMITÉ"** asistentes y cuando menos uno de los "**PARTICIPANTES"** presentes (primero de la hoja de registro, cuando aplique), rubricaran cuando menos la primera hoja de los documentos solicitados en el numeral 9 de estas **"BASES"**;

g. Todos los documentos presentados quedarán en poder de la **"CONVOCANTE"** para su análisis, constancia de los actos y posterior "**FALLO"**;

h. En el supuesto de que algún "**PARTICIPANTE"** no cumpla con la obligación de sostener todas y cada una de las condiciones de sus propuestas, o las retire antes de la emisión de la resolución que recaiga en el presente **"PROCEDIMIENTO DE ADQUISICIÓN"**, el Encargado de la Dirección General de Abastecimientos o el funcionario que éste designe para tal efecto, podrá suspender o cancelar el registro del Padrón, conforme a la normatividad aplicable.

Si por cualquier causa el **"COMITÉ"** no cuente con quorum legal para sesionar en la fecha establecida para el acto de presentación y apertura de propuestas, o se deba suspender la sesión por causas justificadas, se solicitará a los **"PARTICIPANTES"** que hayan comparecido, que procedan al registro y a entrega de los sobres con sus propuestas, firmándose estos en su presencia por al menos dos miembros del "**COMITÉ"**, quedando a resguardo del Secretario del "**COMITÉ"** junto con la lista de asistencia, bajo su más estricta responsabilidad, y hasta el momento de su apertura, debiéndose proceder a la apertura de los sobres en la Sesión inmediata siguiente, para lo cual se notificará a los **"PARTICIPANTES"** el día y hora en que se celebrará.

9.2. Criterios para la evaluación de las propuestas y la adjudicación.

El Presente "PROCEDIMIENTO DE ADQUISICIÓN", será adjudicado a uno o varios **"PARTICIPANTES"** por partidas.

Se establece como criterio de evaluación el "Binario", mediante el cual sólo se Adjudica a quien cumpla con los requisitos establecidos por la convocante ("PROPUESTA TÉCNICA") y oferte el precio más bajo ("PROPUESTA ECONÓMICA"), considerando los criterios establecidos en la propia Ley, en este supuesto, la "CONVOCANTE" dictaminara al menos las dos "PROPOSICIONES" cuyo precio resulte ser más bajo, de no resultar estar solventes, se evaluarán las que les sigan en precio. Para lo cual será indispensable cumplir con los requisitos especificados en el Anexo 1 (Carta de Requerimientos Técnicos).

La "DEPENDENCIA REQUIRENTE" emitirá un Dictamen Técnico, en el cual se señalará si los "LICITANTES" cumplen con los requisitos especificados en el Anexo 1 (Carta de Requerimientos Técnicos), y en caso de que estos no cumplan, deberá estar debidamente justificado, una vez emitido dicho dictamen, la "CONVOCANTE" deberá elaborar un Dictamen Económico, el cual deberá contener la evaluación de los "LICITANTES" que cumplieron con los requerimientos técnicos mínimos solicitados por la "DEPENDENCIA REQUIRENTE".

La convocante podrá declinar las proposiciones cuyo costo sea de tal forma desproporcionado con respecto al del mercado, que evidencie no poder cumplir con el bien y/o servicio requerido.

No será objeto de evaluación, las condiciones establecidas por la convocante que tengan como propósito facilitar la presentación de las proposiciones y agilizar la conducción; así como cualquier otro requisito cuyo incumplimiento, por sí mismo, no afecte la solvencia de las propuestas. La inobservancia por parte de los licitantes respecto a dichas condiciones o requisitos no será motivo para desechar sus propuestas.

9.2.1 CRITERIOS DE PREFERENCIA, EMPATE Y PRECIOS NO CONVENIENTE

De acuerdo al apartado 1 del artículo 68 de la **"LEY"**, la **"SECRETARÍA"** o el **"COMITÉ"**, según sea el caso, podrán distribuir la adjudicación de los bienes o servicios entre los proveedores empatados, bajo los criterios señalados en el apartado 2 del artículo 49 y 68 de la **"LEY"** y de conformidad a lo dispuesto en el artículo 70 de su "**REGLAMENTO"**.

Para aplicar los criterios de preferencia señalados en el artículo 49 de la Ley, cuando se establezca que la adjudicación será en su totalidad a un solo participante la diferencia de precios deberá analizarse respecto del importe total de las propuestas y cuando sea por sub-partidas, la diferencia de precios deberá analizarse respecto de las mismas sub-partidas en cada una de las proposiciones.

En caso de resultar aplicable, para efecto de determinar los mejores grados de protección al medio ambiente, deberá escucharse la opinión de la Secretaría de Medio Ambiente y Desarrollo Territorial; mientras que para determinar los grados de preferencia y respecto de innovaciones tecnológicas, la Secretaría de Innovación, Ciencia y Tecnología, habrá de proponer los lineamientos que para tal efecto emita el **"COMITÉ"**.

Para determinar el precio no conveniente o no aceptable se aplicará lo establecido en los artículos 71 y 69 apartado 1, fracción III de la **"LEY"**, en relación con su correlativo 69, segundo párrafo de su **"REGLAMENTO"**

10. ACLARACIÓN DE LAS PROPUESTAS.

La **"DIRECCIÓN DE ÁREA"**, a través de los funcionarios adscritos a la misma, o por conducto del comprador, en su caso, podrán solicitar aclaraciones relacionadas con las propuestas, a cualquier "**PARTICIPANTE"** por el medio oficial que disponga, con fundamento en lo previsto en el artículo 69 apartado 6 de la "**LEY"**.

11. COMUNICACIÓN.

Salvo lo dispuesto en el párrafo que antecede, desde la apertura de las propuestas y hasta el momento de la notificación de la adjudicación, los **"PARTICIPANTES"** no se pondrán poner en contacto con la **"CONVOCANTE"**, para tratar cualquier aspecto relativo a la evaluación de su propuesta. Cualquier intento por parte de un "**PARTICIPANTE"** de ejercer influencia sobre la "**CONVOCANTE"** para la evaluación o adjudicación, dará lugar a que se deseche su **"PROPUESTA"**.

12. DESECHAMIENTO DE PROPUESTAS DE LOS "PARTICIPANTES".

La "**CONVOCANTE"** a través del "**COMITÉ"**, desechará total o parcialmente las propuestas de los **"PARTICIPANTES"** que incurran en cualquiera de las siguientes situaciones:

a. Se encuentren en alguno de los casos previstos por el Artículo 52 de la "**LEY"**, o se compruebe su incumplimiento o mala calidad como **"PROVEEDOR"** del Gobierno del Estado, y las sanciones aplicadas con motivo de su incumplimiento se encuentren en vigor.

b. Si incumple con cualquiera de los requisitos solicitados en las presentes **"BASES"** y sus anexos.

c. Si un socio o administrador forma parte de dos o más de las empresas **"PARTICIPANTES"**, o forma parte de alguna empresa a la que se le haya cancelado o suspendido el registro en el Padrón.

d. Cuando la propuesta presentada no esté firmada por la persona legalmente facultada para ello.

e. La falta de cualquier documento solicitado.

f. La presentación de datos falsos.

g. Cuando de diversos elementos se advierta la posible existencia de arreglo entre los **"PARTICIPANTES"** para elevar los precios objeto del presente **"PROCEDIMIENTO DE ADQUISICIÓN"**.

h. Si se acredita que al "**PARTICIPANTE"** que corresponda se le hubieren rescindido uno o más contratos por causas imputables al mismo y/o las sanciones aplicadas con motivo de incumplimiento se encuentren en vigor.

i. Si el "**PARTICIPANTE"** no demuestra tener capacidad administrativa, fiscal, financiera, legal, técnica, de producción o distribución adecuada para atender el requerimiento de los servicios en las condiciones solicitadas.

j. Si las ofertas presentadas no se realizan con estricto apego a las necesidades mínimas planteadas por la **"CONVOCANTE"** en las presentes **"BASES"**, de acuerdo a la descripción de las especificaciones y servicios requeridos.

k. Si la propuesta económica del **"PROVEEDOR"** en este **"PROCEDIMIENTO DE ADQUISICIÓN"**, resulta superior a la del mercado a tal grado que la **"CONVOCANTE"** presuma que no representa una opción que convenga a los mejores intereses del Estado, atendiendo a lo dispuesto por el artículo 24, apartado 1, fracción VII de la "**LEY"**, para la adjudicación de los Bienes o servicios materia de este **"PROCEDIMIENTO DE ADQUISICIÓN".**

l. Si el importe de la propuesta presentada es de tal forma inferior a la del mercado a tal grado, que la **"CONVOCANTE"** considere que el participante no podrá prestar los servicios, por lo que incurrirá en incumplimiento.

m. Cuando el "**PARTICIPANTE"** se niegue a que le practiquen visitas de verificación o inspección por parte de la **"CONVOCANTE",** en caso de que ésta decida realizar visitas.

13. SUSPENSIÓN O CANCELACIÓN DEL "PROCEDIMIENTO DE ADQUISICIÓN".

La "**CONVOCANTE"** a través del "**COMITÉ"**, podrá cancelar o suspender parcial o totalmente el **"PROCEDIMIENTO DE ADQUISICIÓN"**, de acuerdo a las causales que se describen en el apartado 3 del artículo 71 de la **"LEY"** y en el artículo, 74, 75 y 76 de su Reglamento o los supuestos que a continuación se señalan:

- **a.** Por caso fortuito o fuerza mayor o cuando ocurran razones de interés general.
- **b.** Cuando se advierta que las **"BASES"** difieren de las especificaciones de los servicios que se pretenden adquirir.
- **c.** Si se presume o acredita la existencia de irregularidades.
- **d.** Si ninguna de las ofertas propuestas en este **"PROCEDIMIENTO DE ADQUISICIÓN"**, aseguran al Gobierno de Estado de Jalisco las mejores condiciones disponibles para la adjudicación de los servicios materia de este **"PROCEDIMIENTO DE ADQUISICIÓN"**, por resultar superiores a los del mercado o ser inferiores a tal grado que la **"CONVOCANTE"** presuma que ninguno de los **"PARTICIPANTES"** podrá cumplir con el suministro de los mismos.
- **e.** Por orden escrita debidamente fundada y motivada o por resolución firme de autoridad judicial; por la "**CONTRALORÍA"** con motivo de inconformidades; así como por la "**DIRECCIÓN"**, en los casos en que tenga conocimiento de alguna irregularidad.
- **f.** A solicitud de la **"DEPENDENCIA REQUIRENTE",** cuando dicha solicitud se encuentre debidamente justificada.

En caso de que el **"PROCEDIMIENTO DE ADQUISICIÓN"** sea suspendido o cancelado se dará aviso a todos los **"PARTICIPANTES"**.

14. DECLARACIÓN DE "PROCEDIMIENTO DE ADQUISICIÓN" DESIERTO.

El **COMITÉ"**, podrá declarar parcial o totalmente desierto el **"PROCEDIMIENTO DE ADQUISICIÓN"** de conformidad con el artículo 71, apartado 1 de la **"LEY"** o los supuestos que a continuación se señalan:

- **a.** Cuando no se reciba por lo menos una propuesta en el acto de presentación y apertura de propuestas
- **b.** Cuando ninguna de las propuestas cumpla con todos los requisitos solicitados en estas **"BASES"**.
- **c.** Si a criterio de la "**DIRECCIÓN"** ninguna de las propuestas cubre los elementos que garanticen al Gobierno del Estado las mejores condiciones.
- **d.** Si la oferta del Participante que resulte ser más económica y que cumpla técnicamente, excede el 10% o inferior en un 40% respecto de la media de precios que arroje la investigación de mercado del **"PROCEDIMIENTO DE ADQUISICIÓN"**.
- **e.** Si después de efectuada la evaluación técnica y económica no sea posible adjudicar a ningún Participante.

15. REDUCCIÓN DE CANTIDADES.

El **"COMITÉ"** podrá autorizar a solicitud del **"ÁREA REQUIRENTE",** y cuando se encuentre debidamente justificado, reducciones de las cantidades o bienes o servicios materia de la licitación pública, cuando el presupuesto asignado al procedimiento de contratación sea rebasado por las proposiciones presentadas. Al efecto, los responsables del dictamen económico verificarán previamente que los

precios de la misma son aceptables; el "**ÁREA REQUIRENTE"** emitirá oficio en el que se indique la necesidad y conveniencia de efectuar la reducción respectiva, así como la justificación para no reasignar recursos a fin de cubrir el faltante.

16. NOTIFICACIÓN DEL "FALLO" O "RESOLUCIÓN".

Dentro de los 20 días naturales siguientes al acto de presentación y apertura de propuestas, de acuerdo a lo establecido en el apartado 1 del artículo 69 de la "**LEY"**, se dará a conocer la resolución del presente procedimiento a través del "**SECG"**, en la página web del ente o por correo electrónico manifestado por el participante en el numeral 9 (nueve) del Anexo 4 "Carta de Proposición".

Así mismo se fijará un ejemplar del acta de fallo en el tablero oficial de la "**SECRETARÍA"** durante un periodo mínimo de 10 días naturales, siendo de la exclusiva responsabilidad de los **"PROVEEDOR"** el acudir a enterarse de su contenido.

La notificación del "**FALLO"** o **"RESOLUCIÓN"** podrá diferirse o anticiparse en los términos del artículo 65 fracción III de la **"LEY"**.

Con la notificación del "**FALLO"** o **"RESOLUCIÓN"** por el que se adjudica el **"CONTRATO"**, las obligaciones derivadas de éste serán exigibles de conformidad al artículo 77 apartado 1 de la **"LEY"**.

17. FACULTADES DEL "COMITÉ"

El **"COMITÉ"** resolverá cualquier situación no prevista en estas **"BASES"** y tendrá las siguientes facultades:

- **a.** Dispensar defectos de las propuestas, cuya importancia en sí no sea relevante, siempre que exista la presunción de que el "**PARTICIPANTE"** no obró de mala fe.
- **b.** Rechazar propuestas cuyo importe sea de tal forma inferior, que la **"CONVOCANTE"** considere que el **"PARTICIPANTE"** no podrá prestar los servicios, por lo que incurrirá en incumplimiento.
- **c.** Si al revisar las propuestas existiera error aritmético y/o mecanográfico, se reconocerá el resultado correcto y el importe total será el que resulte de las correcciones realizadas.
- **d.** Cancelar, suspender o declarar desierto el procedimiento.
- **e.** Verificar todos los datos y documentos proporcionados en la propuesta correspondiente, y si se determina que por omisión o dolo el **"PARTICIPANTE"**, no estuviera en posibilidad de cumplir con lo solicitado en estas **"BASES"** y sus anexos, el **"COMITÉ"** podrá adjudicar al **"PARTICIPANTE"** que hubiera obtenido el segundo lugar de acuerdo a los dictámenes que se practiquen a las propuestas presentadas o convocar a un nuevo **"PROCEDIMIENTO DE ADQUISICIÓN"** si así lo considera conveniente.
- **f.** Solicitar el apoyo a cualquiera de las áreas técnicas del gobierno del estado, con el fin de emitir su resolución;
- **g.** Solicitar al personal de la **"SECRETARÍA"** que hagan las visitas de inspección - en caso de ser necesarias - a las instalaciones de los **"PARTICIPANTES"**, con el fin de constatar su existencia, capacidad de producción, y demás elementos necesarios, para asegurar el cumplimiento de las obligaciones que se deriven de una posible adjudicación, o allegarse de elementos para emitir su resolución. Emitir su "**RESOLUCIÓN"** sobre las mejores

condiciones de calidad, servicio, precio, pago y tiempo de entrega ofertadas por los **"PROVEEDORES"**, con motivo de las solicitudes de aprovisionamiento, materia de su competencia, para la adquisición, enajenación y arrendamiento de bienes muebles y la contratación de servicios

h. Realizar las aclaraciones pertinentes respecto a lo establecido en las presentes **"BASES"**; y

i. Demás descritas en el artículo 24 de la **"LEY"**.

De conformidad con los artículos 23, 24 y 31 de la **"LEY"**, las consultas, asesorías, análisis opinión, orientación y "**RESOLUCIONES"** que son emitidas por el **"COMITÉ"** de Adquisiciones son tomadas considerando única y exclusivamente la información, documentación y dictámenes que lo sustenten o fundamente y que son presentados por parte de los "**LICITANTES"** y Servicios Públicos a quienes corresponda, siendo de quien los presenta la responsabilidad de su revisión, acciones, veracidad, faltas u omisiones en su contenido.

18. FIRMA DEL "CONTRATO".

El **"PARTICIPANTE"** adjudicado, se obliga a proporcionar la documentación que le sea requerida y firmar el **"CONTRATO"** en un plazo de 10 días hábiles contados a partir de la fecha de la notificación del "**FALLO"** o "**RESOLUCIÓN"**, conforme al numeral 16 de las presentes **"BASES"**. Una vez firmado en su totalidad se le proporcionará un ejemplar, previa entrega de las garantías de cumplimiento del **"CONTRATO"**, esto de conformidad con el artículo 76 de la **"LEY"**. El **"CONTRATO"** podrá ser modificado de acuerdo a lo establecido en los artículos 80 y 81 de la **"LEY"**.

La persona que deberá acudir a la firma del **"CONTRATO"** tendrá que ser el Representante Legal y/o apoderado legal con facultades para contratar y obligarse, que se encuentre registrado como tal en el padrón de proveedores, acreditando su personalidad jurídica mediante original de su Identificación Oficial vigente (cartilla, pasaporte, cédula profesional o credencial para votar con fotografía).

El **"CONTRATO"** deberá suscribirse en los formatos, términos y condiciones que determine la Dirección General Jurídica de la **"SECRETARÍA"** y/o **"DEPENDENCIA REQUIRENTE"**, mismo que corresponderá en todo momento a lo establecido en las presentes **"BASES"**, el Anexo 1 y la propuesta del **"PROVEEDOR"** adjudicado.

Si el interesado no firma el **"CONTRATO"** por causas imputables al mismo, la **"SECRETARÍA"** por conducto de la "**DIRECCIÓN GENERAL"**, sin necesidad de un nuevo procedimiento, deberá adjudicar el **"CONTRATO"** al **"PARTICIPANTE"** que haya obtenido el segundo lugar, siempre que la diferencia en precio con respecto a la proposición inicialmente adjudicada no sea superior a un margen del diez por ciento (10%). En caso de que hubiera más de un **"PARTICIPANTE"** que se encuentre dentro de ese margen, se le convocará a una nueva sesión en donde podrán mejorar su oferta económica y se adjudicará a quien presente la de menor precio.

De resultar conveniente se podrá cancelar e iniciar un nuevo **"PROCEDIMIENTO DE ADQUISICIÓN"**.

19. VIGENCIA DEL "CONTRATO".

El **"CONTRATO"** a celebrarse con el **"PARTICIPANTE"** que resulte adjudicado en el presente procedimiento, tendrá una vigencia a partir de la fecha de la firma del **"CONTRATO"** y hasta la conclusión de la entrega de los bienes/prestación del servicio objeto del **"CONTRATO",** en atención a los plazos establecidos en las presentes "BASES", sus anexos y la propuesta del **"PROVEEDOR"** adjudicado**,** y podrá prorrogarse a solicitud de la **"DEPENDENCIA REQUIRENTE** "conforme a lo previsto en el artículo 80 de la **"LEY"**.

20. ANTICIPO.

Se podrá otorgar al proveedor adjudicado en la presente licitación un anticipo de hasta el 50% (cincuenta por ciento) de la cantidad total del contrato, siempre y cuando así lo señale en su propuesta y previa exhibición de póliza de fianza que garantice el monto total del mismo, de conformidad el artículo 84 numeral 1 fracción II de la Ley y el numeral 3 de las presentes bases.

21. GARANTÍAS.

En caso de que el monto total del **"CONTRATO"** incluyendo el **"I.V.A."**, sea superior a el equivalente a cuatro mil veces el valor diario de la Unidad de Medida y Actualización, el **"PROVEEDOR"** deberá entregar una garantía del **10%** (diez por ciento) del monto total del **"CONTRATO"** "**I.V.A."** incluido, para responder por el cumplimiento de las obligaciones establecidas en las presentes **"BASES"** y en el **"CONTRATO"** respectivo, de conformidad a la normatividad vigente.

La garantía deberá ser a través de fianza, cheque certificado o de caja. Ésta deberá ser expedida por afianzadora nacional y contener el texto del **Anexo 13** (fianza del 10% del cumplimiento del **"CONTRATO"**) a favor de la Secretaría de la Hacienda Pública, previsto en el artículo 76 fracción IX y 84 de la **"LEY"**. Dichas garantías deberán constituirse en **moneda nacional** y estarán en vigor a partir de la fecha del **"CONTRATO"**, pudiendo ser exigibles en cualquier tiempo, en la cual, la Compañía Afianzadora se deberá sujetar a la Competencia de los Tribunales del Primer Partido Judicial del Estado de Jalisco, así como aceptar el afianzamiento en caso de que se otorgue alguna prórroga a su fiado, o se celebre acuerdo modificatorio al **"CONTRATO"** principal con éste, sin necesidad de que se notifique a la afianzadora las prórrogas que en su caso se otorguen al fiado.

Igualmente, deberán constituir una garantía equivalente al 100% del o los anticipos I.V.A. incluido, a través de los medios antes señalados.

22. SANCIONES.

Se podrá cancelar/rescindir el pedido y/o "CONTRATO" y podrá hacerse efectiva la garantía de cumplimiento de "CONTRATO" en lo dispuesto en el artículo 116 de la "LEY", en los siguientes casos:

a. Cuando el **"PROVEEDOR"** no cumpla con alguna de las obligaciones estipuladas en el **"CONTRATO"**.
b. Cuando hubiese transcurrido el plazo adicional que se concede a los **"PROVEEDORES"**, para corregir las causas de rechazos que en su caso se efectúen.
c. En caso de entregar productos o servicios con especificaciones diferentes a las ofertadas, la "**DIRECCIÓN GENERAL"** considerará estas variaciones como un acto doloso y será razón suficiente

para hacer efectiva la garantía de cumplimiento de **"CONTRATO"** y la cancelación total del pedido y/o **"CONTRATO"**, aun cuando el incumplimiento sea parcial e independientemente de los procedimientos legales que se originen.

d. En el supuesto de que el proveedor adjudicado se encuentre dentro de las listas a que se refiere el artículo 69 B del Código Fiscal de la Federación.

23. DE LA PENALIZACIÓN POR ATRASO EN LA ENTREGA / EN LA PRESTACIÓN DEL SERVICIO.

En caso que el **"PROVEEDOR"** tenga atraso en la entrega de los bienes / en la prestación del servicio por cualquier causa que no sea derivada de la **"SECRETARÍA"** y/o la **"DEPENDENCIA REQUIRENTE"**, se le aplicará una pena convencional de conformidad a la siguiente tabla:

DÍAS DE ATRASO (NATURALES)	% DE LA SANCIÓN SOBRE EL MONTO DE LA PARCIALIDAD/TOTAL
De 01 uno hasta 05 cinco	3% tres por ciento
De 06 seis hasta 10 diez	6% seis por ciento
De 11 diez hasta 20 veinte	10% diez por ciento
De 21 veintiún días de atraso en adelante	**Se rescindirá el "CONTRATO" a criterio de la "SECRETARÍA"**

24. DEL RECHAZO Y DEVOLUCIONES.

En caso de que los bienes entregados por el **"PROVEEDOR"** sean defectuosos, faltos de calidad en general o tengan diferentes especificaciones a las solicitadas, la **"SECRETARÍA"** podrá rechazarlos, ya sea que no los reciba, o los regrese por haber detectado el incumplimiento posterior a la recepción, en caso de haberse realizado el pago, el **"PROVEEDOR"** se obliga devolver las cantidades pagadas con los intereses correspondientes, aplicando una tasa equivalente al interés legal sobre el monto a devolver, y a recibir a su costa los bienes que sean rechazados por la **"SECRETARÍA"** o la **"DEPENDENCIA REQUIRENTE"**, lo anterior sin perjuicio de que se pueda hacer efectiva la garantía señalada en el numeral 21 de las presentes **"BASES"**, y ejercerse las acciones correspondientes por daños y perjuicios.

En caso de que el servicio prestado por el **"PROVEEDOR"** sea falto de calidad en general, no se presente con elementos capacitados, o no cumpla con las diferentes especificaciones solicitadas, la **"SECRETARÍA"** podrá rechazarlos, en caso de haberse realizado el pago, el **"PROVEEDOR"** se obliga devolver las cantidades pagadas con los intereses correspondientes, aplicando una tasa equivalente al interés legal sobre el monto a devolver, lo anterior sin perjuicio de que se pueda hacer efectiva la garantía señalada en el numeral 21 de las presentes **"BASES",** y ejercerse las acciones correspondientes por daños y perjuicios.

Aunado a lo anterior, se deberá de dar vista a la Dirección General Jurídica de la" SECRETARÍA**"** o, de la dependencia competente para efectos de que se proceda a llevar a cabo el procedimiento correspondiente en términos de la normatividad aplicable por el incumplimiento del proveedor.

25. DE LA OPINIÓN POSITIVA DE LA OBLIGACIONES FISCALES (SAT).

El **"PARTICIPANTE"** deberá presentar el documento vigente expedido por el Servicio de Administración Tributaria (SAT) emita una opinión **positiva** de cumplimiento de obligaciones fiscales, la cual podrá obtenerse por Internet en la página del SAT, en la opción "Mi portal", con la Clave de Identificación Electrónica Fortalecida.

Dicho documento se deberá presentar en sentido positivo con vigencia no mayor a 30 días de la fecha establecida para la presentación y apertura de propuestas, el cual se verificará el código QR contenido en el documento, para lo cual el **"PARTICIPANTE"** deberá cerciorarse de que la impresión del mismo sea legible para llevar a cabo la verificación.

Las inconsistencias en este punto, serán motivo de desechamiento de la **"PROPUESTA"** del **"PARTICIPANTE"**.

26. DE LA OPINIÓN POSITIVA DE LAS OBLIGACIONES EN MATERIA DE SEGURIDAD SOCIAL (IMSS).

El **"PARTICIPANTE"** deberá presentar la opinión del cumplimiento de obligaciones en materia de Seguridad Social, o en su caso deberá presentar el documento del cual se desprenda que no cuenta con trabajadores dados de alta, en cualquier caso, el documento deberá ser emitido por el Instituto Mexicano del Seguro Social.

Dicho documento se deberá presentar en sentido positivo con vigencia no mayor a 30 días de la fecha establecida para la presentación y apertura de propuestas, el cual se verificará el código QR contenido en el documento, para lo cual el **"PARTICIPANTE"** deberá cerciorarse de que la impresión del mismo sea legible para llevar a cabo la verificación.

Las inconsistencias en este punto, serán motivo de desechamiento de la **"PROPUESTA"** del **"PARTICIPANTE"**.

27. INCONFORMIDADES.

Ante el Órgano interno de Control de la Secretaría de Administración, con domicilio en Prolongación Avenida Alcalde No. 1221, Col. Miraflores, Guadalajara, Jalisco, (ingreso opcional por puerta posterior de Av. Magisterio s/n), o la Contraloría del Estado, con domicilio en Av. Ignacio L. Vallarta número 1252, Col. Americana. Teléfono 01-(33)1543-9470/

Se dará curso al procedimiento de inconformidad conforme a lo establecido por los artículos 91 y 92 de la **"LEY"**.

28. DERECHOS DE LOS LICITANTES Y "PROVEEDORES".

1. Inconformarse en contra de los actos de la "**LICITACIÓN"**, su cancelación y la falta de formalización del **"CONTRATO"** en términos de los artículos 90 a 109 de la **"LEY"**;
2. Tener acceso a la información relacionada con la "**CONVOCATORIA"**, igualdad de condiciones para todos los interesados en participar y que no sean establecidos requisitos que tengan por objeto o efecto limitar el proceso de competencia y libre concurrencia.

3. Derecho al pago en los términos pactados en el **"CONTRATO"**, o cuando no se establezcan plazos específicos dentro de los veinte días naturales siguientes a partir de la entrega de la factura respectiva, previa entrega de los bienes o prestación de los servicios en los términos del **"CONTRATO"** de conformidad con el artículo 87 de la **"LEY"**;
4. Solicitar el procedimiento de conciliación ante cualquier diferencia derivada del cumplimiento del **"CONTRATO"** o pedidos en términos de los artículos 110 a 112 de la **"LEY"**;
5. Denunciar cualquier irregularidad o queja derivada del procedimiento ante el órgano correspondiente.

29. DECLARACIÓN DE APORTACIÓN CINCO AL MILLAR PARA EL FONDO IMPULSO JALISCO.

De conformidad con el artículo 149 de la **"LEY"** los participantes deberán de manera obligatoria declarar por escrito en los términos del **Anexo 7,** su voluntad o su negativa para la aportación/retención cinco al millar del monto total del contrato antes de **"I.V.A."**, para que sea destinado al **"FONDO"**. Bajo ningún supuesto dicha aportación/retención deberá incrementar su propuesta económica ni repercutir en la calidad de los bienes y/o servicios a entregar, su contravención será causa de desechamiento de la propuesta presentada.

En caso de aceptar realizar dicha aportación, la misma le será retenida por la Secretaría de la Hacienda Pública en una sola ministración en el primer pago, por lo que deberá señalar el concepto de retención del cinco al millar en el CFDI que se emita para efectos de pago.

En caso de aceptar realizar dicha aportación, esta deberá ser en los términos establecidos en el Acuerdo número PF/AS/169/2021, suscrito por el C.P.C. Juan Partida Morales, en su carácter de Secretario de la Hacienda Pública, y publicado en el Periódico Oficial "El Estado de Jalisco" el día 05 de agosto del año 2021.

Guadalajara, Jalisco; 21 de octubre del 2022.

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

LICITACIÓN PÚBLICA LOCAL
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"
"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

RELACIÓN DE ANEXOS

DOCUMENTACIÓN QUE CONTENDRÁ LA OFERTA A PRESENTAR EN HOJA MEMBRETADA DE LA EMPRESA	Punto de referencia 9.1	Documento que se entrega
Anexo 2 (Propuesta Técnica). Más los documentos solicitados en el anexo 1.	a)	
Anexo 3 (Propuesta Económica).	b)	
Anexo 4 (Carta de Proposición).	c)	
Anexo 5 (Acreditación) o documentos que lo acredite.	d)	
Anexo 6 (Declaración de integridad y NO COLUSIÓN de proveedores).	e)	
Anexo 7 (Declaración de aportación cinco al millar para el Fondo Impulso Jalisco).	f)	
Anexo 8 (Manifiesto de Opinión Positiva de Cumplimiento de Obligaciones Fiscales y Constancia).	g)	
Anexo 9 (Manifiesto de Opinión de Cumplimiento de Obligaciones en Materia de Seguridad Social y Constancia) .	h)	
Anexo 10 (Identificación Oficial Vigente).	i)	
Anexo 11 (Manifestación de estar al corriente de sus Obligaciones Patronales y Tributarias).	j)	
Anexo 12 (Estratificación)	k)	

LICITACIÓN PÚBLICA LOCAL
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"
"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

NOTAS ACLARATORIAS
1. La convocatoria no estará a discusión en la junta de aclaraciones, ya que el objetivo de esta es EXCLUSIVAMENTE la aclaración de las dudas formuladas en este documento.
2. Solo se considerarán las solicitudes recibidas en tiempo y forma, conforme a las características del numeral 5 de la convocatoria.
3. Para facilitar la respuesta de sus preguntas deberá de presentarlas en formato digital en Word.

De conformidad al artículo 63 de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios y artículo 64 de su Reglamento, en mi calidad de persona física/representante legal de la empresa, **manifiesto bajo protesta de decir verdad** lo siguiente: **Es mi interés en participar en la Licitación Pública Local LPL297/2022**

Licitante:
Dirección:
Teléfono:
Correo:
No. De **"PROVEEDOR"**:
(Nota: En caso de no contar con él, manifestar bajo protesta de decir verdad que se compromete a inscribirse en el RUPC en caso de resultar adjudicado)
Firma:

Ejemplo de preguntas (no en tabla)
Pregunta 1 …
Pregunta 2 …
…

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

LICITACIÓN PÚBLICA LOCAL
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"
"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

MANIFIESTO DE PERSONALIDAD

Guadalajara Jalisco, a ___ de ____ del 2022.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Dirección General de Abastecimientos

Declaro bajo protesta de decir verdad, que cuento con las facultades suficientes para intervenir en el Acto de Presentación y Apertura de Proposiciones y presentar la propuesta en sobre cerrado (a nombre propio/a nombre de mi representada) en mi carácter de (persona física/representante legal/apoderado) asimismo, manifiesto que (no me encuentro/mi representada no se encuentra) en ninguno de los supuestos establecidos en el artículo 52 de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

LA PRESENTACIÓN DE ESTE DOCUMENTO ES DE CARÁCTER OBLIGATORIO. SIN ÉL NO SE PODRÁ PARTICIPAR NI ENTREGAR PROPUESTA ALGUNA ANTE LA UNIDAD CENTRALIZADA DE COMPRAS, de conformidad con el artículo 59, numeral 1 párrafos VI y VIII de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

Nota: en caso de no ser el representante legal, este documento fungirá como Carta Poder simple, por lo que la figura de la persona que asista será la de "Apoderado", y en cuyo caso, este documento deberá ser firmado también por el Representante Legal.

ATENTAMENTE

_____
Nombre y firma del Participante
o Representante Legal del mismo.

ATENTAMENTE

_____
Nombre y firma de quien recibe el poder

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

Anexo 1
LPL297/2022
Carta de Requerimientos Técnicos (Anexo Técnico)

PARTIDAS

SUB-PARTIDA	CANT.	U.M.	DESCRIPCIÓN
1	1.00	EQUIPO	ADQUISICION DE EQUIPO DE TELECOMUNICACIONES, INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ.
2	1.00	EQUIPO	ADQUISICION DE EQUIPO DE TELECOMUNICACIONES, INFRAESTRUCTURA DE SEGURIDAD LÓGICA PERIMETRAL PARA LAS DEPENDENCIAS DEL GEJ.

- Todas las Especificaciones Señaladas en este Anexo son Mínimas, por lo que el Licitante Podrá Ofertar Bienes y/o Servicios con Especificaciones y Características Superiores, si así lo considera Conveniente.

- Preferentemente, los participantes deberán presentar la totalidad de su propuesta debidamente foliada a efecto de facilitar la revisión.

- Tiempo de entrega a más tardar el 30 de noviembre 2022.

Jalisco

Secretaría de Administración

Adquisición de infraestructura de telecomunicaciones para Dependencias del GE

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

1. GLOSARIO:

Siglas o palabra	Significado
DIC	*Dirección de Infraestructura y Comunicaciones*
GEJ	*Gobierno del Estado de Jalisco*
DGTI	*Dirección General de Tecnologías de la Información*

2. ANTECEDENTES

La Dirección General de Tecnologías de la Información de la Secretaría de Administración es responsable de la correcta operación de la red de telecomunicaciones del Gobierno del Estado. En la actualidad, las dependencias del GEJ cuentan con enlaces de telecomunicaciones robustos y con altas capacidades, pero debido a que el equipo de telecomunicaciones existente es obsoleto y no apto para cubrir la demanda de servicios de red, no es posible aprovechar los servicios en su máxima capacidad.

3. JUSTIFICACIÓN

Actualmente se encuentran en etapa de despliegue e implementación los enlaces de telecomunicaciones del proyecto Red Jalisco, por lo que, para realizar la correcta integración y aprovechar la máxima capacidad de estos servicios, resulta necesario contar con equipos de última generación y con características avanzadas.

4. OBJETIVOS

La DIC requiere de la adquisición de infraestructura de telecomunicaciones de alta capacidad y última tecnología para dotar de mayor calidad en la conectividad y acceso a los servicios de voz y datos, lo que permitirá garantizar y optimizar la operación de los servicios tecnológicos que operan en el GEJ.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Secretaría de Administración

Adquisición de infraestructura de telecomunicaciones para Dependencias del GEJ

FOLIO INTERNO № 1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

5. REQUERIMIENTO

Partida 1.

Suministro de infraestructura de telecomunicaciones para Dependencias del GEJ.

A. Suministro de 02 (dos) módulos de red para expansión de puertos SFP/SFP+ para equipos Core del GEJ.

El proveedor participante deberá suministrar módulos red para la expansión de la capacidad de puertos SFP/SFP+ de los equipos Core de la red del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de hardware.

- El módulo deberá contar con al menos 48 puertos de red con funcionalidad "nonblocking".
- Los puertos de red deberán soportar velocidades de 1, 10 y 25 GE.
- Los puertos deberán ser compatibles con transceptores tipo SFP, SFP+ y SFP28 en su totalidad.
- El módulo deberá soportar el reenvío de paquetes IPv6 "wire-rate" mediante tecnología ASIC.
- El módulo deberá soportar encriptación AES-256 con el algoritmo MACsec-256, el cual deberá ser procesado por medio de la tecnología ASIC existente en el Core del GEJ.
- El MTBF del módulo deberá ser de al menos 600,000 horas.
- El módulo deberá ser compatible de manera nativa y sin adaptaciones con el equipo Core del GEJ Cisco 9600 y la supervisora C9600-SUP-1.

B. Suministro de 04 (cuatro) módulos transceptores QSFP para equipos Core del GEJ.

El proveedor participante deberá suministrar módulos de red para la expansión de la capacidad de los servicios de telecomunicaciones de tipo QSFP para los equipos Core de la red del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Características de hardware.

- El módulo deberá ser de tipo QSFP.
- El módulo de red deberá soportar velocidades de 100 GE.
- El módulo deberá de soportar la conexión en caliente (hot-swappable).
- El módulo deberá ser capaz de interoperar con otros módulos compatibles con el estándar IEEE 100GBASE.
- El módulo deberá soportar altas velocidades en cumplimiento con el estándar IEEE 802.3bm.
- El módulo deberá soportar distancias de al menos 100 metros con fibras OM4.
- El módulo deberá ser compatibles con fibra multimodo (MM) y conectores MPO.
- El módulo deberá ser capaz de ofrecer velocidades de 100GE sobre 12 fibras paralelas en terminación MPO.
- Deberá considerarse un jumper de fibra de al menos 10 metros compatible con el módulo.
- El módulo deberá ser compatible de manera nativa y sin adaptaciones o configuraciones adicionales con el equipo Core del GEJ Cisco 9600.

FOLIO INTERNO № 1695 DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

C. Suministro de 60 (sesenta) puntos de acceso inalámbrico para extensión de cobertura en oficinas del GEJ.

El proveedor participante deberá suministrar puntos de acceso inalámbricos para la expansión de la cobertura de red en las oficinas del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de hardware.

- El punto de acceso deberá soportar la instalación en ambientes de exterior y ser compatible con el estándar IP67.
- El punto de acceso deberá soportar tecnología "dual-band" y contar con radios en 2.4 GHz y 5 GHz.
- El punto de acceso deberá integrar un beacon para la operación de bluetooth con bajo consumo de energía.
- El punto de acceso deberá integrar un radio para escaneo y analítica de RF.
- El punto de acceso deberá contar con un radio dedicado para la operación en tiempo real de los servicios de seguridad WIDS/WIPS.
- El punto de acceso deberá incluir las antenas de exterior necesarias para la correcta operación y a su máxima capacidad con al menos las siguientes características:
  - Operación en dual-band.
  - Frecuencias de operación 2.4 GHz y 5 GHz.
  - Tipo omnidireccionales.
  - Ganancia de 4/7 dBi.
  - Conexión directa (sin cables).
- El punto de acceso deberá ser compatible con los siguientes estándares de red:
  - 802.11b/g/n/ax en banda de 2.4 GHz.
  - 802.11a/n/ac/ax en banda de 5 GHz.
  - 4x4:4 MU-MIMO 802.11ax.
  - SU-MIMO, UL MU-MIMO y DL MU-MIMO.
- El punto de acceso deberá integrar al menos un puerto RJ45 con soporte para velocidades de 10/100/1000/2.5G BASE-T.
- El punto de acceso deberá soportar velocidades de red de al menos 3 Gbps en operación concurrente de los radios de 2.4 GHz y 5 GHz.
- El MTBF del punto de acceso deberá ser de al menos 1'500,000 horas.

COORDINACIÓN GENERAL DE MODERNIZACIÓN GUBERNAMENTAL 04 OCT. 2022 VALIDACIÓN TÉCNICA DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Características de seguridad.

- El punto de acceso deberá permitir el tagueo de VLAN mediante el protocolo 802.1q.
- El punto de acceso deberá contar con la capacidad de generar túneles de VPN Ipsec.
- El punto de acceso deberá permitir la integración con los protocolos de autenticación 802.1x y LDAP.
- El punto de acceso deberá permitir el aislamiento para dispositivos de invitados.
- El punto de acceso deberá soportar protocolos de seguridad WEP, WPA, WPA2-PSK, WPA2 Enterprise con 802.1X, WPA3 Personal, WPA3 Enterprise.
- El punto de acceso deberá soportar protocolos de cifrado EAP-TLS, EAP-TTLS, EAP-MSCHAPv2, EAP-SIM.
- El punto de acceso deberá soportar encriptación por medio de AES y TKIP.
- El punto de acceso deberá contar con capacidades de firewall de capa 7.

FOLIO INTERNO № 1695
DIRECCIÓN GENERAL DE PLANEACIÓN

- El punto de acceso deberá contar con la capacidad de administración de políticas para dispositivos móviles.

Características operativas.

- El punto de acceso deberá soportar la operación en ambientes de alta densidad y de uso intensivo.
- El punto de acceso deberá garantizar la operación de servicios de alto desempeño como voz y video de alta calidad.
- El punto de acceso deberá soportar el control de tráfico basado en aplicación.
- El punto de acceso deberá soportar auto configuración y operación "plug-and-play".
- El punto de acceso deberá permitir la optimización de los servicios de voz y video.
- El punto de acceso deberá soportar la funcionalidad de "fast roaming" con soporte de los protocolos PMK, OKC, & 802.11r en capa 2 y "roaming" distribuido o centralizado en capa 3.
- El punto de acceso deberá permitir las actualizaciones automáticas, mismas que serán realizadas vía la consola de administración.
- El punto de acceso deberá tener la capacidad de realizar informes de análisis de ubicación integrados y seguimiento de dispositivos.
- El punto de acceso deberá tener la capacidad de realizar informes globales de análisis de tráfico L7 por red, por dispositivo y por aplicación.
- El punto de acceso deberá contar con la capacidad de administración y monitoreo desde una consola en la nube.
- El punto de acceso deberá incluir licencia nivel enterprise o similar por tres años para su correcta operación.
- Para garantizar la compatibilidad con la infraestructura inalámbrica existente en él GEJ, el punto de acceso deberá ser compatible de manera nativa y sin adaptaciones o configuraciones adicionales con la nube de la tecnología existente en el GEJ Cisco Meraki.

D. Suministro de 500 (quinientos) teléfonos ip y licencias para servicio de las Dependencias del GEJ.

El proveedor participante deberá suministrar teléfonos ip para servicio de las Dependencias del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de hardware.

- Compatible de manera nativa con el conmutador ip existente en el GEJ Cisco Unified Communication Manager versión 14, se deberá incluir la licencia en la versión "Collaboration Flex Plan 3 (Software & Licensing) Calling EA".
- Pantalla monocromática panorámica con resolución de 384 x 106.
- Incluir un puerto Gigabit Ethernet para conectar al switch, adicional debe contar con un puerto Gigabit Ethernet para conectar a una PC directamente al teléfono.
- Incluir un altavoz.
- Incluir botones exclusivos para las funciones de mensajería, directorio telefónico, servicios y configuración.
- Soporte para alimentación por PoE.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Estándares y protocolos mínimos requeridos.

FOLIO INTERNO № 1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Soporte para propagar a través del teléfono la VLAN de datos hacia una PC.
- Soporte de Bluetooth versión 3.0 Class 1.
- Soporte del protocolo SIP.
- Soporte para los codecs: G.711a-law y mu-law, G.722, G.729a, códec de velocidad de baja conectividad (iLBC) y códec de audio de voz de internet (iSAC).
- Soporte para configuración via XML.
- Soporte del protocolo de descubrimiento y estándares 802.1Q/p, y permita con un encabezado de VLAN 801.1Q que contiene las anulaciones de ID de VLAN configuradas por el ID de VLAN de administrador.
- Soporte de criptografía.

Funcionalidades mínimas requeridas.

- Marcación abreviada.
- Tonos de llamada y ajuste de nivel de volumen.
- Brillo de pantalla ajustable.
- Saludo.
- Respuesta automática.
- Detección automática de auriculares.
- cBarge.
- Campo de lámpara ocupado (BLF).
- Devolución de llamada.
- Desvió de llamadas.
- Notificación de desvío de llamadas.
- Filtro de llamadas.
- Listas de historial de llamadas.
- Estacionamiento de llamadas.
- Captura de llamadas.
- Temporizador de llamadas.
- Llamada en espera.
- Llamar al acompañante.
- Identificador de llamadas.
- Directorio corporativo.
- Conferencia.
- Cross Cluster Extension Mobility (EMCC)
- Transferencia directa.
- Extensión de movilidad.
- Servicio de marcación rápida.
- Códigos de acceso forzado para control de llamadas a PSTN.
- Captura de llamadas grupales.
- Intercomunicador.
- Desvió inmediato.
- Identificador de llamadas maliciosas.
- Indicador de mensajes en espera.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

04 OCT. 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO
1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Conferencia Meet-me.
- Música en espera (MoH).
- Silenciar.
- Timbre distintivo dentro y fuera de la red.
- Directorio personal.
- Marcado previo antes de enviar.
- Privacidad.
- Llamada automática de línea privada (PLAR).
- Volver a marcar.
- Tono de llamada por aparición de línea.
- Localizador uniforme de recursos de servicio (URL).
- Línea compartida.
- Monitoreo y grabación silenciosos.
- Marcación rápida.
- Visualización de fecha y hora.
- Transferencia.
- Marcación de identificador uniforme de recursos (URI).
- Buzón de voz visual.
- Correo de voz.
- Entrenamiento de susurros.

E. Suministro de 180 (ciento ochenta) equipos switch de 24 puertos para oficinas del GEJ.

El proveedor participante deberá suministrar equipos switch de 24 puertos para oficinas del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de Hardware por equipo.

- 24 puertos PoE+ con capacidad 10/100/1000 Base-T.
- 4 puertos fijos de enlace ascendente de 1/10Gbps en SFP/SFP+.
- 1 puerto de consola para administración.
- Capacidad de al menos 380 watts garantizados para suministro de PoE.
- Capacidad de ahorro de energía con la inactividad del puerto y el ajuste automático de la energía del mismo puerto.
- Montaje en una unidad de rack de 19 pulgadas.
- Deberá incluir herrajes para montaje en rack.
- Capacidad de apilamiento (stacking).
- Capacidad de switcheo de al menos 125 Gbps.
- Tasa de reenvió de al menos 96 Mpps.
- Fuente de alimentación incluida.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Características y estándares soportados por los equipos.

FOLIO INTERNO № 1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá contar con mecanismos que validen la autenticidad del hardware y software que utiliza el equipo y eviten que dichos componentes sean modificados.
- Protocolos de ruteo: OSPF, OSPFv3.
- Soporte para al menos 4,000 VLANs.
- Soporte de protocolos ipv4 e ipv6.
- Soporte de al menos 4000 rutas ipv4.
- Soporte de al menos 1000 rutas ipv6.
- Soporte de al menos 2000 reglas de ACL's en ipv4.
- Soporte de al menos 2000 reglas de ACL's en ipv6.
- Soporte de al menos 32000 entradas de direcciones MAC.
- Soporte de al menos 4000 entradas de ARP.
- Soporte en el equipo para estándares de modelado y configuración de redes basadas en software como YANG o similar y NETCONF o similar respectivamente.
- Soporte de protocolos: STP (IEEE 802.1d), RSTP (IEEE 802.1w), y MSTP (IEEE802.1s).
- Soporte para implementar colas de prioridades por puerto permitiendo priorizar el tráfico y la interoperación de voz, video o datos mediante el protocolo IEEE 802.1P CoS ("Class of Service").
- Detección automática dispositivos de red mediante políticas del protocolo 802.1x.
- Soporte para protocolos AAA: RADIUS, TACACS, LOCAL.
- Soporte para protocolo de monitoreo y gestión SNMP v1, v2 y v3.
- Soporte para administración vía CLI y GUI.
- Soporte para administración vía protocolo SSHv2 y Telnet.
- Soporte de protocolo DHCP: client, server y relay.
- Licencia para administración centralizada incluida.

F. Suministro de 150 (ciento cincuenta) equipos switch de 48 puertos para oficinas del GEJ.

El proveedor participante deberá suministrar equipos switch de 48 puertos para oficinas del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de Hardware por equipo.

- 48 puertos PoE+ con capacidad 10/100/1000 Base-T.
- 4 puertos fijos de enlace ascendente de 1/10Gbps en SFP/SFP+.
- 1 puerto de consola para administración.
- Capacidad de al menos 380 watts garantizados para suministro de PoE.
- Capacidad de ahorro de energía con la inactividad del puerto y el ajuste automático de la energía del mismo puerto.
- Montaje en una unidad de rack de 19 pulgadas.
- Deberá incluir herrajes para montaje en rack.
- Capacidad de apilamiento (stacking).
- Capacidad de switcheo de al menos 175 Gbps.
- Tasa de reenvió de al menos 125 Mpps.
- Fuente de alimentación incluida.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

04 OCT. 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Características y estándares soportados por los equipos.

- Deberá contar con mecanismos que validen la autenticidad del hardware y software que utiliza el equipo y eviten que dichos componentes sean modificados.
- Protocolos de ruteo: OSPF, OSPFv3.
- Soporte para al menos 4,000 VLANs.
- Soporte de protocolos ipv4 e ipv6.
- Soporte de al menos 4000 rutas ipv4.
- Soporte de al menos 1000 rutas ipv6.
- Soporte de al menos 2000 reglas de ACL's en ipv4.
- Soporte de al menos 2000 reglas de ACL's en ipv6.
- Soporte de al menos 32000 entradas de direcciones MAC.
- Soporte de al menos 4000 entradas de ARP.
- Soporte en el equipo para estándares de modelado y configuración de redes basadas en software como YANG o similar y NETCONF o similar respectivamente.
- Soporte de protocolos: STP (IEEE 802.1d), RSTP (IEEE 802.1w), y MSTP (IEEE802.1s).
- Soporte para implementar colas de prioridades por puerto permitiendo priorizar el tráfico y la interoperación de voz, video o datos mediante el protocolo IEEE 802.1P CoS ("Class of Service").
- Detección automática dispositivos de red mediante políticas del protocolo 802.1x.
- Soporte para protocolos AAA: RADIUS, TACACS, LOCAL.
- Soporte para protocolo de monitoreo y gestión SNMP v1, v2 y v3.
- Soporte para administración vía CLI y GUI.
- Soporte para administración vía protocolo SSHv2 y Telnet.
- Soporte de protocolo DHCP: client, server y relay.
- Licencia para administración centralizada incluida.

G. Suministro de 30 (treinta) módulos transceptores SFP+ para equipos de telecomunicaciones del GEJ.

El proveedor participante deberá suministrar módulos transceptores para la conectividad de infraestructura de red del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de hardware.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- El módulo deberá soportar el estándar 10GBase-SR.
- El módulo deberá soportar el estándar IEEE 802.3ae
- El módulo deberá tener factor de forma SFP+.
- El módulo deberá soportar tazas de transmisión de 10Gbps.
- El módulo deberá tener un rango de transmisión mínimo de 300 metros.
- El módulo deberá soportar conectores tipo LC.
- El módulo deberá soportar operar de manera plug-and-play.
- El módulo deberá ser compatible con fibras multimodo (MM).
- El módulo deberá tener una longitud de onda de 850nm.
- Deberá considerarse un jumper de fibra de al menos 5 metros compatible con el módulo.

FOLIO INTERNO № 1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- El módulo deberá ser compatible de manera nativa y sin adaptaciones o configuraciones adicionales con los equipos solicitados en los consecutivos E y F de la partida 1 del presente anexo.

H. Suministro de 10 (diez) módulos transceptores SFP+ para equipos de telecomunicaciones del GEJ.

El proveedor participante deberá suministrar módulos transceptores para la conectividad de infraestructura de red del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de hardware.

- El módulo deberá soportar el estándar 10GBase-LR.
- El módulo deberá soportar el estándar IEEE 802.3ae
- El módulo deberá tener factor de forma SFP+.
- El módulo deberá soportar tazas de transmisión de 10Gbps.
- El módulo deberá tener un rango de transmisión mínimo de 10 kilómetros.
- El módulo deberá soportar conectores tipo LC.
- El módulo deberá soportar operar de manera plug-and-play.
- El módulo deberá ser compatible con fibras monomodo (SM).
- El módulo deberá tener una longitud de onda de 1310nm.
- Deberá considerarse un jumper de fibra de al menos 5 metros compatible con el módulo.
- El módulo deberá ser compatible de manera nativa y sin adaptaciones o configuraciones adicionales con los equipos solicitados en los consecutivos E y F de la partida 1 del presente anexo.

I. Suministro de 100 (cien) equipos GPON para oficinas del GEJ.

El proveedor participante deberá suministrar equipos GPON para oficinas del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de Hardware por equipo.

- El equipo deberá soportar ambientes de exterior con nivel de protección al menos IP40.
- El equipo deberá contener un mecanismo de forma nativa para la protección contra sobrecargas.
- El equipo deberá tener al menos 1 puerto SFP+ XGS-PON para NNI.
- El equipo deberá tener al menos 1 puerto BOB XGS-PON para NNI.
- El equipo deberá tener al menos 8 puertos GE PoE++ para UNI.
- El equipo deberá tener al menos 1 puertos DI tipo Phoenix de 4 pines.
- El equipo deberá tener al menos 1 puertos DO tipo Phoenix de 3 pines.
- El equipo deberá ofrecer una capacidad de al menos 200 W para PoE.
- El equipo deberá incluir su fuente de alimentación eléctrica.
- Deberá incluir herrajes para montaje en rack.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

04 OCT. 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Características soportadas por los equipos.

- El equipo deberá soportar autenticación por 802.1x.
- El equipo deberá tener un puerto PON con soporte SC/UPC.
- El equipo deberá soportar una velocidad de transmisión de al menos RX 9 Gbit/s, TX 9 Gbit/s.

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- El equipo deberá soportar una distancia de transmisión de al menos 10 km.
- El equipo deberá soportar una sensibilidad del receptor óptico de -28dBm.
- El equipo deberá soportar una sobrecarga de potencia óptica de -8dBm.

Se deberá considerar para cada equipo GPON un convertidor de medios SFP a RJ45 para la conectividad hacia la infraestructura de red del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de hardware.

- El convertidor deberá integrar un puerto RJ45 10/100/1000Mbps.
- El puerto de red deberá tener la capacidad de auto negociación (Half-Duplex/Full-Duplex).
- El convertidor deberá integrar un puerto GE SFP.
- Deberá incluir un módulo SFP "hot-swappable" compatible con el convertidor.
- El módulo SFP deberá recibir fibra monomodo (SM) de 1310 nm y conector LC.
- El convertidor deberá incluir un panel de estado donde se identifique de manera visual mediante leds la operación del dispositivo.

Características de operación.

- El convertidor deberá tener la capacidad de convertir señales recibidas por medio de fibra óptica a señal entregada por medios de cobre y viceversa.
- El convertidor deberá tener la capacidad de detectar de forma automática el modo MDI/MDI-X.
- El convertidor deberá tener la capacidad de trabajar en distancias desde 0.55 hasta 10 kilómetros.
- El convertidor deberá ser compatible con los estándares:
  - IEEE 802.3ab.
  - IEEE 802.3z.
  - 1000Base-SX/LX/LH.
  - 1000Base-T.

Partida 2.

Suministro de infraestructura de seguridad lógica perimetral para Dependencias del GEJ, para garantizar la correcta operación y mantener los mismos estándares de seguridad la solución propuesta para esta partida deberá ser de una sola marca.

A. Suministro de 01 (uno) equipo de seguridad para la protección de aplicaciones web y APIs del GEJ.

El proveedor participante deberá suministrar un equipo de seguridad para la protección de aplicaciones web del GEJ, el cual deberá cumplir con las siguientes características mínimas.

GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Características de desempeño por equipo.

FOLIO INTERNO 1695 DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- El equipo deberá contar con un Throughput para HTTP de al menos 10 Gbps.
- El equipo deberá contar con una latencia no mayor a 5 ms.
- El equipo deberá contar con hardware dedicado para la encriptación/desencriptación SSL y TLS.
- El equipo deberá contar con licencias de aplicaciones ilimitadas.
- El equipo deberá soportar la capacidad de generar un cluster a nivel de hardware para alta disponibilidad de tipo activo/activo y/o activo/pasivo.

Características de hardware.

- El equipo deberá contar con al menos 8 Interfaces GE RJ45.
- El equipo deberá contar con al menos 10 Interfaces SFP+.
- El equipo deberá contar con al menos 2 puertos USB.
- El equipo deberá contar con al menos 2 x 960 GB SSD de almacenamiento.
- El equipo deberá soportar al menos 90 sistemas virtuales lógicos (contextos) por dispositivo.
- El equipo deberá incluir fuentes de alimentación redundantes y con soporte para reemplazo en caliente (hot-swappable) y soporte para 100-240 VAC.

Funcionalidades.

- La solución deberá consistir en una plataforma de protección de aplicaciones web.
- La solución deberá brindar seguridad para aplicaciones basada en OWASP.
- La solución deberá utilizar motores de detección WAF tradicionales basados en firmas de ataques, reputación de direcciones IP, validación de protocolos, etc.
- La solución deberá contar con un motor de descubrimiento y protección de API.

Seguridad Web.

- Aprendizaje automático basado en inteligencia artificial.
- Perfilado automático (lista blanca).
- Servidor web y firmas de aplicaciones (lista negra).
- Reputación IP.
- Geolocalización de IP.
- Cumplimiento HTTP RFC.
- Soporte nativo para HTTP / 2.
- Verificación de OpenAPI 3.0.
- Protección de WebSocket y aplicación de firmas.
- Protección del hombre en el navegador (MiTB).

Protección contra ataques de aplicaciones.

- OWASP Top 10.
- Cross Site Scripting.
- Inyección SQL.
- Falsificación de solicitud de sitios cruzados.
- Secuestro de sesión.
- Escáner de vulnerabilidad incorporado.
- Integración de escáner de terceros (parches virtuales).
- Escaneo de carga de archivos con AV y sandbox.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO No 1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Servicios de seguridad.

- Firmas de servicios web.
- Conformidad con el protocolo XML y JSON.
- Detección de malware.
- Parches virtuales.
- Validación de protocolo.
- Protección de fuerza bruta.
- Firma y cifrado de cookies.
- Puntuación y ponderación de amenazas.
- Detección SQLi basada en sintaxis.
- Seguridad del encabezado HTTP.
- Mensaje de error personalizado y manejo de código de error.
- Firmas de intrusión del sistema operativo.
- Protección conocida contra amenazas y ataques de día cero.
- L4 Firewall de red con estado.
- Prevención DoS.
- Protección de correlación avanzada utilizando múltiples elementos de seguridad.
- Prevención de fuga de datos.
- Protección de desfiguración web.

Entrega de aplicaciones.

- Balanceo de carga del servidor de capa 7.
- Reescritura de URL.
- Enrutamiento de contenido.
- Descarga de HTTPS / SSL.
- Compresión HTTP.
- Almacenamiento en caché.

Autenticación.

- Autenticación activa y pasiva.
- Publicación del sitio y 550.
- Acceso RSA para autenticación de 2 factores.
- Soporte LDAP, RADIUS y SAML.
- Soporte de certificado de cliente SSL.
- CAPTCHA y Real Browser Enforcement (RBE).

Gestión de informes.

- Interfaz de usuario web.
- Interfaz de línea de comando.
- Análisis gráfico y herramientas de informes.
- Administración central para múltiples dispositivos.
- Agrupación de HA activa/ activa.
- REST API.
- Registro e informes centralizados.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

04 OCT. 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

12 de 72

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Seguimiento de usuario/ dispositivo.
- Tableros en tiempo real.
- Panel de control de bot.
- OWASP Top 10 categorización de ataques.
- Geo IP Analytics.
- SNMP, Syslog y registro/ monitoreo de correo electrónico.
- Dominios administrativos con RBAC completo.

Licenciamiento.
Se deberán considerar las licencias necesarias por 24 meses de protección WAF, servicio de protección web, reputación de IP y soporte técnico 24x7 con remplazo avanzado de hardware y actualizaciones de firmware.

B. Suministro de 08 (ocho) equipos de seguridad lógica para el GEJ.

El proveedor participante deberá suministrar equipos de seguridad lógica y licenciamiento requerido por 24 meses para el GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de desempeño por equipo.

- El equipo deberá contar con un Throughput en Firewall tanto en IPv4 como en IPv6 de al menos 25 Gbps para paquetes UDP de 1518, 25 de 512 bytes y de 10 Gbps en paquetes UDP de 64 bytes.
- El equipo deberá contar con un Throughput VPN IPSEC de por lo menos 10 Gbps.
- El equipo deberá contar con un Throughput IPS de al menos 5 Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad protección ante amenazas de 3 Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad NGFW de 3.5 Mbps.
- El equipo deberá soportar al menos 3'000,000 de sesiones concurrentes.
- El equipo deberá soportar 250,000 nuevas sesiones por segundo.
- El equipo deberá contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 500 usuarios de VPN SSL.
- El equipo deberá generar al menos 15,000 VPN's IPSec Client to Gateway.
- El equipo deberá generar al menos 2,000 VPN's IPSec Gateway to Gateway
- El equipo deberá soportar la configuración de 10,000 políticas de firewall.

Características de Hardware por equipo.

- El equipo deberá contar con al menos 16 Interfaces GE RJ45.
- El equipo deberá contar con al menos 8 Interfaces SFP.
- El equipo deberá contar con al menos 4 Interfaces SFP+.
- El equipo deberá soportar al menos 10 sistemas virtuales lógicos (contextos) por dispositivo.
- El equipo deberá contar con al menos 1 puerto USB.
- El equipo deberá contar con al menos 1 Interfaz RJ45 gestión por consola.
- El equipo deberá contar con al menos 1 x 480 GB de almacenamiento.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Licenciamiento.

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Se deberán considerar las licencias necesarias por 24 meses para habilitar los servicios de IPS, servicio de protección avanzada anti malware, control de aplicaciones, filtrado web y de video y servicio de antispam. Soporte técnico 24x7, remplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Características Generales:

- La solución deberá 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.
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- Las funcionalidades de protección de red que conformarán la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.
- La plataforma deberá estar optimizada para análisis de contenido de aplicaciones en capa 7.
- Deberá incluir los cables de alimentación.
- La gestión del equipo deberá ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
- Los dispositivos de protección de red deberán soportar 4094 VLANs Tags 802.1q.
- Los dispositivos de protección de red deberán soportar agregación de enlaces 802.3ad y LACP.
- Los dispositivos de protección de red deberán soportar Policy based routing y policy based forwar-ding.
- Los dispositivos de protección de red deberán soportar encaminamiento de multicast (PIM-SM y PIM-DM).
- Los dispositivos de protección de red deberán soportar DHCP Relay.
- Los dispositivos de protección de red deberán soportar DHCP Server.
- Los dispositivos de protección de red deberán soportar sFlow.
- Los dispositivos de protección de red deberán soportar Jumbo Frames.
- Los dispositivos de protección de red deberán soportar sub-interfaces Ethernet lógicas.
- Deberá ser compatible con NAT dinámica (varios-a-1).
- Deberá ser compatible con NAT dinámica (muchos-a-muchos).
- Deberá soportar NAT estática (1-a-1).
- Deberá admitir NAT estática (muchos-a-muchos).
- Deberá ser compatible con NAT estático bidireccional 1-a-1.
- Deberá ser compatible con la traducción de puertos (PAT).
- Deberá ser compatible con NAT Origen.
- Deberá ser compatible con NAT de destino.
- Deberá soportar NAT de origen y NAT de destino de forma simultánea.
- Deberá soportar NAT de origen y NAT de destino en la misma política.
- Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.
- Tendrá que ser compatible con NAT64 y NAT46 e implementar el protocolo ECMP.
- Deberá soportar SD-WAN de forma nativa.
- Deberá soportar el balanceo de enlace hash por IP de origen.
- Deberá soportar el balanceo de enlace por hash de IP de origen y destino.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO No. 1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá 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.
- Debe poder implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales.
- Permitirá 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, memo-ria, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
- Podrá enviar logs a sistemas de gestión externos simultáneamente.
- Tendrá la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.
- Podrá implementar la optimización del tráfico entre dos dispositivos.
- Para IPv4, deberá soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
- Para IPv6, deberá soportar enrutamiento estático y dinámico (OSPFv3).
- Deberá soportar OSPF graceful restart.
- Será compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
- Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster.
- La configuración de alta disponibilidad sincronizará: Sesiones.
- La configuración de alta disponibilidad sincronizará: Configuraciones, podrá incluir, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red.
- La configuración de alta disponibilidad deberá sincronizar: Las asociaciones de seguridad VPN.
- La configuración de alta disponibilidad deberá sincronizar: Tablas FIB.
- En modo HA (Modo de alta disponibilidad) permitirá la supervisión de fallos de enlace.
- Deberá soportar la creación de sistemas virtuales en el mismo equipo.
- Para una alta disponibilidad, el uso de clústeres virtuales será posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos.
- Permitirá 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.
- La solución de gestión será compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluirá, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.
- Deberá contar con control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Out-bound), deberá 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).
- Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red.

Jefatura COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

04 OCT 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- El tejido de seguridad podrá identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.
- La consola de administración deberá soportar como mínimo, inglés, español.
- La consola deberá soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.

Control por Política de Firewall.

- Deberá soportar controles de zona de seguridad.
- Deberá contar con políticas de control por puerto y protocolo.
- Deberá 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.
- Deberá contar con control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
- El Firewall podrá aplicar la inspección de control de aplicaciones, antivirus, filtrado web, fil-trado DNS, IPS directamente a las políticas de seguridad.
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet puedrán agregarse directamente a las políticas de firewall.
- Deberá 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.
- Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).
- Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, Ali-Cloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.
- Deberá soportar el protocolo estándar de la industria VXLAN.
- La solución permitirá la implementación sin asistencia de SD-WAN.
- En SD-WAN deberá soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN.
- La solución deberá soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Control de Aplicación.

- El dispositivo de protección de red tendrá la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
- Podrá detectar miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El 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.
- Deberá reconoce al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, lin-ked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail 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;

FOLIO INTERNO No. 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Identificará el uso de tácticas evasivas, es decir, Tendrá 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.
- Para tráfico cifrado SSL, podrá descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
- Identificará el uso de tácticas evasivas a través de las comunicaciones cifradas.
- Deberá actualizar de la base de firmas de la aplicación de forma automática.
- Limitará el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos.
- Para mantener la seguridad de red eficiente deberá soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
- Permitirá 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.
- El fabricante podrá solicitar la inclusión de aplicaciones en su base de datos.
- Permitirá la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitiendo a Hangouts el chat, pero impedir la llamada de video.
- Permitirá la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Será posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- Será posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
- Será posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación.
- Será posible configurar Application Override seleccionando las aplicaciones individualmente.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Prevención de Amenazas.

- Para proteger el entorno contra los ataques, deberá contar con un módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
- Incluirá firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (anti-virus y anti-spyware).
- Las características de IPS y antivirus deberán 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.
- Sincronizará las firmas de IPS, antivirus, anti-spyware cuando se implemente en alta disponibilidad.
- Deberá 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.
- Permitirá el bloqueo de vulnerabilidades y exploits conocidos.
- Incluirá la protección contra ataques de denegación de servicio.

FOLIO INTERNO # 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, Análisis para detectar anomalías de protocolo, Tendrá los siguientes mecanismos de inspección IPS: Desfragmentación IP, Tendrá los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP, Tendrá los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets).
- Deberá ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
- Deberá detectar y bloquear los escaneos de puertos de origen.
- Deberá bloquear ataques realizados por gusanos (worms) conocidos.
- Deberá contar con firmas específicas para la mitigación de ataques DoS y DDoS.
- Deberá contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buf-fer overflow).
- Deberá permitir crear firmas personalizadas en la interfaz gráfica del producto.
- Deberá identificar y bloquear la comunicación con redes de bots.
- Deberá 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.
- Deberá ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Deberá 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.
- Los eventos deberán identificar el país que origen o la amenaza.
- Deberá incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- Deberá tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
- Deberá 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.
- Deberá proporcionar 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).

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Identificación de Usuarios.

- Deberá 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.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basado en usuarios y grupos de usuarios.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basado 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.

- Deberá tener integración con RADIUS para identificar a los usuarios y grupos que Permitirán las políticas de granularidad / control basado en usuarios y grupos de usuarios.
- Deberá tener la integración LDAP para la identificación de los usuarios y grupos que Permitirán granularidad en las políticas/control basado en usuarios y grupos de usuarios.
- Deberá 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 autentificación residente en el equipo de seguridad (portal cautivo).
- Deberá soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que Permitirá una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios.
- Deberá implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
- Deberá permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
- Deberá incluir al menos dos tokens de forma nativa, lo que Permitirá la autenticación de dos factores;

Filtrado de URL.

- Deberá permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
- Deberá tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito.
- Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Deberá tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL.
- Deberá tener por lo menos 75 categorías de URL.
- Deberá tener la funcionalidad de exclusión de URLs por categoría.
- Deberá permitir página de bloqueo personalizada.
- Deberá permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).
- Además del Explicit Web Proxy, deberá soportar r proxy web transparente.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

04 OCT. 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

QoS Traffic Shaping.

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo sea excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere que la solución que, además de que deberá permitir o denegar dichas solicitudes, deberá 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.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo.

FOLIO INTERNO
1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluido, pero no limitado a Skype, BitTorrent, Azureus y YouTube.
- Deberá soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS deberá permitir la definición de tráfico con ancho de banda garantizado.
- En QoS deberá permitir la definición de tráfico con máximo ancho de banda.
- En QoS deberá permitir la definición de colas de prioridad.
- Deberá soportar marcación de paquetes DiffServ, incluso por aplicación.
- Deberá soportar la modificación de los valores de DSCP para Diffserv.
- Deberá soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
- Deberá soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

Filtro de Datos.

- Deberá permitir la creación de filtros para archivos y datos predefinidos.
- Los archivos deberán ser identificados por tamaño y tipo.
- Deberá permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones.
- Deberá soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
- Deberá soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos.
- Permitirá 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.

- Deberá soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países.
- Deberá permitir la visualización de los países de origen y destino en los registros de acceso.
- Deberá permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

VPN.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá soportar VPN de sitio-a-sitio y cliente-a-sitio.
- Deberá soportar VPN IPSec.
- Deberá soportar VPN SSL.
- La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
- La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
- La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
- Tendrá interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
- Deberá soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN
ESTRATÉGICA

- Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting.
- Deberá 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.
- Deberá 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.
- Deberá suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
- Deberá permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
- Deberá mantener una conexión segura con el portal durante la sesión.
- El agente de VPN SSL o IPSEC cliente-a-sitio deberá ser compatible con al menos Windows y Mac OS.

C. Suministro de 07 (siete) equipos de seguridad lógica del GEJ.

El proveedor participante deberá suministrar equipos de seguridad lógica y licenciamiento requerido por 24 meses para el GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de desempeño por equipo.

- El equipo deberá contar con un Throughput en Firewall tanto en IPv4 como en IPv6 de al menos 20 Gbps para paquetes UDP de 1518, 15 de 512 bytes y de 10 Gbps en paquetes UDP de 64 bytes.
- El equipo deberá contar con un Throughput VPN IPSEC de por lo menos 10 Gbps.
- El equipo deberá contar con un Throughput IPS de al menos 2.5 Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad protección ante amenazas de 1 Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad NGFW de 1.5 Gbps.
- El equipo deberá soportar al menos 1.5 millones de Sesiones concurrentes.
- El equipo deberá soportar 56,000 nuevas sesiones por segundo.
- El equipo deberá contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 500 usuarios de VPN SSL.
- El equipo deberá generar al menos 15,000 VPN's IPSec Client to Gateway.
- El equipo deberá generar al menos 2000 VPN's IPSec Gateway to Gateway
- El equipo deberá soportar la configuración de 10,000 políticas de firewall.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN DE INNOVACIÓN TECNOLÓGICA

Características de Hardware por equipo.

- El equipo deberá contar con al menos 12 Interfaces GE RJ45.
- El equipo deberá contar con al menos 4 Interfaces SFP.
- El equipo deberá contar con al menos 2 Interfaces SFP+.
- El equipo deberá soportar al menos 10 sistemas virtuales lógicos (contextos) por equipo.
- El equipo deberá contar con al menos 1 Interfaces RJ45 para gestión.
- El equipo deberá contar con al menos 1 x 480 GB de almacenamiento.
- El equipo deberá contar con al menos 1 puertos USB.

Licenciamiento.

FOLIO INTERNO № 1695

Se deberán considerar las licencias necesarias por 24 meses para habilitar los servicios de IPS, servicio de protección avanzada anti malware, control de aplicaciones, filtrado web y de video y servicio de antispam. Soporte técnico 24x7, remplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Características Generales:

- La solución deberá 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.
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- Las funcionalidades de protección de red que conformarán la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.
- La plataforma deberá estar optimizada para análisis de contenido de aplicaciones en capa 7.
- Deberá incluir los cables de alimentación.
- La gestión del equipo deberá ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
- Los dispositivos de protección de red deberán soportar 4094 VLANs Tags 802.1q.
- Los dispositivos de protección de red deberán soportar agregación de enlaces 802.3ad y LACP.
- Los dispositivos de protección de red deberán soportar Policy based routing y policy based forwar-ding.
- Los dispositivos de protección de red deberán soportar encaminamiento de multicast (PIM-SM y PIM-DM).
- Los dispositivos de protección de red deberán soportar DHCP Relay.
- Los dispositivos de protección de red deberán soportar DHCP Server.
- Los dispositivos de protección de red deberán soportar sFlow.
- Los dispositivos de protección de red deberán soportar Jumbo Frames.
- Los dispositivos de protección de red deberán soportar sub-interfaces Ethernet lógicas.
- Deberá ser compatible con NAT dinámica (varios-a-1).
- Deberá ser compatible con NAT dinámica (muchos-a-muchos).
- Deberá soportar NAT estática (1-a-1).
- Deberá admitir NAT estática (muchos-a-muchos).
- Deberá ser compatible con NAT estático bidireccional 1-a-1.
- Deberá ser compatible con la traducción de puertos (PAT).
- Deberá ser compatible con NAT Origen.
- Deberá ser compatible con NAT de destino.
- Deberá soportar NAT de origen y NAT de destino de forma simultánea.
- Deberá soportar NAT de origen y NAT de destino en la misma política.
- Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.
- Tendrá que ser compatible con NAT64 y NAT46 e implementar el protocolo ECMP.
- Deberá soportar SD-WAN de forma nativa.
- Deberá soportar el balanceo de enlace hash por IP de origen.
- Deberá soportar el balanceo de enlace por hash de IP de origen y destino.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO # 1695 DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá 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.
- Debe poder implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales.
- Permitirá 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, memo-ria, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
- Podrá enviar logs a sistemas de gestión externos simultáneamente.
- Tendrá la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.
- Podrá implementar la optimización del tráfico entre dos dispositivos.
- Para IPv4, deberá soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
- Para IPv6, deberá soportar enrutamiento estático y dinámico (OSPFv3).
- Deberá soportar OSPF graceful restart.
- Será compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
- Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster.
- La configuración de alta disponibilidad sincronizará: Sesiones.
- La configuración de alta disponibilidad sincronizará: Configuraciones, podrá incluir, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red.
- La configuración de alta disponibilidad deberá sincronizar: Las asociaciones de seguridad VPN.
- La configuración de alta disponibilidad deberá sincronizar: Tablas FIB.
- En modo HA (Modo de alta disponibilidad) permitirá la supervisión de fallos de enlace.
- Deberá soportar la creación de sistemas virtuales en el mismo equipo.
- Para una alta disponibilidad, el uso de clústeres virtuales será posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos.
- Permitirá 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.
- La solución de gestión será compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluirá, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.
- Deberá contar con control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Out-bound), deberá 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).
- Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL 04 OCT. 2022 VALIDACIÓN TÉCNICA DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- El tejido de seguridad podrá identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.
- La consola de administración deberá soportar como mínimo, inglés, español.
- La consola deberá soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.

Control por Política de Firewall.

- Deberá soportar controles de zona de seguridad.
- Deberá contar con políticas de control por puerto y protocolo.
- Deberá 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.
- Deberá contar con control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
- El Firewall podrá aplicar la inspección de control de aplicaciones, antivirus, filtrado web, fil-trado DNS, IPS directamente a las políticas de seguridad.
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet puedrán agregarse directamente a las políticas de firewall.
- Deberá 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.
- Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).
- Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, Ali-Cloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.
- Deberá soportar el protocolo estándar de la industria VXLAN.
- La solución permitirá la implementación sin asistencia de SD-WAN.
- En SD-WAN deberá soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN.
- La solución deberá soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Control de Aplicación.

- El dispositivo de protección de red tendrá la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
- Podrá detectar miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El 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.
- Deberá reconoce al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, lin-ked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail 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;

FOLIO INTERNO
1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Identificará el uso de tácticas evasivas, es decir, Tendrá 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.
- Para tráfico cifrado SSL, podrá descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
- Identificará el uso de tácticas evasivas a través de las comunicaciones cifradas.
- Deberá actualizar de la base de firmas de la aplicación de forma automática.
- Limitará el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos.
- Para mantener la seguridad de red eficiente deberá soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
- Permitirá 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.
- El fabricante podrá solicitar la inclusión de aplicaciones en su base de datos.
- Permitirá la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitiendo a Hangouts el chat, pero impedir la llamada de video.
- Permitirá la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Será posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- Será posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
- Será posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación.
- Será posible configurar Application Override seleccionando las aplicaciones individualmente.

Prevención de Amenazas.

- Para proteger el entorno contra los ataques, deberá contar con un módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
- Incluirá firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (anti-virus y anti-spyware).
- Las características de IPS y antivirus deberán 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.
- Sincronizará las firmas de IPS, antivirus, anti-spyware cuando se implemente en alta disponibilidad.
- Deberá 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.
- Permitirá el bloqueo de vulnerabilidades y exploits conocidos.
- Incluirá la protección contra ataques de denegación de servicio.

04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, Análisis para detectar anomalías de protocolo, Tendrá los siguientes mecanismos de inspección IPS: Desfragmentación IP, Tendrá los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP, Tendrá los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets).
- Deberá ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
- Deberá detectar y bloquear los escaneos de puertos de origen.
- Deberá bloquear ataques realizados por gusanos (worms) conocidos.
- Deberá contar con firmas específicas para la mitigación de ataques DoS y DDoS.
- Deberá contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buf-fer overflow).
- Deberá permitir crear firmas personalizadas en la interfaz gráfica del producto.
- Deberá identificar y bloquear la comunicación con redes de bots.
- Deberá 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.
- Deberá ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Deberá 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.
- Los eventos deberán identificar el país que origen o la amenaza.
- Deberá incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- Deberá tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
- Deberá 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.
- Deberá proporcionar 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).

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Identificación de Usuarios.

- Deberá 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.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basado en usuarios y grupos de usuarios.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basado 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.

AT_V2 **26 de 72**

FOLIO INTERNO
No 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá tener integración con RADIUS para identificar a los usuarios y grupos que Permitirán las políticas de granularidad / control basado en usuarios y grupos de usuarios.
- Deberá tener la integración LDAP para la identificación de los usuarios y grupos que Permitirán granularidad en las políticas/control basado en usuarios y grupos de usuarios.
- Deberá 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 autentificación residente en el equipo de seguridad (portal cautivo).
- Deberá soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que Permitirá una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios.
- Deberá implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
- Deberá permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
- Deberá incluir al menos dos tokens de forma nativa, lo que Permitirá la autenticación de dos factores;

Filtrado de URL.

- Deberá permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
- Deberá tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito.
- Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Deberá tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL.
- Deberá tener por lo menos 75 categorías de URL.
- Deberá tener la funcionalidad de exclusión de URLs por categoría.
- Deberá permitir página de bloqueo personalizada.
- Deberá permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).
- Además del Explicit Web Proxy, deberá soportar r proxy web transparente.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

QoS Traffic Shaping.

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo sea excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere que la solución que, además de que deberá permitir o denegar dichas solicitudes, deberá 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.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo.

FOLIO INTERNO № 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluido, pero no limitado a Skype, BitTorrent, Azureus y YouTube.
- Deberá soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS deberá permitir la definición de tráfico con ancho de banda garantizado.
- En QoS deberá permitir la definición de tráfico con máximo ancho de banda.
- En QoS deberá permitir la definición de colas de prioridad.
- Deberá soportar marcación de paquetes DiffServ, incluso por aplicación.
- Deberá soportar la modificación de los valores de DSCP para Diffserv.
- Deberá soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
- Deberá soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

Filtro de Datos.

- Deberá permitir la creación de filtros para archivos y datos predefinidos.
- Los archivos deberán ser identificados por tamaño y tipo.
- Deberá permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones.
- Deberá soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
- Deberá soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos.
- Permitirá 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.

- Deberá soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países.
- Deberá permitir la visualización de los países de origen y destino en los registros de acceso.
- Deberá permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

VPN.

- Deberá soportar VPN de sitio-a-sitio y cliente-a-sitio.
- Deberá soportar VPN IPSec.
- Deberá soportar VPN SSL.
- La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
- La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
- La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
- Tendrá interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
- Deberá soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.

FOLIO INTERNO
Nº 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting.
- Deberá 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.
- Deberá 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.
- Deberá suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
- Deberá permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
- Deberá mantener una conexión segura con el portal durante la sesión.
- El agente de VPN SSL o IPSEC cliente-a-sitio deberá ser compatible con al menos Windows y Mac OS.

D. Suministro de 07 (siete) equipos de seguridad lógica para el GEJ.

El proveedor participante deberá suministrar equipos de seguridad lógica y licenciamiento requerido por 24 meses para el GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de desempeño por equipo.

- El equipo deberá contar con un Throughput en Firewall tanto en IPv4 como en IPv6 de al menos 20 Gbps para paquetes UDP de 1518, 15 de 512 bytes y de 10 Gbps en paquetes UDP de 64 bytes.
- El equipo deberá contar con un Throughput VPN IPSEC de por lo menos 10 Gbps.
- El equipo deberá contar con un Throughput IPS de al menos 2.5 Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad protección ante amenazas de 1 Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad NGFW de 1.5 Gbps.
- El equipo deberá soportar al menos 1.5 millones de Sesiones concurrentes.
- El equipo deberá soportar 56,000 nuevas sesiones por segundo.
- El equipo deberá contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 500 usuarios de VPN SSL.
- El equipo deberá generar al menos 15,000 VPN's IPSec Client to Gateway.
- El equipo deberá generar al menos 2000 VPN's IPSec Gateway to Gateway
- El equipo deberá soportar la configuración de 10,000 políticas de firewall.

Características de Hardware por equipo.

- El equipo deberá contar con al menos 12 Interfaces GE RJ45.
- El equipo deberá contar con al menos 4 Interfaces SFP.
- El equipo deberá contar con al menos 2 Interfaces SFP+.
- El equipo deberá soportar al menos 10 sistemas virtuales lógicos (contextos) por equipo.
- El equipo deberá contar con al menos 1 Interfaces RJ45 para gestión.
- El equipo deberá contar con al menos 1 x 480 GB de almacenamiento.
- El equipo deberá contar con al menos 1 puertos USB.

Licenciamiento.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Se deberán considerar las licencias necesarias por 24 meses para habilitar los servicios de IPS, servicio de protección avanzada anti malware y control de aplicaciones. Soporte técnico 24x7, remplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Características Generales:

- La solución deberá 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.
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- Las funcionalidades de protección de red que conformarán la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.
- La plataforma deberá estar optimizada para análisis de contenido de aplicaciones en capa 7.
- Deberá incluir los cables de alimentación.
- La gestión del equipo deberá ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
- Los dispositivos de protección de red deberán soportar 4094 VLANs Tags 802.1q.
- Los dispositivos de protección de red deberán soportar agregación de enlaces 802.3ad y LACP.
- Los dispositivos de protección de red deberán soportar Policy based routing y policy based forwar-ding.
- Los dispositivos de protección de red deberán soportar encaminamiento de multicast (PIM-SM y PIM-DM).
- Los dispositivos de protección de red deberán soportar DHCP Relay.
- Los dispositivos de protección de red deberán soportar DHCP Server.
- Los dispositivos de protección de red deberán soportar sFlow.
- Los dispositivos de protección de red deberán soportar Jumbo Frames.
- Los dispositivos de protección de red deberán soportar sub-interfaces Ethernet lógicas.
- Deberá ser compatible con NAT dinámica (varios-a-1).
- Deberá ser compatible con NAT dinámica (muchos-a-muchos).
- Deberá soportar NAT estática (1-a-1).
- Deberá admitir NAT estática (muchos-a-muchos).
- Deberá ser compatible con NAT estático bidireccional 1-a-1.
- Deberá ser compatible con la traducción de puertos (PAT).
- Deberá ser compatible con NAT Origen.
- Deberá ser compatible con NAT de destino.
- Deberá soportar NAT de origen y NAT de destino de forma simultánea.
- Deberá soportar NAT de origen y NAT de destino en la misma política.
- Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.
- Tendrá que ser compatible con NAT64 y NAT46 e implementar el protocolo ECMP.
- Deberá soportar SD-WAN de forma nativa.
- Deberá soportar el balanceo de enlace hash por IP de origen.
- Deberá soportar el balanceo de enlace por hash de IP de origen y destino.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO

1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá 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.
- Debe poder implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales.
- Permitirá 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, memo-ria, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
- Podrá enviar logs a sistemas de gestión externos simultáneamente.
- Tendrá la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.
- Podrá implementar la optimización del tráfico entre dos dispositivos.
- Para IPv4, deberá soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
- Para IPv6, deberá soportar enrutamiento estático y dinámico (OSPFv3).
- Deberá soportar OSPF graceful restart.
- Será compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
- Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster.
- La configuración de alta disponibilidad sincronizará: Sesiones.
- La configuración de alta disponibilidad sincronizará: Configuraciones, podrá incluir, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red.
- La configuración de alta disponibilidad deberá sincronizar: Las asociaciones de seguridad VPN.
- La configuración de alta disponibilidad deberá sincronizar: Tablas FIB.
- En modo HA (Modo de alta disponibilidad) permitirá la supervisión de fallos de enlace.
- Deberá soportar la creación de sistemas virtuales en el mismo equipo.
- Para una alta disponibilidad, el uso de clústeres virtuales será posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos.
- Permitirá 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.
- La solución de gestión será compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluirá, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.
- Deberá contar con control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Out-bound), deberá 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).
- Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

04 OCT 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

31 de 72

FOLIO INTERNO
No. 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- El tejido de seguridad podrá identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.
- La consola de administración deberá soportar como mínimo, inglés, español.
- La consola deberá soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.

Control por Política de Firewall.

- Deberá soportar controles de zona de seguridad.
- Deberá contar con políticas de control por puerto y protocolo.
- Deberá 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.
- Deberá contar con control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
- El Firewall podrá aplicar la inspección de control de aplicaciones, antivirus, filtrado web, fil-trado DNS, IPS directamente a las políticas de seguridad.
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet puedrán agregarse directamente a las políticas de firewall.
- Deberá 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.
- Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).
- Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, Ali-Cloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.
- Deberá soportar el protocolo estándar de la industria VXLAN.
- La solución permitirá la implementación sin asistencia de SD-WAN.
- En SD-WAN deberá soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN.
- La solución deberá soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

Control de Aplicación.

- El dispositivo de protección de red tendrá la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
- Podrá detectar miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El 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.
- Deberá reconoce al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, lin-ked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail 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;

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO
No 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Identificará el uso de tácticas evasivas, es decir, Tendrá 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.
- Para tráfico cifrado SSL, podrá descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
- Identificará el uso de tácticas evasivas a través de las comunicaciones cifradas.
- Deberá actualizar de la base de firmas de la aplicación de forma automática.
- Limitará el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos.
- Para mantener la seguridad de red eficiente deberá soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
- Permitirá 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.
- El fabricante podrá solicitar la inclusión de aplicaciones en su base de datos.
- Permitirá la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitiendo a Hangouts el chat, pero impedir la llamada de video.
- Permitirá la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Será posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- Será posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
- Será posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación.
- Será posible configurar Application Override seleccionando las aplicaciones individualmente.

Prevención de Amenazas.

- Para proteger el entorno contra los ataques, deberá contar con un módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
- Incluirá firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (anti-virus y anti-spyware).
- Las características de IPS y antivirus deberán 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.
- Sincronizará las firmas de IPS, antivirus, anti-spyware cuando se implemente en alta disponibilidad.
- Deberá 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.
- Permitirá el bloqueo de vulnerabilidades y exploits conocidos.
- Incluirá la protección contra ataques de denegación de servicio.

04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO № 1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, Análisis para detectar anomalías de protocolo, Tendrá los siguientes mecanismos de inspección IPS: Desfragmentación IP, Tendrá los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP, Tendrá los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets).
- Deberá ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
- Deberá detectar y bloquear los escaneos de puertos de origen.
- Deberá bloquear ataques realizados por gusanos (worms) conocidos.
- Deberá contar con firmas específicas para la mitigación de ataques DoS y DDoS.
- Deberá contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buf-fer overflow).
- Deberá permitir crear firmas personalizadas en la interfaz gráfica del producto.
- Deberá identificar y bloquear la comunicación con redes de bots.
- Deberá 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.
- Deberá ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Deberá 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.
- Los eventos deberán identificar el país que origen o la amenaza.
- Deberá incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- Deberá tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
- Deberá 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.
- Deberá proporcionar 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).

COMISIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

04 OCT. 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Identificación de Usuarios.

- Deberá 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.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basado en usuarios y grupos de usuarios.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basado 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.

FOLIO INTERNO
1695
DIRECCIÓN GENERAL DE PLANEACIÓN

- Deberá tener integración con RADIUS para identificar a los usuarios y grupos que Permitirán las políticas de granularidad / control basado en usuarios y grupos de usuarios.
- Deberá tener la integración LDAP para la identificación de los usuarios y grupos que Permitirán granularidad en las políticas/control basado en usuarios y grupos de usuarios.
- Deberá 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 autentificación residente en el equipo de seguridad (portal cautivo).
- Deberá soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que Permitirá una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios.
- Deberá implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
- Deberá permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
- Deberá incluir al menos dos tokens de forma nativa, lo que Permitirá la autenticación de dos factores;

Filtrado de URL.

- Deberá permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
- Deberá tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito.
- Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Deberá tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL.
- Deberá tener por lo menos 75 categorías de URL.
- Deberá tener la funcionalidad de exclusión de URLs por categoría.
- Deberá permitir página de bloqueo personalizada.
- Deberá permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).
- Además del Explicit Web Proxy, deberá soportar r proxy web transparente.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA

QoS Traffic Shaping.

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo sea excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere que la solución que, además de que deberá permitir o denegar dichas solicitudes, deberá 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.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo.

FOLIO INTER
1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluido, pero no limitado a Skype, BitTorrent, Azureus y YouTube.
- Deberá soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS deberá permitir la definición de tráfico con ancho de banda garantizado.
- En QoS deberá permitir la definición de tráfico con máximo ancho de banda.
- En QoS deberá permitir la definición de colas de prioridad.
- Deberá soportar marcación de paquetes DiffServ, incluso por aplicación.
- Deberá soportar la modificación de los valores de DSCP para Diffserv.
- Deberá soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
- Deberá soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

Filtro de Datos.

- Deberá permitir la creación de filtros para archivos y datos predefinidos.
- Los archivos deberán ser identificados por tamaño y tipo.
- Deberá permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones.
- Deberá soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
- Deberá soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos.
- Permitirá 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.

- Deberá soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países.
- Deberá permitir la visualización de los países de origen y destino en los registros de acceso.
- Deberá permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

VPN.

- Deberá soportar VPN de sitio-a-sitio y cliente-a-sitio.
- Deberá soportar VPN IPSec.
- Deberá soportar VPN SSL.
- La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
- La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
- La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
- Tendrá interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

FOLIO INTERNO 1695 DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.
- Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting.
- Deberá 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.
- Deberá 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.
- Deberá suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
- Deberá permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
- Deberá mantener una conexión segura con el portal durante la sesión.
- El agente de VPN SSL o IPSEC cliente-a-sitio deberá ser compatible con al menos Windows y Mac OS.

E. Suministro de 25 (veinticinco) equipos de seguridad lógica para el GEJ.

El proveedor participante deberá suministrar equipos de seguridad lógica y licenciamiento requerido por 24 meses para el GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de desempeño por equipo.

- El equipo deberá contar con un Throughput en Firewall tanto en IPv4 como en IPv6 de al menos 10 Gbps para paquetes UDP de 1518, 10 de 512 bytes y de 7 Gbps en paquetes UDP de 64 bytes.
- El equipo deberá contar con un Throughput VPN IPSEC de por lo menos 6 Gbps.
- El equipo deberá contar con un Throughput IPS de al menos 1 Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad protección ante amenazas de 900 Mbps.
- El equipo deberá contar con un Throughput en la funcionalidad NGFW de 1 Gbps.
- El equipo deberá soportar al menos 1.5 millones de Sesiones concurrentes.
- El equipo deberá soportar 45,000 nuevas sesiones por segundo.
- El equipo deberá contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 200 usuarios de VPN SSL.
- El equipo deberá generar al menos 2,500 VPN's IPSec Client to Gateway.
- El equipo deberá generar al menos 200 VPN's IPSec Gateway to Gateway
- El equipo deberá soportar la configuración de 5,000 políticas de firewall.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL 04 OCT. 2022 VALIDACIÓN TÉCNICA DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Características de Hardware por equipo.

- El equipo deberá contar con al menos 6 Interfaces GE RJ45.
- El equipo deberá contar con al menos 2 Interfaces GE RJ45 auxiliares que podrán ser utilizada con puerto LAN/WAN.
- El equipo deberá contar con al menos 2 Interfaces SFP.
- El equipo deberá soportar al menos 10 sistemas virtuales lógicos (contextos) por equipo.
- El equipo deberá contar con al menos 1 Interfaces RJ45 para gestión.
- El equipo deberá contar con al menos 1 puertos USB.
- El equipo deberá contar con capacidad de integrar fuentes redundantes.

FOLIO INTERNO
1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Licenciamiento.

Se deberán considerar las licencias necesarias por 24 meses para habilitar los servicios de IPS, servicio de protección avanzada anti malware, control de aplicaciones, filtrado web y de video y servicio de antispam. Soporte técnico 24x7, remplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Características Generales:

- La solución deberá 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.
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- Las funcionalidades de protección de red que conformarán la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.
- La plataforma deberá estar optimizada para análisis de contenido de aplicaciones en capa 7.
- Deberá incluir los cables de alimentación.
- La gestión del equipo deberá ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
- Los dispositivos de protección de red deberán soportar 4094 VLANs Tags 802.1q.
- Los dispositivos de protección de red deberán soportar agregación de enlaces 802.3ad y LACP.
- Los dispositivos de protección de red deberán soportar Policy based routing y policy based forwar-ding.
- Los dispositivos de protección de red deberán soportar encaminamiento de multicast (PIM-SM y PIM-DM).
- Los dispositivos de protección de red deberán soportar DHCP Relay.
- Los dispositivos de protección de red deberán soportar DHCP Server.
- Los dispositivos de protección de red deberán soportar sFlow.
- Los dispositivos de protección de red deberán soportar Jumbo Frames.
- Los dispositivos de protección de red deberán soportar sub-interfaces Ethernet lógicas.
- Deberá ser compatible con NAT dinámica (varios-a-1).
- Deberá ser compatible con NAT dinámica (muchos-a-muchos).
- Deberá soportar NAT estática (1-a-1).
- Deberá admitir NAT estática (muchos-a-muchos).
- Deberá ser compatible con NAT estático bidireccional 1-a-1.
- Deberá ser compatible con la traducción de puertos (PAT).
- Deberá ser compatible con NAT Origen.
- Deberá ser compatible con NAT de destino.
- Deberá soportar NAT de origen y NAT de destino de forma simultánea.
- Deberá soportar NAT de origen y NAT de destino en la misma política.
- Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.
- Tendrá que ser compatible con NAT64 y NAT46 e implementar el protocolo ECMP.
- Deberá soportar SD-WAN de forma nativa.
- Deberá soportar el balanceo de enlace hash por IP de origen.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO No. 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá soportar el balanceo de enlace por hash de IP de origen y destino.
- Deberá 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.
- Debe poder implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales.
- Permitirá 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, memo-ria, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
- Podrá enviar logs a sistemas de gestión externos simultáneamente.
- Tendrá la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.
- Podrá implementar la optimización del tráfico entre dos dispositivos.
- Para IPv4, deberá soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
- Para IPv6, deberá soportar enrutamiento estático y dinámico (OSPFv3).
- Deberá soportar OSPF graceful restart.
- Será compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
- Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster.
- La configuración de alta disponibilidad sincronizará: Sesiones.
- La configuración de alta disponibilidad sincronizará: Configuraciones, podrá incluir, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red.
- La configuración de alta disponibilidad deberá sincronizar: Las asociaciones de seguridad VPN.
- La configuración de alta disponibilidad deberá sincronizar: Tablas FIB.
- En modo HA (Modo de alta disponibilidad) permitirá la supervisión de fallos de enlace.
- Deberá soportar la creación de sistemas virtuales en el mismo equipo.
- Para una alta disponibilidad, el uso de clústeres virtuales será posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos.
- Permitirá 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.
- La solución de gestión será compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluirá, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.
- Deberá contar con control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Out-bound), deberá 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).

04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

FOLIO No. 1695

DIRECCIÓN GENERAL DE TECNOLOGÍAS

- Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red.
- El tejido de seguridad podrá identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.
- La consola de administración deberá soportar como mínimo, inglés, español.
- La consola deberá soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.

Control por Política de Firewall.

- Deberá soportar controles de zona de seguridad.
- Deberá contar con políticas de control por puerto y protocolo.
- Deberá 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.
- Deberá contar con control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
- El Firewall podrá aplicar la inspección de control de aplicaciones, antivirus, filtrado web, fil-trado DNS, IPS directamente a las políticas de seguridad.
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet puedrán agregarse directamente a las políticas de firewall.
- Deberá 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.
- Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).
- Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, Ali-Cloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.
- Deberá soportar el protocolo estándar de la industria VXLAN.
- La solución permitirá la implementación sin asistencia de SD-WAN.
- En SD-WAN deberá soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN.
- La solución deberá soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

COORDINACIÓN GENERAL DE MODERNIZACIÓN GUBERNAMENTAL

04 OCT. 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Control de Aplicación.

- El dispositivo de protección de red tendrá la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
- Podrá detectar miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El 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.
- Deberá reconoce al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, lin-ked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active

FOLIO INTERNO Nº 1695 DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

- Identificará el uso de tácticas evasivas, es decir, Tendrá 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.
- Para tráfico cifrado SSL, podrá descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
- Identificará el uso de tácticas evasivas a través de las comunicaciones cifradas.
- Deberá actualizar de la base de firmas de la aplicación de forma automática.
- Limitará el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos.
- Para mantener la seguridad de red eficiente deberá soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
- Permitirá 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.
- El fabricante podrá solicitar la inclusión de aplicaciones en su base de datos.
- Permitirá la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitiendo a Hangouts el chat, pero impedir la llamada de video.
- Permitirá la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Será posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- Será posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
- Será posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación.
- Será posible configurar Application Override seleccionando las aplicaciones individualmente.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL 04 OCT. 2022 VALIDACIÓN TÉCNICA DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Prevención de Amenazas.

- Para proteger el entorno contra los ataques, deberá contar con un módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
- Incluirá firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (anti-virus y anti-spyware).
- Las características de IPS y antivirus deberán 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.
- Sincronizará las firmas de IPS, antivirus, anti-spyware cuando se implemente en alta disponibilidad.
- Deberá 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.

FOLIO INTERNO 1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Permitirá el bloqueo de vulnerabilidades y exploits conocidos.
- Incluirá la protección contra ataques de denegación de servicio.
- Deberá tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, Análisis para detectar anomalías de protocolo, Tendrá los siguientes mecanismos de inspección IPS: Desfragmentación IP, Tendrá los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP, Tendrá los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets).
- Deberá ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
- Deberá detectar y bloquear los escaneos de puertos de origen.
- Deberá bloquear ataques realizados por gusanos (worms) conocidos.
- Deberá contar con firmas específicas para la mitigación de ataques DoS y DDoS.
- Deberá contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buf-fer overflow).
- Deberá permitir crear firmas personalizadas en la interfaz gráfica del producto.
- Deberá identificar y bloquear la comunicación con redes de bots.
- Deberá 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.
- Deberá ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Deberá 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.
- Los eventos deberán identificar el país que origen o la amenaza.
- Deberá incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- Deberá tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
- Deberá 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.
- Deberá proporcionar 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).

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

04 OCT. 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Identificación de Usuarios.

- Deberá 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.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basado en usuarios y grupos de usuarios.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basado en usuarios y grupos de usuarios, soporte a

FOLIO INTERNO № 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

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.

- Deberá tener integración con RADIUS para identificar a los usuarios y grupos que Permitirán las políticas de granularidad / control basado en usuarios y grupos de usuarios.
- Deberá tener la integración LDAP para la identificación de los usuarios y grupos que Permitirán granularidad en las políticas/control basado en usuarios y grupos de usuarios.
- Deberá 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 autentificación residente en el equipo de seguridad (portal cautivo).
- Deberá soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que Permitirá una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios.
- Deberá implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
- Deberá permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
- Deberá incluir al menos dos tokens de forma nativa, lo que Permitirá la autenticación de dos factores;

Filtrado de URL.

- Deberá permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
- Deberá tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito.
- Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Deberá tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL.
- Deberá tener por lo menos 75 categorías de URL.
- Deberá tener la funcionalidad de exclusión de URLs por categoría.
- Deberá permitir página de bloqueo personalizada.
- Deberá permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).
- Además del Explicit Web Proxy, deberá soportar r proxy web transparente.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

QoS Traffic Shaping.

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo sea excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere que la solución que, además de que deberá permitir o denegar dichas solicitudes, deberá 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.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo.

FOLIO INTERNO № 1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluido, pero no limitado a Skype, BitTorrent, Azureus y YouTube.
- Deberá soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS deberá permitir la definición de tráfico con ancho de banda garantizado.
- En QoS deberá permitir la definición de tráfico con máximo ancho de banda.
- En QoS deberá permitir la definición de colas de prioridad.
- Deberá soportar marcación de paquetes DiffServ, incluso por aplicación.
- Deberá soportar la modificación de los valores de DSCP para Diffserv.
- Deberá soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
- Deberá soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

Filtro de Datos.

- Deberá permitir la creación de filtros para archivos y datos predefinidos.
- Los archivos deberán ser identificados por tamaño y tipo.
- Deberá permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones.
- Deberá soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
- Deberá soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos.
- Permitirá 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.

- Deberá soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países.
- Deberá permitir la visualización de los países de origen y destino en los registros de acceso.
- Deberá permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

VPN.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

04 OCT. 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá soportar VPN de sitio-a-sitio y cliente-a-sitio.
- Deberá soportar VPN IPSec.
- Deberá soportar VPN SSL.
- La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
- La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
- La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
- Tendrá interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
- Deberá soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.

FOLIO INTERNO Nº 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting.
- Deberá 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.
- Deberá 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.
- Deberá suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
- Deberá permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
- Deberá mantener una conexión segura con el portal durante la sesión.
- El agente de VPN SSL o IPSEC cliente-a-sitio deberá ser compatible con al menos Windows y Mac OS.

F. Suministro de 20 (veinte) equipos de seguridad lógica para el GEJ.

El proveedor participante deberá suministrar equipos de seguridad lógica y licenciamiento requerido por 24 meses para el GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de desempeño por equipo.

- El equipo deberá contar con un Throughput en Firewall tanto en IPv4 como en IPv6 de al menos 10 Gbps para paquetes UDP de 1518, 10 de 512 bytes y de 7 Gbps en paquetes UDP de 64 bytes.
- El equipo deberá contar con un Throughput VPN IPSEC de por lo menos 6 Gbps.
- El equipo deberá contar con un Throughput IPS de al menos 1 Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad protección ante amenazas de 900 Mbps.
- El equipo deberá contar con un Throughput en la funcionalidad NGFW de 1 Gbps.
- El equipo deberá soportar al menos 1.5 millones de Sesiones concurrentes.
- El equipo deberá soportar 45,000 nuevas sesiones por segundo.
- El equipo deberá contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 200 usuarios de VPN SSL.
- El equipo deberá generar al menos 2,500 VPN's IPSec Client to Gateway.
- El equipo deberá generar al menos 200 VPN's IPSec Gateway to Gateway.
- El equipo deberá soportar la configuración de 5,000 políticas de firewall.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Características de Hardware por equipo.

- El equipo deberá contar con al menos 6 Interfaces GE RJ45.
- El equipo deberá contar con al menos 2 Interfaces GE RJ45 auxiliares que podrán ser utilizada con puerto LAN/WAN.
- El equipo deberá contar con al menos 2 Interfaces SFP.
- El equipo deberá soportar al menos 10 sistemas virtuales lógicos (contextos) por equipo.
- El equipo deberá contar con al menos 1 Interfaces RJ45 para gestión.
- El equipo deberá contar con al menos 1 puertos USB.
- El equipo deberá contar con capacidad de integrar fuentes redundantes.

Licenciamiento.

FOLIO INTERNO
1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Se deberán considerar las licencias necesarias por 24 meses para habilitar los servicios de IPS, servicio de protección avanzada anti malware y control de aplicaciones. Soporte técnico 24x7, remplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Características Generales:

- La solución deberá 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.
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- Las funcionalidades de protección de red que conformarán la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.
- La plataforma deberá estar optimizada para análisis de contenido de aplicaciones en capa 7.
- Deberá incluir los cables de alimentación.
- La gestión del equipo deberá ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
- Los dispositivos de protección de red deberán soportar 4094 VLANs Tags 802.1q.
- Los dispositivos de protección de red deberán soportar agregación de enlaces 802.3ad y LACP.
- Los dispositivos de protección de red deberán soportar Policy based routing y policy based forwar-ding.
- Los dispositivos de protección de red deberán soportar encaminamiento de multicast (PIM-SM y PIM-DM).
- Los dispositivos de protección de red deberán soportar DHCP Relay.
- Los dispositivos de protección de red deberán soportar DHCP Server.
- Los dispositivos de protección de red deberán soportar sFlow.
- Los dispositivos de protección de red deberán soportar Jumbo Frames.
- Los dispositivos de protección de red deberán soportar sub-interfaces Ethernet lógicas.
- Deberá ser compatible con NAT dinámica (varios-a-1).
- Deberá ser compatible con NAT dinámica (muchos-a-muchos).
- Deberá soportar NAT estática (1-a-1).
- Deberá admitir NAT estática (muchos-a-muchos).
- Deberá ser compatible con NAT estático bidireccional 1-a-1.
- Deberá ser compatible con la traducción de puertos (PAT).
- Deberá ser compatible con NAT Origen.
- Deberá ser compatible con NAT de destino.
- Deberá soportar NAT de origen y NAT de destino de forma simultánea.
- Deberá soportar NAT de origen y NAT de destino en la misma política.
- Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.
- Tendrá que ser compatible con NAT64 y NAT46 e implementar el protocolo ECMP.
- Deberá soportar SD-WAN de forma nativa.
- Deberá soportar el balanceo de enlace hash por IP de origen.
- Deberá soportar el balanceo de enlace por hash de IP de origen y destino.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá 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.
- Debe poder implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales.
- Permitirá 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, memo-ria, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
- Podrá enviar logs a sistemas de gestión externos simultáneamente.
- Tendrá la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.
- Podrá implementar la optimización del tráfico entre dos dispositivos.
- Para IPv4, deberá soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
- Para IPv6, deberá soportar enrutamiento estático y dinámico (OSPFv3).
- Deberá soportar OSPF graceful restart.
- Será compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
- Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster.
- La configuración de alta disponibilidad sincronizará: Sesiones.
- La configuración de alta disponibilidad sincronizará: Configuraciones, podrá incluir, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red.
- La configuración de alta disponibilidad deberá sincronizar: Las asociaciones de seguridad VPN.
- La configuración de alta disponibilidad deberá sincronizar: Tablas FIB.
- En modo HA (Modo de alta disponibilidad) permitirá la supervisión de fallos de enlace.
- Deberá soportar la creación de sistemas virtuales en el mismo equipo.
- Para una alta disponibilidad, el uso de clústeres virtuales será posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos.
- Permitirá 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.
- La solución de gestión será compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluirá, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.
- Deberá contar con control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Out-bound), deberá 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).
- Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red.

GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- El tejido de seguridad podrá identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.
- La consola de administración deberá soportar como mínimo, inglés, español.
- La consola deberá soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.

Control por Política de Firewall.

- Deberá soportar controles de zona de seguridad.
- Deberá contar con políticas de control por puerto y protocolo.
- Deberá 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.
- Deberá contar con control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
- El Firewall podrá aplicar la inspección de control de aplicaciones, antivirus, filtrado web, fil-trado DNS, IPS directamente a las políticas de seguridad.
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet puedrán agregarse directamente a las políticas de firewall.
- Deberá 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.
- Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).
- Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, Ali-Cloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.
- Deberá soportar el protocolo estándar de la industria VXLAN.
- La solución permitirá la implementación sin asistencia de SD-WAN.
- En SD-WAN deberá soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN.
- La solución deberá soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Control de Aplicación.

- El dispositivo de protección de red tendrá la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
- Podrá detectar miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El 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.
- Deberá reconoce al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, lin-ked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail 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;

Av. Fray Antonio Alcalde#1221,
Col. Miraflores, C.P. 44270,
Guadalajara, Jalisco, México

FOLIO INTERNO
No. 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Identificará el uso de tácticas evasivas, es decir, Tendrá 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.
- Para tráfico cifrado SSL, podrá descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
- Identificará el uso de tácticas evasivas a través de las comunicaciones cifradas.
- Deberá actualizar de la base de firmas de la aplicación de forma automática.
- Limitará el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos.
- Para mantener la seguridad de red eficiente deberá soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
- Permitirá 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.
- El fabricante podrá solicitar la inclusión de aplicaciones en su base de datos.
- Permitirá la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitiendo a Hangouts el chat, pero impedir la llamada de video.
- Permitirá la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Será posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- Será posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
- Será posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación.
- Será posible configurar Application Override seleccionando las aplicaciones individualmente.

Prevención de Amenazas.

- Para proteger el entorno contra los ataques, deberá contar con un módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
- Incluirá firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (anti-virus y anti-spyware).
- Las características de IPS y antivirus deberán 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.
- Sincronizará las firmas de IPS, antivirus, anti-spyware cuando se implemente en alta disponibilidad.
- Deberá 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.
- Permitirá el bloqueo de vulnerabilidades y exploits conocidos.
- Incluirá la protección contra ataques de denegación de servicio.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN

- Deberá tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, Análisis para detectar anomalías de protocolo, Tendrá los siguientes mecanismos de inspección IPS: Desfragmentación IP, Tendrá los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP, Tendrá los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets).
- Deberá ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
- Deberá detectar y bloquear los escaneos de puertos de origen.
- Deberá bloquear ataques realizados por gusanos (worms) conocidos.
- Deberá contar con firmas específicas para la mitigación de ataques DoS y DDoS.
- Deberá contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buf-fer overflow).
- Deberá permitir crear firmas personalizadas en la interfaz gráfica del producto.
- Deberá identificar y bloquear la comunicación con redes de bots.
- Deberá 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.
- Deberá ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Deberá 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.
- Los eventos deberán identificar el país que origen o la amenaza.
- Deberá incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- Deberá tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
- Deberá 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.
- Deberá proporcionar 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).

04 OCT. 2022
VALIDACIÓN TÉCNICA

Identificación de Usuarios.

- Deberá 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.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basado en usuarios y grupos de usuarios.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basado 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.

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE TECNOLOGÍA

- Deberá tener integración con RADIUS para identificar a los usuarios y grupos que Permitirán las políticas de granularidad / control basado en usuarios y grupos de usuarios.
- Deberá tener la integración LDAP para la identificación de los usuarios y grupos que Permitirán granularidad en las políticas/control basado en usuarios y grupos de usuarios.
- Deberá 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 autentificación residente en el equipo de seguridad (portal cautivo).
- Deberá soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que Permitirá una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios.
- Deberá implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
- Deberá permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
- Deberá incluir al menos dos tokens de forma nativa, lo que Permitirá la autenticación de dos factores;

Filtrado de URL.

- Deberá permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
- Deberá tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito.
- Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Deberá tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL.
- Deberá tener por lo menos 75 categorías de URL.
- Deberá tener la funcionalidad de exclusión de URLs por categoría.
- Deberá permitir página de bloqueo personalizada.
- Deberá permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).
- Además del Explicit Web Proxy, deberá soportar r proxy web transparente.

GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA

QoS Traffic Shaping.

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo sea excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere que la solución que, además de que deberá permitir o denegar dichas solicitudes, deberá 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.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo.

FOLIO INTERNO
No. 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluido, pero no limitado a Skype, BitTorrent, Azureus y YouTube.
- Deberá soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS deberá permitir la definición de tráfico con ancho de banda garantizado.
- En QoS deberá permitir la definición de tráfico con máximo ancho de banda.
- En QoS deberá permitir la definición de colas de prioridad.
- Deberá soportar marcación de paquetes DiffServ, incluso por aplicación.
- Deberá soportar la modificación de los valores de DSCP para Diffserv.
- Deberá soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
- Deberá soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

Filtro de Datos.

- Deberá permitir la creación de filtros para archivos y datos predefinidos.
- Los archivos deberán ser identificados por tamaño y tipo.
- Deberá permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones.
- Deberá soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
- Deberá soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos.
- Permitirá 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.

- Deberá soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países.
- Deberá permitir la visualización de los países de origen y destino en los registros de acceso.
- Deberá permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

VPN.

- Deberá soportar VPN de sitio-a-sitio y cliente-a-sitio.
- Deberá soportar VPN IPSec.
- Deberá soportar VPN SSL.
- La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
- La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
- La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
- Tendrá interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.
- Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting.
- Deberá 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.
- Deberá 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.
- Deberá suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
- Deberá permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
- Deberá mantener una conexión segura con el portal durante la sesión.
- El agente de VPN SSL o IPSEC cliente-a-sitio deberá ser compatible con al menos Windows y Mac OS.

G. Suministro de 150 (ciento cincuenta) equipos de seguridad lógica para el GEJ.

El proveedor participante deberá suministrar equipos de seguridad lógica y licenciamiento requerido por 24 meses para el GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de desempeño por equipo.

- El equipo deberá contar con un Throughput en Firewall tanto en IPv4 como en IPv6 de al menos 5 Gbps para paquetes UDP de 1518, 5 de 512 bytes y de 5 Gbps en paquetes UDP de 64 bytes.
- El equipo deberá contar con un Throughput VPN IPSEC de por lo menos 4 Gbps.
- El equipo deberá contar con un Throughput IPS de al menos 1 Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad protección ante amenazas de 600 Mbps.
- El equipo deberá contar con un Throughput en la funcionalidad NGFW de 800 Mbps.
- El equipo deberá soportar al menos 700,000 sesiones concurrentes.
- El equipo deberá soportar 35,000 nuevas sesiones por segundo.
- El equipo deberá contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 200 usuarios de VPN SSL.
- El equipo deberá generar al menos 250 VPN's IPSec Client to Gateway.
- El equipo deberá generar al menos 200 VPN's IPSec Gateway to Gateway.
- El equipo deberá soportar la configuración de 5,000 políticas de firewall.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Características de Hardware por equipo.

- El equipo deberá contar con al menos 3 Interfaces GE RJ45.
- El equipo deberá contar con al menos 1 Interface WAN.
- El equipo deberá contar con al menos 1 Interface auxiliar que podrá ser utilizada con puerto LAN/WAN.
- El equipo deberá soportar al menos 10 sistemas virtuales lógicos (contextos) por dispositivo.
- El equipo deberá contar con al menos 1 puertos USB.
- El equipo deberá contar con al menos 1 Interfaz RJ45 gestión por consola.

Licenciamiento.

Jefatura de Gabinete FOLIO INTERNO 1695 DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Se deberán considerar las licencias necesarias por 24 meses para habilitar los servicios de IPS, servicio de protección avanzada anti malware, control de aplicaciones, filtrado web y de video y servicio de antispam. Soporte técnico 24x7, remplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Características Generales:

- La solución deberá 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.
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- Las funcionalidades de protección de red que conformarán la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.
- La plataforma deberá estar optimizada para análisis de contenido de aplicaciones en capa 7.
- Deberá incluir los cables de alimentación.
- La gestión del equipo deberá ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
- Los dispositivos de protección de red deberán soportar 4094 VLANs Tags 802.1q.
- Los dispositivos de protección de red deberán soportar agregación de enlaces 802.3ad y LACP.
- Los dispositivos de protección de red deberán soportar Policy based routing y policy based forwar-ding.
- Los dispositivos de protección de red deberán soportar encaminamiento de multicast (PIM-SM y PIM-DM).
- Los dispositivos de protección de red deberán soportar DHCP Relay.
- Los dispositivos de protección de red deberán soportar DHCP Server.
- Los dispositivos de protección de red deberán soportar sFlow.
- Los dispositivos de protección de red deberán soportar Jumbo Frames.
- Los dispositivos de protección de red deberán soportar sub-interfaces Ethernet lógicas.
- Deberá ser compatible con NAT dinámica (varios-a-1).
- Deberá ser compatible con NAT dinámica (muchos-a-muchos).
- Deberá soportar NAT estática (1-a-1).
- Deberá admitir NAT estática (muchos-a-muchos).
- Deberá ser compatible con NAT estático bidireccional 1-a-1.
- Deberá ser compatible con la traducción de puertos (PAT).
- Deberá ser compatible con NAT Origen.
- Deberá ser compatible con NAT de destino.
- Deberá soportar NAT de origen y NAT de destino de forma simultánea.
- Deberá soportar NAT de origen y NAT de destino en la misma política.
- Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.
- Tendrá que ser compatible con NAT64 y NAT46 e implementar el protocolo ECMP.
- Deberá soportar SD-WAN de forma nativa.
- Deberá soportar el balanceo de enlace hash por IP de origen.
- Deberá soportar el balanceo de enlace por hash de IP de origen y destino.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL 04 OCT. 2022 VALIDACIÓN TÉCNICA DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá 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.
- Debe poder implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales.
- Permitirá 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, memo-ria, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
- Podrá enviar logs a sistemas de gestión externos simultáneamente.
- Tendrá la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.
- Podrá implementar la optimización del tráfico entre dos dispositivos.
- Para IPv4, deberá soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
- Para IPv6, deberá soportar enrutamiento estático y dinámico (OSPFv3).
- Deberá soportar OSPF graceful restart.
- Será compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
- Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster.
- La configuración de alta disponibilidad sincronizará: Sesiones.
- La configuración de alta disponibilidad sincronizará: Configuraciones, podrá incluir, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red.
- La configuración de alta disponibilidad deberá sincronizar: Las asociaciones de seguridad VPN.
- La configuración de alta disponibilidad deberá sincronizar: Tablas FIB.
- En modo HA (Modo de alta disponibilidad) permitirá la supervisión de fallos de enlace.
- Deberá soportar la creación de sistemas virtuales en el mismo equipo.
- Para una alta disponibilidad, el uso de clústeres virtuales será posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos.
- Permitirá 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.
- La solución de gestión será compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluirá, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.
- Deberá contar con control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Out-bound), deberá 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).
- Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red.

COORDINACIÓN GENERAL DE INNOVACIÓN
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO
Nº 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- El tejido de seguridad podrá identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.
- La consola de administración deberá soportar como mínimo, inglés, español.
- La consola deberá soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.

Control por Política de Firewall.

- Deberá soportar controles de zona de seguridad.
- Deberá contar con políticas de control por puerto y protocolo.
- Deberá 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.
- Deberá contar con control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
- El Firewall podrá aplicar la inspección de control de aplicaciones, antivirus, filtrado web, fil-trado DNS, IPS directamente a las políticas de seguridad.
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet puedrán agregarse directamente a las políticas de firewall.
- Deberá 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.
- Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).
- Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, Ali-Cloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.
- Deberá soportar el protocolo estándar de la industria VXLAN.
- La solución permitirá la implementación sin asistencia de SD-WAN.
- En SD-WAN deberá soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN.
- La solución deberá soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Control de Aplicación.

- El dispositivo de protección de red tendrá la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
- Podrá detectar miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El 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.
- Deberá reconoce al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, lin-ked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail 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;

FOLIO INTERNO № 1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Identificará el uso de tácticas evasivas, es decir, Tendrá 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.
- Para tráfico cifrado SSL, podrá descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
- Identificará el uso de tácticas evasivas a través de las comunicaciones cifradas.
- Deberá actualizar de la base de firmas de la aplicación de forma automática.
- Limitará el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos.
- Para mantener la seguridad de red eficiente deberá soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
- Permitirá 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.
- El fabricante podrá solicitar la inclusión de aplicaciones en su base de datos.
- Permitirá la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitiendo a Hangouts el chat, pero impedir la llamada de video.
- Permitirá la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Será posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- Será posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
- Será posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación.
- Será posible configurar Application Override seleccionando las aplicaciones individualmente.

Prevención de Amenazas.

- Para proteger el entorno contra los ataques, deberá contar con un módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
- Incluirá firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (anti-virus y anti-spyware).
- Las características de IPS y antivirus deberán 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.
- Sincronizará las firmas de IPS, antivirus, anti-spyware cuando se implemente en alta disponibilidad.
- Deberá 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.
- Permitirá el bloqueo de vulnerabilidades y exploits conocidos.
- Incluirá la protección contra ataques de denegación de servicio.

04 OCT. 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO № 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, Análisis para detectar anomalías de protocolo, Tendrá los siguientes mecanismos de inspección IPS: Desfragmentación IP, Tendrá los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP, Tendrá los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato Incorrecto (malformed packets).
- Deberá ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
- Deberá detectar y bloquear los escaneos de puertos de origen.
- Deberá bloquear ataques realizados por gusanos (worms) conocidos.
- Deberá contar con firmas específicas para la mitigación de ataques DoS y DDoS.
- Deberá contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buf-fer overflow).
- Deberá permitir crear firmas personalizadas en la interfaz gráfica del producto.
- Deberá identificar y bloquear la comunicación con redes de bots.
- Deberá 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.
- Deberá ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Deberá 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.
- Los eventos deberán identificar el país que origen o la amenaza.
- Deberá incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- Deberá tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
- Deberá 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.
- Deberá proporcionar 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).

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Identificación de Usuarios.

- Deberá 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.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basado en usuarios y grupos de usuarios.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basado 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.

FOLIO INTERNO No 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá tener integración con RADIUS para identificar a los usuarios y grupos que Permitirán las políticas de granularidad / control basado en usuarios y grupos de usuarios.
- Deberá tener la integración LDAP para la identificación de los usuarios y grupos que Permitirán granularidad en las políticas/control basado en usuarios y grupos de usuarios.
- Deberá 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 autentificación residente en el equipo de seguridad (portal cautivo).
- Deberá soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que Permitirá una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios.
- Deberá implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
- Deberá permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
- Deberá incluir al menos dos tokens de forma nativa, lo que Permitirá la autenticación de dos factores;

Filtrado de URL.

- Deberá permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
- Deberá tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito.
- Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Deberá tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL.
- Deberá tener por lo menos 75 categorías de URL.
- Deberá tener la funcionalidad de exclusión de URLs por categoría.
- Deberá permitir página de bloqueo personalizada.
- Deberá permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).
- Además del Explicit Web Proxy, deberá soportar r proxy web transparente.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

QoS Traffic Shaping.

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo sea excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere que la solución que, además de que deberá permitir o denegar dichas solicitudes, deberá 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.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo.

FOLIO INTERNO
1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluido, pero no limitado a Skype, BitTorrent, Azureus y YouTube.
- Deberá soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS deberá permitir la definición de tráfico con ancho de banda garantizado.
- En QoS deberá permitir la definición de tráfico con máximo ancho de banda.
- En QoS deberá permitir la definición de colas de prioridad.
- Deberá soportar marcación de paquetes DiffServ, incluso por aplicación.
- Deberá soportar la modificación de los valores de DSCP para Diffserv.
- Deberá soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
- Deberá soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

Filtro de Datos.

- Deberá permitir la creación de filtros para archivos y datos predefinidos.
- Los archivos deberán ser identificados por tamaño y tipo.
- Deberá permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones.
- Deberá soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
- Deberá soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos.
- Permitirá 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.

- Deberá soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países.
- Deberá permitir la visualización de los países de origen y destino en los registros de acceso.
- Deberá permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

VPN.

- Deberá soportar VPN de sitio-a-sitio y cliente-a-sitio.
- Deberá soportar VPN IPSec.
- Deberá soportar VPN SSL.
- La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
- La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
- La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
- Tendrá interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
- Deberá soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.

Jefatura de Gabinete FOLIO No. 1395

- Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting.
- Deberá 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.
- Deberá 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.
- Deberá suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
- Deberá permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
- Deberá mantener una conexión segura con el portal durante la sesión.
- El agente de VPN SSL o IPSEC cliente-a-sitio deberá ser compatible con al menos Windows y Mac OS.

H. Suministro de 30 (treinta) equipos de seguridad lógica para el GEJ.

El proveedor participante deberá suministrar equipos de seguridad lógica y licenciamiento requerido por 24 meses para el GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de desempeño por equipo.

- El equipo deberá contar con un Throughput en Firewall tanto en IPv4 como en IPv6 de al menos 5 Gbps para paquetes UDP de 1518, 5 de 512 bytes y de 5 Gbps en paquetes UDP de 64 bytes.
- El equipo deberá contar con un Throughput VPN IPSEC de por lo menos 4 Gbps.
- El equipo deberá contar con un Throughput IPS de al menos 1 Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad protección ante amenazas de 600 Mbps.
- El equipo deberá contar con un Throughput en la funcionalidad NGFW de 800 Mbps.
- El equipo deberá soportar al menos 700,000 sesiones concurrentes.
- El equipo deberá soportar 35,000 nuevas sesiones por segundo.
- El equipo deberá contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 200 usuarios de VPN SSL.
- El equipo deberá generar al menos 250 VPN's IPSec Client to Gateway.
- El equipo deberá generar al menos 200 VPN's IPSec Gateway to Gateway.
- El equipo deberá soportar la configuración de 5,000 políticas de firewall.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Características de Hardware por equipo.

- El equipo deberá contar con al menos 3 Interfaces GE RJ45.
- El equipo deberá contar con al menos 1 Interface WAN.
- El equipo deberá contar con al menos 1 Interface auxiliar que podrá ser utilizada con puerto LAN/WAN.
- El equipo deberá soportar al menos 10 sistemas virtuales lógicos (contextos) por dispositivo.
- El equipo deberá contar con al menos 1 puertos USB.
- El equipo deberá contar con al menos 1 Interfaz RJ45 gestión por consola.

Licenciamiento.

FOLIO INTERNO № 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Se deberán considerar las licencias necesarias por 24 meses para habilitar los servicios de IPS, servicio de protección avanzada anti malware y control de aplicaciones. Soporte técnico 24x7, remplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Características Generales:

- La solución deberá 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.
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- Las funcionalidades de protección de red que conformarán la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.
- La plataforma deberá estar optimizada para análisis de contenido de aplicaciones en capa 7.
- Deberá incluir los cables de alimentación.
- La gestión del equipo deberá ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
- Los dispositivos de protección de red deberán soportar 4094 VLANs Tags 802.1q.
- Los dispositivos de protección de red deberán soportar agregación de enlaces 802.3ad y LACP.
- Los dispositivos de protección de red deberán soportar Policy based routing y policy based forwar-ding.
- Los dispositivos de protección de red deberán soportar encaminamiento de multicast (PIM-SM y PIM-DM).
- Los dispositivos de protección de red deberán soportar DHCP Relay.
- Los dispositivos de protección de red deberán soportar DHCP Server.
- Los dispositivos de protección de red deberán soportar sFlow.
- Los dispositivos de protección de red deberán soportar Jumbo Frames.
- Los dispositivos de protección de red deberán soportar sub-interfaces Ethernet lógicas.
- Deberá ser compatible con NAT dinámica (varios-a-1).
- Deberá ser compatible con NAT dinámica (muchos-a-muchos).
- Deberá soportar NAT estática (1-a-1).
- Deberá admitir NAT estática (muchos-a-muchos).
- Deberá ser compatible con NAT estático bidireccional 1-a-1.
- Deberá ser compatible con la traducción de puertos (PAT).
- Deberá ser compatible con NAT Origen.
- Deberá ser compatible con NAT de destino.
- Deberá soportar NAT de origen y NAT de destino de forma simultánea.
- Deberá soportar NAT de origen y NAT de destino en la misma política.
- Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.
- Tendrá que ser compatible con NAT64 y NAT46 e implementar el protocolo ECMP.
- Deberá soportar SD-WAN de forma nativa.
- Deberá soportar el balanceo de enlace hash por IP de origen.
- Deberá soportar el balanceo de enlace por hash de IP de origen y destino.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO Nº 1695

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá 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.
- Debe poder implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales.
- Permitirá 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, memo-ria, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
- Podrá enviar logs a sistemas de gestión externos simultáneamente.
- Tendrá la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.
- Podrá implementar la optimización del tráfico entre dos dispositivos.
- Para IPv4, deberá soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
- Para IPv6, deberá soportar enrutamiento estático y dinámico (OSPFv3).
- Deberá soportar OSPF graceful restart.
- Será compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
- Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
- Deberá soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster.
- La configuración de alta disponibilidad sincronizará: Sesiones.
- La configuración de alta disponibilidad sincronizará: Configuraciones, podrá incluir, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red.
- La configuración de alta disponibilidad deberá sincronizar: Las asociaciones de seguridad VPN.
- La configuración de alta disponibilidad deberá sincronizar: Tablas FIB.
- En modo HA (Modo de alta disponibilidad) permitirá la supervisión de fallos de enlace.
- Deberá soportar la creación de sistemas virtuales en el mismo equipo.
- Para una alta disponibilidad, el uso de clústeres virtuales será posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos.
- Permitirá 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.
- La solución de gestión será compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluirá, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.
- Deberá contar con control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Out-bound), deberá 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).
- Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

04 OCT. 2022

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO
1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- El tejido de seguridad podrá identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.
- La consola de administración deberá soportar como mínimo, inglés, español.
- La consola deberá soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.

Control por Política de Firewall.

- Deberá soportar controles de zona de seguridad.
- Deberá contar con políticas de control por puerto y protocolo.
- Deberá 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.
- Deberá contar con control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
- El Firewall podrá aplicar la inspección de control de aplicaciones, antivirus, filtrado web, fil-trado DNS, IPS directamente a las políticas de seguridad.
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet puedrán agregarse directamente a las políticas de firewall.
- Deberá 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.
- Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).
- Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, Ali-Cloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.
- Deberá soportar el protocolo estándar de la industria VXLAN.
- La solución permitirá la implementación sin asistencia de SD-WAN.
- En SD-WAN deberá soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN.
- La solución deberá soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

Control de Aplicación.

- El dispositivo de protección de red tendrá la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
- Podrá detectar miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El 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.
- Deberá reconoce al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, lin-ked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail 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;

04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO IN... Nº 1695 DIRECCIÓN GENERAL DE P... TECNOLÓGICA

- Identificará el uso de tácticas evasivas, es decir, Tendrá 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.
- Para tráfico cifrado SSL, podrá descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
- Identificará el uso de tácticas evasivas a través de las comunicaciones cifradas.
- Deberá actualizar de la base de firmas de la aplicación de forma automática.
- Limitará el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos.
- Para mantener la seguridad de red eficiente deberá soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
- Permitirá 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.
- El fabricante podrá solicitar la inclusión de aplicaciones en su base de datos.
- Permitirá la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Permitirá la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitiendo a Hangouts el chat, pero impedir la llamada de video.
- Permitirá la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Será posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- Será posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
- Será posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación.
- Será posible configurar Application Override seleccionando las aplicaciones individualmente.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Prevención de Amenazas.

- Para proteger el entorno contra los ataques, deberá contar con un módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
- Incluirá firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (anti-virus y anti-spyware).
- Las características de IPS y antivirus deberán 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.
- Sincronizará las firmas de IPS, antivirus, anti-spyware cuando se implemente en alta disponibilidad.
- Deberá 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.
- Permitirá el bloqueo de vulnerabilidades y exploits conocidos.
- Incluirá la protección contra ataques de denegación de servicio.

FOLIO INTERNO # 1695 DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, Análisis para detectar anomalías de protocolo, Tendrá los siguientes mecanismos de inspección IPS: Desfragmentación IP, Tendrá los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP, Tendrá los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets).
- Deberá ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
- Deberá detectar y bloquear los escaneos de puertos de origen.
- Deberá bloquear ataques realizados por gusanos (worms) conocidos.
- Deberá contar con firmas específicas para la mitigación de ataques DoS y DDoS.
- Deberá contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buf-fer overflow).
- Deberá permitir crear firmas personalizadas en la interfaz gráfica del producto.
- Deberá identificar y bloquear la comunicación con redes de bots.
- Deberá 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.
- Deberá ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Deberá 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.
- Los eventos deberán identificar el país que origen o la amenaza.
- Deberá incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- Deberá tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
- Deberá 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.
- Deberá proporcionar 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).

SECRETARÍA DE PLANEACIÓN, GOBERNANZA E INNOVACIÓN GUBERNAMENTAL 04 OCT. 2022 VALIDACIÓN TÉCNICA DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Identificación de Usuarios.

- Deberá 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.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basado en usuarios y grupos de usuarios.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basado 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.

FOLIO INTERNO No. 1695 DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá tener integración con RADIUS para identificar a los usuarios y grupos que Permitirán las políticas de granularidad / control basado en usuarios y grupos de usuarios.
- Deberá tener la integración LDAP para la identificación de los usuarios y grupos que Permitirán granularidad en las políticas/control basado en usuarios y grupos de usuarios.
- Deberá 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 autentificación residente en el equipo de seguridad (portal cautivo).
- Deberá soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que Permitirá una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios.
- Deberá implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
- Deberá permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
- Deberá incluir al menos dos tokens de forma nativa, lo que Permitirá la autenticación de dos factores;

Filtrado de URL.

- Deberá permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
- Deberá tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito.
- Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Deberá tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL.
- Deberá tener por lo menos 75 categorías de URL.
- Deberá tener la funcionalidad de exclusión de URLs por categoría.
- Deberá permitir página de bloqueo personalizada.
- Deberá permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).
- Además del Explicit Web Proxy, deberá soportar r proxy web transparente.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL 04 OCT. 2022 VALIDACIÓN TÉCNICA DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

QoS Traffic Shaping.

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo sea excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere que la solución que, además de que deberá permitir o denegar dichas solicitudes, deberá 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.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo.
- Deberá soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluido, pero no limitado a Skype, BitTorrent, Azureus y YouTube.
- Deberá soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.

FOLIO INTERNO # 1695 DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- En QoS deberá permitir la definición de tráfico con ancho de banda garantizado.
- En QoS deberá permitir la definición de tráfico con máximo ancho de banda.
- En QoS deberá permitir la definición de colas de prioridad.
- Deberá soportar marcación de paquetes DiffServ, incluso por aplicación.
- Deberá soportar la modificación de los valores de DSCP para Diffserv.
- Deberá soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
- Deberá soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

Filtro de Datos.

- Deberá permitir la creación de filtros para archivos y datos predefinidos.
- Los archivos deberán ser identificados por tamaño y tipo.
- Deberá permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones.
- Deberá soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
- Deberá soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos.
- Permitirá 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.

- Deberá soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países.
- Deberá permitir la visualización de los países de origen y destino en los registros de acceso.
- Deberá permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL 04 OCT. 2022 VALIDACIÓN TÉCNICA DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

VPN.

- Deberá soportar VPN de sitio-a-sitio y cliente-a-sitio.
- Deberá soportar VPN IPSec.
- Deberá soportar VPN SSL.
- La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
- La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
- La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
- Tendrá interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
- Deberá soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.
- Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting.

FOLIO INTERNO Nº 1695 DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá 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.
- Deberá 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.
- Deberá suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
- Deberá permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
- Deberá mantener una conexión segura con el portal durante la sesión.
- El agente de VPN SSL o IPSEC cliente-a-sitio deberá ser compatible con al menos Windows y Mac OS.

I. Suministro de 50 (cincuenta) módulos transceptores SFP+ para equipos de telecomunicaciones del GEJ.

El proveedor participante deberá suministrar módulos transceptores para la conectividad de infraestructura de red del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de hardware.

- El módulo deberá soportar el estándar 10GBase-SR.
- El módulo deberá soportar el estándar IEEE 802.3ae
- El módulo deberá tener factor de forma SFP+.
- El módulo deberá soportar tazas de transmisión de 10Gbps.
- El módulo deberá tener un rango de transmisión mínimo de 300 metros.
- El módulo deberá soportar conectores tipo LC.
- El módulo deberá soportar operar de manera plug-and-play.
- El módulo deberá ser compatible con fibras multimodo (MM).
- El módulo deberá tener una longitud de onda de 850nm.
- Deberá considerarse un jumper de fibra de al menos 5 metros compatible con el módulo.
- El módulo deberá ser compatible de manera nativa y sin adaptaciones o configuraciones adicionales con los equipos solicitados en los consecutivos A, B y C de la partida 2 del presente anexo.

J. Suministro de 20 (veinte) módulos transceptores SFP+ para equipos de telecomunicaciones del GEJ.

El proveedor participante deberá suministrar módulos transceptores para la conectividad de infraestructura de red del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de hardware.

- El módulo deberá soportar el estándar 10GBase-LR.
- El módulo deberá soportar el estándar IEEE 802.3ae
- El módulo deberá tener factor de forma SFP+.
- El módulo deberá soportar tazas de transmisión de 10Gbps.
- El módulo deberá tener un rango de transmisión mínimo de 10 kilómetros.
- El módulo deberá soportar conectores tipo LC.
- El módulo deberá soportar operar de manera plug-and-play.
- El módulo deberá ser compatible con fibras monomodo (SM).
- El módulo deberá tener una longitud de onda de 1310nm.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL 04 OCT. 2022 VALIDACIÓN TÉCNICA DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Jefatura de Gabinete FOLIO INTERN
№ 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

- Deberá considerarse un jumper de fibra de al menos 5 metros compatible con el módulo.
- El módulo deberá ser compatible de manera nativa y sin adaptaciones o configuraciones adicionales con los equipos solicitados en los consecutivos A, B y C de la partida 2 del presente anexo.

K. Suministro de 50 (cincuenta) módulos transceptores SFP para equipos de telecomunicaciones del GEJ.

El proveedor participante deberá suministrar módulos transceptores para la conectividad de infraestructura de red del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de hardware.

- El módulo deberá soportar el estándar 1000Base-SX.
- El módulo deberá soportar el estándar IEEE 802.3z
- El módulo deberá tener factor de forma SFP.
- El módulo deberá soportar tazas de transmisión de 1.25Gbps.
- El módulo deberá tener un rango de transmisión mínimo de 300 metros.
- El módulo deberá soportar conectores tipo LC.
- El módulo deberá soportar operar de manera plug-and-play.
- El módulo deberá ser compatible con fibras multimodo (MM).
- El módulo deberá tener una longitud de onda de 850nm.
- Deberá considerarse un jumper de fibra de al menos 5 metros compatible con el módulo.
- El módulo deberá ser compatible de manera nativa y sin adaptaciones o configuraciones adicionales con los equipos solicitados en los consecutivos A, B y C de la partida 2 del presente anexo.

L. Suministro de 10 (diez) módulos transceptores SFP para equipos de telecomunicaciones del GEJ.

El proveedor participante deberá suministrar módulos transceptores para la conectividad de infraestructura de red del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada uno.

Características de hardware.

- El módulo deberá soportar el estándar 1000Base-LX.
- El módulo deberá soportar el estándar IEEE 802.3z
- El módulo deberá tener factor de forma SFP.
- El módulo deberá soportar tazas de transmisión de 1.25Gbps.
- El módulo deberá tener un rango de transmisión mínimo de 10 kilómetros.
- El módulo deberá soportar conectores tipo LC.
- El módulo deberá soportar operar de manera plug-and-play.
- El módulo deberá ser compatible con fibras monomodo (SM).
- El módulo deberá tener una longitud de onda de 1310nm.
- Deberá considerarse un jumper de fibra de al menos 5 metros compatible con el módulo.
- El módulo deberá ser compatible de manera nativa y sin adaptaciones o configuraciones adicionales con los equipos solicitados en los consecutivos A, B y C de la partida 2 del presente anexo.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Nº 1695
DIRECCIÓN GENERAL DE TECNOLOGÍAS

M. Suministro de 02 (dos) fuentes de poder para equipos de seguridad lógica del GEJ.

El proveedor participante deberá suministrar fuentes de poder para infraestructura de seguridad lógica del GEJ, los cuales deberán cumplir con las siguientes características mínimas cada una.

Características de hardware.

- La fuente de poder deberá soportar un voltaje de entrada desde 100 hasta 240 VAC.
- La fuente de poder deberá soportar una frecuencia de 50-60 Hz.
- La fuente de poder deberá soportar la instalación en caliente (hot-swappable).
- La fuente de poder deberá incluir cable de corriente con NEMA C-14.
- La fuente de poder deberá ser compatible de manera nativa y sin adaptaciones con equipos Fortigate 601E existentes en el GEJ.

6. GARANTIAS

Partida 1 garantía de 12 (doce) meses en equipos a partir de la entrega.
Partida 2 garantía de 24 (veinticuatro) meses en equipos y soporte por parte del fabricante a partir de la entrega.

7. OBLIGACIONES DE LOS PARTICIPANTES

Toda la documentación listada en este apartado forma parte de la propuesta técnica del proveedor participante.

Para la partida 1 y sus incisos el proveedor participante deberá presentar lo siguiente:

- El proveedor participante deberá presentar carta de distribuidor autorizado con el nivel más alto emitida por el o los fabricantes de los equipos de telecomunicaciones, la(s) carta(s) deberá(n) ser vigentes en original y/o digital mencionando el número de concurso al cual participa.
- El proveedor participante deberá presentar carta en original y/o digital emitida por el fabricante o los fabricantes de los equipos de telecomunicaciones donde valide técnicamente el BOM propuesto mencionando el número de concurso al cual participa, dicha carta podrá ser validada con el o los fabricantes para garantizar su autenticidad.

Para la partida 2 el proveedor participante deberá presentar lo siguiente:

- El proveedor participante deberá presentar carta de canal certificado, emitida por el fabricante de los equipos de seguridad lógica perimetral, donde se mencione que cuenta con la capacidad para suministrar los equipos requeridos, la carta deberá ser vigente, en original y/o digital mencionando el número de concurso al cual participa.
- El proveedor participante deberá presentar carta en original y/o digital emitida por el fabricante de los equipos de seguridad perimetral donde valide técnicamente el BOM propuesto mencionando el

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

FOLIO INTERNO № 1695
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

número de concurso al cual participa, dicha carta podrá ser validada con el fabricante para garantizar su autenticidad.

Para todas las partidas el proveedor participante deberá presentar lo siguiente

- El proveedor participante deberá de mencionar marca, modelo y especificaciones técnicas y garantía en su cotización y propuesta técnica.
- El proveedor participante deberá presentar Datasheet del equipo a renovar con link de la página oficial del fabricante, en el cual se corroborará la información de acuerdo a su cotización.
- El proveedor participante deberá demostrar que cuenta con oficinas operativas dentro de la zona Metropolitana de Guadalajara mediante copia de comprobante de domicilio no mayor a dos meses.
- El proveedor participante podrá ofertar características superiores a las solicitadas, lo cual deberá ser corroborado por el fabricante como superior mediante carta original haciendo mención al número de concurso.
- El proveedor participante deberá presentar carta bajo protesta de decir verdad en la que mencione que está considerando dentro de su propuesta económica cualquier tipo de componente, hardware, software, viatico, traslados, costos de importación, etc. Necesarios para la correcta entrega del equipo, y en ningún caso se deberá generar un costo extra para el GEJ.

8. ENTREGABLES

Toda la documentación listada en este apartado forma parte de la evidencia, una vez entregado el equipo al área requirente.

- Garantía por escrito de acuerdo con lo especificado en el apartado 6. GARANTIAS.
- Garantía por escrito donde se mencione su cobertura, medio de contacto. Así como, la marca, modelo y número de serie de los equipos suministrados.
- Memoria fotográfica de la entrega de los equipos suministrados.

9. RESPONSABLES DEL REQUERIMIENTO

Responsable de elaborar el requerimiento	
Nombre: Rafael Rosas Ismerio	
Puesto: Director de Infraestructura y Comunicaciones	
e-mail: rafael.rosas@jalisco.gob.mx	
Fecha: 04 de octubre de 2022	Tel. /ext. 3338182800/22850
Firma:	

Responsable de autorizar el requerimiento	
Nombre: Rafael Rosas Ismerio	
Puesto: Director de Infraestructura y Comunicaciones	
e-mail: rafael.rosas@jalisco.gob.mx	
Fecha: 04 de octubre de 2022	Tel. /ext. 3338182800/22850
Firma:	

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

Vigencia del documento: 90 días a partir del sello de validación.

04 OCT. 2022
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

ANEXO 2

LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"
"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

Guadalajara Jalisco, a ___ dé ____ de 2022.
AT'N: Dirección General de Abastecimientos

(PROPUESTA TÉCNICA)

PARTIDA	UNIDAD DE MEDIDA	CANTIDAD	DESCRIPCIÓN

NOTA: Se deberá realizar el desglose a detalle, considerando lo previsto en el Anexo 1, Carta de Requerimientos Técnicos (Anexo Técnico) y cumpliendo con lo requerido dentro del mismo, tomando como base para su llenado el catálogo de conceptos que se adjunta a las presentes bases y que sirven como archivo de la propuesta económica.

TIEMPO DE ENTREGA: (De no señalar fecha específica, el Licitante deberá señalar el número de días naturales, tomando en cuenta que estos se contarán a partir de la suscripción del contrato en caso de resultar adjudicado)

En caso de ser adjudicado proporcionaré bienes y/o servicios en los términos y condiciones del presente anexo, la orden de reparación y/o contrato, la convocatoria y las modificaciones que se deriven de las aclaraciones del presente procedimiento.

Seré responsable por los defectos, vicios ocultos o falta de calidad en general de los bienes por cualquier otro incumplimiento en que puedan incurrir en los términos de la orden de compra y contrato.

ATENTAMENTE

_____

Nombre y firma del Participante o
Representante Legal del mismo.

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

ANEXO 3
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"
"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

Guadalajara Jalisco, a ___ de ____ del 2022.

AT'N: Dirección General de Abastecimientos

PROPUESTA ECONÓMICA

PARTIDA	UNIDAD DE MEDIDA	CANTIDAD	DESCRIPCIÓN	P.U	P. TOTAL
				SUB TOTAL	
				IVA	
				GRAN TOTAL	

CANTIDAD CON LETRA:

TIEMPO DE ENTREGA: (De no señalar fecha específica, el Licitante deberá señalar el número de días naturales, tomando en cuenta que estos se contarán a partir de la suscripción del contrato en caso de resultar adjudicado)

CONDICIONES DE PAGO:
(De solicitar pagos parciales, deberá especificar el monto de cada parcialidad contra entrega y entera satisfacción de la dependencia).

NOTA. - En caso de considerar que alguna sub-partida, concepto, bien o servicio ofertado no tendrá costo alguno, deberá precisar en el renglón correspondiente: S/C, N/A o en su defecto plasmar el número "0".

Declaro bajo protesta de decir verdad que los precios cotizados tienen una vigencia de 30 treinta días naturales contados a partir de la resolución de adjudicación y que los precios incluyen todos los costos involucrados y se presentan en moneda nacional con los impuestos desglosados.

Manifiesto que los precios cotizados en la presente propuesta, serán los mismos en caso de que la Dirección General de Abastecimientos y/o el **"COMITÉ"** según corresponda opte por realizar ajustes al momento de adjudicar de forma parcial los bienes o servicios objeto de este **"PROCEDIMIENTO DE ADQUISICIÓN"**.

ATENTAMENTE

Nombre y firma del Participante
o Representante Legal del mismo.

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

ANEXO 4
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"
"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

CARTA DE PROPOSICIÓN

Guadalajara Jalisco, a ___ de ____ del 2022.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Dirección General de Abastecimientos

En atención al procedimiento de **Licitación Pública Local LPL297/2022 CON CONCURRENCIA DEL "COMITÉ"** relativo a la **"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ".** (En lo subsecuente **"PROCEDIMIENTO DE ADQUISICIÓN"**), el suscrito (nombre del firmante) en mi calidad de Representante Legal de (Nombre del Participante), manifiesto **bajo protesta de decir verdad** que:

1. Que cuento con facultades suficientes para suscribir la propuesta en el presente **"PROCEDIMIENTO DE ADQUISICIÓN"**, así como para la firma y presentación de los documentos y el contrato que se deriven de éste, a nombre y representación de (Persona Física o Jurídica). Así mismo, manifiesto que cuento con número de **"PROVEEDOR"** (XXXXXXXXXXXX) y con Registro Federal de Contribuyentes (XXXXXXXXX), y en su caso me comprometo a realizar los trámites de registro y actualización ante el Padrón de proveedores en los términos señalados en las presentes **"BASES"**, para la firma del contrato que llegare a celebrarse en caso de resultar adjudicado.
2. Que mi representada señala (o "que señalo") como domicilio para todos los efectos legales, así como para oír y recibir todo tipo de notificaciones a que haya, lugar la finca marcada con el número xx de la calle xx, de la colonia XXXXXXXXXXXXX, de la ciudad de xx, C.P. XXXXX, teléfono xx, fax xxxx y correo electrónico XXXXXX.(Deberá señalar domicilio dentro del estado de Jalisco.)
3. Que he leído, revisado y analizado con detalle todas las condiciones de las **"BASES"** del presente **"PROCEDIMIENTO DE ADQUISICIÓN"**, las especificaciones correspondientes y el juego de Anexos que me fueron proporcionados por la Secretaría de Administración del Gobierno de Jalisco, obligándome a cumplir con lo estipulado en cada uno de ellos y/o acatar las aclaraciones realizadas por las áreas técnicas del presente procedimiento.
4. Que mi representante entregará (o "Que entregaré") los bienes y/o servicios a que se refiere el presente Procedimiento de Licitación de acuerdo con las especificaciones y condiciones requeridas en las **"BASES"** de este **"PROCEDIMIENTO DE ADQUISICIÓN"**, con los precios unitarios señalados en mi propuesta económica.
5. Que se han formulado cuidadosamente todos y cada uno de los precios unitarios que se proponen, tomando en consideración las circunstancias previsibles que puedan influir sobre ellos. Dichos precios se presentan en moneda nacional e incluyen todos los cargos directos e indirectos que se originen en la elaboración de los bienes y/o servicios hasta su recepción total por parte del Gobierno del Estado.
6. Manifiesto que los precios cotizados en la presente propuesta, serán los mismos en caso de que la Dirección General de Abastecimientos opte por realizar ajustes al momento de adjudicar de forma parcial los bienes o servicios objeto de este **"PROCEDIMIENTO DE ADQUISICIÓN"**.

7. En caso de resultar favorecidos, nos comprometemos (O “me comprometeré) a firmar el contrato en los términos señalados en las **“BASES”** del presente **“PROCEDIMIENTO DE ADQUISICIÓN”**.
8. Que mi representante no se encuentra (o “Que no me encuentro”) en alguno de los supuestos del artículo 52 de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios, y tampoco en las situaciones previstas para el **DESECHAMIENTO DE LAS “PROPUESTAS” DE LOS “PARTICIPANTES”** que se indican en las **“BASES”** del presente **“PROCEDIMIENTO DE ADQUISICIÓN”**.
9. Mi representada señala (o “Que señalo”) como domicilio para todos los efectos legales a que haya lugar la finca marcada con el número _____ de la calle _____, de la colonia ____, de la ciudad de _____, C.P. _____, teléfono _____, fax _____ y correo electrónico _____@_____; solicitándoles y manifestando mi conformidad de que todas las notificaciones que se tengan que practicar y aún las personales, se me hagan por correo electrónico en la cuenta anteriormente señalada, sujetándome a lo que establecen los artículos 106 y 107 del Código de Procedimientos Civiles del Estado de Jalisco, aplicado supletoriamente, para que la autoridad estatal lleve a cabo las notificaciones correspondientes.
10. Que por mí o a través de interpósita persona, me abstendré de adoptar conductas, para que los servidores públicos, induzcan o alteren las evaluaciones de las cotizaciones, el resultado del procedimiento, u otros aspectos que otorguen condiciones más ventajosas con relación a los demás Oferentes.
11. Que no me encuentro dentro de las listas a que se refiere el artículo 69 B del Código Fiscal de la Federación.

ATENTAMENTE

_____

Nombre y firma del Participante
o Representante Legal del mismo

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

ANEXO 5
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"

"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

Guadalajara Jalisco, a ___ de ____ del 2022.

ACREDITACIÓN

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Dirección General de Abastecimientos

Yo, (nombre), manifiesto **bajo protesta de decir verdad**, que los datos aquí asentados son ciertos y han sido verificados, , manifiesto que actúo en nombre y cuenta propia y, que no me encuentro inhabilitado por resolución de autoridad competente alguno, así como que cuento con facultades suficientes para suscribir la cotización y comprometerme en el **Procedimiento de Licitación Pública Local LPL297/2022 CON CONCURRENCIA DEL "COMITÉ"**, así como con los documentos que se deriven de éste, a nombre y representación de (persona física o moral).

Nombre del Licitante :		
No. de Registro del RUPC (en caso de contar con él)		
No. de Registro Federal de Contribuyentes:		
Domicilio: (Calle, Número exterior-interior, Colonia, Código Postal)		
Municipio o Delegación:		**Entidad Federativa:**
Teléfono (s):	**Fax:**	**Correo Electrónico:**
Objeto Social: tal y como aparece en el acta constitutiva (persona moral) o actividad preponderante (persona física)		

ersonas Morales:

Número de Escritura Pública: (Acta Constitutiva y, de haberlas, sus reformas y modificaciones)
Fecha y lugar de expedición:
Nombre del Fedatario Público, mencionando si es Titular o Suplente**:**
Fecha de inscripción en el Registro Público de la Propiedad y de Comercio:
Tomo: **Libro:** **Agregado con número al Apéndice:**

*****NOTA: En caso de que hubiere modificaciones **relevantes** al Acta Constitutiva (cambio de razón social, de domicilio fiscal, de giro o actividad, etc.), deberá mencionar los datos anteriores que correspondan a dicha modificación y la referencia de la causa de la misma.

ersonas Físicas:

Número de folio de la Credencial de Elector:

P O D E R	Para Personas Morales o Físicas que comparezcan a través de Apoderado, mediante **Poder General** o **Especial para Actos de Administración o de Dominio**. **Número de Escritura Pública:** **Tipo de poder:** **Nombre del Fedatario Público**, mencionando si es Titular o Suplente**:** **Lugar y fecha de expedición:** **Fecha de inscripción en el Registro Público de la Propiedad y de Comercio:** **Tomo: Libro: Agregado con número al Apéndice:**

RELACION DE SOCIOS, ACCIONISTAS Y, PRINCIPALES ÓRGANOS DE DIRECCIÓN (ADMINISTRADOR GENERAL ÚNICO O, CONSEJO DE ADMINSTRACIÓN).

NOMBRE	APELLIDO PATERNO	APELLIDO MATERNO	CARGO

ATENTAMENTE

_____

Nombre y firma del Licitante
o Representante Legal

ANEXO 6

LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"
"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

DECLARACIÓN DE INTEGRIDAD Y NO COLUSIÓN DE PROVEEDORES.

Guadalajara Jalisco, a ___ de ____ del 2022.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Dirección General de Abastecimientos

En cumplimiento con los requisitos establecidos en el presente **"PROCEDIMIENTO DE ADQUISICIÓN"** para la **Licitación Pública Local LPL297/2022 CON CONCURRENCIA DEL "COMITÉ"** para la entrega de los **"____",** por medio del presente manifiesto bajo protesta de decir verdad que por sí mismos o a través de interpósita persona, el **"PROVEEDOR"** (persona física o moral), a quien represento, se abstendrá de adoptar conductas, para que los servidores públicos de la Dirección General de Abastecimientos de la Secretaría de Administración y/o Unidad Centralizada de Compras, induzcan o alteren la evaluaciones de las proposiciones, el resultado del procedimiento u otros aspectos que otorguen condiciones más ventajosas con relación a los demás **"PARTICIPANTES"**, así como la celebración de acuerdos colusorios.

A su vez manifiesto no encontrarme dentro de los supuestos establecidos en el artículo 52 de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

Bajo protesta de decir verdad manifiesto que no cuento con vínculos o relaciones de negocios, personales o familiares, así como posibles conflictos de interés relacionados con servidores públicos que intervienen en el procedimiento de licitación. Asimismo, no desempeño empleo, cargo o comisión en el servicio público o, en caso de desempeñarlo, con la formalización del contrato respectivo no se actualiza causal alguna de conflicto de interés.

Personas morales/ Bajo protesta de decir verdad manifiesto que los socios, accionistas, administrador general único o, en su caso miembros del consejo de administración y, representantes o apoderados legales de mi representada no cuentan con vínculos o relaciones de negocios, personales o familiares, así como posibles conflictos de interés relacionados con servidores públicos que intervienen en el procedimiento de licitación. Asimismo, que las personas referidas no desempeñan empleo, cargo o comisión en el servicio público o, en caso de desempeñarlo, con la formalización del contrato respectivo no se actualiza causal alguna de conflicto de interés.

ATENTAMENTE

_____
Nombre y firma del Licitante
o Representante Legal

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

ANEXO 7
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"

"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

DECLARACIÓN DE APORTACIÓN CINCO AL MILLAR PARA EL FONDO IMPULSO JALISCO.

Guadalajara Jalisco, a __ de ____ del 2022.

AT'N: Dirección General de Abastecimientos

PRESENTE.

Yo, (nombre) en mi carácter de (persona física/representante legal de la empresa" xxxx") manifiesto que, SI/NO es mi voluntad el realizar la aportación cinco al millar del monto total del contrato, antes de IVA, para ser aportado al Fondo Impulso Jalisco con el propósito de promover y procurar la reactivación económica en el Estado, esto en el supuesto de resultar adjudicado en el presente proceso de adquisición.

Así mismo manifiesto que dicha aportación voluntaria no repercute en la integración de mi propuesta económica ni en la calidad de los bienes y/o servicios a entregar, así como mi consentimiento para que la Secretaría de la Hacienda Pública realice la retención de tal aportación en una sola ministración en el primer pago, ya sea pago de anticipo, pago parcial o pago total. **(En caso de que el participante manifieste NO realizar la aportación al Fondo Impulso Jalisco, el presente párrafo quedará sin efecto)**

Lo anterior señalado en los artículos 143, 145, 148 y 149 de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

ATENTAMENTE

_____

Nombre y firma del Licitante

o Representante Legal

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

ANEXO 8
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"

"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

ARTÍCULO 32-D

Guadalajara Jalisco, a ___ de ___ del 2022.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Dirección General de Abastecimientos

Nombre completo), en mi carácter de Representante Legal de la empresa (Nombre de la Empresa), manifiesto estar al corriente de con mis obligaciones fiscales, por lo que anexo la Constancia de opinión positiva del cumplimiento de obligaciones Fiscales, documento vigente expedido por el SAT, conforme a lo establecido en el Artículo 32-D, del Código Fiscal de la Federación.

ATENTAMENTE

_____
Nombre y firma del Licitante
o Representante Legal

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

ANEXO 9
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"

"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

Cumplimiento obligaciones IMSS

Guadalajara Jalisco, a ___ de _____ del 2022.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Dirección General de Abastecimientos

(Nombre completo), en mi carácter de Representante Legal de la empresa (Nombre de la Empresa), manifiesto estar al corriente de mis obligaciones fiscales en materia de Seguridad Social, por lo que anexo la Constancia de opinión positiva de cumplimiento de obligaciones en materia de Seguridad Social, documento vigente expedido el IMSS, de conformidad al acuerdo acdo.sa1.hct.101214/281.p.dir, publicada en el Diario Oficial de la Federación el día 27 de febrero de 2015.

ATENTAMENTE

_____
Nombre y firma del Licitante
o Representante Legal

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

ANEXO 10
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"

"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

IDENTIFICACIÓN VIGENTE DE LA PERSONA FÍSICA O DEL REPRESENTANTE LEGAL DE LA PERSONA MORAL QUE FIRMA LA PROPOSICIÓN.

Guadalajara Jalisco, a ___ de ___ del 2022.

ANVERSO

REVERSO

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL

ANEXO 11
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"

"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

MANIFESTACIÓN DE ESTAR AL CORRIENTE EN MIS OBLIGACIONES PATRONALES Y TRIBUTARIAS.

Guadalajara Jalisco, a __ de ____ del 2022.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE

AT'N: Dirección General de Abastecimientos

En cumplimiento con los requisitos establecidos en el presente **"PROCEDIMIENTO DE ADQUISICIÓN"** para la **Licitación Pública Local LPL297/2022 CON concurrencia** del **"COMITÉ" "ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ" ,** por medio del presente manifiesto bajo protesta de decir verdad a la Secretaría de Administración, que el **"PROVEEDOR"** (persona física o moral), a quien represento, está al corriente en sus obligaciones patronales como son: el pago de cuotas de seguridad social, del Infonavit, así como todas las obligaciones laborales y tributarias a que estoy obligado.

ATENTAMENTE

_____
Nombre y firma del Licitante
o Representante Legal

ANEXO 12
LPL297/2022
CON CONCURRENCIA DEL "COMITÉ"

"ADQUISICION DE INFRAESTRUCTURA DE TELECOMUNICACIONES PARA DEPENDENCIAS DEL GEJ"

ESTRATIFICACIÓN

Guadalajara Jalisco, a __ de ____ del 2022.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Dirección General de Abastecimientos

Me refiero al procedimiento de **Licitación Pública Local LPL297/2022 CON CONCURRENCIA del "COMITÉ"**, en el que mí representada, la empresa _____ (**2**) _____, participa a través de la presente proposición.

Al respecto y de conformidad con lo dispuesto por el numeral 1 del artículo 68 de la Ley, **MANIFIESTO BAJO PROTESTA DE DECIR VERDAD** que mi representada está constituida conforme a las leyes mexicanas, con Registro Federal de Contribuyentes _____(**3**)_____, y asimismo que considerando los criterios (sector, número total de trabajadores y ventas anuales) establecidos en el Acuerdo por el que se establece la estratificación de las micro, pequeñas y medianas empresas, publicado en el Diario Oficial de la Federación el 30 de junio de 2009, mi representada tiene un Tope Máximo Combinado de _____(**4**)_____, con base en lo cual se estratifica como una empresa _____(**5**)_____.

De igual forma, declaro que la presente manifestación la hago teniendo pleno conocimiento de que la omisión, simulación o presentación de información falsa, en el artículo 69 de la Ley General de Responsabilidades Administrativas, sancionable por los artículos 116, 117 y 118 de la **"LEY"**, y los diversos numerales 155 al 161 de su **"REGLAMENTO"**, así como en términos de lo dispuesto por el artículo 81 de la Ley General de Responsabilidades Administrativas.

ATENTAMENTE

_____
Nombre y firma del Licitante
o Representante Legal

Llenar los campos conforme aplique tomando en cuenta los rangos previstos en el Acuerdo antes mencionado.

1	Señalar la fecha de suscripción del documento.
2	Anotar el nombre, razón social o denominación del licitante.
3	Indicar el Registro Federal de Contribuyentes del licitante.
4	Señalar el número que resulte de la aplicación de la expresión: Tope Máximo Combinado = (Trabajadores) x10% + (Ventas anuales en millones de pesos) x 90%. Para tales efectos puede utilizar la calculadora MIPyMES disponible en la página http://www.comprasdegobierno.gob.mx/calculadora Para el concepto “Trabajadores”, utilizar el total de los trabajadores con los que cuenta la empresa a la fecha de la emisión de la manifestación. Para el concepto “ventas anuales”, utilizar los datos conforme al reporte de su ejercicio fiscal correspondiente a la última declaración anual de impuestos federales, expresados en millones de pesos.
5	Señalar el tamaño de la empresa (Micro, Pequeña o Mediana), conforme al resultado de la operación señalada en el numeral anterior.

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44270,

Guadalajara, Jalisco, México

ANEXO 13

TEXTO DE LA FIANZA DEL 10% DE GARANTÍA DE CUMPLIMIENTO DEL CONTRATO

(NOMBRE DE LA AFIANZADORA), EN EL EJERCICIO DE LA AUTORIZACIÓN QUE ME OTORGA EL GOBIERNO FEDERAL A TRAVÉS DE LA SECRETARÍA DE LA HACIENDA Y CRÉDITO PÚBLICO EN LOS TÉRMINOS DE LOS ARTÍCULOS 11 y 36 DE LA LEY DE INSTITUCIONES DE SEGUROS Y DE FIANZAS, ME CONSTITUYO FIADORA POR LA SUMA DE $ (CANTIDAD CON NÚMERO) (CANTIDAD CON LETRA) **A FAVOR DE LA SECRETARÍA DE LA HACIENDA PUBLICA** CON DOMICILIO EN CALLE PEDRO MORENO 281, C.P. 44100, COL. CENTRO, A EFECTO DE

GARANTIZAR POR (NOMBRE DEL **"PROVEEDOR"**) CON DOMICILIO EN ___COLONIA ___CIUDAD ___EL FIEL Y EXACTO CUMPLIMIENTO DE TODAS Y CADA UNA DE LAS OBLIGACIONES PACTADAS EN EL CONTRATO **NÚMERO____(ANOTAR EL NÚMERO)_____, DE FECHA_____, CELEBRADO ENTRE NUESTRO FIADO Y EL GOBIERNO DEL ESTADO DE JALISCO, CON UN IMPORTE TOTAL DE $_____. ASÍ MISMO, SE ACEPTA SUJETARNOS A LA COMPETENCIA DE LOS TRIBUNALES DEL PRIMER PARTIDO JUDICIAL DEL ESTADO DE JALISCO, ACEPTANDO CONTINUAR AFIANZANDO A MI FIADO, EN CASO DE QUE SE LE OTORGUE ALGUNA PRÓRROGA DE CUMPLIMIETNO O SE CELEBRE CON ÉSTE, CUALQUIER ACUERDO MODIFICATORIO AL CONTRATO PRINCIPAL.**

ESTA FIANZA ESTARÁ EN VIGOR DESDE LA FECHA DE FIRMA DEL CONTRATO Y HASTA POR 12 MESES CONTADOS A PARTIR DE LA FECHA DE TERMINACIÓN DEL CONTRATO.

ADICIONALMENTE ESTA FIANZA PODRÁ SER EXIGIBLE EN CUALQUIER TIEMPO PARA GARANTIZAR LAS OBLIGACIONES DEL **CONTRATO,"BASES" Y/O CONVOCATORIA** DEL PROCEDIMIENTO QUE LE DIERON ORIGEN, **Y/O** LA BUENA CALIDAD EN GENERAL DE LOS BIENES Y SERVICIOS, CUANDO SEAN DE CARACTERÍSTICAS INFERIORES A LAS SOLICITADAS EN LAS **"BASES" Y/O CONVOCATORIA** DEL **"PROCEDIMIENTO DE ADQUISICIÓN"** ANTERIORMENTE SEÑALADO Y/O CUANDO DIFIERAN EN PERJUICIO DE LA SECRETARÌA Y/O LA DEPENDENCIA, ASÍ COMO LA REPARACIÓN DE LOS DEFECTOS Y VICIOS OCULTOS, DAÑOS Y PERJUICIOS QUE PUDIEREN APARECER Y QUE SEAN IMPUTABLES A NUESTRO FIADO CON MOTIVO DE LA CONTRATACIÓN QUE SE MENCIONA Y SOLO PODRÁ SER CANCELADA CON LA PRESENTACIÓN DE SU ORIGINAL POR PARTE DE NUESTRO FIADO.

IGUALMENTE, EN EL CASO QUE SE OTORGUE PRÓRROGA AL CUMPLIMIENTO **DEL CONTRATO,** ASÍ COMO DURANTE LA SUBSTANCIACIÓN DE JUICIOS, RECURSOS O INCONFORMIDADES DE LOS BIENES Y/O SERVICIOS CONTRATADOS ESTA FIANZA CONTINUARÁ VIGENTE HASTA SU TOTAL RESOLUCIÓN.

EN CASO DE QUE LA PRESENTE FIANZA SE HAGA EXIGIBLE, LA AFIANZADORA Y EL FIADO ACEPTAN EXPRESAMENTE SOMETERSE AL PROCEDIMIENTO DE EJECUCIÓN ESTABLECIDO EN LOS ARTÍCULOS 279, 280, 281, 282, 283 Y 178 Y DEMÁS RELATIVOS DE LA LEY DE INSTITUCIONES DE SEGUROS Y DE FIANZAS EN VIGOR, PARA LA EFECTIVIDAD DE LAS FIANZAS, AÚN PARA EL CASO DE QUE PROCEDA EL COBRO DE INTERESES, CON MOTIVO DEL PAGO EXTEMPORÁNEO DEL IMPORTE DE LA PÓLIZA DE FIANZA REQUERIDA ACEPTANDO SOMETERSE A LA COMPETENCIA DE LOS TRIBUNALES DEL PRIMER PARTIDO JUDICIAL DEL ESTADO DE JALISCO, RENUNCIANDO A LOS TRIBUNALES QUE POR RAZÓN DE SU DOMICILIO PRESENTE O FUTURO, LES PUDIERA CORRESPONDER.

EL INCUMPLIMIENTO DE LA OBLIGACIÓN GARANTIZADA SE ACREDITARÁ ACOMPAÑANDO A SU ESCRITO DE RECLAMACIÓN LOS DOCUMENTOS QUE COMPRUEBEN LA EXISTENCIA Y EXIGIBILIDAD DE LA OBLIGACIÓN GARANTIZADA EN TÉRMINOS DEL ART. 279 DE LA LEY, CON INDEPENDENCIA DE LO ANTERIOR, LA INSTITUCIÓN TENDRÁ DERECHO A SOLICITAR AL BENEFICIARIO TODO TIPO DE INFORMACIÓN O DOCUMENTACIÓN QUE SEA NECESARIA RELACIONADA CON LA FIANZA MOTIVO DE LA RECLAMACIÓN EN TÉRMINO
DEL MISMO NUMERAL.
FIN DEL TEXTO.