Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

GOBIERNO DEL ESTADO DE JALISCO

Poder Ejecutivo
Secretaría de Administración

DIRECCIÓN DEL COMITÉ DE ADQUISICIONES

"BASES"

Licitación Pública Local
LPL251/2019 Con Concurrencia del Comité

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

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, LPL251/2019 con Concurrencia del Comité** para la **"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"**, en lo subsecuente "Proceso de Adquisición", el cual se llevará a cabo con **Recursos Estatales y FONE,** del **Ejercicio 2019** y de conformidad a lo establecido en las siguientes:

B A S E S

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

"BASES" O "CONVOCATORIA"	Es el llamado a los interesados a participar en determinado procedimiento de adquisiciones o enajenación, que contiene las condiciones y requisitos de participación.
"COMITÉ"	Comité de Adquisiciones de la Administración Pública Centralizada del Poder Ejecutivo del Estado de Jalisco
"CONTRALORÍA"	Órgano de Control del Gobierno del Estado de Jalisco, con domicilio en Av. Ignacio L. Vallarta número 1252, Col. Americana. Teléfono 01-(33)1543-9470
"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"**.
"DEPENDENCIA REQUIRENTE"	Secretaría de Administración
"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)
"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 proceso
"I.V.A."	Impuesto al Valor Agregado.
"LEY"	Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
"PARTICIPANTE" O "LICITANTE"	Persona Física o Jurídica que presenta propuesta en el proceso de adquisición.
"PROPUESTA" O "PROPOSICIÓN"	La propuesta técnica y económica que presenten los **"PARTICIPANTES"**
"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 Estatal de Compras Gubernamentales.
"SECRETARÍA"	Secretaría 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.

CALENDARIO DE ACTIVIDADES
(ACTOS)

A C T O	PERÍODO O DÍA	HORA	LUGAR
Publicación de "**CONVOCATORIA**"/"**BASES**"	25 de octubre de 2019	A partir de las 15:00 horas	Portal de Compras Jalisco y/o el SECG.
Recepción de preguntas	28 de octubre de 2019	Hasta las 10:00 horas	De manera física en la Dirección del Comité de Adquisiciones, ubicado en el **"DOMICILIO"**
Registro para el Acto de Junta Aclaratoria	31 de octubre de 2019	De las 15:30 a las 15:59 horas	En el "**DOMICILIO**".
Acto de Junta Aclaratoria	31 de octubre de 2019	A partir de las 16:00 horas	En el "**DOMICILIO**".
Registro para la Presentación de Propuestas.	04 de noviembre de 2019	De las 15:15 a las 15:45 horas	En el "**DOMICILIO**".
Presentación y Apertura de propuestas.	04 de noviembre de 2019	A partir de las 16:00 horas	En la Oficina de Recepción y Apertura, en el "**DOMICILIO**".
"FALLO" O "RESOLUCIÓN" de la convocatoria.	Dentro de los 20 días naturales siguientes a la fecha de presentación y apertura de propuestas.		A través del "**SECG**" y/o el correo electrónico.

1. ESPECIFICACIONES.

El objeto del presente proceso es la contratación de "ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO" 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 bienes y/o servicios, objeto de este proceso de adquisición deberá ser en un plazo no mayor a lo estipulado en el anexo 1, la entrega será de conformidad con las características y especificaciones que se establecerán en el **"CONTRATO"**. Las obligaciones correrán a partir de la notificación del **"FALLO" O "RESOLUCIÓN"** y bajo la estricta responsabilidad del **"PROVEEDOR"**, quien se asegurará de su adecuado transporte/adecuada prestación hasta su correcta recepción a entera satisfacción de la "**DEPENDENCIA REQUIRENTE"**.

Se considerará que el **"PROVEEDOR"** ha entregado los bienes y/o servicios, objeto de este proceso 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 y/o servicios a entera satisfacción por parte del personal técnico responsable. En caso de que se trate de Tecnologías de la Información y Comunicación, el Oficio de recepción de bienes a entera satisfacción deberá ser emitido por la Dirección General de Planeación Tecnológica, de la Coordinación General de Innovación Gubernamental, de la Jefatura de Gabinete.

3. PAGO.

El pago se efectuará una vez que sea realizada la entrega parcial y/o total de los bienes y/o 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 "**SECRETARÍA",** de conformidad con los lineamientos de la Secretaría de la Hacienda Pública del Estado de Jalisco**.**

Documentos para pago parcial o total.

a. Original y copia de la factura, comprobante fiscal digital por internet (CFDI) respectivo en pdf y xlm expedido a favor de la Secretaría de la Hacienda Pública del Estado de Jalisco, 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.

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

c. Original de la Orden de compra, en caso de parcialidad solo Copia, y original de la última parcialidad.(cuando aplique)

d. Original del anexo de entregas, en caso de parcialidad solo copia. (cuando aplique)

e. Copia del Acta de **"FALLO" O "RESOLUCIÓN".**

f. Original del **"CONTRATO"**.

g. Original del oficio de Recepción de los bienes a entera satisfacción. (cuando aplique)

h. 1 copia de la garantía de cumplimiento de **"CONTRATO"** a nombre de la Secretaría de la Hacienda Pública del Estado de Jalisco, 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.

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 y/o 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 del Estado de Jalisco, 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 y/o 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.

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.

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 artículo 17 de la **"LEY"**, deberá realizar su alta en el término de **72 horas, prorrogables de acuerdo al artículo 27 del "REGLAMENTO",** a partir de la notificación de

adjudicación, 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 proceso 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. Los **"PARTICIPANTES"** no tendrán facultades para hacer declaraciones en prensa o cualquier medio de difusión. Tampoco podrán duplicar, grabar, copiar o de cualquier otra forma reproducir la información sin la autorización expresa de la Dependencia requirente. La contravención a lo dispuesto, generará la obligación a cargo del participante que la incumpla, de indemnizar a la dependencia requirente por los daños y perjuicios causados con motivo del incumplimiento.

5. JUNTA ACLARATORIA.

Los "LICITANTES" que estén interesados en participar en el proceso 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, a más tardar a las 10:00 horas del 28 de octubre del 2019, de conformidad con los artículos 62 apartado 4, 63 y 70 de la "LEY", 63, 64 y 65 de su "REGLAMENTO".

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 31 de octubre del 2019 de 15:30 horas a 15:59 horas en el "DOMICILIO" de la presente convocatoria.

El acto de Junta de Aclaraciones se llevará a cabo a las 16:00 horas del día 31 de octubre del 2019 en el "DOMICILIO" de la presente convocatoria, donde se dará respuesta a las preguntas recibidas.

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

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 VERIFICACION.

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 o su representante legal.
- **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 proceso 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. 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).

g. 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.

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

i. 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.

j. 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.
- Las hojas foliadas en el orden solicitado, por ejemplo: 1/3, 2/3, 3/3
- 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				
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
	Industria	Desde 51 Hasta 100		
	Servicios	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 a las 16**:00 horas del día 04 de noviembre del 2019,** en la Sala de Juntas de la **"SECRETARÍA"**, en el Mezzanine del edificio, ubicado en el **"DOMICILIO"**.

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**.

Cualquier **"PROVEEDOR"** que no se haya registrado en tiempo y forma, no se tomará en cuenta su propuesta.

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

a. **Anexo 2** (Propuesta Técnica).
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** (Estratificación) Obligatorio solo para **"PARTICIPANTES"** MIPYME.
g. **Anexo 8** (**Manifiesto de Opinión Positiva de Cumplimiento de Obligaciones Fiscales y Constancia impresa)**. De acuerdo al numeral 24 de las presentes **"BASES"**.
h. **Anexo 9** (**Manifiesto de Opinión de Cumplimiento de Obligaciones en Materia de Seguridad Social y Constancia) solo en caso de no estar registrados en el padrón de proveedores**. De acuerdo al numeral 25 de las presentes **"BASES"**.
i. **Anexo 10** (Identificación Oficial Vigente).
j. **Anexo 11** Solo Para proveedores Nacionales Manifestación de Estar al Corriente en Obligaciones Patronales y Tributarias.
k. **Documentos solicitados en el Anexo 1 de las "BASES"**

La falta de cualquiera de los documentos anteriormente descritos 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 un Representante 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;

d. En el momento en que se indique, los **"PARTICIPANTES"** ingresarán a la sala, llevándose a cabo la declaración oficial de apertura del acto;

e. Se hará mención de los **"PARTICIPANTES"** presentes;

f. 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;

g. Los **"PARTICIPANTES"** darán lectura al total de su oferta económica I.V.A. incluido;

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

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

j. 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 proceso de adquisición, el Director General de Abastecimientos o el funcionario que éste designe para tal efecto, podrá suspender o cancelar el registro del Padrón.

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 proceso de adquisición, será adjudicado a uno o varios **"PARTICIPANTES"**.

Para la evaluación se procederá conforme a lo señalado en el apartado 2 del Artículo 66 de la **"LEY"**, en los "Procedimientos de Licitación Pública" y en el artículo 69 de su 2 "**REGLAMENTO"**, en donde se aceptarán las ofertas que cumplan con los requerimientos establecidos en este proceso y cubran las características técnicas establecidas en el Anexo 1 (Carta de Requerimientos Técnicos)

Se establece como criterio de evaluación el "Binario", mediante el cual sólo se Adjudica a quien cumpla con los requisitos establecidos por la **"CONVOCANTE"** y oferte el precio más bajo, considerando los criterios establecidos en propia "**LEY"**, en este supuesto, la **"CONVOCANTE"** evaluará al menos las dos **"PROPUESTAS"**

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).

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"**, la diferencia de precios deberá analizarse respecto de las mismas partidas en cada una de las proposiciones, y no por el total de estas.

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 el artículo 69 apartado 1, fracción III de la **"LEY"**.

10. ACLARACIÓN DE LAS PROPUESTAS.

El Director General de Abastecimientos o el funcionario que éste designe, podrá solicitar aclaraciones relacionadas con las propuestas, a cualquier "**PARTICIPANTE"** por el medio 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 proceso 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. 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 PROCESO DE ADQUISICIÓN.

La "**CONVOCANTE"** a través del "**COMITÉ"**, podrá cancelar o suspender parcial o totalmente el proceso 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 proceso de adquisición, aseguran al Gobierno de Estado de Jalisco las mejores condiciones disponibles para la adjudicación de los servicios materia de este proceso 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.

En caso de que el proceso de adquisición sea suspendido o cancelado se dará aviso a todos los **"PARTICIPANTES"**.

14. DECLARACIÓN DE PROCESO DE ADQUISICIÓN DESIERTO.

El **COMITÉ"**, podrá declarar parcial o totalmente desierto el proceso 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 pudiera ser objeto de adjudicación, excede el presupuesto autorizado para este proceso de adquisición.
- **e.** Si después de efectuada la evaluación técnica y económica no sea posible adjudicar a ningún Participante.

15. NOTIFICACIÓN DEL "FALLO" O "RESOLUCIÓN".

Sera dentro de los veinte 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 proceso a través del "**SECG"**, en la página web del ente y/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" O "RESOLUCIÓN" 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"**.

16. 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 proceso.

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 la evaluación que se practique a las propuestas presentadas o convocar a un nuevo proceso 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. Realizar las aclaraciones pertinentes respecto a lo establecido en las presentes **"BASES"**; y

h. 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.

17. 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 15 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 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"**, 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 les 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 proceso de adquisición.

18. VIGENCIA DEL "CONTRATO".

El **"CONTRATO"** a celebrarse con el **"PARTICIPANTE"** que resulte adjudicado en el presente proceso, tendrá una vigencia a partir de la fecha de la firma del **"CONTRATO"** y hasta la conclusión de la entrega de los bienes y/o 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 conforme a lo previsto en el artículo 80 de la **"LEY"**.

19. ANTICIPO.

No se otorgara anticipo para el presente proceso.

20. GARANTÍAS.

En caso de que el monto total del **"CONTRATO"** incluyendo el **"I.V.A."**, sea superior a **$400,000.^{00}** M.N. (cuatrocientos mil pesos $^{00}/_{100}$ moneda nacional), 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 12** (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.

21. SANCIONES.

Se podrá cancelar 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 caso de rescisión del **"CONTRATO"** por parte de la **"SECRETARÍA"** por cualquiera de las causas previstas en las presentes **"BASES"** o en el **"CONTRATO"**.

22. DE LA PENALIZACIÓN POR ATRASO EN LA ENTREGA.

En caso que el **"PROVEEDOR"** tenga atraso en la entrega de los bienes 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"**

23. 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 20 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 20 de las presentes **"BASES",** y ejercerse las acciones correspondientes por daños y perjuicios.

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

El **"PARTICIPANTE"** deberá presentar el documento actualizado donde 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.

Lo anterior, se solicita de conformidad con los términos de la disposición 2.1.39. de la resolución Miscelánea Fiscal para 2019, publicada en el Diario Oficial de la Federación.

Dicho documento se deberá presentar en sentido positivo y será verificado 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"**.

25. 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.

26. INCONFORMIDADES.

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

27. 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 proceso 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.

Guadalajara, Jalisco; 25 de octubre del 2019.

LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

RELACIÓN DE ANEXOS

DOCUMENTACIÓN QUE CONTENDRÁ LA OFERTA A PRESENTAR EN HOJA MEMBRETADA DE LA EMPRESA	Punto de referencia 9	Documento que se entrega
Anexo 2 (Propuesta Técnica).	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 (Estratificación) Obligatorio para "PARTICIPANTES" MYPIMES.	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 (Sólo para proveedores Nacionales, manifestación de estar al corriente de sus Obligaciones Patronales y Tributarias).	j)	

LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

	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 LPL__/2019**

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:

LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

MANIFIESTO DE PERSONALIDAD

Guadalajara Jalisco, a ___ de ____ del 2019.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Lic. Luis Arturo López Sahagún
Director 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. 44100,

Guadalajara, Jalisco, México

ANEXO 1

CARTA DE REQUERIMIENTOS TÉCNICOS

LPL251 /2019

SOLICITUD	PARTIDAS
35-242-2019	1
35-272-2019	2
35-230-2019	3
35-225-2019	4
35-270-2019	5
35-241-2019	6
35-273-2019	7
35-239-2019	8
35-233-2019	9

PARTIDA 1 (SOLICITUD DE APROVISIONAMIENTO 35-242-2019)

Secretaria Administración

Servicio de Enlace Dedicado

1. GLOSARIO

- ✓ DIC: Dirección de Infraestructura y Comunicaciones.
- ✓ GEJ: Gobierno del Estado de Jalisco
- ✓ DGTI: Dirección General de Tecnologías de la Información.

2. ANTECEDENTES:

La tendencia en los últimos años en el Gobierno del Estado fue arrendar enlaces de telecomunicaciones los cuales se sujetaban a velocidades según presupuesto lo cual hacia complicado poder ofrecer mejores anchos de banda a las dependencias, por lo anterior, resulta fundamental que el Gobierno comience a hacer inversiones en infraestructura propia la cual pueda brindar servicios de mayor capacidad las instituciones que de ella dependen.

3. JUSTIFICACION

Actualmente la DGTI opera con servicios de conectividad arrendados los cuales imposibilitan la capacidad de crecimiento con infraestructura propia y crean dependencia con proveedores. Por lo anterior es necesario contar con enlaces dedicados que pasen a ser parte del inventario de activos del Gobierno del estado para su uso y aprovechamiento para mas servicios y dependencias.

4. OBJETIVOS:

La DGTI del Gobierno de Jalisco, tiene como objetivo, garantizar la disponibilidad, continuidad e integridad de los enlaces de servicio de internet, por lo tanto es indispensable contar con infraestructura propia que permita un crecimiento granular incrementando las velocidades de navegación y conexión entre dependencias.

5. INFORMACIÓN DEL REQUERIMIENTO:

Servicio de enlace dedicado punto a punto 10G

El proveedor deberá entregar los servicios de enlace dedicado a 10Gb en las siguientes puntas:

a) Secretaria de Administración.
- Av. Fray Antonio Alcalde 1221, Miraflores, 44266 Guadalajara, Jal.

Página **1** de **5**

LA VIGENCIA DE ESTE ANEXO SERA POR 90 DIAS A PARTIR DE LA FIRMA DE VALIDACIÓN DEL MISMO

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

03 SEP. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Secretaria Administración

Servicio de Enlace Dedicado

b) Secretaria de Educación.
- Av. Central Guillermo Gonzalez Camarena 615, Poniente, 45136 Zapopan, Jal.

c) POP de conexión.
- Av Chapultepec Sur 236, Lafayette, 44160 Guadalajara, Jal

- Dentro de la cobertura del servicio Enlace de fibra Optica de Secretaria de Administración al pop de conexión, se deberá considerar la rehabilitación y reforzamiento de infraestructura para anillo de fibra óptica de al menos 96 hilos para dotar de conectividad a la Secretaria de Administración ubicada en Av. Alcalde #1351, Col. Miraflores. C.P. 44270, Guadalajara, Jal.
  - La propuesta deberá incluir un plano detallado con la trayectoria a utilizar. Dicho plano deberá incluir al menos distancias, cruces, tipo de trayectoria, registros y cualquier otro dato relevante para su identificación.
  - La distancia lineal máxima a considerar es de aproximadamente 15.7 km, y la distancia óptica de hasta 17.5 km.
  - La trayectoria propuesta deberá incluir reforzamientos subterráneos con perforación direccional y/o canalización de hasta 480 metros evitando cualquier cargo por terceros.
  - La fibra deberá ser entregada en punta con conectores LC-LC para conectar en los GBICS con las mismas características.

- Las conexiones deberán quedar de la siguiente manera:
  1. Punta A Secretaria de Administración hacia Punta B Secretaria de Educación.
  2. Punta A Secretaria de Administración hacia Punta B Pop de conexión. (Ruta Principal).
  3. Punta A Secretaria de Administración hacia Punta B Pop de conexión. (Ruta Redundante).

- Como se observa en la explicación anterior, deberán habilitarse 3 rutas de las cuales las conexiones 2 y 3 deberán tomar rutas físicas totalmente distintas.

- Todos los misceláneos y nueva fibra deberán ser compatibles con la infraestructura existente de la cual se destacan las características mínimas:
  - Cable de fibra óptica tipo monomodo con doble cubierta armado seco 96F G652D D0003O S EX, con la capacidad de trasmitir 10gb OS1/OS2.
  - Atenuación máxima de fibra: 1,310NM 0.34 dB/km, 1,550NM 0.20 dB/km.
  - Diámetro de núcleo / campo modal (UM): 8.7-9.5/9.9-10.9
  - Cable diseñado para utilizarse en instalaciones de planta externa, específicamente en ducteria, contra roedores, con tubos holgados construidos con PP seco libre de gel, con hilo de bloqueo de agua como protección contra el agua, con doble cubierta de polietileno.

LA VIGENCIA DE ESTE ANEXO SERA POR 90 DIAS A PARTIR DE LA FIRMA DE VALIDACIÓN DEL MISMO

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
03 SEP. 2019
VALIDACIÓN TÉCNICA
COORDINACIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

aditivos que proporcionen una protección superior contra la radiación UV, los hongos, la abrasión y otros factores ambientales. Con armadura de aleación de cromo y acero corrugado altamente resistente para un desempeño excepcional frente a la compresión y la corrosión.

- Cable seco con franja dorsal naranja de 4mm, con leyenda "Propiedad Gobierno del estado Contacto: XXXX"
- Estándar IEC (International Electrotechnical Commission), de cable para instalaciones de telecomunicaciones.
- Cable anti flama, que cumpla con las especificaciones técnicas de las normas:
- IEC 332-1 No propagación llama
- IEC 332-2-C No propagación del incendio
- IEC 60793-1 Especificaciones genéricas para fibra óptica
- IEC 60793-2 Especificaciones de producto para fibra óptica.
- IEC 60794-1-2-E1 Tensión
- IEC 60794-1-2-E3 Aplastamiento
- IEC 60794-1-2-E4 Impacto
- IEC 60794-1-2-E6 Curva repetida
- IEC 60794-1-2-E7 Torsión
- IEC 60794-1-2-E11A Radio de curvatura
- IEC 60794-1-2-F1 Ciclos de temperatura
- IEC 60794-1-2-F5B Penetración del agua

- Las actividades mínimas que se deberán considerar para las nuevas rutas de fibra serán las siguientes:
  - Rehabilitación de infraestructura existente
  - Reforzamientos subterráneos con perforación direccional y/o canalización.
  - Suministro e instalación de registro.
  - Suministro de ducto.
  - Limpieza de registros y vías.
  - Inmersión de cable en tramo canalizado.
  - Suministro de fibra óptica de al menos 96 hilos.
  - Empalmes.

- ✓ La fibra deberá ser en su totalidad del gobierno del estado de Jalisco, por lo tanto, no se aceptarán propuestas utilizando fibra preinstalada o en arrendamiento.
- ✓ El proveedor será responsable de la gestión administrativa como permisos y adecuaciones a fin de llevar a cabo la instalación en cumplimiento con la normativa vigente.
- ✓ Cualquier trabajo que implique obra civil para canalización deberá estar incluido en la propuesta, así como reparaciones derivadas de trabajos de inmersión.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

03 SEP. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

LA VIGENCIA DE ESTE ANEXO SERA POR 90 DIAS A PARTIR DE LA FIRMA DE VALIDACION DEL MISMO

Secretaria Administración

Servicio de Enlace Dedicado

6. GARANTIAS:

El periodo deberá ser por 12 meses a partir de la entrega de los servicios.

El proveedor deberá llevar a cabo la implementación y entrega de servicios en un periodo no mayor a 3 meses posterior a la adjudicación.

7. OBLIGACIONES DEL PARTICIPANTE:

El participante deberá de cumplir con los siguientes requisitos:

- El proveedor adjudicado deberá considerar todos los materiales y herramientas necesarios para realizar la rehabilitación y reforzamientos subterráneos necesarios, (Fibra, OTDR, fusionadora, materiales, conectores, herramienta especializada, etc.)
- El proveedor adjudicado deberá incluir como parte de la rehabilitación y reforzamientos subterráneos todo lo necesario para la correcta ejecución de la misma (Misceláneos, Mano de Obra, Herramientas, Materiales, así como proporcionar al menos 2 números de celular para reporte de emergencias).
- El proveedor adjudicado deberá entregar memoria técnica considerando los planos de AutoCAD, diagrama unifilar, ubicaciones de registros, trayectorias con los domicilios de todo anillo de fibra óptica.
- La propuesta deberá incluir todas las características antes señaladas.
- El proveedor adjudicado deberá entregar 2 tantos de la memoria técnica, una impresa y otra en formato digital.
- El proveedor adjudicado en conjunto con la DIT definirá el programa de obra donde se especifiquen las fechas para efectuar los trabajos.
- El proveedor deberá presentar evidencia de haber ejecutado proyectos de fibra de igual o mayor magnitud

8. RESPONSABLES DE REQUERIMIENTO:

Responsable de elaborar el requerimiento	
Nombre: Stephany Crystin Cárdenas Patiño	
Puesto : Asistente administrativo	
e-mail: stephany.cardenas@jalisco.gob.mx	
Fecha: 29 Julio 2019	Tel. /ext. 38182872 ext. 26587
Firma:	

Responsable de autorizar el requerimiento	
Nombre: Miguel Ángel Romo Rubio	
Puesto: Dirección de Infraestructura y Comunicaciones	
e-mail: miguel.romo@jalisco.gob.mx	
Fecha: 29 Julio 2019	Tel. /ext. 3818 2800 Ext. 26255
Firma:	

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

03 SEP. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

LA VIGENCIA DE ESTE ANEXO SERA POR 90 DIAS A PARTIR DE LA FIRMA DE VALIDACION DEL MISMO

PARTIDA 2 (SOLICITUD DE APROVISIONAMIENTO 35-272-2019)

Secretaría de Administración

Póliza de mantenimiento a sistema de telefonía IP

1. GLOSARIO:

CUCM - Cisco Unified Communications Manager

GEJ – Gobierno del Estado de Jalisco.

VM – Virtual Machine

2. ANTECEDENTES

El Gobierno del estado de Jalisco cuenta con una plataforma de correo de colaboración del fabricante cisco, la cual es necesario mantener en operación correctamente debido a la criticidad. Recientemente se han llevado a cabo migraciones de servicios por lo que resulta indispensable garantizar la integridad del sistema.

3. JUSTIFICACIÓN

Derivado de los constantes cambios en configuración por las alta, bajas y modificaciones de servicios que se brindan a las distintas dependencias, es necesario contar con una poliza de soporte de segundo nivel, la cual permita realizar las configuraciones y en caso de ser necesario las correcciones de manera inmediata ante incidentes que puedan poner en riesgo la operación.

4. OBJETIVOS

El objetivo es contar con una póliza de soporte de segundo nivel que se encargue de atender incidentes críticos o configuraciones avanzadas para la integración o baja de servicios de telecomunicaciones.

5. REQUERIMIENTO

A) Póliza de mantenimiento a sistema de telefonía IP del Gobierno del Estado de Jalisco.

El proveedor deberá de brindar una póliza de soporte y mantenimiento por 12 meses de la plataforma de telefonía IP. A continuación se describen los requerimientos técnicos y de los niveles de servicio solicitados por la convocante.
El equipamiento que deberá de considerar el participante dentro de su propuesta para brindar el servicio de póliza de soporte y mantenimiento, se muestra en la siguiente tabla.

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

06 SEP. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
de 4

1

Secretaría de Administración

Póliza de mantenimiento a sistema de telefonía IP

Marca	Modelo / Descripcion	Versión / Cantidad	Tipo de Soporte requerido
Cisco	CUCM	10.5	24x7
VM	Publisher	1	24x7
VM	Subscriber	5	24x7
Cisco	IP Phone	4579	24x7
Cisco	Gateway	70	24x7

Tabla 1.- Equipamiento a considerar para la póliza de soporte y mantenimiento

Se deben de tener las siguientes consideraciones para brindar el servicio de la póliza de soporte y mantenimiento:

- El periodo solicitado para la póliza de soporte y mantenimiento es de 12 meses a partir de la firma de contrato.
- El soporte se deberá de brindar en la modalidad de 24x7 de acuerdo a la "Tabla 1" con reemplazo de partes al día hábil siguiente.
- El soporte no tendrá límite de eventos.
- El proveedor será responsable de levantar y dar seguimiento a tickets y escalacion con el fabricante según sea el caso hasta su cierre.
- El proveedor deberá considerar el ofrecimiento de una "Mesa de servicio" siendo este el conducto para solicitar soporte técnico en español.
- Para el levantamiento y seguimiento de tickets el proveedor deberá de proporcionar el acceso a una plataforma web de gestión de tickets.
- Se deberán de brindar al menos los siguientes medios de contacto hacia la mesa de servicio para el levantamiento y seguimiento a incidentes:
  - Soporte telefónico.
  - Soporte vía aplicación de acceso remoto brindada por el proveedor.
  - Soporte vía correo electrónico.
  - Plataforma Web.
- La mesa de servicios deberá cumplir con el seguimiento de buenas prácticas de acuerdo a la metodología de ITIL Ver3 actualización 2011.
- La mesa de servicios será responsable de los procesos de gestión de eventos, gestión de incidentes, gestión de problemas y gestión de peticiones.
- Los niveles de servicio acordados (SLA´s) que se brindarán para los diferentes tipos de tickets se detallan a continuación:
  - *Incidente Prioridad 1.*- Afectación grave o total en el servicio. Tiempo de solución máximo de 4 Horas.
  - *Incidente Prioridad 2.*-Fallas menores que impliquen la afectación parcial en el servicio o en algún componente de la solución. Tiempo de solución máximo 1 día hábil.
  - *Requerimientos.*- Los requerimientos de configuración que puedan ser planeados y no impliquen la afectación en la operación de los servicios, así como las actualizaciones de los sistemas y obtención de reportes. Tiempo máximo de solución conforme al requerimiento.

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

06 SEP. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Secretaría de Administración

Póliza de mantenimiento a sistema de telefonía IP

- La póliza deberá soportar todos los servicios profesionales especializados de segundo nivel entre los cuales se deberán incluir, altas, bajas, modificaciones y optimizaciones de teléfonos, claves, patrones de ruta, gateways, sincronización, respaldos, updates, upgrades, y cualquier otro requerimiento de configuración de segundo nivel.
- La póliza deberá incluir la renovación de la plataforma de videoconferencia webex para 40 sesiones simultaneas por un periodo de 12 meses.
- La propuesta deberá incluir una capacitación especializada a nivel asociado en voz para 2 personas con duración mínima de 20hrs.

6.- GARANTIAS

La vigencia de la póliza deberá ser por 12 meses a partir de la firma de contrato.

7.- OBLIGACIONES DE LOS PARTICIPANTES

El participante deberá de cumplir con los siguientes requisitos:

- El participante deberá incluir en su propuesta carta expedida por el fabricante donde lo acredite como canal certificado.
- Todas las especificaciones señaladas en este anexo son mínimas, por lo tanto el Licitante podrá ofertar bienes y servicios con especificaciones superiores, si así lo considera conveniente.
- El licitante deberá de contar dentro del personal de la empresa con al menos 2 ingenieros certificados vigentes a nivel profesional en colaboración o voz.
- El licitante deberá de contar dentro del personal de la empresa con al menos 1 ingeniero certificado en ITIL Fundamentos, será indispensable incluir dicho certificado en la propuesta.
- El proveedor deberá de demostrar residencia dentro de la zona metropolitana de Guadalajara con el objetivo de garantizar los tiempos de respuesta solicitados en el anexo.
- El proveedor deberá de demostrar residencia dentro de la zona metropolitana de Guadalajara con el objetivo de garantizar los tiempos de respuesta solicitados en el anexo.
- La dependencia se reserva el derecho de validar la documentación con el fabricante.
- El licitante deberá resentar dos cartas de recomendación de entidades donde se verifique la participación de dos proyectos similares, mostrar evidencia de contratos y/o órdenes de compra
- El licitante deberá contar con al menos un ingeniero CCNP Collaboration
- El licitante deberá demostrar contar con al menos un Proyect Manager con su certificado y mencionar el esquema de escalación
- El licitante deberá tomar en cuenta que el sistema para la mesa de Servicio de ayuda incluya por lo menos 8 procesos de ITIL V3 y que lo consiste en su propuesta.
- Incluir un diagrama de flujo donde se ejemplifique la atención de incidentes y solicitudes de servicio en la mesa

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
06 SEP. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
de 4

3

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Secretaría de Administración

Póliza de mantenimiento a sistema de telefonía IP

8. RESPONSABLES DEL REQUERIMIENTO

Responsable de elaborar el requerimiento		Responsable de autorizar el requerimiento	
Nombre: Stephany Crystin Cárdenas Patiño		Nombre: Miguel Ángel Romo Rubio	
Puesto : Asistente administrativo		Puesto: Dirección de Infraestructura y Comunicaciones	
e-mail: stephany.cardenas@jalisco.gob.mx		e-mail: miguel.romo@jalisco.gob.mx	
Fecha: 29 Agosto 2019	Tel. /ext. 38182872 ext. 26587	Fecha: 29 Agosto 2019	Tel. /ext. 3818 2800 Ext. 26255
Firma:		Firma:	

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

06 SEP. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Vigencia del documento: 60 días a partir del sello de validación

de **4**

Jalisco
GOBIERNO DEL ESTADO

PARTIDA 3 (SOLICITUD DE APROVISIONAMIENTO 35-230-2019)

Jalisco

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a sistema de monitoreo y gestión de red.

1. GLOSARIO:

- ✓ WAN - Red de área amplia
- ✓ LAN – Red de área local.
- ✓ SNMP - Protocolo simple de administración de red
- ✓ SMTP - Simple Mail Transfer Protocol o Protocolo para Transferencia Simple de Correo.
- ✓ IP – Protocolo de internet.

2. ANTECEDENTES

La dependencia cuenta actualmente con un sistema de monitoreo y gestión de conectividad el cual requiere renovación y actualización a la última versión del fabricante a fin de garantizar la disponibilidad de los servicios monitoreados.

3. JUSTIFICACIÓN

Derivado de la creciente demanda de servicios de red y sistemas web ofrecidos a la ciudadanía es fundamental contar con una solución que permita garantizar el monitoreo predictivo de cada uno de los servicios, por lo tanto, se requiere la actualización del sistema de monitoreo actual a fin de garantizar el correcto monitoreo de los sistemas.

4. OBJETIVOS

El objetivo del presente proyecto es llevar a cabo la renovación de la póliza de mantenimiento preventivo y correctivo de la solución de monitoreo de red avanzado así como los servicios especializados por parte del fabricante a fin de mantener el sistema de monitoreo de redes del Gobierno del Estado de Jalisco en óptimas condiciones previniendo así las caídas de sistemas o reducción de tiempos de respuesta ante incidentes.

5. REQUERIMIENTO

Póliza de mantenimiento y soporte avanzado del sistema de monitoreo y gestión de red

Deberá tener la capacidad de monitoreo de Redes
gestión de salud de red
Gestión de Salud de la Red

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
de **6**

1

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a sistema de monitoreo y gestión de red.

Visualización de problemas con la WAN/router. Monitoreo de routers e interfaces, ancho de banda, enlaces WAN para su disponibilidad y rendimiento.

Monitoreo de VoIP
Monitoreo activo de la calidad de llamadas VoIP a lo largo de la estructura WAN e identificación de rendimiento bajo de VoIP

Mapeo de redes
Mapeo automático de la red L1/L2 para poder visualizar y determinar con precisión las interrupciones en la red y la degradación del rendimiento.

Monitoreo de WAN RTT
Monitoreo continuo de disponibilidad de enlaces WAN, latencia y mejora del rendimiento con la tecnología de Cisco IP SLA.

Monitoreo de la Configuración de Red
Capacidad de automatización de los cambios basado en las pólizas, configuración y conformidad en los dispositivos de red a través de TI.

Análisis de tráfico en la red
Análisis del tráfico de la red basándose en el flujo para monitorear exactamente cómo es que el ancho de banda está siendo utilizado por los usuarios, aplicaciones, etc.

Gestión de Servidores a través de múltiples proveedores de SO.
Monitoreo de servers
Monitoreo tanto de los servidores físicos como los virtuales a través de múltiples proveedores de Sistemas Operativos como Windows, Linux, Solaris, Unix, VMWare, etc.

Monitoreo de VMWare
Monitoreo a profundidad y sin agentes de los servidores virtualizados de VMWare que estén usando hasta 70 VMWare monitores de rendimiento.

Monitoreo de Hyper-V
Use credenciales del tipo WMI para monitorear profundamente el rendimiento de los proveedores e invitados de Microsoft Hyper-V con más de 40 unidades de profundidad.

Monitoreo de Citrix XenServer
Monitoreo y gestión de Host, VMs y Repositorios de Almacenamiento de Citrix XenServer y obtención de la visibilidad requerida para su rendimiento.

Monitoreo procesos
Monitoreo y gestión de los dispositivos que están siendo ejecutados en los dispositivos encontrados a través de SNMP/ WMI/ CLI

Jefatura de Gabinete
COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
de **6**

2

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a sistema de monitoreo y gestión de red.

Monitoreo de salud de sistemas
De deberá usar procotolos como SNMP, WMI o CLI, para monitorear los recursos del sistema y recuperar la información del rendimiento.

Visualización del rendimiento el ancho de banda
Análisis del Tráfico en la Red
Monitoreo de Ancho de banda
Rastreo del uso del ancho de banda de su red de trabajo en tiempo real y mantenga el control de los principales usuarios de la banda ancha de tu red.

Monitoreo de Tráfico del Router
Monitoreo continuo de los dispositivos de red (routers y switchers) usando flujos y generar información crítica para asegurar el uso adecuado de ancho de banda de la red de trabajo.

Monitoreo de Cisco AVC
Visibilidad profunda sobre el consumo de ancho de banda por aplicación.

Análisis avanzado de seguridad
Módulo de análisis avanzado de seguridad
Detección de amenazas y ataques usando la tecnología SME.

Monitoreo de Cisco IPSLA
Monitoreo de las estadísticas que están afectando al VoIP, el rendimiento de video

Reportes de Cisco NBAR
Reconocimiento de una amplia variedad de aplicaciones que usan puertos dinámicos. Clasifica y toma las acciones apropiadas en las aplicaciones importantes y las que no lo son.

Gestión de la Configuración de Red
Respaldo de configuración
Calendarización de respaldos de la configuración cuando son requeridos. Las configuraciones respaldadas son versionadas y almacenadas de modo seguro en un formato encriptado.

Comparación de Configuraciones
Comparación de dos versiones de configuración del mismo dispositivo o de diferentes dispositivos. La diferencia en las configuraciones es resaltada lado a lado para una observación rápida.

Gestión de cambios
Rastreo en tiempo real los cambios a la configuración mediante mensajes syslog generados por los dispositivos. Los cambios detectados deberán ser notificados inmediatamente por e-mail.

Supervisión de conformidad
Definición de reglas y gestión de las configuraciones de los dispositivos para los estándares de conformidad a ser definidos. También generación de reportes para las regulaciones SOX, HIPAA, etc.

Actualización del Firmware y transferencia de imágenes del SO

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
de **6**

3

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a sistema de monitoreo y gestión de red.

Automatización de tareas repetitivas como la actualización del Firmware, la transferencia de imágenes del SO, configuración de avisos de banner, etc. con la ayuda de scripts avanzados (Configlets).

Rastreo de la actividad del usuario
Deberá mantener al corriente un reporte completo de quién, qué y dónde de los cambios de configuración necesita auditoría.

Gestión de Switches y Direcciones IP
Gestión de Direcciones IP
Revisión de la dirección IP si está disponible o no, en la red de trabajo.

Gestión de Switches
Revisión de todos los switches en la red y mapeo de los puertos de los switch a los dispositivos hasta su localización física.

Rastreo y resolución de fallos antes de que ocurran.
Gestión de Fallas
Herramientas monitoreo de redes
flujos de trabajo de TI
Automatización de flujos de trabajo de TI

Procesamiento de Trampas SNMP
Una máquina de procesamiento de trampas basada robustamente en reglas, que soporta manejar hasta 300 tramps SNMP por segundo.

Monitoreo de Event Log
Un monitor de Eventlog centralizado para monitorear accesos de seguridad importantes a través de todos los servidores de Windows y todas las estaciones de trabajo en tu red de trabajo.

Monitoreo de Syslog
Un método basado en reglas de monitoreo de Syslog para leer los Syslogs entrantes y asociar alertas a esos Syslogs.

Reportes de desempeño de las redes
Analiza la disponibilidad de red, las tendencias usadas y el análisis del desempeño en más de 100 reportes personalizables.

Gestión de sistemas
Monitoreo activo de los sistemas de TI como routers, switches, servidores (físicos y virtuales), carga de equilibrador de carga.

Gestión del centro de datos
Un centro de monitoreo de datos integrado para monitorear proactivamente servidores, aplicaciones y ancho de banda desde una sola consola en la red.

Jefatura COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
de **6**

4

Jalisco
GOBIERNO DEL ESTADO

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a sistema de monitoreo y gestión de red.

Escala a más de 1 millón de interfaces y asegurar una alta disponibilidad
Escalabilidad de Clase Empresarial
Monitoreo de la Red Empresarial
Una consola unificada de monitoreo de redes para la infraestructura distribuida. Escala hasta 100,000 interfaces o 10,000 dispositivos.

Análisis de la Causa Raíz
El módulo de Análisis de la Causa Raíz deberá ofrecer la visibilidad en tiempo real de los eventos recientes que ayude a identificar rápidamente las fallas en la red.

Gestión de Configuración de la Base de Datos
Deberá proveer una visibilidad profunda sobre los bienes presentes en el entorno de TI. Que ayude a asegurar tiempo de actividad y disponibilidad del servicio.

Descubrimiento automático de Redes
Deberá poder descubrir hasta 15,000 interfaces en un minuto.

La propuesta deberá incluir una capacitación remota oficial para 1 persona con duración de 20 horas

6.- GARANTIAS

La garantía de los servicios y vigencias deberán ser por 12 meses a partir de la firma de contrato.

7.- OBLIGACIONES DE LOS PARTICIPANTES

- En la propuesta se deberá de incluir la cantidad, número de parte, modelo y descripción de los productos.
- Los componentes propuestos deberán ser de última generación de acuerdo a las características del Road Map por fabricante.
- Todas las especificaciones señaladas en este anexo son mínimas, por lo tanto, el participante podrá ofertar bienes con especificaciones superiores, si así lo considera conveniente.
- El participante deberá de considerar la instalación y puesta a punto de la solución incluyendo la totalidad de interfaces, cables y conectores necesarios para la correcta operación de la solución.
- El participante deberá de considerar cualquier otro tipo de componente en HW, SW, mano de obra, viáticos, traslados, etc. Que se requieran para la correcta instalación, configuración y puesta a punto.
- El licenciamiento deberá incluir capacidad de monitoreo de 5000 puertos IP, 500 dispositivos, 500 interfaces, 5 firewall.

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
de 6

5

Jalisco

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a sistema de monitoreo y gestión de red.

- El proveedor adjudicado deberá entregar memoria técnica a detalle de la instalación.
- Para garantizar la correcta instalación, el participante deberá de contar con al menos 1 ingeniero certificado en la solución.
- El participante deberá incluir en su propuesta carta bajo protesta de decir verdad de que cuenta con oficinas operativas en la zona metropolitana de Guadalajara con el objetivo de garantizar los tiempos de respuesta.
- El participante deberá incluir carta por parte del fabricante donde se mencione que es distribuidor autorizado de la solución.

8. RESPONSABLES DEL REQUERIMIENTO

Responsable de elaborar el requerimiento	
Nombre: Stephany Crystin Cárdenas Patiño	
Puesto : Asistente administrativo	
e-mail: stephany.cardenas@jalisco.gob.mx	
Fecha: 29 Julio 2019	Tel. /ext. 38182872 ext. 26587
Firma:	

Responsable de autorizar el requerimiento	
Nombre: Miguel Ángel Romo Rubio	
Puesto: Dirección de Infraestructura y Comunicaciones	
e-mail: miguel.romo@jalisco.gob.mx	
Fecha: 29 Julio 2019	Tel. /ext. 3818 2800 Ext. 26255
Firma:	

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
de **6**

6

PARTIDA 4 (SOLICITUD DE APROVISIONAMIENTO 35-225-2019)

Jalisco

Secretaria de Administración

Adquisición de sistema de video proyección

1. GLOSARIO:

Siglas o palabra	Significado
Videowall	*Muro de video proyección*
N/A	

2. ANTECEDENTES

La secretaria de administración cuenta con un sistema videowall obsoleto el cual debido al uso constante y años de uso ha dejado de funcionar correctamente y no existen piezas de reemplazo

3. JUSTIFICACIÓN

Se requiere la renovación del videowall del centro de monitoreo de la secretaria de administración toda vez que esta área es la responsable de monitorear los enlaces y servicios que brindan conectividad a las distintas dependencias del poder ejecutivo.

4. OBJETIVOS

Contar con las herramientas de monitoreo y control necesarias para el correcto diagnostico y seguimiento de incidentes en tiempo real.
El muro de video es necesario para identificar incidentes en tiempo real y ejecutar acciones de colaboración que permitan la rápida solución y acción preventiva con el equipo de respuesta inmediata.

5. REQUERIMIENTO

Progresivo 1

Cantidad: 2

Sistema de pantalla LED con al menos las siguientes características:

La pantalla deberá estar conformada por gabinetes de pantalla led.

La calidad de vista a distancia en pitch deberá ser de 2.8mm o inferior.

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

1 de 4

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Secretaria de Administración

Adquisición de sistema de video proyección

Los gabinetes no deberán medir mas de 1000mm x 250mm.

Deberá tener la capacidad estándar de Easy Assembly para su fácil instalación.

Deberá soportar al menos resolución total en pixeles de 686 x 888.

El sistema deberá contar con certificación IP40 para interior.

El sistema deberá operar con un brillo de al menos 1000 nits.

La frecuencia de frames deberá ser del al menos 3840Hz .

El consumo máximo a fin de reducir costos eléctricos deberá ser de 415w por metro cuadrado en blancos y con brillo máximo.

Se deberá garantizar una vida útil del led de 100,000 horas.

La solución deberá incluir el procesador de video que soporte la carga máxima de procesamiento sin bloqueos, congelamientos o pantallas negras.

Deberá soportar al menos entradas de tipo HDMI, SDI, VGA y DVI.

La propuesta deberá incluir la instalación y puesta a punto de la solución.

La propuesta deberá incluir la entrega de generación de planos de ingenierías.

La medida mínima del sistema propuesto deberá ser de 3 x 2 metros reales sin marcos o bordes.

La solución deberá incluir modulo de conferencias a través de una consola central de control con una tableta especializada y sistema de control bipartita.

La consola central deberá soportar conectividad HDMI para pantallas 1080p o superior además de al menos tres puertos USB, un puerto de red en velocidad gigabit ethernet y una toma para auriculares.

El sistema deberá permitir compartir pantalla u otro contenido desde cualquier portátil.

La instalación deberá incluir todos los herrajes, materiales y accesorios necesarios para su correcta instalación con artículos del mismo fabricante.

En materia de montaje se deberá incluir el modelado y diseño de front para coberturas de montaje y sistemas de ventilación acorde a las especificaciones del fabricante en muros de hasta 100m2.

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

Jalisco

Secretaria de Administración

Adquisición de sistema de video proyección

6. GARANTIAS

Toda la solución deberá incluir al menos 1 año de garantía.

7. OBLIGACIONES DE LOS PARTICIPANTES

- *Podrá ofertar características iguales o superiores a las solicitadas, lo cual deberá ser corroborado por el fabricante que se oferte como superior mediante carta por el representante legal.*
- *El proveedor deberá incluir la instalación y puesta a punto.*
- *La propuesta deberá incluir todos los misceláneos necesarios para la correcta instalación sin que esto implique un costo extra para la convocante.*
- *El proveedor deberá incluir una capacitación especializada para todo el sistema.*
- *No se aceptarán soluciones con bordes, reconstruidas, o multimarcas por lo que deberá ser una solución homogénea.*
- *Toda la solución deberá ser completamente nueva.*
- *La propuesta deberá considerar el desmontaje y empaquetado del sistema existente.*
- *Con el objetivo de garantizar la correcta instalación de la solución, el proveedor deberá presentar evidencia de contar con personal certificado para la instalación del sistema propuesto.*
- *El proveedor deberá incluir en su propuesta evidencia de que los equipos propuestos cumplen con certificaciones de calidad y RoHS*

8. ENTREGABLES

Sistema de video muro y todos sus accesorios.

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Secretaria de Administración

Adquisición de sistema de video proyección

9. RESPONSABLES DEL REQUERIMIENTO

Responsable de elaborar el requerimiento		Responsable de autorizar el requerimiento	
Nombre: Stephany Cristyn Cardenas Patino		Nombre: Miguel Angel Romo Rubio	
Puesto: Asistente administrativo		Puesto: Director de Infraestructura y Comunicaciones	
e-mail: stephany.cardenas@jalisco.gob.mx		e-mail: miguel.romo@jalisco.gob.mx	
Fecha: 11/08/2019	Tel. /ext. 26587	Fecha:11/08/2019	Tel. /ext. 26255
Firma:		Firma:	

Vigencia del documento: 60 días a partir del sello de validación

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

4 de 4

PARTIDA 5 (SOLICITUD DE APROVISIONAMIENTO 35-270-2019)

Jalisco

Secretaría de Administración

Póliza de mantenimiento y actualiación del Sistema de Depósitos Vehiculares

1. GLOSARIO:

Siglas o palabra	Significado
Software flexible	*Desarrollar una gran parte del software según los requerimientos estándares del mercado, ahorrando tiempo de desarrollo y costos.*
Diseño web adaptable (diseño responsivo)	*Técnica de diseño y maquetación web para visualizar el mismo contenido de la página web en diferentes dispositivos como teléfonos móviles, tabletas y ordenadores de sobremesa.*
Facilidad de crecimiento	*El sistema debe de estar estructurado con la visión de poder integrar más módulos permitiendo la reutilización de funciones y estructuras de acceso a datos, interfaces, etc.*
Web services	*Interconexión con otros sistemas tipo REST.*
Composer	*Composer es un administrador de paquetes a nivel de aplicación para el lenguaje de programación PHP que proporciona un formato estándar para administrar las dependencias del software PHP y las bibliotecas requeridas*
P.A.E.	*Procedimiento Administrativo de Ejecución*

2. ANTECEDENTES

La Dirección de Depósitos Vehiculares perteneciente a la Secretaría de Administración, actualmente cuenta con el Sistema de Administración de Depósitos Vehiculares, cuya función principal es integrar en una sola plataforma de forma modular los procesos administrativos y operativos relacionados a la gestión de los diversos depósitos vehiculares con los que se cuentan en los municipios conurbanos de la zona metropolitana de Guadalajara, pero ahora, las necesidades han cambiado y se requiere actualizar el sistema con mayores funcionalidades y cambios en los módulos.

3. JUSTIFICACIÓN

Parte de los servicios que se ofrecen a la ciudadanía es la localización de los vehículos en los depósitos vehiculares, además de una mejor administración y gestión en los mismos depósitos, por lo tanto, se requiere de una actualización al desarrollo de software tanto de consulta para la ciudadanía como de control en la administración los depósitos vehiculares.

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

06 SEP. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

1 de 5

a. *10% hasta 100% dependiendo el caso*

5. *Administración: es la configuración de los depósitos, el acomodo del mismo en cajones almacenes con diferentes roles:*
   a. *Administrador; todos los permisos*
   b. *Jefe de patio;*
      i. *Cambio de ubicación dentro del deposito*
      ii. *Reclamaciones o incidencias*
      iii. *Búsqueda y consulta de vehículos, autoridades y compañía de grúa*
   c. *Perito;*
      i. *Modificación de datos de vehículo*
   d. *Auditor; podrá observar todos los procesos ejecutados dentro del sistema*
6. *Almacén Fiscal; entradas y salidas de mercancía*
7. *Catálogos: es la configuración de los listados de (Autoridades, Usuarios, Tipo de Vehículos, Compañía de grúas, Tarifas, Razón de la detención).*
8. *Cajas: donde se realizan las bajas de los inventarios de acuerdo a los pagos realizados para liberar el vehículo.*
9. *P.A.E.: Modulo donde entran en procedimiento para poderlos (Rematar, Compactar, Comodato) que será administrado por Secretaria de Hacienda.*
10. *De manera automática después de 180 días de pensión deberá pasar a procedimiento de embargo.*
11. *Bloqueo Administrativo: Todos los vehículos que tengan más de 180 días de Guarda y Custodia, cambiar estatus en el padrón vehicular del estado de Jalisco a "bloqueo administrativo" a través de web service.*
12. *Tablero de control: se desarrollará reportes gráficos (por fecha, autoridad, compañía de grúa, deposito, entre otros).*
13. *Pagos en línea (módulos: 4 y 7).*

Página para consulta ciudadana: el sistema deberá generar una vista para el ciudadano en donde podrá hacer una búsqueda de su vehículo en cualquiera de los depósitos colocando el número de serie y placa del vehículo.

Especificaciones técnicas:

- *Desarrollo con lenguaje optimizado y diseñado especialmente para aplicaciones de alta demanda en plataformas web como PHP 7.1.3 o superior y Laravel 5.1 o superior o CodeIgniter 3.1.10 o superior. En su defecto, el lenguaje de programación podrá ser en java 7 o superior.*
- *Arquitectura de desarrollo de la aplicación MVC (Modelo, Vista, Controlador) y Composer.*
- *Tipo de aplicación: el sistema deberá funcionar bajo entorno web y deberá instalarse en un servidor web con certificado SSL.*
- *Desarrollo de web services para intercomunicar con otros sistemas.*

Plataforma tecnológica (hardware):

- *Sistema operativo Ubuntu 18.04 LTS*
- *Base de datos: MySQL 5.7 o superior o MaríaDB 10.0 o superior*
- *Servidor Apache 2.2 o superior*

Requerimientos de hardware:

- *10 tabletas de uso rudo con las siguientes características:*
  - *Tamaño de la pantalla: 8 pulgadas*
  - *Procesador: 1.6 GHz*

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

06 SEP. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Secretaría de Administración

Póliza de mantenimiento y actualiación del Sistema de Depósitos Vehiculares

8. ENTREGABLES

- *Código fuente de la actualización del software desarrollado.*
- *Plan de trabajo de implementación del software con definición detallada de entregables.*
- *Documentación de casos de usos.*
- *Documentación técnica de la base de datos.*
- *Documentación referente a la operación del sistema (manual de administrador, manual de usuario, etc.)*
- *Diagrama de la arquitectura de implementación de la solución.*
- *Manuales de usuario y administración del sistema.*
- *Cursos de capacitación para el uso y administración del sistema.*
- *Documento de resultados de las pruebas hechas al software.*
- *Documentos de confiabilidad.*
- *10 tabletas con kit de conexión y funda protectora.*

9. RESPONSABLES DEL REQUERIMIENTO

Responsable de elaborar el requerimiento	
Nombre: David Daniel Tapia Ramírez	
Puesto: Encargado de Área B Depósitos Vehiculares de la Secretaria de Administración	
e-mail: daniel.tapia@jalisco.gob.mx	
Fecha: 05-Agosto-2019	Tel. /ext.
Firma:	

Responsable de autorizar el requerimiento	
Nombre: Adolfo Eletvan Chávez Manzo	
Puesto: Director de Depósitos Vehiculares de la Secretaria de Administración	
e-mail: adolfo.chavez@jalisco.gob.mx	
Fecha: 05 –Agosto-2019	Tel. /ext.
Firma:	

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

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

06 SEP. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

5 de **5**

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

PARTIDA 6 (SOLICITUD DE APROVISIONAMIENTO 35-241-2019)

Secretaria de Administración

Póliza de antivirus

1. GLOSARIO:

[Anotar en orden alfabético las siglas o palabras técnicas y su correspondiente significado]

Siglas o palabra	Significado

2. ANTECEDENTES

Debido al próximo término en la vigencia del contrato anual de de Antivirus, es de vital importancia su renovación en Organismos y Poder Ejecutivo.

3. JUSTIFICACIÓN

Es indispensable contar con un Software Antivirus que brinde la protección y seguridad a la información institucional que se almacena en los equipos de cómputo (PC's de escritorio, estaciones de trabajo, laptops, servidores) y que además cuente con opciones de antispam y firewall y que funcione para todas las versiones del Sistema Operativo Microsoft Windows, Linux y Mac OS.

4. OBJETIVOS

Proteger al equipo de virus que podrían causar daño, tanto a datos como a la seguridad en general del equipo.
Facilitar una navegación segura en Internet. Al descargar cualquier archivo a nuestro equipo puede contener software malicioso que puede dañar el equipo.

5. REQUERIMIENTO

Progresivo N° : **1**
Descripción: **Antivirus Administrable por Consola**

INSTALACIÓN DE SOLUCIÓN DE ANTIVIRUS PARA EL GOBIERNO DEL ESTADO DE JALISCO.

1. **Características de protección en puntos finales**

La solución deberá brindar protección para servidores, equipos móviles, y estaciones de trabajo sobre Windows XP, Windows Vista, Windows 7 (32 y 64 bits) Windows 8, Windows 8.1, Windows 10, Windows Server 2003, Windows Server 2008, Windows Server 2012 o cualquier versión de Microsoft en su ultima actualizacion, Mac OS (todas sus versiones) y Linux. Deberá ser capaz de proveer funcionalidad de protección con las siguientes tecnologías:

30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

1 de 8

[redacted]

Secretaria de Administración

Póliza de antivirus

- Antivirus
- Antispyware
- Firewall
- Motor de prevención contra intrusos
- Motor de detección de intrusos
- Control de aplicaciones
- Control de dispositivos
- Control Web
- Terminal Server

La solución deberá permitir que el uso e integración de las tecnologías de protección sea a través de políticas configurables y flexibles en un esquema jerárquico (dominios, sitios, grupos, subgrupo, cliente, usuario, localidades, etc.) para aplicar a perfiles de usuario o equipos en base a los criterios definidos por la Dirección General de Tecnologías de las Información de la Secretaría de Administración del Gobierno del Estado de Jalisco y deberán asignarse desde la consola de administración de la solución.

La solución de protección deberá ser configurable para definir de forma flexible diferentes niveles de interacción con el usuario final, es decir permitir al usuario realizar algunas o varias funciones o restringirlas por completo.

La solución de protección deberá permitir que las actualizaciones llámese versiones, parches, adecuaciones o modificaciones propias de la solución de protección puedan realizarse de forma automatizada con escasa o nula interacción administrativa teniendo en cuenta un parque de equipos protegidos de al menos 16,434 unidades. Lo anterior deberá realizarse desde la consola central.

La solución deberá ser capaz de prevenir la desinstalación sin autorización de la herramienta e incluso poder utilizar una contraseña.

La solución deberá ser capaz de evitar que los procesos correspondientes que proveen la protección sean manipulados o comprometidos en forma mal intencionada o sin autorización.

La solución deberá ser capaz de enviar en forma automática a la consola y al fabricante los riesgos de seguridad detectados para su revisión y valoración.

En caso de ser necesario, la solución deberá poder desinstalar cualquier antivirus existente antes de hacer la instalación del nuevo, mediante las mejores prácticas asegurando el buen funcionamiento del equipo de cómputo.

La solución deberá permitir la configuración flexible de acciones a tomar ante la detección de riesgos de seguridad.

La solución deberá ser capaz de configurar notificaciones sobre la detección de riesgos en base a roles o perfiles de responsabilidad definidos por la Dirección General de Tecnologías de las Información de la Secretaría de Administración del Gobierno del Estado de Jalisco.

La solución deberá ser capaz de soportar esquemas de replicación, balanceo de cargas en las consolas de administración centralizadas para estar abiertos a la implementación de planes de recuperación de desastres y disponibilidad de servicio.

La solución deberá ser capaz de integrarse al directorio activo para importar y configurar estructuras organizacionales (usuarios y equipos) para ser cubiertos con la protección de seguridad.

Jefatura COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Póliza de antivirus

La solución debe ser capaz de manejar diferentes formas de instalación en los equipos de los usuarios finales (por ejemplo interactiva, silenciosa, reiniciar equipo o no)

La solución deberá contar con el respaldo de una base de datos de conocimientos, descargas, actualizaciones, documentación, soporte, seguimientos de casos de escalación, despliegue de información provista y mantenida directamente por el fabricante.

La solución deberá ser capaz de manejar un esquema que incluya cuarentena centralizada de los riesgos de seguridad detectados.

La solución deberá de ser capaz de proveer protección de seguridad tanto a usuarios finales administrados centralmente como a usuarios finales descentralizados.

La solución deberá de ser capaz de proveer protección de seguridad tanto a usuarios finales como a servidores de propósitos específicos o aplicativos.

La solución deberá de ser capaz de poder remover antivirus de diversos fabricantes antes de poderse instalar el cliente.

La solución deberá ser capaz de soportar la administración centralizada de un ambiente de mínimo 16,434 usuarios finales.

La solución deberá ser capaz de soportar el uso de BDs externas (no propietarias de la solución) por ejemplo SQL server.

La tecnología de protección provista por la solución deberá ser altamente efectiva para la detección y remoción de riesgos de seguridad en la categoría de rootkits, amenazas de virus, gusanos troyanos, software espía, software malicioso, entre otros.

La instalación del agente de protección deberá poder realizarse de al menos los siguientes métodos: local utilizando la media de instalación, remotamente desde la consola, por medio de un servidor de Intranet o utilizando herramientas de distribución de terceros.

La comunicación del agente con la consola de administración deberá poder realizarse por medio de los protocolos http y https para no provocar modificaciones en la configuración de los switches.

La solución deberá actualizar su contenido (firmas de detección de virus, firmas de detección de intrusos, listado de aplicaciones) desde la consola de administración, desde Internet, desde un equipo definido para la actualización local, inclusive en forma manual.

La solución de protección deberá incluir tecnología de antivirus y antispyware que detecte intentos de infección desde unidades de disco, unidades removibles, unidades compartidas, así como memoria.

La solución de protección podrá ser configurada para que al intentar abrir la interface del usuario solicite una contraseña, en caso de no conocer la contraseña, el usuario no podrá abrir la interface.

Las políticas para la solución de protección deberán poderse aplicar por computadora o por usuario, deberán poderse aplicar por grupo, subgrupo o a todo el universo de equipos.

La solución de protección deberá tener capacidad para identificar el tipo de red al cual se está conectando para adecuar las políticas de protección de antivirus y antispyware, Firewall, IPS, control de Dispositivos, así como de políticas de actualización. La detección de la ubicación deberá poder realizarse por al menos las siguientes variables: rango de dirección IP, dirección IP/nombre del servidor de nombres DNS, dirección IP/nombre del servidor de WINS, default Gateway.

COORDINACIÓN GENERAL DE ADMINISTRACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Secretaria de Administración

Póliza de antivirus

2. Administración

Deberá contar con una consola de administración centralizada, desde la cual se pueda monitorear el estado de la seguridad en los equipos de cómputo del Gobierno del Estado de Jalisco.

La consola deberá tener la capacidad de ser accedida desde cualquier punto de la red utilizando a través de un navegador (Internet Explorer, Mozilla Firefox, Chrome).

La consola deberá indicar por medio de una representación gráfica el estado actual de la seguridad, los niveles de seguridad deberán poder ser definidos por el personal que indique la convocante.

La consola de administración deberá mostrar en una gráfica el estado de la actualización de los patrones de detección en los agentes. En una tabla de mayor detalle deberá indicar el nombre del equipo, su dirección IP, el usuario que se firmó en el equipo y el sistema operativo.

La consola de administración deberá mostrar en una gráfica los intentos de infección más recientes, así como los equipos que presentaron dichos intentos de infección indicando además la acción tomada por el agente de protección.

La consola de administración deberá mostrar un indicativo del estado de la seguridad en Internet, este estado deberá permitir al administrador de la solución identificar los niveles de riesgo del exterior para poder realizar ajustes en las políticas de protección.

La consola de administración deberá funcionar como un repositorio central de políticas para las tecnologías de Antivirus, firewall personal, detección y prevención de intrusos así como de protección al sistema operativo y control de dispositivos.

La consola de administración deberá contar con un esquema de autenticación local, con enlace al directorio activo o con un enlace por medio de RSA para autenticación fuerte.

La consola de administración deberá permitir la creación de administración por roles, para permitir una segregación de funciones.

La consola de administración deberá permitir la generación de reportes gráficos que permitan
Identificar:

Los intentos de infección más repetidos en el ambiente de la convocante, los equipos con mayor
Número intentos de infección, versión del agente de protección instalado en los equipos y un reporte de los equipos con las firmas de contenido.

La consola de administración deberá integrar una función que permita reconocer equipos que no tengan el agente de protección instalado. Para posteriormente enviárselo a través de la consola.

La consola de administración deberá permitir la instalación remota del agente de protección en los equipos que no cuenten con él. La instalación deberá poderse realizar dando el nombre del equipo, su dirección IP o una lista combinando ambas opciones.

La consola de administración deberá permitir la creación de roles para definir diferentes niveles de administración.

La tecnología de antivirus deberá contar con certificación ICSA Labs en los siguientes rubros: Antivirus cleaning criteria y Desktop/Server antivirus detection.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE [illegible]

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Póliza de antivirus

La tecnología de antivirus de la solución deberá ser capaz de detectar y eliminar spyware.

La tecnología de antivirus de la solución deberá ser capaz de analizar los mensajes de correo electrónico recibidos en los protocolos SMTP (Simple Mail Transfer Protocolo) y POP3 (Post Office Protocol).

La tecnología antivirus de la solución deberá poder actualizar sus definiciones de virus desde Internet, el servidor central y desde un repositorio local, (será decisión de la Dirección General de Tecnologías de las Información de la Secretaría de Administración del Gobierno del Estado de Jalisco determinar el método más adecuado teniendo en cuenta diversos factores), la actualización de definiciones deberá poderse programar para realizarse en un horario que no provoque afectación a la red.

La tecnología antivirus de la solución deberá ser capaz de realizar las actualizaciones de forma óptima, firmas de virus así como el motor de búsqueda (por ejemplo utilizando actualizaciones diferenciales y métodos de distribución).

La tecnología antivirus de la solución deberá ser capaz de analizar archivos comprimidos en al menos los siguientes formatos: ZIP, RAR, y TAR deberá ser capaz de analizar hasta 10 niveles de compresión.

La tecnología de antivirus de la solución deberá ser capaz de definir exclusiones por tipo de archivo, directorios y tipo de amenaza.

La tecnología de antivirus deberá realizar escaneos de los equipos de manera eficiente, excluyendo todos aquellos archivos que basados en reputación por parte del fabricante, no representen un riesgo, al contar con una buena reputación.

Las políticas de antivirus de la solución deberán poderse adaptar de acuerdo al reconocimiento de la red a la cual se está conectando.

El fabricante de la solución deberá tener su propio centro de investigación y respuesta de virus, además debe poder generar actualización a contenidos para las tecnologías de antivirus, el firewall personal y detección y prevención de intrusos.

La tecnología de antivirus deberá contar con tecnología de reputación, es decir que valide si un archivo goza de mala reputación para que este sea bloqueado, o si goza de buena reputación para que este sea excluido.

El agente deberá ofrecer protección al descargar archivos desde internet, al validar que el archivo descargado tenga una reputación aceptable, o en términos de distribución y antigüedad del mismo a nivel mundial.

La solución deberá contar con herramientas con permitan escanear máquinas virtuales off-line.

La solución deberá contar con la capacidad de excluir en las máquinas virtuales, todos aquellos archivos que ya hayan sido escaneados de una imagen base, con la finalidad de reducir el consumo de recursos.

3. Características de la tecnología de firewall personal y prevención de intrusos

La tecnología de firewall personal de la solución deberá ser de tipo stateful inspection capaz de analizar el tráfico en paquetes de tipo TCP, UDP, IP y en flujo de datos.

La tecnología de firewall de la solución deberá permitir la definición de reglas por aplicación, por protocolo.

La tecnología de firewall de la solución deberá integrar un módulo de detección y prevención de intrusos, deberá contener firmas de ataques, estas firmas deberán ser actualizadas desde Internet o desde el servidor central.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

La tecnología de firewall de la solución deberá ser capaz de detectar y deshabilitar controladores de programas como WinPcap y VMware por considerarse riesgosos.

La tecnología de firewall de la solución deberá contener un módulo que permita el reconocimiento de explotación de vulnerabilidades no importando el método de explotación que se esté utilizando.

La tecnología de firewall de la solución deberá tener un módulo de inspección profunda para los protocolos DHCP, DNS y WINS.

La tecnología de firewall de la solución deberá ser capaz de configurar el navegador en modo seguro de tal manera que no publique la versión del navegador ni la dirección IP con la que sale a Internet.

La tecnología de firewall de la solución deberá ser capaz de detectar y bloquear ataques de OS fingerprint y de generación de secuencias de TCP.

La tecnología de detección de intrusos de la solución deberá incluir ataques en diferentes categorías, las categorías incluidas deberán ser: ataques de buffer overflow, puertas traseras, ataques de negación de servicios, puertas traseras, programas de P2P, mensajeros y propagación de amenazas.

La tecnología de detección de intrusos también se deberá integrar al navegador de internet, para brindar protección a los usuarios finales.

4. Características de control de aplicaciones para protección de sistema Operativo

La tecnología de protección de la solución al sistema operativo debe incluir mecanismos que eviten la ejecución de procesos maliciosos, estos procesos deberán poder ser definidos a través de políticas.

La tecnología de protección de la solución al sistema operativo deberá incluir mecanismos que eviten la escritura, lectura o modificación de archivos o directorios. Estos deberán poderse definir a través de políticas.

La tecnología de protección de la solución al sistema operativo deberá incluir mecanismos que eviten la escritura, modificación o eliminación de llaves de registro. Las llaves de registro a proteger deberán definirse por medio de políticas.

5. Características de bloqueo de dispositivos

La tecnología de bloqueo de dispositivos de la solución deberá permitir el bloqueo de los siguientes dispositivos: USB, bluetooth, PCMCIA, SCSI. Tarjetas inalámbricas, además deberá permitir la definición de nuevos dispositivos por medio del Class ID y Device ID.

La tecnología de bloqueo de dispositivos de la solución deberá permitir la creación de exclusiones para permitir el bloqueo de USB pero no del teclado y el Mouse por ejemplo.

La tecnología de bloqueo de dispositivos de la solución deberá permitir el bloqueo de ejecución de programas desde dispositivos removibles. La tecnología de bloqueo de dispositivos de la solución deberá permitir utilizar los dispositivos removibles como solo lectura.

6. Servicios

El alcance de los servicios ofrecidos deberá cubrir la instalación y puesta a punto de la solución ofertada. Se tomará como modelo la dependencia que la convocante elija y ahí se realizará la instalación en sitio para la totalidad de los equipos existentes en dicha dependencia.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Secretaria de Administración

Póliza de antivirus

Se deberá realizar la instalación y puesta a punto de la totalidad de las consolas de la solución. Se deberá brindar apoyo remoto y presencial, en caso de requerirse, al personal que la convocante designe para realizar la instalación de la solución en el resto de los equipos del Gobierno del Estado de Jalisco.

6. GARANTIAS

Garantia por 1 año de servicio a partir del 6 de diciembre del 2019

7. OBLIGACIONES DE LOS PARTICIPANTES

- La totalidad de las partidas serán adjudicadas a un solo proveedor.
- La propuesta debe incluir capacitación en línea permanente, ofrecida por el proveedor.
- El licitante deberá considerar cualquier componente de equipamiento, programas, mano de obra, viáticos, traslados etc. que se requieran para la correcta instalación, configuración, puesta a punto de la solución y capacitación, estos puntos deberán de estar incluidos en el precio de su propuesta.
- La propuesta debe incluir el diagrama de la arquitectura de la solución.
- El adjudicado deberá presentar, previo al arranque de los trabajos una propuesta de plan de trabajo apegado a las mejores prácticas, el cual será validado por personal de la convocante, en el cual se muestren las principales actividades, tiempos y responsables para la implementación, capacitación, incluyendo, en caso de requerirse, la desinstalación del producto a sustituir.
- El licitante adjudicado deberá de entregar memoria técnica a detalle de la instalación de cada uno de los componentes que integran la presente solicitud y de la operación del conjunto de la misma.
- En la propuesta se deberá incluir de manera detallada la cantidad, número de parte, modelo y descripción de los productos y servicios ofertados, en los supuestos de descritos en párrafos anteriores.
- El licitante deberá entregar carta en la que el fabricante lo acredite como canal autorizado para ofrecer los productos de la solución presentada.
- El licitante deberá contar con al menos 2 personas certificadas para la implementación de la solución. Deberá anexar copia de los certificados vigentes de dicho personal.
- La propuesta deberá incluir la puesta a punto de las consolas necesarias para la correcta operación de la solución.
- La propuesta deberá incluir soporte técnico por el período ofertado.
- El alcance de la solución será de 16,434 (dieciséis mil cuatrocientos treinta y cuatro) licencias en servidores y estaciones de propiedad del Gobierno del Estado de Jalisco.
- El licitante deberá entregar carta con los requerimientos mínimos de hardware, **mismos que deberá ser compatible con todos los sistemas operativos y servidores**, para la instalación del antivirus en clientes y servidores de tal manera que valide el correcto funcionamiento del antivirus en las estaciones de trabajo. En caso de encontrar equipo con características inferiores presentar reporte.
- Deberá presentar carta indicando que respetará el precio acordado para todas las dependencias del Poder Ejecutivo, así como a sus Organismos Públicos Descentralizados, Desconcentrados y Municipios del Estado de Jalisco que posteriormente requieran licencias a fin de homologar todas las dependencias de Gobierno Estatal y Municipal en lo que respecta a protección de antivirus.
- La propuesta deberá incluir un documento de los niveles de SLAs, (de acuerdo al anexo A), así como un esquema de escalamiento de acuerdo a severidad.

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

- En el documento SLA, deberá incluir, números locales de la Zona Metropolitana de Guadalajara de su área de soporte técnico y celulares de los ingenieros que brindarán el soporte técnico.
- La carta anterior deberá describir detalladamente el servicio de soporte técnico y solución de problemas, cuya escalación será, en primera instancia remota (número telefónico, correo-e, chat) y posteriormente, en caso de requerirse, deberá ser presencial sin costo adicional. Estos servicios deberán ser independientes a los que ofrezca el fabricante ya que se considerará al fabricante como el último nivel del escalación de soporte técnico y solución de problemas.
- Al finalizar cada soporte técnico, el Proveedor deberá entregar un reporte que evidencie su asistencia técnica, firmado y sellado por el encargado de administrar la herramienta en el sitio o dependencias del poder ejecutivo y organismos públicos descentralizados y desconectados.
- El proveedor deberá llevar una bitácora de registro para la solución de incidentes, la cual deberá incluir número de evento, ticket o folio, seguimiento y fechas de levantamiento y solución. Esta bitácora deberá entregarse a la Dirección General de Tecnologías de la Información de la Secretaría de Administración, al finalizar cada mes del contrato.
- El precio ofertado deberá ser el mismo para todo el Gobierno del Estado de Jalisco.
- El proveedor deberá ser el responsable del transporte hacia/desde las diferentes dependencias a nivel estatal donde haya necesidad de instalar la herramienta o brindar soporte por fallos a la misma.
- Para un mejor control del ingreso del personal técnico del Proveedor, involucrados en la instalación de la herramienta a las diferentes oficinas de las dependencias, estos deberán portar en lugar visible distintivos que los acrediten como empleado de la empresa.
- El Proveedor deberá presentar carta compromiso especificando que el tipo de licenciamiento no va ligado al hardware en donde sea instalado, de tal forma que deberá existir una licencia por dependencia, cada licencia deberá ser corporativa y a Nombre del **Gobierno del Estado de Jalisco/Nombre de la dependencia** para usarse en el momento que se requiera sin necesidad de trámites adicionales.
- La vigencia del licenciamiento será durante el periodo de un año y comenzará a partir del día **06 de Diciembre del 2019**

8. RESPONSABLES DEL REQUERIMIENTO

Responsable de elaborar el requerimiento		Responsable de autorizar el requerimiento	
Nombre: Stephany Cristyn Cárdenas Patino		Nombre: Miguel Angel Romo Rubio	
Puesto: Asistente administrativo		Puesto: Director de Infraestructura y Comunicaciones	
e-mail: stephany.cardenas@jalisco.gob.mx		e-mail: miguel.romo@jalisco.gob.mx	
Fecha: 11/08/2019	Tel. /ext. 26587	Fecha:11/08/2019	Tel. /ext. 26255
Firma:		Firma:	

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

PARTIDA 7 (SOLICITUD DE APROVISIONAMIENTO 35-273-2019)

Jalisco
GOBIERNO DEL ESTADO

SECRETARÍA DE ADMINISTRACIÓN

LICENCIA QLIK SENSE

1. GLOSARIO:

Siglas o palabra	Significado
Inteligencia de negocio	*Uso de estrategias y herramientas que sirven para transformar información en conocimiento, con el objetivo de mejorar el proceso de toma de decisiones en una empresa o gobierno.*
Qlik Sense	*Software analítico de Inteligencia de Negocio de Qlik, que ofrece flexibilidad y capacidad de análisis de mercado.*
SLA	*Por sus siglas en inglés (Service Level Agreements) Acuerdos de Nivel de Servicio.*

2. ANTECEDENTES

Teniendo en cuenta que las fuentes de datos se han multiplicado como internet y redes sociales, dispositivos de interconexión digital, información de dispositivos móviles, etc. también ha aumentado la complejidad para extraer conocimiento relevante de toda esa información. Partiendo de ahí, la inteligencia de negocio combina la información interna y externa que se genera alrededor de una empresa o gobierno. Su relevancia radica en la complejidad de recopilar los datos, procesarlos, analizarlos y presentarlos de forma que cualquiera los pueda entender. Así pues, una herramienta de inteligencia de negocios sofisticada es capaz de analizar y procesar infinidad de datos, de infinidad de fuentes y de ayudar a las empresas o gobiernos a extraer conclusiones para mejorar de manera informada.

3. JUSTIFICACIÓN

Mejorar la administración y gobierno de datos desde aplicaciones web, que permitan visualizar en tiempo real la información para una mayor capacidad de análisis y proyección.

4. OBJETIVOS

Promover el uso de herramientas de inteligencia de negocios en los sistemas, para una exploración intuitiva de datos, búsquedas y visualizaciones más rápidas e inteligentes que ayudarán a la toma de decisiones basadas en datos y estadísticas obtenidas del banco de información que se genera en los sistemas del gobierno del estado de Jalisco.
Atender las peticiones propias y de las demás dependencias del poder ejecutivo que se deriven con el uso de las herramientas de inteligencia de negocio en los sistemas.

5. REQUERIMIENTO

1. *Adquisición de licencia de Software de Inteligencia de Negocio Qlik Sense edición Enterprise.*

Incluye:

- *Qlik NPrinting. Capacidades avanzadas de generación y distribución de informes.*
- *Qlik GeoAnalytics. Analítica basada en la ubicación*

2. *100 horas de consultoría especializada y / o capacitación.*

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
05 SEP. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

SECRETARÍA DE ADMINISTRACIÓN

LICENCIA QLIK SENSE

6. GARANTIAS

El proveedor ofrecerá la garantía de servicios objeto del contrato por 12 meses a partir de la fecha de entrega del producto.

7. OBLIGACIONES DE LOS PARTICIPANTES

Se deberá entregar por escrito el acuerdo de nivel de servicio (SLA) detallando los alcances y horarios de atención, con las siguientes especificaciones:

- *Atención a requerimientos críticos de 1 a 2 horas.*
- *Atención a requerimientos no críticos de 2 a 4 horas.*

8. ENTREGABLES

- *Adquisición de licencia de Software de Inteligencia de Negocios Qlik Sense edición Enterprise para 10 usuarios.*
- *Garantía por escrito de acuerdo a lo descrito en el apartado 6.*

9. RESPONSABLES DEL REQUERIMIENTO

Responsable de elaborar el requerimiento	
Nombre: Lic. Blanca Estela Valencia Casillas	
Puesto: Enlace Administrativo	
e-mail: blanca.valencia@jalisco.gob.mx	
Fecha: Septiembre 04, 2019	Tel. /ext. 26390
Firma:	

Responsable de autorizar el requerimiento	
Nombre: Eliseo Zúñiga Gutiérrez	
Puesto: Director General de Tecnologías de la Información	
e-mail: eliseo.zuniga@@jalisco.gob.mx	
Fecha: Septiembre 04, 2019	Tel. /ext. 26288
Firma:	

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

05 SEP. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

Vigencia del documento: 60 días a partir del sello de validación

AT_V2

2 de **2**

PARTIDA 8 (SOLICITUD DE APROVISIONAMIENTO 35-239-2019)

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a infraestructura de seguridad lógica perimetral

1. GLOSARIO:

- ✓ AV.- Antivirus
- ✓ NGFW.- Cortafuegos de siguiente generación
- ✓ CF.- Filtrado de contenido
- ✓ AS.- Anti SPAM
- ✓ HW.- Hardware

2. ANTECEDENTES

Las diversas secretarías y dependencias del Gobierno del Estado de Jalisco cuentan con equipos de seguridad perimetral lógica y sistema que permiten mantener bajo seguridad lógica los recursos y la información que se genera en la Red Global Digital del Gobierno del Estado de Jalisco.

3. JUSTIFICACIÓN

Los ataques informáticos cada vez son más frecuentes y los métodos de ataque son cada vez más avanzados y poco comunes, es por ello que el Gobierno del Estado de Jalisco busca estar a la vanguardia en temas de seguridad informática para cuidar de la información y los recursos tecnológicos a través de la póliza de mantenimiento y

4. OBJETIVOS

Apoyar la Política de Seguridad de la Información para garantizar la disponibilidad, continuidad, integridad y confidencialidad de los sistemas de comunicaciones del Gobierno del Estado de Jalisco, a través de servicios, mantenimiento, soporte y licenciamiento de la plataforma de seguridad informática con la que se cuenta actualmente.

5. REQUERIMIENTO

A) Póliza de mantenimiento de los componentes de Seguridad Informática Perimetral y filtrado de contenidos

El proveedor deberá de brindar una póliza de soporte y mantenimiento por 12 meses de la plataforma de Seguridad Informática Perimetral y filtrado de contenidos. A continuación, se describen los requerimientos técnicos y de los niveles de servicio solicitados por la convocante.

El equipamiento que deberá de considerar el participante dentro de su propuesta para brindar el servicio de póliza de soporte y mantenimiento, así como el licenciamiento requerido para la actualización de firmas del fabricante se muestra en la siguiente tabla.

AT_V2
1 de 35

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a infraestructura de seguridad lógica perimetral

Marca	Modelo	Cantidad de equipos	Dependencia Responsable de la Infraestructura	Tipo de Soporte requerido	Licencia requerida en terminación conjunta al 5 de Diciembre del 2020
Fortinet	Fortigate 1500D	2	Secretaria de la Hacienda Pública de Jalisco	24x7	AV,FortiGuard NGFW Service,CF,AS,FortiGuard Industrial Security Service,FortiGuard Security Audit Update,Fortiguard FortiCASB,24x7 Email,24x7 Comprehensive Support,Advance HW,Firmware & General Updates
Fortinet	Fortigate 200D	2	Secretaria de Administración	24x7	AV,FortiGuard NGFW Service,CF,AS,24x7 Email,24x7 Comprehensive Support,Advance HW,Firmware & General Updates
Fortinet	Fortigate 3000D	2	Secretaria de Administración	24x7	AV,FortiGuard NGFW Service,CF,AS,FortiGuard Industrial Security Service,FortiGuard Security Audit Update,Fortiguard FortiCASB,24x7 Email,24x7 Comprehensive Support,Advance HW,Firmware & General Updates
Fortinet	Fortigate 51E	20	Secretaria de Administración	8x5	AV,FortiGuard NGFW Service,CF,AS,Return and Replace,Firmware & General Updates,8x5 Enhanced Support
Fortinet	Fortigate 60D	1	Secretaria de Administración	8x5	AV,FortiGuard NGFW Service,CF,AS,Return and Replace,Firmware & General Updates,8x5 Enhanced Support
Fortinet	FortiManager VM-Base (1 - 110 Dispositivos)	1	Secretaria de Administración	24x7	24x7 Email,24x7 Comprehensive Support,Advance HW,Firmware & General Updates

AT_V2
2 de **35**

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

[redacted]

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a infraestructura de seguridad lógica perimetral

Fortinet	Fortigate 61E	4	Secretaria de Administración	8x5	AV,FortiGuard NGFW Service,CF,AS,Return and Replace,Firmware & General Updates,8x5 Enhanced Support
Fortinet	Fortigate 101E	3	Secretaria de Administración	8x5	AV,FortiGuard NGFW Service,CF,AS,Return and Replace,Firmware & General Updates,8x5 Enhanced Support
Fortinet	Fortigate 201E	3	Secretaria de Administración	8x5	AV,FortiGuard NGFW Service,CF,AS,Return and Replace,Firmware & General Updates,8x5 Enhanced Support
Fortinet	Fortigate 300D	1	Supremo Tribunal de Justicia del Estado de Jalisco	24x7	AV,FortiGuard NGFW Service,CF,AS,24x7 Email,24x7 Comprehensive Support,Advance HW,Firmware & General Updates

Tabla 1.- Equipamiento a considerar para la póliza de soporte y mantenimiento

Se deben de tener las siguientes consideraciones para brindar el servicio de la póliza de soporte y mantenimiento:

- El periodo solicitado para el licenciamiento y la póliza de soporte y mantenimiento es de 12 meses a partir del 6 de Diciembre del 2019.
- El licenciamiento deberá de entregarse a más tardar 3 semanas después de la firma del contrato pudiéndose verificar la activación de la misma en el portal del fabricante.
- El participante deberá de considerar que cada dependencia mencionada en la "Tabla 1" se le entregará una póliza personalizada con sus propios accesos para la atención de sus equipos.
- Se deberá proporcionar el licenciamiento de los siguientes servicios conforme a la columna "Licencia requerida en terminación conjunta al 5 de Diciembre del 2020" de la Tabla 1.
- Las actualizaciones de las firmas de seguridad, filtrado web y antispam, IPS, Botnet y de dispositivos móviles se deberán de realizar de manera automática.
- El licenciamiento deberá de incluir todas las actualizaciones y parches del sistema operativo (firmware) de los equipos.
- El soporte se deberá de brindar en la modalidad de 24x7 u 8x5 de acuerdo a la "Tabla 1" con reemplazo de partes al día hábil siguiente.
- El soporte no tendrá límite de eventos.
- El proveedor será responsable de levantar y dar seguimiento a tickets y RMA´s con el fabricante hasta su cierre.
- El proveedor deberá considerar el ofrecimiento de una "Mesa de servicio" siendo este el conducto para solicitar soporte técnico en español.

AT_V2
3 de 35

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

- Para el levantamiento y seguimiento de tickets el proveedor deberá de proporcionar el acceso a una plataforma web de gestión de tickets.
- Se deberán de brindar al menos los siguientes medios de contacto hacia la mesa de servicio para el levantamiento y seguimiento a incidentes:
  - Soporte telefónico.
  - Soporte vía aplicación de acceso remoto brindada por el proveedor.
  - Soporte vía correo electrónico.
  - Plataforma Web.
- La mesa de servicios deberá cumplir con el seguimiento de buenas prácticas de acuerdo a la metodología de ITIL Ver3 actualización 2011.
- La mesa de servicios será responsable de los procesos de gestión de eventos, gestión de incidentes, gestión de problemas y gestión de peticiones.
- Los niveles de servicio acordados (SLA´s) que se brindarán para los diferentes tipos de tickets se detallan a continuación:
  - *Incidente Prioridad 1.*- Afectación grave o total en el servicio. Tiempo de solución máximo de 4 Horas.
  - *Incidente Prioridad 2.*-Fallas menores que impliquen la afectación parcial en el servicio o en algún componente de la solución. Tiempo de solución máximo 1 día hábil.
  - *Requerimientos.*- Los requerimientos de configuración que puedan ser planeados y no impliquen la afectación en la operación de los servicios, así como las actualizaciones de los sistemas y obtención de reportes. Tiempo máximo de solución conforme al requerimiento.

B) Equipamiento requerido para la renovación y mejora de la infraestructura de seguridad lógica de la Secretaría de Administración.

Como parte de la póliza de soporte se requiere el suministro de equipamiento para el robustecimiento, actualización tecnológica y licenciamiento del fabricante. Las condiciones generales se mencionan a continuación:

- Todos los equipos y sistemas requeridos en este inciso deberán de ser nuevos y de última generación
- Todos los equipos y sistemas requeridos en este inciso deberán de contar con 12 meses de licenciamiento y soporte por parte del fabricante.
- Todos los equipos y sistemas requeridos en este inciso deberán de contar con 12 meses de soporte en modalidad 24x7 bajo las mismas consideraciones que los equipos mencionados en el inciso "A) Póliza de mantenimiento de los componentes de Seguridad Informática Perimetral y filtrado de contenidos" de este documento.
- El participante deberá de considerar los servicios profesionales requeridos para la instalación, configuración y puesta a punto de los equipos.
- Se deberán anexar a la propuesta las hojas de datos del fabricante de los equipos propuestos.
- El proveedor deberá de entregar una memoria técnica al final de la instalación de los equipos.
- Con la finalidad de garantizar la interoperabilidad todos los equipos y sistemas requeridos en este inciso deberán de ser de la misma marca que los equipos a los que se les solicita el soporte y licenciamiento en el inciso A de este anexo.

AT_V2
4 de **35**

[redacted]

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Componente	Cantidad de equipos Requeridos
Sistema de Seguridad Lógica "Tipo A"	1
Sistema de Consolidación de Logs y Administración de Reportes	1
Sistema de Autenticación	1

Tabla 2.- Equipamiento requerido Administración

A continuación se muestran las funcionalidades y lineamientos técnicos mínimos de los equipos y sistemas requeridos:

Sistema de Seguridad Lógica "Tipo A"

El Componente solicitado en este apartado es el suministro, instalación, configuración, puesta a punto y el licenciamiento requerido por 12 meses de **un** equipo Cortafuegos de siguiente generación (NGFW) que cumpla como mínimo con los siguientes lineamientos técnicos y funcionalidades en un solo equipo (Appliance):

Características de Desempeño por equipo.

- El equipo debe contar con un Throughput en Firewall tanto en IPv4 como en IPv6 de al menos 238 Gbps para paquetes UDP de 1518 y 512 bytes y de 150 Gbps en paquetes UDP de 64 bytes.
- El equipo debe contar con un Throughput en firewall de 225 Mpps en paquetes UDP de 64 bytes con una latencia de 4µs.
- El equipo debe contar con un Throughput VPN IPSEC de por lo menos 140 Gbps.
- El equipo debe contar con un Throughput IPS de al menos 44 Gbps.
- El equipo debe contar con un Throughput en la funcionalidad protección ante amenazas de 23 Gbps.
- El equipo debe contar con un Throughput en la funcionalidad NGFW de 34 Gbps.
- El equipo debe soportar al menos 50 millones de Sesiones concurrentes.
- El equipo debe soportar 460,000 nuevas sesiones por segundo.
- El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 30,000 usuarios de VPN SSL.
- El equipo debe poder generar al menos 200,000 VPN's IPSec Client to Gateway.
- El equipo debe poder generar al menos 40,000 VPN's IPSec Gateway to Gateway
- El equipo debe soportar la configuración de 200,000 políticas de firewall.

Características de Hardware por equipo.

- El equipo deberá de contar con al menos 4 Interfaces 100 GE QSFP28.
- El equipo deberá de contar con al menos 24 Interfaces 10 GE SFP+.
- El equipo deberá de contar con al menos 32 Interfaces 1 GE RJ45.
- El equipo deberá de contar con al menos 2 Interfaces 1 GE RJ45 para gestión y HA.

AT_V2
5 de 35

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
3 0 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

- El equipo deberá de contar con dos fuentes de poder redundantes con características de Hot Swap mismas que deberán de operar a 100-240v AC, 50-60 Hz.

Módulos de interconexión por equipo.

Cada equipo deberá de incluir los siguientes módulos de interconexión:

- 4 módulos transceptores 100 GE QSFP28, SR, 4 canales de fibra óptica.
- 8 módulos transceptores SFP+ 10 GE SR.
- 8 módulos transceptores 1 GE SFP RJ45

Licenciamiento

El licenciamiento con el que deberán de contar los equipos son 12 meses de 24x7 FortiCare y FortiGuard Unified (UTM).

El cual incluye: Advanced Hardware Replacement (NBD), Firmware and General Upgrades, VPN, Traffic Management, UTM Services Bundle (Application Control, IPS, AV, Botnet IP/Domain, Mobile Malware Service, Web Filtering, Antispam, FortiSandbox Cloud including Virus Outbreak and Content Disarm & Reconstruct Services).

Funcionalidades y consideraciones

- El dispositivo deberá de ser de propósito específico "Hardware", no se aceptarán soluciones basadas en equipos de propósito genérico ejecutadas sobre un Sistema Operativo Convencional, (Linux, Unix, Microsoft Windows, Mac OS, FreeBSD).
- El dispositivo deberá de estar basado en tecnología ASIC "Application-Specific Integrated Circuit".
- Las reglas de Firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.
- El firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo que indique.
- Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
- Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.
- La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.
- En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID.
- En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.
- Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario)
- Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.

AT_V2
6 de **35**

GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a infraestructura de seguridad lógica perimetral

- Soporte de autenticación de dos factores para la gestión del equipo y para el acceso a las VPN de acceso remoto.
- Capacidades de Detección y Prevención de Intrusos, estas se deben de poder implementar tanto en línea como fuera de línea de manera simultánea en diferentes segmentos de red, donde el término en línea significa que el tráfico a ser inspeccionado pasará a través del equipo.
- El detector y preventor de intrusos deberá de soportar captar ataques tanto basados en Anomalías como basados en firmas, pudiendo soportar la mitigación de ataques de denegación de servicios.
- Capacidad de poder asignar parámetros de modelado de tráfico (traffic shapping) sobre reglas de firewall, aplicado en distintos sentidos de una misma sesión y con capacidad de definir el ancho de banda máximo y el garantizado.
- Soporte para configuraciones de alta disponibilidad en activo/activo, activo/pasivo y clúster.
- Licencias ilimitadas por usuarios.
- Capacidad de integrarse con servidores de autenticación RADIUS.
- Capacidad nativa de integrarse con directorios LDAP.
- Permitir la integración con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On".
- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
- Deberá de contener la aplicación de antivirus integrado a la plataforma y permitir la configuración de antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP.
- El antivirus deberá incluir capacidades de detección y detención de tráfico SPYWARE, ADWARE y otros tipos de MALWARE/GRAYWARE que pudieran circular por la red.
- El antivirus deberá proveer acciones específicas para la detección y neutralización de "Botnet".
- Deberá de contener la aplicación de AntiSPAM mediante el protocolo SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado en el mensaje.
- En cuanto a filtro de URL´s deberá de permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida.
- Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.
- Deberá de contar con optimización de WAN debe configurarse mediante reglas que definirán el tráfico a optimizar al menos con los siguientes parámetros:
  - Dirección IP o grupo de direcciones IP de origen.
  - Dirección IP o grupo de direcciones IP de destino.
  - Rango de puertos de destino.
- Capacidad de obtener reportes sobre el comportamiento del tráfico mostrando información al menos de aplicaciones, direcciones IP, dispositivos, sistemas operativos y GeoIP.
- Soporte para la virtualización de los servicios de seguridad mediante Firewalls virtuales, Sistemas virtuales o dominios virtuales, cada instancia deberá de estar aislada lógicamente de las demás y soportar las funcionalidades de VPN, URL Filtering, IPS, y antivirus.
- Deberá de contar con licencia para al menos 10 instancias virtuales.

AT_V2
7 de 35

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a infraestructura de seguridad lógica perimetral

- Permitir la inspección de contenido encriptado por SSL y no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.
- Deberá de permitir el control de aplicaciones a partir de la inspección de los datos independientemente del puerto y el protocolo por el cual se direccione el tráfico, pudiéndose realizar las siguientes acciones: permitir, bloquear y registrar en logs.
- Deberá de soportar prevención de fuga de información (DLP) con reglas que al menos analicen los archivos de tipo MS-Word, PDF, Texto y comprimidos, que se han enviados por los protocolos, HTTP, POP3, SMTP, IMAP y FTP. Ante la detección de una posible fuga de información deben aplicarse al menos las siguientes acciones: Bloquear el tráfico del usuario, bloquear el tráfico de la IP origen, registrar el evento.
- Deberá de contar con Certificación por ICSA Labs para Firewall, IPSec, IPS, Antivirus y SSL VPN.
- Utilizar Técnicas de calidad de servicio estándares: DSCP y WMM/802.11e.
- Capacidades de visibilidad y control de aplicaciones y contenidos.
- Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.
- Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.
- Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
- La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para buscadores tales como Google, Yahoo! y Bing.
- Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.
- Será posible exceptuar la inspección de HTTPS por categoría.
- Modo de operación NAT o también llamada Gateway y el modo Puente o también llamado transparente.
- En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
- Las instancias virtuales podrán de igual forma trabar en modo NAT o transparente.
- Soporte de protocolos IPv4 e IPv6.
- Soporte de políticas de ruteo basado en protocolo, puertos, interfaz fuente y destino, direcciones IP fuente y destino.
- Soporte de rutas estáticas.
- Soporte de Protocolos de enrutamiento OSPF, RIP, BGP y Multicast PIM Sparse Mode y Dense Mode.
- Soporte a ruteo dinámico RIPng, OSPFv3, BGP4+.
- Soporte balanceo de tráfico mediante ECMP (EqualCostMulti-Path)
- Soporte de funcionalidad SD WAN.
- Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.
- Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.

Jefatura COORDINACIÓN GENERAL DE INNOVACIÓN
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
8 de 35

[redacted]

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a infraestructura de seguridad lógica perimetral

- Manejo y etiquetado de VLAN's 802.1Q.
- Gestión y configuración del equipo vía HTTPS y SSH.
- La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.
- Permitir políticas basadas en el sistema operativo del usuario.
- Actualización automática de las firmas de seguridad tanto del antivirus como del preventor de intrusos.

Sistema de Consolidación de Logs y Administración de Reportes

El sistema de Consolidación de Logs y Administración de Reportes consiste en un equipo que permita el reporte, análisis y almacenamiento de bitácoras generada en los equipos Cortafuegos.

Capacidades de Desempeño y Hardware

- Almacenamiento incluido como mínimo de 24TB
- Maneja por lo menos 18000 Logs por segundo.
- Conectividad con al menos 2 interfaces GE RJ45
- El equipo deberá de poder particionar el arreglo de disco duros en al menos Raid 0, 1, 5, 6, 10, 50, 60
- El equipo deberá tener la capacidad de recibir los logs de al menos 2000 dispositivos desde un inicio sin necesidad de un licenciamiento adicional.
- El equipo deberá de poder manejar al menos 600 GB de logs por día.

Licenciamiento

l licenciamiento con el que deberán de contar los equipos son 12 meses de 24x7 FortiCare y suscripción de Indicador de Compromiso (IOC)

Funcionalidades y características

- El sistema deberá permitir el Almacenamiento de Logs y Reportes.
- El sistema de be ser tipo "appliance" (dispositivo de propósito específico "Hardware")
- Interface de administración gráfica (GUI) vía Web (HTTPS)
- Interface de administración vía CLI (Línea de comando) vía protocolo SSH y consola accediendo directamente en el equipo por puerto especifico.
- Capacidad de definir administradores para la solución, de modo que pueda segmentarse la responsabilidad de los administradores por tareas operativas.
- Permite integrar dispositivos para que reporten actividad o logs, estableciendo comunicaciones de tipo seguras con dichos dispositivos.
- Permite asignar cuotas de espacio en disco por dispositivo, de modo que un solo dispositivo no consuma la totalidad del disco de la solución.
- Debe tener la posibilidad de enviar los Logs a bases de datos remotas de SQL.
- Todas las funciones están consolidadas en el dispositivo.

Generación de reportes:

- Permite generar reportes personalizados, permite al administrador de la solución el definir el contenido de los reportes.
- El contenido de los reportes incluye los datos en formato tabular (tablas) y/o gráficas (pie-chart, graph-chart)
- Genera reportes de: Utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos.

AT_V2
9 de 35

2 0 AGO. 2019
VALIDACIÓN TÉCNICA

[redacted]

- Genera reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente y/o por destino.
- Genera reportes de las páginas y/o categorías de URL visitadas con mayor frecuencia, por fuente y/o por destino.
- Permite de generar la incidencia de virus detectados/removidos a nivel red por fuente y/o por destino.
- Permite generar un reporte de las actividades administrativas (ingresos de administradores, cambios de configuración) realizadas.
- Permite personalizar los criterios bajo los cuales será obtenido el reporte, tales como origen, destinos, servicios, fechas y/o día de la semana.
- Permite especificar el período de tiempo específico para el cual el reporte va a ser obtenido, por períodos relativos (hoy, ayer, esta semana, semana pasada, este mes, mes pasado) o bien por períodos absolutos (de la fecha día/mes/año a la fecha día/mes/año).
- Permite la calendarización de reportes.
- Permite generar reportes en formato PDF y DOC.
- Tiene la opción de generar reportes en idioma inglés y en idioma español
- Permite enviar el reporte vía correo electrónico.

Análisis forense y correlación de eventos:

- Permite hacer búsquedas por usuario (Username) o dirección IP, para que toda la información almacenada de dicho Username o dirección IP sea mostrada en un reporte donde pueda darse seguimiento a su actividad.
- Permite hacer análisis de vulnerabilidades y generar un reporte de cuales vulnerabilidades fueron encontradas, Esta funcionalidad no debe de tener límite de equipos.

Almacenamiento de Contenido:

- Permite recibir bitácoras de los protocolos HTTP, SMTP para poder almacenar los mensajes que han fluido en la red a través de dichos protocolos, para su posterior visualización y análisis.
- Los mensajes pueden ser almacenados completamente, o solo un "resumen" de la conexión. El mensaje completo exhibirá el contenido completo, mientras que el resumen solo mostrará fuente y destino de la comunicación, así como su duración.
- Permite hacer búsquedas sobre los mensajes almacenados

Sistema de Autenticación

El sistema de autenticación deberá de permitir hacer una gestión de identidades de usuario.

Características de desempeño y hardware

- Licenciado para soportar al menos 500 usuarios locales o remotos
- Licenciado para permitir al menos 500 tokens
- Licenciado para permitir al menos 100 dispositivos (NAS Radius Cliente)
- Licenciado para permitir al menos 50 grupos de usuarios
- Estar licenciado para soportar al menos 10 certificados de Autoridades Certificadoras
- Estar licenciado para soportar al menos 250 certificados de usuarios
- Tener al menos 4 interfaces de 1Gbps RJ-45
- Tener al menos 1TB de espacio en disco

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

10 de **35**

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Jalisco

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a infraestructura de seguridad lógica perimetral

Licenciamiento

El licenciamiento con el que deberán de contar los equipos son 12 meses de 24x7 FortiCare.

Tokens para 2FA

Se deberá de entregar junto con la solución **300 tokens físicos** con One Time Password (OTP) que permitan hacer una solución de dos factores de autenticación (2FA) los cuales deberán de contar con licenciamiento de por vida. El token deberá de tener un tamaño de llavero que permita la flexibilidad y movilidad del mismo, no requerirá de la instalación de ningún software para su uso por parte de los usuraios y generará y mostrará una contraseña de 6 dígitos cada 60 segundos en su pantalla LCD que permitirá verificar el acceso a los usuarios.

Requisitos Mínimos de Funcionalidad

- Soportar gestión por interfaz gráfica (GUI) por HTTP y/o HTTPS
- Soportar gestión en interfaz basada en línea de comando (CLI) por TELNET y/o SSH
- Permitir definir perfiles de gestión para la solución, de forma a segmentar la responsabilidad de los administradores según tareas operacionales
- Tener indicación visual, centralizada, de información crítica: estado de la licencia, versión de firmware, consumo de CPU/Memoria/Disco, cantidad de usuarios creados y licenciados
- Soportar actualización del firmware por interfaz gráfica por proceso simplificado y sencillo
- Soportar customización de mensajes estándar de la solución como páginas de error, portales de autenticación, auto registro, recuperación de contraseña y otros. Soportar también la inclusión, cambios y eliminación de imágenes en los mensajes/paginas sin la necesidad de recursos o conectividad externa
- Soportar configuración de Alta Disponibilidad (HA), reduciendo al máximo los periodos de interrupción
- Soportar implementación de HA como "Activo-Pasivo" o sincronizando la configuración entre dos equipos activos
- Permitir el sincronismo automático de la configuración entre todos los equipos que componen la solución en HA
- Soportar implementación de HA sincronizando configuración con appliances en localidades geográficamente separados
- Soportar la opción de backup criptografado
- Soportar backup automatizado (agendado por criterios predefinidos) y no solamente bajo demanda
- Soportar el backup completo de la configuración, incluyendo base de usuarios, tokens, certificados, configuración de single-sign-on, etc. La solución debe de permitir la recuperación de toda la configuración directamente de la interfaz grafica
- Soportar NTP (Network Time Protocol), para sincronismo de horários
- Soportar enrutamiento estático

AT_V2
11 de **35**

30 AGO. 2019
VALIDACIÓN TÉCNICA

[redacted]

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a infraestructura de seguridad lógica perimetral

- Soportar SNMP v1, v2 y v3 permitiendo consultar MIB própra y envio de Traps
- Soportar nativamente Trap SNMP reportando cambio del estado de HA
- Soportar el envío de e-mails como si fuera servidor propio (localhost) o integrando con servidores externos para el envío de los mensajes a usuarios o administradores
- El equipo debe de permitir envió de e-mails conexo a reset de contraseña, aprobación de nuevos usuarios, auto registro de usuarios y autenticación de segundo factor (token)
- Permitir el envió de mensajes SMS para los usuarios a través de gateways SMS de terceros o su propio servicio de envío de SMS, siendo este licenciado o no
- Soportar el registro de todos los eventos que los usuarios de su base local ejecutem, como creación de un usuario, cambio de contraseña o cambios de información general
- Soportar la clasificación de logs de acuerdo a la necesidad del administrador: por usuario que hizo el cambio, por fecha, en orden ascendente, en orden descendente, etc
- La solución debe realizar la autenticación para gestión de identidad de los usuarios de red, ayudando a simplificar la gestión de los mismos siendo un punto central donde múltiples métodos de autenticación puedan ser consolidados
- Soportar autenticación de dos factores (two-factor authentication)
- Debe tener soporte a autenticación de dos factores por lo menos en dos tipos de token, siendo el primero físico (token) y el segundo lógico como software para dispositivos móviles, e-mail o SMS, permitiendo que se pueda elegir cuales tipos se utilizará para cada usuario
- La solución debe permitir que se defina un perfil de complejidad mínimo para las contraseñas de todos los usuarios registrados en la base local, permitiendo la definición de cantidad mínima de letras minúsculas, mayúsculas, caracteres numéricos, caracteres especiales, etc.
- La solución debe de permitir crear políticas de bloqueo automático de los usuarios después de una serie de errores de autenticación, impidiendo ataques de fuerza bruta
- La solución debe soportar crear usuarios en base local, que puedan ser utilizados en la autenticación de los dispositivos según necesario
- La solución debe de permitir crear usuarios en masa en la base de datos local a través de importación de lista de usuarios que se creen contenida en archivos externos
- La solución debe de permitir crear nuevos usuarios en la base de datos local y que el creador/administrados pueda definir una contraseña en ese momento
- La solución debe de permitir crear nuevos usuarios en la base de datos local donde el equipo genere una contraseña aleatoria y envíe al usuario
- La solución debe de permitir crear nuevos usuarios en la base local sin la definición de una contraseña, obligando a que el usuario utilice el token como factor unico de autenticación
- Debe de permitir asociar los tokens a los usuarios creados localmente en la base de datos
- Debe de permitir que los propios usuarios hagan el registro de sus tokens y informen la pérdida de un token automáticamente, sin la necesidad de involucrar a uno administrador
- Permitir la eliminación automática en masa de usuarios deshabilitados, basado en criterios definidos

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
12 de **35**

[redacted]

- La solución debe tener formas que permitan a los usuarios locales resetear sus contraseñas de forma segura sin la intervención de administradores, a través de correo electrónico o preguntas de seguridad
- Debe de soportar la creación de grupos de usuarios, que puedan ser utilizados en la autenticación de dispositivos según necesidad
- Los tokens deben de generar códigos con al menos 6 dígitos y en intervalos no superiores a 60 segundos
- Soportar autenticación de dos factores por hardware dedicado (Token)
- Soportar autenticación de dos factores por aplicativo mobile (iPhone e Android)
- Soportar autenticación de dos factores por envío de mensajes SMS
- Soportar autenticación de dos factores por envío de e-mail
- Soportar la sincronización con dispositivo en hardware de generación de OTP (One Time Password)
- Permitir sincronizar los tokens con el equipo para el correcto funcionamiento de los mismos
- Permitir deshabilitar un token cuando se pierde o es robado, permitiendo su reactivación posterior cuando/si se recuperado
- Debe de permitir desasociación de un token de usuario y asociación a otro cuando necesario, permitiendo reutilización de los mismos
- Debe de continuar permitiendo autenticación de dos factores en clientes Windows aunque su equipo este offline
- Debe de tener un portal web para auto registro de modo que los usuarios puedan accederlo, llenar sus datos y enviar el registro. Luego del usuario hacer el registro el administrador deberá de ser automáticamente notificado para aprobar o denegar el registro antes de que lo mismo se active
- La solución debe de funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), permitiendo autenticación a dispositivos compatibles con el protocolo
- La solución debe de soportar integración con servidor RADIUS remoto
- La solución debe de poder funcionar como servidor LDAP (Lightweight Directory Access Protocol), permitiendo autenticación a dispositivos compatibles con el protocolo
- La solución debe de tener un servidor LDAP interno que permita ser configurado de forma jerárquica, para la correcta gestión por grupos o unidades organizativas de usuarios locales
- La solución debe de soportar integración con servidor LDAP remoto (como Microsoft Active Directory)
- La solución debe de soportar autenticación de usuarios con credenciales de medios sociales de terceros como Facebook, Twitter, LinkedIn e Google+
- La solución debe de permitir que los usuarios que no tengan cuenta local o en medios sociales puedan autenticarse en un registro rápido, que garantiza la trazabilidad mínima a través de validación de dirección de e-mail o número de teléfono
- Debe de soportar Security Assertion Markup Language (SAML), que actúe como un Proveedor de Identidad (Indentity Provider - IDP) estableciendo un relacionamiento de confianza para

AT_V2
13 de 35

30 AGO. 2019
VALIDACIÓN TÉCNICA

[redacted]

autenticación segura de usuarios que intentan acceder a un Proveedor de Servicios (Service Provider -SP)

- La solución debe de soportar nativamente (sin redireciones) la integración y autenticación de switches y otros dispositivos compatibles con 802.1X
- Debe de brindar nativamente (sin redireciones a equipos de terceros) la integración de clientes finales para ofrecer autenticación 802.1X, por ejemplo un cliente que utilice Windows podrá configurar su equipo para el soporte a 802.1X
- Soportar los seguientes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS y EAP-GTC
- Soportar interoperabilidad con equipos de acceso (swtiches) de otros fabricantes, para autenticación de puertos en la solución a través de 802.1X
- Debe de soportar bypass de autenticación de 802.1X para dispositivos conocidos que no soporten este estándar, siendo que la liberación deberá de ser basada en la direción MAC de los equipos previamente registrados, donde estes tendrán acceso a la red sin la necesidad de autenticación del usuario o dispositivo
- La solución debe de funcionar como Autoridad Certificadora (CA)
- Debe de permitir la gestión de los certificados digitales, con emisión y revocación
- Debe permitir el uso de CA's de confianza para validación de certificados emitidos por CA's existentes
- Debe soportar OCSP para que se pueda ofrecer una lista de certificados revocados (CRL)
- Debe de tener base de autenticación de VPN Site-to-Site a través de Certificados
- Debe soportar SCEP server (Simple Certificate Enrollment Protocol), permitiendo la firma de requisiciones de certificados digitales (CSR) automaticamente o con actuación del administrador
- Debe de crear y firmar certificados X.509 para utilización en servidores http y ssh, asi como para los clientes de servicios https, ssh y VPNs IPSec
- Debe de ser capaz de importar otros certificados de CA's asi como la lista de certificados revocados
- Debe de ser capaz de permitir al administrador generar, firmar y revocar certificados digitales para los usuarios.
- La solución debe de tener la capacidad de brindar servicios SSO (Single Sign-On), con autenticación transparente (pasiva) de usuarios en sistemas compatibles
- Debe de ser capaz de integrarse a un directorio activo (Windows AD) y ofrecer la funcionalidad de SSO, donde la autenticación automática/transparente vía SSO para los servicios necesarios sea basada en la autenticación previa del usuario en el dominio
- Debe permitir definir una lista de usuarios de SSO que deben de ser ignorados, evitando la interferencia de cuentas de servicios como antivirus o scripts de GPO
- Debe de soportar SSO basado en Radius (RSSO - RADIUS Single Sign-On)

Jefatura de Gabinete — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

14 de 35

[redacted]

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a infraestructura de seguridad lógica perimetral

C) Equipamiento requerido para la renovación y mejora de la infraestructura de seguridad lógica de la Secretaría de Educación Jalisco

Como parte de la póliza de soporte se requiere el suministro de equipamiento para el robustecimiento, actualización tecnológica y licenciamiento del fabricante. Las condiciones generales se mencionan a continuación:

- Todos los equipos y sistemas requeridos en este inciso deberán de ser nuevos y de última generación
- Todos los equipos y sistemas requeridos en este inciso deberán de contar con 36 meses de licenciamiento y soporte por parte del fabricante.
- El participante deberá de considerar los servicios profesionales requeridos para la instalación, y configuración de los equipos.
- Se deberán anexar a la propuesta las hojas de datos del fabricante de los equipos propuestos.
- El proveedor deberá de entregar una memoria técnica al final de la instalación de los equipos.
- Con la finalidad de garantizar la interoperabilidad todos los equipos y sistemas requeridos en este inciso deberán de ser de la misma marca que los equipos a los que se les solicita el soporte y licenciamiento en el inciso A de este anexo.

Componente	Cantidad	Código	Descripción
1	2	FG-2000E-BDL-950-36	6 x 10GE SFP+ slots, 34 x GE RJ45 ports (including 32 x ports, 2 x management/HA ports), SPU NP6 and CP9 hardware accelerated, 480GB SSD onboard storage, dual AC power supplies & Hardware plus 24x7 FortiCare and FortiGuard Unified (UTM) Protection by 3 years
2	2	FS-1048E	Layer 2/3 FortiGate switch controller compatible switch with 48 x GE/10GE SFP/SFP+ slots and 6 x 40GE QSFP+ or 4 x 100GE QSFP28. Dual AC power supplies
	2	FC-10-1E48F-311-02-36	8x5 FortiCare Contract
	30	FS-TRAN-SFP+SR	10GE SFP+ transceiver module, short range for FortiSwitch D Series with SFP+ and SFP/SFP+ slots
3	2	FS-448D-FPOE	Layer 2/3 FortiGate switch controller compatible PoE+ switch with 48 x GE RJ45 ports, 4 x 10 GE SFP+, with automatic Max 740W POE output limit

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

AT_V2
15 de 35

[redacted]

	2	FC-10-W4483-311-02-36	8x5 FortiCare Contract
4	1	FAZ-VM-BASE	Base license for stackable FortiAnalyzer-VM; 1 GB/Day of Logs and 500 GB storage capacity. Unlimited GB/Day when used in collector mode only. Designed for all supported FortiAnalyzer-VM virtual appliance platforms.
	1	FAZ-VM-GB25	Upgrade license for adding 25 GB/Day of Logs and 10 TB storage capacity.
	1	FC3-10-LV0VM-149-02-36	Subscription license for the FortiGuard Indicator of Compromise (IOC) (for 1-26 GB/Day of Logs)
	1	FC3-10-LV0VM-248-02-36	24x7 FortiCare Contract (for 1-26 GB/Day of Logs)
5	1	FG-600E-BDL-950-36	2 x 10GE SFP+ slots, 10 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 8 x switch ports), 8 x GE SFP slots, SPU NP6 and CP9 hardware accelerated & Hardware plus 24x7 FortiCare and FortiGuard Unified (UTM) Protection

Tabla 3.- Equipamiento requerido SEJ

A continuación se muestran las funcionalidades y lineamientos técnicos mínimos de los equipos y sistemas requeridos:

Componente 1

1) Solución UTM/NGFW tipo 1 (2 unidades por 3 años)

1.1) Throughput de por lo menos 60 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete

1.2) Soporte a por lo menos 20M conexiones simultaneas

1.3) Soporte a por lo menos 500K nuevas conexiones por segundo

1.4) Throughput de al menos 65 Gbps de VPN IPSec

1.5) Estar licenciado para, o soportar sin necesidad de licencia, 20K túneles de VPN IPSec site-to-site simultáneos

1.6) Estar licenciado para, o soportar sin necesidad de licencia, 50K túneles de clientes VPN IPSec simultáneos

1.7) Throughput de al menos 6 Gbps de VPN SSL

1.8) Soportar al menos 10K clientes de VPN SSL simultáneos

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

3 0 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT-V2

16 de 35

[redacted]

1.9) Soportar al menos 11.5 Gbps de throughput de IPS

1.10) Soportar al menos 12.5 Gbps de throughput de Inspección SSL

1.11) Throughput de al menos 5 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la solución de seguridad tenga debidamente activadas y operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado múltiples números de desempeño para cualquiera de las funcionalidades, solamente el de valor más pequeño será aceptado.

1.12) Permitir gestionar al menos 1024 Access Points

1.13) Tener al menos 32 interfaces 1Gbps

1.14) Tener al menos 6 interfaces 10Gbps

1.15) Disco de, por lo menos, 480 GBytes para almacenamiento de información local

1.16) Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance

1.17) Soporte a por lo menos 500 sistemas virtuales lógicos (Contextos) por appliance

2) Requisitos Mínimos de Funcionalidad

Características Generales

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

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

2.3) Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;

2.4) La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;

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

2.6) La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;

2.7) Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;

2.8) Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;

2.9) Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;

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

2.11) Los dispositivos de protección de red deben soportar DHCP Relay;

2.12) Los dispositivos de protección de red deben soportar DHCP Server;

2.13) Los dispositivos de protección de red deben soportar sFlow;

2.14) Los dispositivos de protección de red deben soportar Jumbo Frames;

2.15) Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;

2.16) Debe ser compatible con NAT dinámica (varios-a-1);

2.17) Debe ser compatible con NAT dinámica (muchos-a-muchos);

2.18) Debe soportar NAT estática (1-a-1);

2.19) Debe admitir NAT estática (muchos-a-muchos);

2.20) Debe ser compatible con NAT estático bidireccional 1-a-1;

Secretaría de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

17 de **35**

[redacted]

2.21)	Debe ser compatible con la traducción de puertos (PAT);
2.22)	Debe ser compatible con NAT Origen;
2.23)	Debe ser compatible con NAT de destino;
2.24)	Debe soportar NAT de origen y NAT de destino de forma simultánea;
2.25)	Debe soportar NAT de origen y NAT de destino en la misma política
2.26)	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
2.27)	Debe ser compatible con NAT64 y NAT46;
2.28)	Debe implementar el protocolo ECMP;
2.29)	Debe soportar el balanceo de enlace hash por IP de origen;
2.30)	Debe soportar el balanceo de enlace por hash de IP de origen y destino;
2.31)	Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;
2.32)	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
2.33)	Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;
2.34)	Enviar logs a sistemas de gestión externos simultáneamente;
2.35)	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
2.36)	Debe soporta protección contra la suplantación de identidad (anti-spoofing);
2.37)	Implementar la optimización del tráfico entre dos dispositivos;
2.38)	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
2.39)	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
2.40)	Soportar OSPF graceful restart;
2.41)	Los dispositivos de protección deben tener la capacidad de operar simultáneamente en una única instancia de servidor de seguridad, mediante el uso de sus interfaces físicas en los siguientes modos: modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3);
2.42)	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
2.43)	Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
2.44)	Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
2.45)	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
2.46)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
2.47)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
2.48)	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
2.49)	La configuración de alta disponibilidad debe sincronizar: Sesiones;
2.50)	La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
2.51)	La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;

AT_V2
18 de **35**

UNIDAD CENTRAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

2.52) La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
2.53) En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
2.54) Debe soportar la creación de sistemas virtuales en el mismo equipo;
2.55) Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;
2.56) Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;
2.57) La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
2.58) Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);
2.59) Debe soportar un tejido de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;
2.60) El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;
2.61) Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;

Control por Politica de Firewall

2.62) Debe soportar controles de zona de seguridad;
2.63) Debe contar con políticas de control por puerto y protocolo;
2.64) Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
2.65) Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
2.66) Firewall debe poder aplicar la inspección UTM (control de aplicaciones y filtrado web como mínimo) directamente a las políticas de seguridad en vez de usar perfil obligatoriamente;
2.67) Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
2.68) Debe soportar el almacenamiento de bitácoras (logs) en tiempo real tanto para entorno de la nube como entorno local (on-premise);
2.69) Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
2.70) Debe existir una manera de evitar que el almacenamiento de logs en tiempo real no superen la velocidad de subida de los mismos (upload);
2.71) Debe soportar el protocolo estándar de la industria VXLAN;

Control de Aplicación

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

GOBIERNO DEL ESTADO DE JALISCO COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
19 de **35**

[redacted]

2.73)	Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos;
2.74)	Reconocer al menos 1.700 aplicaciones diferentes, 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;
2.75)	Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-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;
2.76)	Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;
2.77)	Debe detectar aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent;
2.78)	Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;
2.79)	Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;
2.80)	Debe hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el tráfico corresponde a la especificación del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTTP. La decodificación de protocolo también debe identificar las características específicas dentro de una aplicación, incluyendo, pero no limitado al intercambio de ficheros dentro de Webex;
2.81)	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
2.82)	Actualización de la base de firmas de la aplicación de forma automática;
2.83)	Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos;
2.84)	Los dispositivos de protección de red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario;
2.85)	Debe ser posible añadir múltiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas;
2.86)	Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;
2.87)	Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
2.88)	Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
2.89)	La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP;

AT_V2
20 de **35**

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

2.90) El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
2.91) Debe alertar al usuario cuando sea bloqueada una aplicación;
2.92) Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
2.93) Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
2.94) Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;
2.95) Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
2.96) Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);
2.97) Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;
2.98) Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
2.99) Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Prevención de Amenazas

2.100) Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
2.101) Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
2.102) Las características de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
2.103) Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
2.104) Debe implementar los siguientes tipos de acciones a las amenazas detectadas por IPS: Permitir, permitir y generar registro, bloquear, bloquear IP del atacante durante un tiempo y enviar tcp-reset;
2.105) Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo;
2.106) Debe ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad;
2.107) Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas;
2.108) Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
2.109) Deber permitir el bloqueo de vulnerabilidades;
2.110) Debe permitir el bloqueo de exploits conocidos;
2.111) Debe incluir la protección contra ataques de denegación de servicio;
2.112) Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones;

AT_V2
21 de **35**

3 0 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN (SEMOVI)

[redacted]

2.113)	Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
2.114)	Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
2.115)	Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico;
2.116)	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
2.117)	Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;
2.118)	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
2.119)	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;
2.120)	Detectar y bloquear los escaneos de puertos de origen;
2.121)	Bloquear ataques realizados por gusanos (worms) conocidos;
2.122)	Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
2.123)	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
2.124)	Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
2.125)	Debe permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración;
2.126)	Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;
2.127)	Soportar el bloqueo de archivos por tipo;
2.128)	Identificar y bloquear la comunicación con redes de bots;
2.129)	Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;
2.130)	Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
2.131)	Debe permitir la captura de paquetes por tipo de firma IPS y definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la alerta, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos;
2.132)	Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
2.133)	Los eventos deben identificar el país que origino la amenaza;
2.134)	Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
2.135)	Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
2.136)	Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

2.137)	El Firewall debería permitirle analizar la implementación del tejido de seguridad para identificar posibles vulnerabilidades y resaltar las mejores prácticas que podrían utilizarse para mejorar la seguridad y el rendimiento general de su red;
2.138)	En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;
2.139)	Los recursos de postura de seguridad deben existir para permitir que el software de seguridad de endpoint aplique protección en tiempo real, antivirus, filtrado de Web y control de aplicaciones en el punto final;
2.140)	Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);
Filtrado de URL	
2.141)	Debe 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);
2.142)	Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad;
2.143)	Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory y la base de datos local;
2.144)	Debe 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;
2.145)	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
2.146)	Debe 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;
2.147)	Tener por lo menos 60 categorías de URL;
2.148)	Debe tener la funcionalidad de exclusión de URLs por categoría;
2.149)	Permitir página de bloqueo personalizada;
2.150)	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);
2.151)	Además del Explicit Web Proxy, soportar proxy web transparente;
Identificación de Usuarios	
2.152)	Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
2.153)	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios;
2.154)	Debe tener integración y soporte para Microsoft Active Directory para los siguientes sistemas operativos: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2;
2.155)	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos

AT_V2
23 de **35**

30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;

2.156) Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;

2.157) Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios;

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

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

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

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

2.162) Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores;

QoS Traffic Shaping

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

2.163) aplicaciones, tanto de audio como de video streaming;

2.164) Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;

2.165) Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;

2.166) Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;

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

2.168) Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;

2.169) En QoS debe permitir la definición de tráfico con ancho de banda garantizado;

2.170) En QoS debe permitir la definición de tráfico con máximo ancho de banda;

2.171) En QoS debe permitir la definición de colas de prioridad;

2.172) Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype;

2.173) Soportar marcación de paquetes DiffServ, incluso por aplicación;

2.174) Soportar la modificación de los valores de DSCP para Diffserv;

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

2.176) Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping;

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

Filtro de Datos

2.178) Permite la creación de filtros para archivos y datos predefinidos;

2.179) Los archivos deben ser identificados por tamaño y tipo;

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
Jefatura de Gabinete
23 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

2.180) Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);

2.181) Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;

2.182) Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;

2.183) Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;

Geo Localización

2.184) Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;

2.185) Debe permitir la visualización de los países de origen y destino en los registros de acceso;

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

VPN

2.187) Soporte VPN de sitio-a-sitio y cliente-a-sitio;

2.188) Soportar VPN IPSec;

2.189) Soportar VPN SSL;

2.190) La VPN IPSec debe ser compatible con 3DES;

2.191) La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;

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

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

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

2.195) La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI;

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

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

2.198) Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;

2.199) La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web;

2.200) Las características de VPN SSL se deben cumplir con o sin el uso de agentes;

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

2.202) Asignación de DNS en la VPN de cliente remoto;

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

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

2.205) Suportar lectura y revisión de CRL (lista de revocación de certificados);

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

2.207) Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Antes de que el usuario se autentique en su estación;

AT_V2
25 de **35**

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

2.208) Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Después de la autenticación de usuario en la estación;
2.209) Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Bajo demanda de los usuarios;
2.210) Deberá mantener una conexión segura con el portal durante la sesión;
2.211) El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (v10.10 o superior);

Wireless Controller

2.212) Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada;
2.213) Soportar servicio de servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos;
2.214) Soporte IPv4 e IPv6 por SSID;
2.215) Permitir elegir si el tráfico de cada SSID se enviará a la controladora o directamente por la interfaz de punto de acceso en una determinada VLAN;
2.216) Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point;
2.217) Soportar monitoreo y supresión de puntos de acceso indebidos;
2.218) Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS;
2.219) Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows;
2.220) Permitir la visualización de los dispositivos inalámbricos conectados por usuario;
2.221) Permitir la visualización de los dispositivos inalámbricos conectados por IP;
2.222) Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación;
2.223) Permitir la visualización de los dispositivos inalámbricos conectados por canal;
2.224) Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado;
2.225) Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal;
2.226) Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación;
2.227) Debe soportar Fast Roaming en autenticación con portal cautivo;
2.228) Debe soportar configuración de portal cautivo por SSID;
2.229) Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico;
2.230) Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP;
2.231) Debe ser compatible con el protocolo 802.1x RADIUS;
2.232) La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal;
2.233) La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática;
2.234) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática;
2.235) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP;

COORDINACIÓN GENERAL DE INNOVACIÓN
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
26 de **35**

[redacted]

2.236) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DNS;
2.237) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Broadcast;
2.238) La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Multicast;
2.239) La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue);
2.240) La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico;
2.241) La controladora deberá contar con mecanismos de protección de tramas de administración de acuerdo a las especificaciones de la alianza Wi-Fi y estándar 802.11ac;
2.242) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP;
2.243) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding;
2.244) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding;
2.245) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication;
2.246) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding;
2.247) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI;
2.248) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack;
2.249) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response;
2.250) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication;
2.251) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection;
2.252) La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge;
2.253) Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas;
2.254) Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso;
2.255) La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible;
2.256) La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario;
2.257) Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID;
2.258) Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso;
2.259) Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio;
2.260) La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh;

AT_V2
27 de 35

COORDINACIÓN GENERAL DE INNOVACIÓN
30 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

2.261)	Ofrecer un mecanismo de creación automática y/o manual de usuarios visitantes y contraseñas, que puedan ser enviados por correo electrónico o SMS a los usuarios, con ajuste de tiempo de expiración de la contraseña;
2.262)	La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS;
2.263)	Debe tener un mecanismo de ajuste automático de potencia de la señal con el fin de reducir la interferencia entre canales entre dos puntos de acceso administrados;
2.264)	Ofrecer un mecanismo de balanceo de trafico/usuarios entre Puntos de acceso;
2.265)	Proporcionar un mecanismo de balanceo de trafico/usuarios entre frecuencias y/o radios de los Puntos de Acceso;
2.266)	Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica;
2.267)	Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión;
2.268)	Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados;
2.269)	La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz;
2.270)	Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados;
2.271)	Debe permitir asociación dinámicas de VLANs a los usuarios autenticados en un SSID especifico mediante protocolo RADIUS;
2.272)	Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID especifico mediante vlan pooling;
2.273)	Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico;
2.274)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones;
2.275)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino;
2.276)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza;
2.277)	La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones;
2.278)	la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico;
2.279)	El controlador inalámbrico debe tener interface de administración integrado en el mismo equipo;
2.280)	El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales;
2.281)	La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico;
2.282)	La controladora inalámbrica deberá soportar aceleración de túnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico;
2.283)	La controladora inalámbrica debe soportar protocolo LLDP;
2.284)	Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta;

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
3 0 AGO. 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

2.285) Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC adyacente;

2.286) Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos;

2.287) La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado;

2.288) La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas;

2.289) La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada;

2.290) Deberá soportar la conversión de Multicast a Unicast para mejorar el rendimiento del tiempo de aire;

2.291) En el entorno de alta disponibilidad, debe existir el concepto de controladores primarios y secundarios en la unidad AP, permitiendo que la unidad decida el orden en el que el AP selecciona una unidad controlador y cómo la unidad AP se conecta a un controlador de backup en el caso de que el controlador primario falle;

2.292) Debe proporcionar la capacidad de crear varias claves pre-compartidas de acceso protegido WiFi (WPA-PSK) para que no sea necesario compartir PSK entre dispositivos;

Componente 2

Hardware Specifications	
Total Network Interfaces (Proposed)	48x GE/10 GE SFP+ ports and 6x 40 GE QSFP+ ports or 4x 100 GE QSFP28 ports
10/100/1000 Service Ports	1
RJ-45 Serial Console Port	1
Form Factor	1 RU Rack Mount
System Specifications	
Switching Capacity (Duplex)	1760 Gbps
Packets Per Second (Duplex)	2620 Mpps
Mac Address Storage	144 K
Network Latency	< 800ns
VLANs Supported	4 K
IPv4/IPv6 Dual Stack Routing Ready Hardware	Yes
Link Aggregation Group Size	Up to 48
Total Link Aggregation Groups	Up to number of ports
Queues/Port	8
Packet Buffers	12 MB
DRAM	8 GB
NAND	128 GB
Dimensions	

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

AT_V2

29 de 35

[redacted]

Jalisco
GOBIERNO DEL ESTADO

Height x Depth x Width (inches)	1.69 x 18.11 x 17.26
Height x Depth x Width (mm)	43 x 460 x 438.5
Weight	18.96 lbs (8.6 kg)
Environment	
Power Required	100–240V AC, 50–60 Hz
Power Consumption (Maximum)	up to 181.7 W
Power Supply	Dual hot swappable AC
Heat Dissipation	620.4 BTU/h
Operating Temperature	32–113°F (0–45°C)
Storage Temperature	4–158°F (-20–70°C)
Humidity	10–90% RH non-condensing
Mean Time Between Failures	> 10 years
Certification and Compliance	
FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2	
Warranty	
Fortinet Warranty	Limited lifetime* warranty on all models

Componente 3

Hardware Specifications	
Total Network Interfaces	48x GE RJ45 and 4x10 GE SFP+ ports Note: SFP+ ports are compatible with 1 GE SFP
Dedicated Management 10/100 Port	1
RJ-45 Serial Console Port	1
Form Factor	1 RU Rack Mount
Power over Ethernet (PoE) Ports	48 (802.3af/at)
PoE Power Budget	740 W
Mean Time Between Failures	> 10 years
System Specifications	
Switching Capacity (Duplex)	176 Gbps
Packets Per Second (Duplex)	262 Mpps
MAC Address Storage	16 K
Network Latency	< 1µs
VLANs Supported	4 K
Link Aggregation Group Size	8
Total Link Aggregation Groups	Up to number of ports
Packet Buffers	1.5 MB
DRAM	1 GB
FLASH	128 MB
Dimensions	

AT_V2
30 de **35**

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

[redacted]

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a infraestructura de seguridad lógica perimetral

Height x Depth x Width (inches)	1.73 x 16.1 x 17.3
Height x Depth x Width (mm)	44 x 410 x 440
Weight	15.45 lbs (7.01 kg)
Environment	
Power Required	100–240V AC, 50–60 Hz
Power Supply	AC built in
Redundant Power	Dual power supplies
Power Consumption (Average / Maximum)	790 W / 792 W
Heat Dissipation	193 BTU/h
Operating Temperature	32–122°F (0–50°C)
Storage Temperature	-4–158°F (-20–70°C)
Humidity	10–90% non-condensing
Certification and Compliance	
FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2	
Warranty	
Fortinet Warranty	Limited lifetime* warranty on all models

Componente 4

FAZ-VM-BASE: Licencia base para FortiAnalyzer-VM apilable; 1 GB / día de registros y 500 GB de capacidad de almacenamiento. GB / día ilimitado cuando se usa solo en modo colector. Diseñado para todas las plataformas de dispositivos virtuales FortiAnalyzer-VM compatibles.

FAZ-VM-GB25: Licencia de actualización para agregar 25 GB / día de registros y 10 TB de capacidad de almacenamiento.

FC3-10-LV0VM-149-02-36: Licencia de suscripción para el indicador de compromiso FortiGuard (COI) (para 1-26 GB / día de registros)

FC3-10-LV0VM-248-02-36: 24x7 FortiCare Contract (for 1-26 GB/Day of Logs)
***Por 3 años.**

Capacity and Performance	
GB/Day of Logs	25
Storage Capacity	+10 TB
Devices/VDOMs (Maximum)	10,000
FortiGuard Indicator of Compromise (IOC)	SI
Hypervisor Requirements	
Hypervisor Support	VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/6.7, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+ and Open

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
31 de 35

[redacted]

	Source Xen 4.1+, KVM on Redhat 6.5+ and Ubuntu 17.04, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI), Alibaba Cloud (AliCloud)
Network Interface Support (Minimum / Maximum)	.1/4
vCPUs (Minimum / Maximum)	2/ Unlimited
Memory Support (Minimum / Maximum)	4 GB / Unlimited

Características

Visibilidad de extremo a extremo
- Correlación de eventos, detección de amenazas e indicador de compromiso (IOC) reduce el tiempo de detección y las amenazas de identidad

Integración de Fortinet Security Fabric
- Se correlaciona con registros de FortiClient, FortiSandbox, FortiWeb y FortiMail para una mayor visibilidad e información crítica de la red.

Alta disponibilidad de nivel empresarial
- Copia de seguridad automática de FortiAnalyzer DB (clúster de hasta 5 nodos) que se puede dispersar geográficamente para la recuperación ante desastres

Automatización de la seguridad
- Reduzca la complejidad y aproveche la automatización a través de la API REST, scripts, conectores y puntadas de automatización para acelerar la seguridad respuesta

Dominios administrativos y multicliente (ADOM)
- Separe los datos del cliente y administre los dominios aprovechando ADOM para cumplir y ser operacionalmente efectivos

Opciones de implementación flexibles y almacenamiento de archivos
- Admite la implementación de dispositivos, máquinas virtuales, hospedados o en la nube. Utilizar AWS, Azure o Google para archivar registros como almacenamiento secundario

-Componente 5

Hardware Specifications	
Interfaces and Modules	
10 GE SFP+ Slots	2
GE RJ45 Interfaces	8
GE SFP Slots	8
GE RJ45 Management Ports	2
USB Ports	2
RJ45 Console Port	1
Local Storage	NIL 2x 240 GB SSD

Jefatura de Gabinete COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2

32 de **35**

[redacted]

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Included Transceivers	2x SFP (SX 1 GE)
System Performance — Enterprise Traffic Mix	
IPS Throughput 2	10 Gbps
NGFW Throughput 2, 4	9.5 Gbps
Threat Protection Throughput 2, 5	7 Gbps
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gbps
Firewall Latency (64 byte, UDP)	2 µs
Firewall Throughput (Packet per Second)	40.5 Mpps
Concurrent Sessions (TCP)	8 Million
New Sessions/Second (TCP)	450,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte) 1	20 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	50,000
SSL-VPN Throughput	7 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10,000
SSL Inspection Throughput (IPS, avg. HTTPS) 3	8 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) 3	5,500
SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3	800,000
Application Control Throughput (HTTP 64K) 2	15 Gbps
CAPWAP Throughput (HTTP 64K)	18 Gbps
Virtual Domains (Default / Maximum)	10/10
Maximum Number of FortiSwitches Supported	64
Maximum Number of FortiAPs (Total / Tunnel)	1,024 / 512
Maximum Number of FortiTokens	5,000
Maximum Number of Registered FortiClients	2,000
High Availability Configurations	Active-Active, Active-Passive, Clustering
Dimensions and Power	
Height x Width x Length (inches)	1.75 x 17.0 x 15.0
Height x Width x Length (mm)	44.45 x 432 x 380

AT_V2
33 de **35**

30 AGO. 2019
VALIDACIÓN TÉCNICA

[redacted]

Weight	16.1 lbs (7.3 kg)
Form Factor	1 RU
Power Consumption (Average / Maximum)	129 W / 244 W
Power Source	100–240V 60–50Hz
Current (Maximum)	6A @ 100V
Heat Dissipation	832 BTU/h
Redundant Power Supplies (Hot Swappable)	optional
Operating Environment and Certifications	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Humidity	10–90% non-condensing
Noise Level	59 dBA
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6

6.- GARANTIAS

Todo el equipamiento deberá contar con 1 año de garantía a partir de su entrega.

La vigencia de la póliza deberá ser del 06/12/2019 al 05/12/2020

Las ubicaciones de los servicios serán en:

- **Secretaria de Administración**
  - Domicilio: Alcalde 1221, Col. Miraflores. Ciudad: Guadalajara, C.P. 44270. / Dirección de Infraestructura Tecnológica Data Center.
- **Secretaria de Hacienda Publica**
  - Domicilio: Calle Magisterio 1499, La Guadalupana, 44220 Guadalajara, Jalisco.
- **Secretaria de Educación Jalisco**
  - Av. Central Guillermo González Camarena 615, Poniente, 45136 Zapopan, Jal., México

7.- OBLIGACIONES DE LOS PARTICIPANTES

El participante deberá de cumplir con los siguientes requisitos:

- El participante deberá incluir en su propuesta carta expedida por el fabricante de los componentes de Seguridad Informática haciendo referencia a que el participante es un canal certificado nivel Platinum.

Jefatura de la oficina — COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL
30 AGO 2019
VALIDACIÓN TÉCNICA
DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
34 de 35

Secretaría de Administración

Póliza de mantenimiento preventivo y correctivo a infraestructura de seguridad lógica perimetral

- El proveedor deberá describir en su propuesta la cantidad, numero de parte, modelo y descripción de los productos y servicios ofertados.
- Todas las especificaciones señaladas en este anexo son mínimas, por lo tanto el Licitante podrá ofertar bienes y servicios con especificaciones superiores, si así lo considera conveniente.
- El proveedor deberá considerar el reemplazo de piezas y refacciones necesarias para garantizar el tiempo de solución máximo de 4 horas de acuerdo a incidentes prioridad uno.
- El licitante deberá de contar dentro del personal de la empresa con al menos 2 ingenieros certificados a nivel NSE7 Network Security Expert 7, será indispensable incluir dichos certificados en la propuesta.
- El licitante deberá de contar dentro del personal de la empresa con al menos 2 ingenieros certificados en ITIL Fundamentos, será indispensable incluir dichos certificados en la propuesta.
- El proveedor deberá de demostrar residencia dentro de la zona metropolitana de Guadalajara con el objetivo de garantizar los tiempos de respuesta solicitados en el anexo.
- El proveedor deberá de demostrar residencia dentro de la zona metropolitana de Guadalajara con el objetivo de garantizar los tiempos de respuesta solicitados en el anexo.
- La dependencia se reserva el derecho de validar la documentación con el fabricante.

8. RESPONSABLES DEL REQUERIMIENTO

Responsable de elaborar el requerimiento	
Nombre: Stephany Crystin Cárdenas Patiño	
Puesto : Asistente administrativo	
e-mail: stephany.cardenas@jalisco.gob.mx	
Fecha: 29 Agosto 2019	Tel. /ext. 38182872 ext. 26587
Firma:	

Responsable de autorizar el requerimiento	
Nombre: Miguel Ángel Romo Rubio	
Puesto: Dirección de Infraestructura y Comunicaciones	
e-mail: miguel.romo@jalisco.gob.mx	
Fecha: 29 Agosto 2019	Tel. /ext. 3818 2800 Ext. 26255
Firma:	

COORDINACIÓN GENERAL DE INNOVACIÓN GUBERNAMENTAL

30 AGO. 2019

VALIDACIÓN TÉCNICA

DIRECCIÓN GENERAL DE PLANEACIÓN TECNOLÓGICA

AT_V2
35 de **35**

[redacted]

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

PARTIDA 9 (SOLICITUD DE APROVISIONAMIENTO 35-233-2019)

Secretaría de Administración

Adquisición de equipamiento de telecomunicaciones

1. GLOSARIO:

[Anotar en orden alfabético las siglas o palabras técnicas y su correspondiente significado]

Siglas o palabra	Significado
DGTI	*Dirección General de Tecnologías de la Información*
DGPT	*Dirección General de Planeación Tecnológica.*

2. ANTECEDENTES

Actualmente la dependencia cuenta con equipamiento de telecomunicaciones en fin de vida por parte del fabricante o con fechas próximas de obsolescencia, por lo tanto resulta fundamental llevar a cabo las acciones necesarias que permitan garantizar la renovación del equipamiento en tiempo y forma.

3. JUSTIFICACIÓN

El equipamiento que actualmente se encuentra instalado es del fabricante Cisco, por lo tanto a fin de garantizar la compatibilidad con la infraestructura existente, las propuestas deberán ser con equipos del mismo fabricante, en cuyos casos lo que podrá variar serán los modelos, siempre y cuando se cumplan con las características mínimas estipuladas.

4. OBJETIVOS

El objetivo de la presenta adquisición es renovar la infraestructura en materia de telecomunicaciones existente, a fin de evitar posibles caídas de servicio por operar con equipos que se encuentran en fin de vida o soporte por parte del fabricante, los cuales debido a su obsolescencia, no es posible encontrar partes que permitan su reparación o reemplazo.

Secretaría de Administración

Adquisición de equipamiento de telecomunicaciones

5. REQUERIMIENTO

PARTIDA: 1
Terminal de comunicación IP Ejecutiva
Cantidad: 36

REQUERIMIENTOS DE HARDWARE

- Deberá de contar con al menos cinco líneas programables.
- Deberá contar con una pantalla de 5 pulgadas a color gráfica WVGA de 24-bit con resolución a 800 x 480 pixeles con la capacidad de reproducir video, proporcionar acceso desplazable a funciones de llamada y acceso a aplicaciones XML basadas en texto
- Deberá contar con una cámara de video en HD 720p con codificación y decodificación H.264
- Deberá contar con la opción de montarse en pared.
- Deberá de contar con un altavoz bidireccional para realizar y recibir llamadas.
- Deberá de contar con una tecla ajuste de volumen para el auricular, el altavoz y el timbre
- Deberá de contar con un switch ó conmutador Ethernet 10/100/1000 BASE-T integrado que proporcione dos puertos RJ-45, uno para la conexión con la red LAN y el otro para un dispositivo Ethernet como una PC o laptop, con la posibilidad de asignar diferentes vlans y así brindar mayor seguridad y confiabilidad en el tráfico de voz y datos
- Deberá soportar la utilización de auriculares mediante puerto USB o RJ-9
- Deberá contar dos puertos USB que se pueda usar para cargar un teléfono celular Smartphone con una salida de 5V
- Deberá de contar con botones dedicados para las siguientes funciones:
- Navegación en pantalla.
- Espera, Transferencia, Conferencia, Acceso a buzón de voz y Directorios
- Silenciar, volumen arriba/abajo y Altavoz
- Debe tener un pad numérico tradicional para marcado
- Deberá de soportar hasta tres módulos de expansión para de 5 a 113 líneas.
- Deberá tener convivencia con muchas marcaciones rápidas o funciones programables.
- Deberá soportar conectividad inalámbrica acorde a los protocolos IEEE 802.11a/b/g/n/ac
- Deberá contar con un puerto para audio externo

REQUERIMIENTOS DE FUNCIONALIDADES

- Debe soportar al menos las siguientes funciones:
- Niveles de volumen ajustables
- Desvío de Llamadas
- Captura de Llamadas
- Espera de Llamadas
- Transferencia de Llamadas
- Conferencias
- Códigos forzados de autorización
- Captura de Llamada por Grupos
- Indicador visual de mensaje en espera

- Música en Espera
- Timbrado Automático de línea privada
- Re-llamar
- Línea compartida
- Contestar automáticamente
- Extensión móvil
- Intercomunicador punto a punto
- No molestar
- Debe soportar ser configurado para reducir su consumo de energía bajo demanda mientras no es utilizado, esto debe ser logrado mediante el uso de un mecanismo ó arquitectura de administración de energía con el fin de ahorrar costos y reducir la huella ecológica
- Debe soportar al menos los siguientes códecs de audio:
  - G.711a
  - G.711u
  - G.729a
  - G722
  - iSAC
  - iLBC
- Debe soportar la funcionalidad de Generación de Ruido de Confort y Detección de Actividad de Voz
- Debe soportar personalizar la pantalla con imágenes de fondo.
- Debe soportar personalizar los tonos de llamada
- Debe soportar 802.1 P/Q
- Debe de soportar el protocolo DHCP
- Debe de soportar el protocolo TFTP para actualizaciones en línea
- Debe de soportar el protocolo RTCP para soporte y monitoreo
- Debe de soportar LLDP-MED
- Debe de contar con medición en tiempo real de métricas de calidad de servicio y SCSR
- Debe ser compatible con la tecnología bluetooth 4.1 LE en un rango de hasta 20 metros y e esta manera poder usar algún auricular de tipo: manos libres

SEGURIDAD

- Debe de soportar certificados
- Debe de soportar autentificación de imagen
- Debe de soportar autentificación de dispositivo
- Debe de soportar autentificación y cifrado de archivos de configuración
- Debe de soportar autentificación y cifrado de señalización usando TLS
- Debe de soportar encriptación de media usando SRTP
- Debe ser capaz de actuar como un suplicante de 802.1X utilizando EAP-FAST y EAP-TLS
- Debe soportar ser acceso vía SSH
- Deberá de contar con un cliente de VPN integrado
- Deberá soportar el algoritmo de cifrado AES-256
- Deberá ser compatible con sistema antirrobo Kensington Security slot

ESPECIFICACIONES

- Debe de soportar el protocolo SIP (Session Initiation Protocol)

- Debe soportar el estándar IEEE PoE 802.3af, 802.3at y UPOE
- Debe de soportar el protocolo SDP (Session Description Protocol)
- Debe de soportar el protocolo IPv4 e IPv6
- Debe soportar también alimentarse localmente con un alimentador de energía
- Debe soportar una temperatura operacional de 0 a 40°C
- Debe soportar una humedad relativa de operación de 10% a 90% (no condensada)

PARTIDA: 2

Terminal de comunicación Básica
Cantidad: 337

REQUERIMIENTOS DE HARDWARE

- Deberá de contar con al menos cuatro líneas programables.
- Deberá contar con una pantalla de 3.2 pulgadas en escala de grises con resolución a 384 x 106 pixeles.
- Deberá contar con la opción de montarse en pared.
- Deberá de contar con un altavoz bidireccional para realizar y recibir llamadas.
- Deberá de contar con una tecla ajuste de volumen para el auricular, el altavoz y el timbre
- Deberá de contar con un switch ó conmutador Ethernet 10/100 BASE-T integrado que proporcione dos puertos RJ-45, uno para la conexión con la red LAN y el otro para un dispositivo Ethernet como una PC o laptop, con la posibilidad de asignar diferentes vlans y así brindar mayor seguridad y confiabilidad en el tráfico de voz y datos
- Deberá soportar la utilización de auriculares mediante puerto RJ-9
- Deberá de contar con botones dedicados para las siguientes funciones:
- Navegación en pantalla.
- Espera, Transferencia, Conferencia, Acceso a buzón de voz y Directorios
- Silenciar, volumen arriba/abajo y Altavoz
- Debe tener un pad numérico tradicional para marcado

REQUERIMIENTOS DE FUNCIONALIDADES

- Debe soportar al menos las siguientes funciones:
- Niveles de volumen ajustables
- Desvío de Llamadas
- Captura de Llamadas
- Espera de Llamadas
- Transferencia de Llamadas
- Conferencias
- Códigos forzados de autorización
- Captura de Llamada por Grupos
- Indicador visual de mensaje en espera
- Música en Espera
- Timbrado Automático de línea privada
- Re-llamar
- Línea compartida
- Contestar automáticamente

- Extensión móvil
- Intercomunicador punto a punto
- No molestar
- Debe soportar ser configurado para reducir su consumo de energía bajo demanda mientras no es utilizado, esto debe ser logrado mediante el uso de un mecanismo ó arquitectura de administración de energía con el fin de ahorrar costos y reducir la huella ecológica
- Debe soportar al menos los siguientes códecs de audio:
- G.711a
- G.711u
- G.729a
- G722
- iLBC
- Debe soportar la funcionalidad de Generación de Ruido de Confort y Detección de Actividad de Voz
- Debe soportar personalizar la pantalla con imágenes de fondo.
- Debe soportar personalizar los tonos de llamada
- Debe soportar 802.1 P/Q
- Debe de soportar el protocolo DHCP
- Debe de soportar el protocolo TFTP para actualizaciones en línea
- Debe de soportar el protocolo RTCP para soporte y monitoreo
- Debe de soportar LLDP-MED
- Debe de contar con medición en tiempo real de métricas de calidad de servicio y SCSR

SEGURIDAD

- Debe de soportar certificados
- Debe de soportar autentificación de imagen
- Debe de soportar autentificación de dispositivo
- Debe de soportar autentificación y cifrado de archivos de configuración
- Debe de soportar autentificación y cifrado de señalización usando TLS
- Debe de soportar encriptación de media usando SRTP
- Debe ser capaz de actuar como un suplicante de 802.1X utilizando EAP-FAST y EAP-TLS
- Debe soportar ser acceso vía SSH
- Deberá de contar con un cliente de VPN integrado
- Deberá soportar el algoritmo de cifrado AES-256

ESPECIFICACIONES

- Debe de soportar el protocolo SIP (Session Initiation Protocol)
- Debe soportar el estándar IEEE PoE 802.3af
- Debe de soportar el protocolo SDP (Session Description Protocol)
- Debe de soportar el protocolo IPv4 e IPv6
- Debe soportar también alimentarse localmente con un alimentador de energía
- Debe soportar una temperatura operacional de 0 a 40°C
- Debe soportar una humedad relativa de operación de 10% a 90% (no condensada)

Secretaría de Administración

Adquisición de equipamiento de telecomunicaciones

PARTIDA: 3

Terminal de comunicación IP Inalambrico
Cantidad: 1

REQUERIMIENTOS DE HARDWARE

- Deberá soportar conectividad inalámbrica acorde a los protocolos IEEE 802.11a/b/g/n/ac.
- Deberá soportar el protocolo de Roaming 802.11r
- Deberá contar con clasificación IP54 para protección contra polvo, salpicaduras y agua.
- Deberá contar con clasificación de tipo MIL-STD-810G por resistencia a golpes
- Deberá de contar con al menos cinco líneas programables.
- Deberá contar con batería recargable con duración de hasta 11.54 horas de tiempo continuo y hasta 45 horas de tiempo en espera
- Deberá contar con una pantalla de 2.4 pulgadas a color gráfica con resolución a 240 x 320 pixeles.
- Deberá de contar con un altavoz bidireccional para realizar y recibir llamadas.
- Deberá contar con dos botones programables para acceder a aplicaciones, características y funciones basadas en pantalla.
- Deberá de contar con una tecla ajuste de volumen para el auricular, el altavoz y el timbre.
- Deberá soportar la utilización de auriculares mediante puerto 3.5mm
- Deberá contar con un cable de alimentación
- Deberá contar con Eliminador de baterías que funcione como cargador y deberá operar a 100-240 VAC de 50 a 60 Hz.
- Deberá contar un puerto USB 2.0
- Deberá de contar con botones dedicados para las siguientes funciones:
  - Encendido
  - Silencio
  - Responder, enviar y volver a marcar
  - Navegación en pantalla.
  - Volumen arriba/abajo y Altavoz
  - Debe tener un pad numérico tradicional para marcado

REQUERIMIENTOS DE FUNCIONALIDADES

- Marcación abreviada
- Brillo de pantalla ajustable y tiempo de espera
- Timbres audibles y vibrantes.
- Respuesta automática
- Detección automática de auriculares y respuesta automática desde auriculares
- Bloqueo automático del teclado
- Devolución de llamada
- Desvío de llamadas
- Listas de historial de llamadas
- Aparcado de llamadas
- Captura de llamadas
- Temporizador de llamadas
- Llamada en espera

- Identificador de llamadas
- Directorio corporativo
- Conferencia
- transferencia directa
- Servicio de movilidad de extensión.
- servicio de marcación rápida
- Captura de llamadas grupales
- Espera
- Tecla de acceso rápido para bloqueo del teclado, modo de timbre silencioso y acceso al correo de voz
- Desvío inmediato
- Unirse
- Volver a marcar el último número
- Llamada maliciosa
- Indicador de mensaje en espera
- Sala de Conferencia
- Música en espera
- Silencio
- Perfiles de red
- Directorio personal
- Presencia
- Privacidad
- Herramienta de informe de calidad
- Rellamada
- Tono de llamada por línea
- línea compartida
- Visualización de hora y fecha
- Transferencia
- retención de red
- hospitalidad
- Soporte para la autenticación mutua de seguridad de la capa de transporte (TLS)
- Plataforma de lanzamiento de aplicaciones
- Notificación de desvío de llamadas
- Autorización forzada y códigos de asuntos del cliente
- Intercomunicador
- movilidad
- Monitoreo y grabación silenciosos.
- Marcación rápida
- Correo de voz
- Configuración del timbre: teléfono activo (timbre, timbre una vez, pitido, flash)
- Búsqueda predictiva en nueva llamada

- Debe soportar al menos los siguientes códecs de audio:
  - G.711a
  - G.711u
  - G.729a
  - G.729ab
  - G722

[redacted]

- iSAC
- iLBC

- Debe de soportar el protocolo DHCP
- Debe de soportar el protocolo TFTP para actualizaciones en línea
- Debe de soportar el protocolo RTCP para soporte y monitoreo
- Debe de contar con medición en tiempo real de métricas de calidad de servicio y SCSR
- Debe ser compatible con la tecnología bluetooth 3.0 en un rango de hasta 20 metros y de esta manera poder usar algún auricular de tipo: manos libres

SEGURIDAD

- Debe de soportar certificados
- Debe de soportar autenticación de imagen
- Debe de soportar autenticación de dispositivo
- Debe de soportar autenticación y cifrado de archivos de configuración
- Debe de soportar autenticación y cifrado de señalización usando TLS
- Debe de soportar encriptación de media usando SRTP

SEGURIDAD INALÁMBRICA

- Debe soportar Acceso protegido a Wi-Fi (WPA) versiones 1 y 2 Personal y Enterprise
- Debe soportar Protocolo de autenticación extensible: autenticación flexible a través de túnel seguro (EAP-FAST)
- Debe soportar Protocolo de autenticación extensible protegido - Tarjeta de token genérico (PEAP-GTC)
- Debe soportar Protocolo de autenticación extensible protegido - Microsoft Challenge Handshake Authentication Protocol Version 2 (PEAP-MSCHAPv2)
- Debe soportar Protocolo de autenticación extensible - Seguridad de la capa de transporte (EAP-TLS)
- Debe soportar Privacidad equivalente por cable estática de 40 y 128 bits (WEP)
- Debe soportar Protocolo de integridad de clave temporal (TKIP) y verificación de integridad de mensaje (MIC)
- Debe soportar Estándar de cifrado avanzado (AES)

ESPECIFICACIONES

- Debe de soportar el protocolo SIP (Session Initiation Protocol)
- Debe de soportar el protocolo SDP (Session Description Protocol)
- Debe de soportar el protocolo IPv4 e IPv6
- Debe soportar también alimentarse localmente con un alimentador de energía
- Debe soportar una temperatura operacional de 0 a 50°C así como una temperatura de -20 a 60°C para la batería
- Debe soportar una humedad relativa de operación de 10% a 90% (no condensada)

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Secretaría de Administración

Adquisición de equipamiento de telecomunicaciones

PARTIDA: 4

Switch
Cantidad: 15

Especificaciones	
Enlaces de bajada total 10/100/1000 o PoE+ puertos de cobre	24 puertos de datos
Configuracion de enlaces de subida	4x 10G enlaces ascendentes fijos
Default primary AC power supply	PWR-C5-125WAC
Fans	Redundante
Software	Escenciales de red
Chassis Dimensions	4.4 x 44.5 x 28.8 cm - 1.73 x 17.5 x 11.3 in
Redes Virtuales	1
Ancho de banda de apilamiento	80 Gbps
Numero total de direcciones Mac	16,000
Número total de rutas Plv4 (ARP más rutas aprendidas)	11,000(8,000 rutas directas y 3000 rutas indirectas)
Entradas de enrutamiento IPv4	3,000
Entradas de enrutamiento IPv6	1,500
Escala de enrutamiento multicast	1,000
Entradas de escala QoS	1,000
Entrada de escala ACL	1,500
Paquete de búfer por SKU	Buffers de 6 MB para modelos Gigabit Ethernet de 24 o 48 puertos
Entradas Flexibles de NetFlow(FNF)	16,000 flujos en modelos Gigabit Ethernet de 24 y 48 puertos
DRAM	2 GB
Flash	4 GB
VLAN IDs	1024
Total de interfaces virtuales conmutadas (SVI)	512
Marcos jumbo	9198 bytes
Ancho de banda inalambrico por switch	N/A
IP SGT binding scale	10K
Número de enlaces IPv4	10k
Número de políticas SGT / DGT	2k
Número de sesiones SXP	200
Especificaciones de Ancho de Banda	
Capacidad de conmutacion	128 Gbps
Tasa de reenvio	95.23 Mpps
Capacidad de conmutacion con apilamiento	208 Gbps
Mean time between failures (hours)	525,990
Peso	
Switch	4.35Kg – 9.59 Lb

[redacted]

Secretaría de Administración

Adquisición de equipamiento de telecomunicaciones

Conectores.	
	El equipo deberá de contar con los siguientes tipos de conectores: • Puertos 1000BASE-T: conectores RJ-45, cableado UTP Cat 5E de 4 pares • Puertos basados en SFP 1000BASE-T: conectores RJ-45, cableado UTP Cat 5E de 4 pares • Transceptores SFP 100BASE-FX, 1000BASE-SX, -LX / LH, -ZX, -BX10, multiplexación por división de longitud de onda densa (DWDM) y multiplexación por división de longitud de onda gruesa (CWDM): conectores de fibra LC (fibra monomodo o multimodo) • Transceptores 10GBASE-SR, LR, LRM (solo C9200), ER, ZR, DWDM SFP +: conectores de fibra LC (fibra monomodo o multimodo) • Conector SFP + • Puertos de apilamiento 160/80: cableado a base de cobre • Puerto de administración de Ethernet: conectores RJ-45, cableado UTP Cat 5 de 4 pares • Puerto de consola de administración: cable RJ- 45 a DB9 para conexiones de PC, adaptador USB-C, adaptador USB • Conector de fuente de alimentación interna: la fuente de alimentación interna es una unidad de rango automático. Admite voltajes de entrada entre 100 y 240 VCA. Use el cable de alimentación de CA suministrado para conectar el conector de alimentación de CA a una toma de corriente de CA.
Conectores de energía	Conector de fuente de alimentación interna: la fuente de alimentación interna es una unidad de rango automático. Admite voltajes de entrada entre 100 y 240 VCA. Use el cable de alimentación de CA

10 de **27**

	suministrado para conectar el conector de alimentación de CA a una toma de corriente de CA
Estandares	EEE 802.1s IEEE 802.1w IEEE 802.1x IEEE 802.1x-Rev IEEE 802.3ad IEEE 802.3af IEEE 802.3at IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports IEEE 802.1D Spanning Tree Protocol IEEE 802.1p CoS prioritization IEEE 802.1Q VLAN IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-X RMON I and II standards SNMPv1, v2c, and v3
Fuente de alimentación.	
Fuente de alimentacion maxima	125w

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

PARTIDA: 5

Módulo SFP MONO MODO 10G BASE 40 KILOMETROS
Cantidad: 6

PARTIDA: 6

Módulo SFP MONO MODO10G BASE 10 KILOMETROS
Cantidad: 24

PARTIDA: 7

SWITCH
Cantidad: 8

Especificaciones	
Enlaces de bajada total 10/100/1000, multigigabit de cobre o fibra SFP	48 puertos PoE+
Fuente de poder disponible PoE	505w
Default primary AC power supply	715w
Fuente de energía default	PWR-C1-350WAC-P
Configuracion de enlaces de subida	4x 10G enlaces ascendentes fijos
Fans	Redundante
Software	Escenciales de red
Chassis Dimensions	4.4 x 44.5 x 28.8 cm - 1.73 x 17.5 x 11.3 in
Redes Virtuales	1
Ancho de banda de apilamiento	80 Gbps
Numero total de direcciones Mac	32,000
Número total de rutas IPv4 (ARP más rutas aprendidas)	32,000(24,000 rutas directas y 8000 rutas indirectas)
Entradas de enrutamiento IPv6	16,000
Escala de enrutamiento multicast	8,000
Entradas de escala QoS	5,120
Entrada de escala ACL	5,120
Paquete de búfer por SKU	Buffers de 16 MB para modelos Gigabit Ethernet de 24 o 48 puertos
Entradas Flexibles de NetFlow(FNF)	64,000 flujos en modelos Gigabit Ethernet de 24 y 48 puertos
DRAM	8 GB
Flash	16 GB
VLAN IDs	4094
Total de interfaces virtuales conmutadas (SVI)	1000
Marcos jumbo	9198 bytes

Puertos enrutados totales por stack	416
Especificaciones de Ancho de Banda	
Tasa de reenvio	95.23 Mpps
Tasa de reenvio con apilamiento	333.33 Mpps
Capacidad de conmutacion con apilamiento	448 Gbps
Capacidad de conmutacion	128 Gbps
Mean time between failures (hours)	340,710
Características de suministro para los modelos PoE / PoE +	
PoE+ on all ports (30W por port)	2 PWR-C1-1100WAC-P o 1 PWR-C1-1100WAC-P y 1 PWR-C1-715WAC-P
Peso	
Switch	6.81Kg – 14.99 Lb
Conectores.	
	El equipo deberá de contar con los siguientes tipos de conectores: • Puertos 1000BASE-T: conectores RJ-45, cableado UTP Cat 5E de 4 pares • Puertos Multigigabit-T: conectores RJ-45, 4 pares Cat 5E, Cat 6, Cat 6A UTP cableado • Puertos basados en SFP 1000BASE-T: conectores RJ-45, cableado UTP Cat 5E de 4 pares • Transceptores SFP: conectores de fibra LC (fibra monomodo o multimodo) • Transceptores SFP +: conectores de fibra LC (fibra monomodo o multimodo) • Transceptores QSFP +: conectores de fibra MPO y LC (fibra monomodo o multimodo) • conector QSFP + • conector SFP + • Puerto de administración de Ethernet: conectores RJ-45, cableado UTP Cat 5 de 4 pares • Puerto de la consola de administración: cable RJ-45 a DB9 para conexiones de PC

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

Conectores de energía	Conector de fuente de alimentación interna: la fuente de alimentación interna es una unidad de rango automático. Admite voltajes de entrada entre 100 y 240 VCA. Use el cable de alimentación de CA suministrado para conectar el conector de alimentación de CA a una toma de corriente de CA
Estandares	EEE 802.1s IEEE 802.1w IEEE 802.1x IEEE 802.1x-Rev IEEE 802.3ad IEEE 802.3af IEEE 802.3at IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports IEEE 802.1D Spanning Tree Protocol IEEE 802.1p CoS prioritization IEEE 802.1Q VLAN IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-X RMON I and II standards SNMPv1, v2c, and v3
Fuente de alimentación.	PWR-C1-715WAC-P
Salida total BTU (nota: 1000 BTU/hr = 293W)	2440 BTU/hr, 715W
Rango de voltaje de entrada y frecuencia	100 to 240 VAC,

	50 to 60 Hz
Corriente de entrada	10-5A
Rating de salida	-56V a 12.8A
Output holdup time	20 ms minimo a 100VAC
Receptáculos de entrada de alimentación	IEC 320-C16 (IEC60320-C16)
Rating del cable de alimentación	15A
Especificaciones fisicas	(H x W x D): 1.58 x 3.25 x 12.20 in Peso: 2.6 lb (1.2 kg)
Temperatura de operación.	Temperatura de funcionamiento normal * y altitudes: -5 ° C a + 45 ° C, hasta 5000 pies (1500 m) -5 ° C a + 40 ° C, hasta 10,000 pies (3000m) * La temperatura ambiente mínima para el arranque en frío es de 32 ° F (0 ° C) Condiciones excepcionales a corto plazo *: -5 ° C a + 50 ° C, hasta 5000 pies (1500m) -5 ° C a + 45 ° C, hasta 10,000 pies (3000m) -5 ° C a + 45 ° C, a nivel del mar con falla de un solo ventilador * No más de lo siguiente en un período de un año: 96 horas consecutivas, o 360 horas en total, o 15 veces
Storage temperature	-40° to 158°F (-40° to 70°C)
Humedad relativa en funcionamiento y no operativa sin condensación	5% to 90% sin condensacion
Altitud	10,000 pies. (3000 meters), hasta 45°C
Cumplimiento de EMI y EMC	FCC Parte 15 (CFR 47) Clase A ICES-003 Clase A EN 55032 Clase A CISPR 32 Clase A AS/NZS 3548 Clase A BSMI Clase A (AC modelos de entrada solamente) VCCI Clase A EN 55024, EN300386, EN 61000-3-2, EN 61000-3-3 EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN 61000-6-1

Cumplimiento de seguridad	UL 60950-1, CAN/CSA-C22.2 No. 60950-1, EN 60950-1, IEC 60950-1, CCC, CE Marca
Indicadores LED.	"AC OK": la alimentación de entrada a la fuente de alimentación está bien "PS OK": la potencia de salida de la fuente de alimentación está bien
Fuente de alimentacion maxima	
PWR-C1-715WAC	715W

PARTIDA: 8

Módulo SFP MULTI MODO 10G BASE
Cantidad: 16

PARTIDA: 9

Módulo SFP MULTI MODO 1000 BASE
Cantidad: 15

PARTIDA: 10

Módulo de Fibra Óptica para Core Chasis de 16 Puertos 10 Gigabit Ethernet
Cantidad: 1

- Deberá estar diseñado para satisfacer la creciente demanda de agregación de flujos de Ethernet de 10 Gigabits en implementaciones de campus, así como para el transporte de Ethernet de 10 Gigabits de alta densidad en un Core Switch. Podrá funcionar en modo de rendimiento para proporcionar una operación de velocidad de línea.

Hardware

- Debertá contar con 16 Puertos y soportar transceptores de factor de forma pequeño conectables (SFP/SFP+), 10/100 / 1000M GLC-T (1G cobre SFP) y 100M FX.
- Deberá admitir la replicación de multidifusión basada en hardware, calidad de servicio (QoS), listas de control de acceso (ACL), tramas gigantes y baja latencia para permitir un rendimiento seguro y predecible para aplicaciones intensivas de ancho de banda.
- Deberá tener una memoria integrada de 2GB

- Deberá contar con un backplane de 80 Gbps.
- Sus puertos deberán estar agrupados en 2 grupos de 8 Puertos y operar de la siguiente manera
  - Sobre-suscripción en 16 puertos en un arreglo de 2:1
  - Modo de rendimiento: 8 Puertos en arreglo 1:1
- Deberá proporcionar un rendimiento de hasta 60Mpps en IPv4 y hasta 30 Mpps en IPv6
- Deberá soportar Jumbo Frames de 9216 bytes
- Deberá admitir tablas de direcciones MAC de 128K
- Deberá soportar NetFlow
- Deberá soportar 60Mpps para envío de MPLS y hasta 60 Mpps para reenvío de VPLS.
- Deberá soportar IGMPv3, IPV4 e IPv6 en túneles IPv6, IPV4 e IPv6 en túneles MPLS (6PE / 6VPE)
- Cifrado de hardware de capa de enlace MACsec (802.1ae) AES de 128 bits
- Asignación de colas basada en clase de servicio (CoS)

Estandares

- Deberá cumplir con los siguientes protocolos:
  - IEEE 802.1d
  - IEEE 802.1p
  - IEEE 802.1q
  - IEEE 802.1s
  - IEEE 802.1w
  - IEEE 802.3x
  - IEEE 802.3ad
  - IEEE 802.3ae
  - IEEE 802.3ak
  - IEEE 802.3aq
  - IEEE 802.3an
  - ETHERLIKE-MIB (RFC 1643)
  - IF-MIB (RFC 1573)
  - Puente MIB (RFC 1493)
  - RMON MIB (RFC 1757)
  - ENTITY-MIB (RFC 2037)
  - HC-RMON
  - RFC1213-MIB (MIB-II)
  - SMON-MIB
- Deberá cumplir con las siguientes normativas
  - Estándares EMC:
    - FCC Parte 15 (CFR 47) Clase A
    - ICES-003 Clase A
    - VCCI Clase A
    - EN55022 Clase A
    - EN55024
    - CISPR24
    - CISPR 22 Clase A
    - AS / NZS CISPR 22 Clase A
    - ETS 300 386
    - KN 22 Clase A

- EN 50082-1
- EN61000-3-2
- EN61000-3-3
- EN61000-6-1
- CNS13438 Clase A
- Serie KN6100 -4

- Estándares de seguridad:
  - UL 60950-1
  - CAN / CSA C22.2 No. 60950
  - EN 60950-1
  - IEC 60950-1
  - AS / NZS 60950-1
  - IEC 60825 Clase 1
  - EN 60825 Clase 1
  - 21CFR 1040

Condiciones Ambientales

- Deberá soportar una temperatura de operación de 0 a 40°C.

PARTIDA: 11

Tarjeta de interfaz WAN / troncal multifunción T1 / E1 de 2 puertos
Cantidad: 5

Estas tarjetas de interfaz flexibles admiten múltiples aplicaciones integradas de datos, voz y video, lo que facilita la migración de datos solamente, así como servicios de voz / video con conmutación de circuitos a una solución de paquetes de voz / video

Funcionalidades

- Deberá permitir que cada puerto se sincronice desde una fuente de reloj independiente para aplicaciones de datos.
- Deberá permitir que las aplicaciones de voz ahora puedan sincronizarse independientemente de las aplicaciones de datos, con todos los puertos para aplicaciones de voz sincronizados desde una sola fuente.
- Deberá admitir T1, T1 fraccional, E1 y E1 fraccional para aplicaciones de voz y WAN.
- Deberá incluir la capacidad de multiplexación de colocar e insertar, que eliminará costosas unidades externas de servicio de canal externo / unidades de servicio de datos (CSU / DSU) y multiplexores de colocar e insertar.
- Deberá simplificar la configuración de red y el ahorro a través del soporte de T1 y E1 en la misma tarjeta.
- Deberá admitir (modelos G.703) E1 no estructurado (G.703) para usar los 2.048 Mbps completos.
- Deberá suministran conectividad PBX y de red telefónica pública conmutada (PSTN) para enrutadores de servicios integrados con las ranuras de expansión.

Hardware

- Deberá contar con dos puertos T1/E1.
- Deberá contar con una tasa de transmisión/recepción de 1.544 Mbps (con un rango de ± 50 bps/32ppm (para T1) y de 2.048 Mbps ± 100 bps / 50 ppm (para E1)
- Deberá contar con una tasa de velocidad de Datos de 1.9854 Mbps por puerto E1
- Deberá realizar codificación bipolar de alta densidad (HDB3)

Estandares

- Deberá cumplir con las siguientes normativas
  - Estándares EMC:
    - EN55024 (CISPR24)
    - EN61000-4-2
    - EN61000-4-3
    - EN41000-4-4
    - EN41000-4-5
    - EN41000-4-6
    - EN41000-4-8
    - EN41000-4-11
    - EN50082-1
    - EN61000-6-2
    - UIT-T K.21
  - Estándares de seguridad:
    - UL 60950
    - CAN / CSA C22.2 No. 60950
    - IEC 60950-1
    - EN 60950-1
    - AS / NZS 60950

Administración

- Deberá ser configurado de forma remota y local, y resolución de problemas por Telnet y consola.
- Deberá soportar SNMP, MIB estandar (MIB II) y RFC 1406 T1 MIB detección de alarmas e informes. y soportar trampas SNMP

Condiciones Ambientales

- Deberá soportar una temperatura de operación de 0 a 40°C.

PARTIDA: 12

Módulo de procesador de señal digital de voz (DSP) de 64 Canales
Cantidad: 5

Proporciona mayor densidad y más potencia de procesamiento, haciendo posible la adición de aplicaciones de medios enriquecidos. La arquitectura DSP mejorada acomoda un nuevo motor de procesamiento de paquetes optimizado para aplicaciones de voz de medios.

Funcionalidades

- Deberá admitir conexiones de voz digital
- Deberá admitir conexiones de voz analógicas
- Deberá admitir conferencias y servicios de transcodificación universal.

Hardware

- Deberá permitir un máximo de 42 canales en codecs de complejidad media
- Deberá permitir un máximo de 28 canales en codecs de alta complejidad
- Deberá admitir la transmisión, donde la re-empaquetación del mismo códec se utiliza para conectar redes diferentes que tienen diferentes períodos de paquetes de códec
- Deberá realizar funciones de compresión, detección de actividad de voz, gestión de fluctuaciones.
- Deberá realizar cancelación de eco con longitud de cola de 128 milisegundos (ms) y cumple con ITU-T G.168.
- Deberá ofrecer múltiples modos de ahorro de energía.
- Deberá contar con memoria de acceso aleatorio dinámico síncrono (SDRAM) de 512 megabits de doble velocidad de datos (DDR)
- Deberá contar con una Interfaz de módulo de memoria dual en línea (DIMM) de 240 pines

Estandares

- Deberá cumplir con las siguientes normativas
  - Estándares EMC:
    - EN55024 (CISPR24)
    - EN61000-4-2
    - EN61000-4-3
    - EN41000-4-4
    - EN41000-4-5
    - EN41000-4-6
    - EN41000-4-8
    - EN41000-4-11
    - EN50082-1
    - EN61000-6-2
    - UIT-T K.21
  - Estándares de seguridad:
    - NOM-019-SCFI-1998
    - UL 60950
    - CAN / CSA C22.2 No. 60950
    - IEC 60950-1
    - EN 60950-1
    - AS / NZS 60950
    - GB4943-95

Secretaría de Administración

Adquisición de equipamiento de telecomunicaciones

Condiciones Ambientales

- Deberá soportar una temperatura de operación de -5 a 55°C.

PARTIDA: 13

PUNTO DE ACCESO INALAMBRICO
Cantidad: 10

CARACTERÍSTICAS

- Se deberá de incluir todo lo necesario para la correcta operación del equipo
- Todo el software deberá residir y ejecutarse con recursos propios del equipo propuesto.
- Se deberá de incluir todo lo necesario para la correcta instalación y operación del equipo.
- Deberá proporcionar múltiples velocidades de enlace ascendente de 2.5 Gbps y 5 Gbps, además de velocidades de 100 Mbps y 1 Gbps. Todas las velocidades están soportadas en cableado categoría 5e, así como 10GBASE-T para cableado Cat 6ª.
- Soporte de 2 Puertos 100/1000/2500/5000 RJ45 para conectividad
- Deberá contar con puerto de Consola RJ45 y botón de reset de fabrica
- Deberá ser basado para uso con controladora o autónomo dependiendo del tipo de software instalado
- El punto de acceso inalámbrico deberá proporcionar acceso a dispositivos de alto rendimiento a través de una sensibilidad y alcance de radio mejoradas con tecnología MU-MIMO (Multiuser multiple-input multiple-output) con 3 flujos espaciales 802.11a/b/g/n/ac Wave1, Wave 2 con dos o tres flujos espaciales y datos de hasta 450 Mbps (802.11n), 1.3 Gbps (802.11ac Wave 1) y 2.6 Gbps (802.11ac Wave 2)
- Deberá ser alimentado vía Power Over Ethernet acorde al standard IEEE802.3af y 802.3at
- Deberá contar con puertos para antenas internas
- El punto de acceso al aire libre puede admitir antenas de banda o bien de una sola banda de antenas en la misma plataforma y es configurable a través de software
- Cuando se configura para puertos de doble banda, el punto de acceso deberá utilizar los dos puertos inferiores de antena para conectarse a antenas omnidireccionales o direccionales de banda dual. Alternativamente, y para una mayor flexibilidad de cobertura de radio, el punto de acceso puede configurarse por software, permitiendo dos puertos de antena separados de 2,4 GHz y dos de 5 GHz.
- Deberá de soportar control de flujo es decir deberá de tener mecanismos para hacer más eficiente la transmisión de datos a través de Gigabit Ethernet

1. CAPACIDADES 802.11n VERSION 2.0

- MIMO 4x4 con tres flujos espaciales
- Combinación de relación máxima (MRC)
- Formación de haces 802.11n y 802.11a / g
- Canales de 20 y 40 MHz
- Velocidades de datos PHY de hasta 450 Mbps (40 MHz con 5 GHz).
- Agregación de paquetes: A-MPDU (Tx / Rx), A-MSDU (Tx / Rx)
- Selección de frecuencia dinámica 802.11 (DFS)
- Soporte de diversidad de desplazamiento cíclico (CSD)

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

2. CAPACIDADES 802.11ac WAVE 1

- MIMO 4x4 con tres flujos espaciales
- MRC
- Formación de haces 802.11ac
- Canales de 20, 40 y 80 MHz
- Velocidades de datos PHY de hasta 1,3 Gbps (80 MHz en 5 GHz)
- Agregación de paquetes: A-MPDU (Tx / Rx), A-MSDU (Tx / Rx)
- 802.11 DFS
- Soporte de CSD

3. CAPACIDADES 802.11ac WAVE 2

- 4x4 MU-MIMO con tres flujos espaciales
- MRC
- Formación de haces 802.11ac
- Canales de 20, 40, 80 y 160 MHz
- Tasas de datos PHY de hasta 5.2 Gbps
- Agregación de paquetes: A-MPDU (Tx / Rx), A-MSDU (Tx / Rx)
- 802.11 DFS
- Soporte de CSD

4. CERTIFICADO DE WI-FI ALLIANCE

- Certificado Wi-Fi a, b, g, n, ac
- Wi-Fi Vantage
- WMM
- Passpoint

5. ANTENA INTEGRADA

- 2.4 GHz, ganancia 4 dBi, antena interna, omnidireccional en azimut
- 5 GHz, ganancia 6 dBi, antena direccional interna, anchura de haz del plano de elevación 90 °
- 5 GHz, ganancia 5 dBi, antena interna, omnidireccional en azimut
- 4x4 MU-MIMO con tres flujos espaciales
- MRC
- Formación de haces 802.11ac
- Canales de 20, 40, 80 y 160 MHz
- Tasas de datos PHY de hasta 5.2 Gbps
- Agregación de paquetes: A-MPDU (Tx / Rx), A-MSDU (Tx / Rx)
- 802.11 DFS
- Soporte de CSD

6. TASAS DE DATOS SOPORTADAS (Mbps)

- 802.11b: 1, 2, 5.5 y 11 Mbps
- 802.11a/g: 6, 9, 12, 18, 24, 36, 48 y 54 Mbps
- 802.11n HT20: 6,5 a 216,7 Mbps (MCS0 a MCS23)
- 802.11n HT40: 13,5 a 450 Mbps (MCS0 a MCS23)
- 802.11ac VHT20: 6,5 a 288,9 Mbps (MCS0 a 8 - SS 1, MCS0 a 9 - SS 2 y 3)

- 802.11ac VHT40: 13,5 a 600 Mbps (MCS0 a 9 - SS 1 a 3)
- 802.11ac VHT80: 29.3 a 1300 Mbps (MCS0 a 9 - SS 1 a 3) 802.11ac VHT160: 58,5 a 2304 Mbps (MCS0 a 9 - SS 1 y 2, MCS0 a 8 - SS 3)

7. RADIOS DE RECUENCIA Y CANALES DE OPERACIÓN DE 20 MHz

- Dominio A:
  - 2.412 a 2.462 GHz; 11 canales
  - 5.280 a 5.320 GHz; 8 canales
  - 5.500 a 5.700 GHz; 8 canales
  - 5.745 a 5.825 GHz; 5 canales
- Dominio B
  - 2.412 a 2.462 GHz; 11 canales
  - 5.180 a 5.320 GHz; 8 canales
  - 5.500 a 5.720 GHz; 4 canales
  - 5.745 a 5.825 GHz; 5 canales
- Dominio C:
  - 2.412 a 2.472 GHz; 13 canales
  - 5.745 a 5.825 GHz; 5 canales
- Dominio D
  - 2.412 a 2.462 GHz; 11 canales
  - 5.180 a 5.320 GHz; 8 canales
  - 5.745 a 5.825 GHz; 5 canales
- E (dominio regulador E):
  - 2.412 a 2.472 GHz; 13 canales
  - 5.180 a 5.320 GHz; 8 canales
  - 5.500 a 5.700 GHz; 8 canales
- F (dominio regulador F):
  - 2.412 a 2.472 GHz; 13 canales
  - 5.745 a 5.805 GHz; 4 canales
- G (dominio regulador G):
  - 2.412 a 2.472 GHz; 13 canales
  - 5.745 a 5.825 GHz; 5 canales
- H (dominio regulador H):
  - 2.412 a 2.472 GHz; 13 canales
  - 5.150 a 5.320 GHz; 8 canales
  - 5.745 a 5.825 GHz; 5 canales
- I (I dominio regulador):
  - 2.412 a 2.472 GHz; 13 canales
  - 5.180 a 5.320 GHz; 8 canales
- K (dominio regulador K):
  - 2.412 a 2.472 GHz; 13 canales
  - 5.180 a 5.320 GHz; 8 canales
  - 5.500 a 5.620 GHz; 7 canales
  - 5.745 a 5.805 GHz; 4 canales
- N (dominio regulador N):
  - 2.412 a 2.462 GHz; 11 canales
  - 5.180 a 5.320 GHz; 8 canales

- o 5.745 a 5.825 GHz; 5 canales
- Q (Q dominio regulador):
  - o 2.412 a 2.472 GHz; 13 canales
  - o 5.180 a 5.320 GHz; 8 canales
  - o 5.500 a 5.700 GHz; 11 canales
- R (R dominio regulatorio):
  - o 2.412 a 2.472 GHz; 13 canales
  - o 5.180 a 5.320 GHz; 8 canales
  - o 5.660 a 5.700 GHz; 3 canales
  - o 5.745 a 5.805 GHZ; 4 canales
- S (dominio regulador S):
  - o 2.412 a 2.472 GHz; 13 canales
  - o 5.180 a 5.320 GHz; 8 canales
  - o 5.500 a 5.700 GHz ;, 11 canales
  - o 5.745 a 5.825 GHz; 5 canales
- T (dominio T regulador):
  - o 2.412 a 2.462 GHz; 11 canales
  - o 5.280 a 5.320 GHz; 3 canales
  - o 5.500 a 5.700 GHz; 8 canales
  - o (excluye 5.600 a 5.640 GHz)
  - o 5.745 a 5.825 GHz; 5 canales
- Z (dominio regulador Z):
  - o 2.412 a 2.462 GHz; 11 canales
  - o 5.180 a 5.320 GHz; 8 canales
  - o 5.500 a 5.700 GHz; 8 canales
  - o (excluye 5.600 a 5.640 GHz)

  5.745 a 5.825 GHz; 5 canales

8. MAXIMO NUMERO DE CANALES NO TRASLAPADOS

- 2.4 GHz
  - o 802.11b/g: 3 (20 MHz)
  - o 802.11n: 3 (20 MHz)
- 5 GHz
  - o 802.11a: 25 FCC, 16 UE (20 MHz)
  - o 802.11n: 25 FCC, 16 UE (20 MHz), 12 FCC, 7 UE (40 MHz)
  - o 802.11ac: 25 FCC, 16 UE (20 MHz), 12 FCC, 7 UE (40 MHz), 6 FCC, 3 UE (80 MHz), 2 FCC, 1 UE (160MHz)

9. POTENCIA DE TRANSMISIÓN MAXIMA (dBm)

- 2.4 GHz
  - o 23 dBm (200mW)
  - o 20 dBm (100 mW)
  - o 17 dBm (50 mW)
  - o 14 dBm (25 mW)

- o 11 dBm (12.5 mW)
- o 8 dBm (6.25m mW)
- o 5 dBm (1.56 mW)

· 5 GHz

- o 23 dBm (200mW)
- o 20 dBm (100 mW)
- o 17 dBm (50 mW)
- o 14 dBm (25 mW)
- o 11 dBm (12.5 mW)
- o 8 dBm (6.25m mW)
- o 5 dBm (1.56 mW)

10. CONFORMIDAD

- UL 60950-1
- CAN / CSA-C22.2 No. 60950-1
- UL 2043
- IEC 60950-1
- EN 60950-1
- EN 50155
- Aprobaciones de radio:
  - o FCC, Parte 15.107, 15.109, 15.247, 15.407, 14-30
  - o RSS-247 (Canadá)
  - o EN 300.328, EN 301.893 (Europa)
  - o ARIB-STD 66 (Japón)
  - o ARIB-STD T71 (Japón)
  - o IME y susceptibilidad (Clase B)
  - o ICES-003 (Canadá)
  - o VCCI (Japón)
  - o EN 301.489-1 y -17 (Europa)
  - o EN 60601-1-2 Requisitos CEM para la Directiva Médica 93/42 / CEE
- Estándares IEEE:
  - o IEEE 802.11a / b / g, 802.11n, 802.11h, 802.11d, 802.11r, 802.11k, 802.11v, 802.11u, 802.11w
  - o IEEE 802.11ac
- Seguridad:
  - o 802.11i, Acceso protegido Wi-Fi 2 (WPA2), WPA
  - o 802.1X
  - o Estándares avanzados de cifrado (AES), TKIP (Temporal Key Integrity Protocol)
- Tipos de protocolo de autenticación extensible (EAP):
  - o EAP-Seguridad de la capa de transporte (TLS)
  - o TLS de Túnel EAP (TTLS) o Microsoft Challenge Handshake Protocolo de autenticación versión 2 (MSCHAPv2)
  - o EAP protegido (PEAP) v0 o EAP-MSCHAPv2
  - o EAP-Autenticación flexible mediante túneles seguros (FAST)
  - o PEAP v1 o EAP-Generic Token Card (GTC)
  - o EAP-Módulo de Identidad del Suscriptor (SIM)
- Multimedia:
  - o Multimedia Wi-Fi (WMM)

- Otros:
  - Boletín FCC OET-65C
  - RSS-102MAC.

- El proveedor será responsable de llevar a cabo la instalación, configuración y puesta a punto de todo el equipamiento a fin de garantizar el correcto funcionamiento de los equipos.
- Todas las configuraciones y entregas de equipamiento se deberán realizar en la secretaria de administración quien llevara a cabo el despliegue y asignación de equipos con el resto de las áreas u oficinas en cuyos casos aplique.

La propuesta deberá incluir los siguientes cursos de capacitación:
2 Cursos de preparación para la certificación CCNA (Con examen)
1 Curso de preparación para la certificación CCNP (Sin examen)
1 Curso de administración de CUCM (Sin examen)

6. GARANTIAS

Todo el equipamiento deberá contar con al menos 1 año de garantía.

7. OBLIGACIONES DE LOS PARTICIPANTES

1. Para garantizar que los productos que distribuye son nuevos, no re manufacturados y cuentan con garantía estándar deberá acreditar mediante carta original de la fabricante dirigida a la convocante que es un Partner autorizado, mínimo de nivel Premier.

2. El participante también deberá presentar una carta de carta de fabricante donde demuestre que cuenta con la experiencia y conocimiento técnicos para dar cumplimento a los requisitos del presente proyecto.

3. El proveedor en su propuesta deberá mencionar marca, modelo, especificaciones y garantías de su cotización, todos los componentes deberán ser homogéneos y venir integrados de fábrica.

4. El proveedor en su propuesta podrá ofertar características superiores a las solicitadas, lo cual deberá ser corroborado por el fabricante del dispositivo que oferte como superior mediante carta.

5. Deberá presentar Datasheet del equipo ofertado con link de página oficial, en el cual puede ser corroborada la información de acuerdo a su cotización

6. Carta del fabricante en al que se señale que el producto cuenta con servicio de soporte proporcionado directamente con el fabricante

7. Carta del fabricante donde se señale que el participante cuenta con al menos 2 ingenieros certificados CCNA Routing & Switching, 1 ingeniero certificado en CCDA o superior.

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

8. Presentar certificados de ingenieros CCNA (Cisco certified Network Associate Routing and Switching) al menos 2 personas.

9. Presentar certificados de ingenieros CCDA o superior (Cisco Certified Design Associate) al menos 1 persona

10. Presentar certificados de ingenieros CCNP Collaboration superior (Cisco Certified Design Associate) al menos 1 persona

11. Presentar el certificado ITIL Foundation v3 al menos 1 persona.

12. A fin de garantizar la correcta ejecución del proyecto y homologación de criterios para la implementación, todas las partidas serán asignadas a un solo proveedor.

13. Las propuestas deberán incluir la totalidad de partidas.

8. RESPONSABLES DEL REQUERIMIENTO

Responsable de elaborar el requerimiento	
Nombre: Stephany Crystin Cardenas Patiño	
Puesto Asistente Administrativo	
e-mail stephany.cardenas@jalisco.gob.mx	
Fecha: 19 de Agosto de 2019	Tel. /ext. 38182800 26587
Firma:	

Responsable de autorizar el requerimiento	
Nombre: Miguel Angel Romo Rubio	
Puesto Director de Infraestructura y Comunicaciones	
e-mail miguel.romo@jalisco.gob.mx	
Fecha: 19 de Agosto de 2019	Tel. /ext. 38182800 26255
Firma:	

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

ANEXO 2

LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

Guadalajara Jalisco, a ___ de ____ de 2019.

(PROPUESTA TÉCNICA)

Progresivo	Cantidad	Unidad de Medida	Artículo	Descripción	Entregables y demás características

NOTA: Se deberá realizar el desglose a detalle del anexo técnico (Especificaciones) cumpliendo con lo requerido en el mismo en formato libre.

En caso de ser adjudicado proporcionaré servicios en los términos y condiciones del presente anexo, la orden de compra 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. 44100,

Guadalajara, Jalisco, México

ANEXO 3

LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

Guadalajara Jalisco, a ___ de ____ del 2019.

PROPUESTA ECONÓMICA

Progresivo	Cantidad	Unidad de Medida	Artículo	Descripción	Precio Unitario	Importe
				SUBTOTAL		
				I.V.A.		
				TOTAL		

CANTIDAD CON LETRA:
TIEMPO DE ENTREGA: (De no señalar fecha específica, el Licitante deberá señalar si el número de días son hábiles o 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).

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 proceso de adquisición.

ATENTAMENTE

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

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

ANEXO 4
LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

CARTA DE PROPOSICIÓN

Guadalajara Jalisco, a ___ de ____ del 2019.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Lic. Luis Arturo López Sahagún
Director General de Abastecimientos

En atención al procedimiento de **Licitación Pública Local LPL251 /2019 CON CONCURRENCIA DEL "COMITÉ"** relativo a la **"____".** (En lo subsecuente "el proceso 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 adjudicación, 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 a que haya lugar la finca marcada con el número xx de la calle xx, de la colonia XXXXXXXXXXXX, de la ciudad de xx, C.P. XXXXX, teléfono xx, fax xxxx y correo electrónico XXXXXX.
3. Que he leído, revisado y analizado con detalle todas las condiciones de las **"BASES"** del presente proceso de adjudicación, 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 proceso de adjudicación, 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 proceso 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 adjudicación.
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 proceso de adjudicación.
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.

ATENTAMENTE

_____

Nombre y firma del Participante
o Representante Legal del mismo

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

ANEXO 5
LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

Guadalajara Jalisco, a ___ de ____ del 2019.

ACREDITACIÓN

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Lic. Luis Arturo López Sahagún
Director General de Abastecimientos

Yo, (nombre), manifiesto **bajo protesta de decir verdad**, que los datos aquí asentados son ciertos y han sido verificados, manifiesto 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 LPL __/2019 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)		

Personas 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:**

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

*****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. *Personas 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:**

ATENTAMENTE

_____

Nombre y firma del Licitante
o Representante Legal

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

ANEXO 6

LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

DECLARACIÓN DE INTEGRIDAD Y NO COLUSIÓN DE PROVEEDORES.

Guadalajara Jalisco, a ___ de ____ del 2019.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Lic. Luis Arturo López Sahagún
Director General de Abastecimientos

En cumplimiento con los requisitos establecidos en el presente Proceso de Adquisición para la **Licitación Pública Local LPL__/2019 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.

ATENTAMENTE

_____
Nombre y firma del Licitante
o Representante Legal

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

ANEXO 7
LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

ESTRATIFICACIÓN

Guadalajara Jalisco, a __ de ____ del 2019. (**1**)

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Lic. Luis Arturo López Sahagún
Director General de Abastecimientos

Me refiero al procedimiento de **Licitación Pública Local LPL __/2019 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

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

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. 44100,

Guadalajara, Jalisco, México

ANEXO 8

LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

ARTÍCULO 32-D

Guadalajara Jalisco, a ___ de ___ del 2019.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Luis Arturo López Sahagún
Director 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. 44100,

Guadalajara, Jalisco, México

ANEXO 9
LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

Cumplimiento obligaciones IMSS

Guadalajara Jalisco, a ___ de _____ del 2019.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Lic. Luis Arturo López Sahagún
Director 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. 44100,

Guadalajara, Jalisco, México

ANEXO 10
LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

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

Guadalajara Jalisco, a ___ de ___ del 2019.

ANVERSO

REVERSO

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

ANEXO 11
LICITACIÓN PÚBLICA LOCAL

LPL251 /2019

"ADQUISICION DE POLIZAS DE MANTENIMIENTO Y LICENCIAMIENTO PARA GOBIERNO DEL ESTADO"

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

Guadalajara Jalisco, a __ de ____ del 2019.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE

AT'N: Lic. Luis Arturo López Sahagún
Director General de Abastecimientos

En cumplimiento con los requisitos establecidos en el presente Proceso de Adquisición para la **Licitación Pública Local LPL __/2019 con concurrencia** del **"COMITÉ" "____",** 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

Av. Fray Antonio Alcalde#1221,

Col. Miraflores, C.P. 44100,

Guadalajara, Jalisco, México

ANEXO 12

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 DEL ESTADO DE JALISCO** CON DOMICILIO EN CALLE PEDRO MORENO 281, 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 POR 12 MESES CONTADOS A PARTIR DE LA FECHA DEL CONTRATO.

ADICIONALMENTE ESTA FIANZA PODRÁ SER EXIGIBLE EN CUALQUIER TIEMPO PARA GARANTIZAR LAS OBLIGACIONES DEL **CONTRATO,"BASES" Y/O CONVOCATORIA** DEL PROCESO 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 PROCESO 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
S DEL MISMO NUMERAL. FIN DEL TEXTO.