PODER EJECUTIVO DEL ESTADO DE JALISCO

DIRECCIÓN GENERAL DE ABASTECIMIENTOS EN COORDINACIÓN CON LA SECRETARIA DE ADMINISTRACIÓN DEL ESTADO DE JALISCO

C O N V O C A T O R I A

EL GOBIERNO DEL ESTADO DE JALISCO, A TRAVÉS DE LA DIRECCIÓN GENERAL DE ABASTECIMIENTOS Y EN COORDINACIÓN CON LA SECRETARÍA DE ADMINISTRACIÓN, DE CONFORMIDAD CON EL ARTÍCULO 62 DEL REGLAMENTO DE LA LEY DE COMPRAS GUBERNAMENTALES, ENAJENACIONES Y CONTRATACIÓN DE SERVICIOS DEL ESTADO DE JALISCO Y SUS MUNICIPIOS, INVITA A LAS EMPRESAS A PARTICIPAR EN LA LICITACIÓN PÚBLICA LOCAL:

No. LPL 774/2026

CONTRATACION DE PÓLIZA DE SERVICIO DE SOPORTE TÉCNICO Y MANTENIMIENTO A LA INFRAESTRUCTURA DE RED SEGURA DEL GEJ

FECHA		ACTIVIDAD	HORARIO	LUGAR
NO APLICA		VISITA DE CAMPO (NO APLICA)	**REGISTRO** **DE LAS:** N/A **A LAS:** N/A **ACTO A LAS:** N/A	NO APLICA
DEL: 20/11/2026	AL: 23/11/2026	RECEPCIÓN DE PREGUNTAS	HASTA LAS: 12:00 hrs	DEBERÁ ENTREGARSE EN FORMATO DIGITAL DE "WORD" (.docx), PODRÁ ENTREGARSE EN CD Ó USB PRESENTANDO EN LAS OFICINAS UBICADAS EN AV. FRAY ANTONIO ALCALDE #1221, COL. MIRAFLORES, C.P. 44270, GUADALAJARA, JALISCO, MÉXICO., O ENVIANDO POR CORREO. EN CASO DE ENVIAR POR CORREO ELECTRONICO, QUE SE HAGA A LOS SIGUIENTES CORREOS: hugo.sanchez@jalisco.gob.mx
26/11/2026		JUNTA ACLARATORIA	**REGISTRO** **DE LAS:** 11:00 hrs **A LAS:** 11:50 hrs **ACTO A LAS:** 12:00 hrs	OFICINAS DE LA DIRECCIÓN GENERAL DE ABASTECIMIENTOS UBICADA EN AV. FRAY ANTONIO ALCALDE #1221, COL. MIRAFLORES, C.P. 44270, GUADALAJARA, JALISCO, MÉXICO.
30/11/2026		ACTO DE PRESENTACIÓN Y APERTURA DE PROPOSICIONES.	**REGISTRO** **DE LAS:** 15:00 hrs **A LAS:** 15:50 hrs **ACTO A LAS:** 16:00 hrs	EN LAS OFICINAS DE LA DIRECCIÓN GENERAL DE ABASTECIMIENTOS UBICADA EN AV. FRAY ANTONIO ALCALDE #1221, COL. MIRAFLORES, C.P. 44270, GUADALAJARA, JALISCO, MÉXICO.

Muestras Físicas:	Visita de Campo	Anexo Técnico	Concurrencia	Carácter	Tipo de Contrato
NO APLICA	NO APLICA	PÚBLICO	CON CONCURRENCIA DEL COMITÉ	LOCAL	CERRADO

DUDAS O COMENTARIOS AL TELÉFONO 3338182800, DE LUNES A VIERNES DE 09:00 A 15:00 HORAS CON HUGO SANCHEZ ESPINOSA EXT. 26103

LAS INCONFORMIDADES SOBRE CONTRATACIONES PÚBLICAS DEBEN PRESENTARSE ANTE LA CONTROLARÍA DEL ESTADO DE ACUERDO A LOS ARTICULOS 90 Y 91 DE LA LEY DE COMPRAS GUBERNAMENTALES, ENAJENACIONES Y CONTRATACIÓN DE SERVICIOS DEL ESTADO DE JALISCO Y SUS MUNICIPIOS

GUADALAJARA, JALISCO MÉXICO **20/11/2026**

JOSE EDUARDO TORRES QUINTANAR.

LICITACIÓN PÚBLICA LOCAL LPL 774/2026 PARA:
"CONTRATACION DE PÓLIZA DE SERVICIO DE SOPORTE TÉCNICO Y MANTENIMIENTO A LA INFRAESTRUCTURA DE RED SEGURA DEL GEJ"
CON CONCURRENCIA DEL COMITÉ
PORTADA

SOBRE EL PROCEDIMIENTO:

CARÁCTER:	LOCAL	**FECHA DE PUBLICACIÓN:**	20/11/2026
DEPENDENCIA SOLICITANTE:	SECRETARIA DE ADMINISTRACION	**PLAZO PARA PREPARAR LA PROPUESTA:**	11 DÍAS
PROPOSICIONES CONJUNTAS:	SI	**ACTO DE PRESENTACIÓN Y APERTURA DE PROPOSICIONES:**	30/11/2026
TIPO DE CONTRATO:	CERRADO	**TIPO DE PLAZOS:**	TIEMPOS NORMALES
ADJUDICACIÓN:	A UN SOLO PROVEEDOR	**METODO DE EVALUACIÓN:**	BINARIO
TIPO ANEXO:	PÚBLICO	**NO(s). DE APROVISIONAMIENTO:**	35-101-2026
DISPONIBLE EN LAS PRESENTES BASES.			
Fecha:	HASTA EL DIA: **NO APLICA**		
Hora:	A LAS: **NO APLICA**	**TESTIGO SOCIAL:**	NO PARTICIPA

VISITA Y/O MUESTRA FÍSICA:

VISITA DE CAMPO:	NO APLICA	**MUESTRA FÍSICA:**	NO APLICA

SOBRE LOS RECURSOS

FUENTE:	11. NO ETIQUETADO RECURSO FISCAL.	**EJERCICIO:**	2026

CALENDARIO LPL 774/2026
LICITACIÓN PÚBLICA LOCAL PARA:
"CONTRATACION DE PÓLIZA DE SERVICIO DE SOPORTE TÉCNICO Y MANTENIMIENTO A LA INFRAESTRUCTURA DE RED SEGURA DEL GEJ"
CON CONCURRENCIA DEL COMITÉ

FECHA DE PUBLICACIÓN:	**20/11/2026**

ACTO DE PRESENTACIÓN Y APERTURA DE PROPOSICIONES:	**30/11/2026**

PLAZO PARA PRESENTAR PREGUNTAS PARA JUNTA ACLARATORIA	
PLAZO PARA PRESENTAR: (FECHAS)	*A PARTIR DEL:* **20/11/2026** *HASTA EL:* **23/11/2026** *A LAS:* **12:00 hrs**
LUGAR DE PRESENTACIÓN FÍSICA:	EN LAS OFICINAS DE LA DIRECCIÓN GENERAL DE ABASTECIMIENTOS UBICADA EN AV. FRAY ANTONIO ALCALDE #1221, COL. MIRAFLORES, C.P. 44270, GUADALAJARA, JALISCO, MÉXICO.
PRESENTACIÓN MEDIANTE CORREO ELECTRONICO:	hugo.sanchez@jalisco.gob.mx

ACTO DE PRESENTACIÓN Y APERTURA DE PROPOSICIONES	
FECHA:	**30/11/2026**
HORARIO DE REGISTRO:	*DE LAS:* **15:00 hrs** *A LAS:* **15:50 hrs**
HORA DE INICIO DEL ACTO:	**16:00 hrs**
LUGAR:	EN LAS OFICINAS DE LA DIRECCIÓN GENERAL DE ABASTECIMIENTOS UBICADA EN AV. FRAY ANTONIO ALCALDE #1221, COL. MIRAFLORES, C.P. 44270, GUADALAJARA, JALISCO, MÉXICO.

JUNTA ACLARATORIA	
FECHA:	26/11/2026
HORARIO DE REGISTRO:	*DE LAS:* **11:00 hrs** *A LAS:* **11:50 hrs**
HORA DE INICIO DEL ACTO:	**12:00 hrs**
LUGAR:	EN LAS OFICINAS DE LA DIRECCIÓN GENERAL DE ABASTECIMIENTOS UBICADA EN AV. FRAY ANTONIO ALCALDE #1221, COL. MIRAFLORES, C.P. 44270, GUADALAJARA, JALISCO, MÉXICO.

ACTO DE RESOLUCIÓN DE FALLO	
FECHA:	CONFORME AL ARTICULO 65 NUMERAL 1 FRACCIÓN TERCERA Y 69 EN LA LEY, PODRÁ EMITIRSE DENTRO DE LOS VEINTE DIAS POSTERIORES A LA APERTURA DE PROPOSICIONES Y EN CASO DE SER NECESARIO DIFERIRSE POR OTROS VEINTE DIAS.
PUBLICACIÓN DIGITAL:	https://compras.jalisco.gob.mx/requisition/tree

MUESTRAS FÍSICAS:	NO APLICA	**Fecha:**
NO APLICA		NO APLICA
		Hora:
		Desde las: NO APLICA Hasta las:
VISITA DE CAMPO:	NO APLICA	**Fecha:**
NO APLICA		NO APLICA
		Hora:
		NO APLICA

**FECHAS ESTABLECIDAS EN (DD/MM/AAAA)*

De conformidad con los artículos: 134 de la CPEUM[1]; 19 apartado 1 fracción XI de la LOPEEJ[2]; 1, 2 fracción IX, artículo 2,3, fracción XXXI, XXXVI, LIX, 9 fracción II, 20 fracción I, 21 del RISAEJ[3]; artículo 1, 2, 3, 4, 5, 23, 24, 31, 34, 35, 36, 37, 38, 39, 47, 55 apartado 1 fracción II, 59, 63, 69, 72 de la LCGECSEJM[4]; artículo 1, 3, 4, 44, 46, 50, 51, 53, 54, 62, 64, 69 del RLCGECSEJM[5]; artículo 1, 2, 6, 15, 16 de la LAAEJM[6]; La Secretaría de Administración del Poder Ejecutivo del Estado de Jalisco en coordinación con la Dirección General de Abastecimientos emite las siguientes

B A S E S D E L I C I T A C I Ó N P Ú B L I C A:

1. Antecedentes.

La Secretaría de Administración del Poder Ejecutivo del Estado de Jalisco, en coordinación con la Dirección General de Abastecimientos, convoca a las personas físicas y jurídicas que estén interesadas en participar del presente proceso de licitación. Proceso fundado y motivado por medio de la **Solicitud de Aprovisionamiento, Fuente de financiamiento y Ejercicio Fiscal** establecidos en la **Portada**.

2. Definiciones.

2.1 ***Acto de presentación y apertura de proposiciones:*** acto en el que se presentan, abren y registran las proposiciones (o propuestas) de los participantes;

2.2 ***Adjudicación:*** declaración competente emitida por parte de la dirección de adquisiciones, contrataciones o en su caso del comité donde se asigna un proveedor el cual cuenta con el mejor resultado en la evaluación combinada de puntos y porcentajes, binaria, o bien, de costo beneficio;

2.3 ***Aportación cinco al millar:*** retención del monto total de los contratos de bienes y servicios antes de I.V.A otorgados bajo convocatoria pública para la licitación pública o adjudicación pública directa, que será aportado al Fondo Impulso Jalisco, equivalente al 0.5 punto cinco por ciento del valor asignado, previa declaración de voluntad suscrita por el aportante;

2.4 ***Dependencia requirente:*** la unidad administrativa del ente público que, de acuerdo con sus necesidades, solicite o requiera formalmente a la unidad centralizada de compras del mismo ente público, la adquisición o arrendamiento de bienes o la prestación de servicios, establecido específicamente en la **Portada;**

2.5 ***Bases:*** es el llamado a los interesados a participar en determinado procedimiento de adquisiciones, contrataciones o enajenación, que además contiene las condiciones y requisitos detallados de participación en dichos procedimientos;

2.6 ***Carácter:*** el carácter de la presente licitación se establece en la **Portada** de las presentes bases, entendiéndose, por tanto, que son:

2.6.1 ***Locales,*** cuando únicamente puedan participar proveedores con domicilio fiscal en el Estado de Jalisco;

2.6.2 ***Nacionales,*** cuando puedan participar proveedores de cualquier parte de la República Mexicana, entendiendo por ellos a los proveedores constituidos o establecidos en el interior de la república que provean de insumos de origen nacional que cuenten por lo menos con el cincuenta por ciento de integración local;

2.6.3 ***Internacionales,*** cuando puedan participar proveedores locales, nacionales y del extranjero;

2.7 ***Comité***: los comités de cada ente público, son los órganos colegiados encargados de intervenir y resolver sobre las adquisiciones, contrataciones y arrendamientos de bienes muebles y contratación de servicios de cualquier naturaleza que se realice, vigilando el estricto cumplimiento de la normatividad aplicable;

2.8 ***Convocante****:* el ente público que a través de su unidad centralizada de compras lleva a cabo los

Fundamento Legal:
[1]Constitución Política de Los Estados Unidos Mexicanos.
[2]Ley Orgánica del Poder Ejecutivo del Estado de Jalisco.
[3]Reglamento Interno de la Secretaria de Administración del Estado de Jalisco
[4]Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
[5]Reglamento de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
[6]Ley de Austeridad y Ahorro del Estado de Jalisco y sus Municipios.

procedimientos de contratación a efecto de adquirir o arrendar bienes o contratar la prestación de servicios que solicite la unidad requirente;

2.9 ***Convocatoria***: es el llamado a los interesados a participar en determinado procedimiento de adquisiciones, contrataciones o enajenaciones, que además contiene las condiciones y requisitos detallados de participación en dichos procedimientos;

2.10 ***Contraloría***: la Contraloría del Estado, misma que ejercerá las funciones encomendadas por la Ley a los Órganos de Control;

2.11 ***Criterios de evaluación:*** los criterios específicos que se utilizarán para la evaluación de las proposiciones y adjudicación de los contratos, establecidos en el anexo técnico;

2.12 ***Desechamiento:*** el desechamiento es el proceso que garantiza que solo participen en los procesos aquellas propuestas que se ajusten plenamente a las condiciones y criterios previamente definidos, asegurando transparencia y equidad en las contrataciones públicas;

2.13 ***Dirección:*** Dirección General de Abastecimientos dependiente de la Secretaría de Administración del Estado de Jalisco;

2.14 ***Documento Público:*** documento que, autorizado por Servidor público adscrito, acredita los hechos que refiere y su fecha;

2.15 ***Ejercicio fiscal:*** el año financiero o fiscal comprendido por 12 meses, empezando el primero de enero y terminando el treinta y uno de diciembre del año establecido en la **Portada** de las bases;

2.16 ***Fianza o póliza:*** cantidad de dinero u objeto de valor que se da para asegurar el cumplimiento de suministros, la seriedad de la oferta y la correcta aplicación de los anticipos u otras obligaciones, misma que será expedida por una institución autorizada en el Estado. Cuando éstos tengan su domicilio fuera de Jalisco, deberán exhibir la garantía, con la aceptación de la afianzadora que la expida de someterse a la competencia de los juzgados del fuero común o federal con jurisdicción en la ciudad de Guadalajara, Jalisco;

2.17 ***Investigación de mercado:*** técnica usada para identificar las características del mercado de bienes y servicios específicos, a fin de proveer a la dependencia requirente de información útil, para planear las adquisiciones de bienes o contratación de servicios y arrendamiento de bienes o la prestación de servicios;

2.18 ***Ley:*** La Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios;

2.19 ***Licitante o Participante:*** la persona física o jurídica que participa en cualquier procedimiento de licitación pública;

2.20 ***Manifiesto:*** Formato que contiene la declaración bajo protesta de conducirse con verdad de una persona física o jurídica;

2.21 ***Muestras físicas:*** bien presentado por los participantes con objeto de analizar, verificar y comprobar la calidad de este;

2.22 ***Multianual:*** se refiere a aquellos contratos cuyos efectos, obligaciones o ejecución se extienden por más de un ejercicio fiscal;

2.23 ***Órgano Interno de Control:*** es la instancia administrativa interna de las dependencias y entidades públicas que tiene como propósito vigilar, prevenir y corregir actos que puedan derivar en irregularidades o incumplimientos de las disposiciones legales y normativas aplicables;

2.24 ***Origen de los recursos:*** precisión sobre cuál es el origen de los recursos pudiendo ser Estatal o Federal;

2.25 ***Portada:*** primera página que contiene toda la información específica del proceso de licitación;

2.26 ***Precio no conveniente:*** Es aquel que resulta excesivo, no competitivo o desproporcionado en comparación

Fundamento Legal:
Art. 2, 55, 59, 64, 65, 67, 69, 72 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 2, 21, 51, 67, 183 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

con los precios de mercado o las estimaciones presupuestales, afectando la eficiencia en el uso de recursos públicos;

2.27 ***Propuesta o proposición:*** documento presentado por los interesados, mediante el cual señalan las características técnicas del bien o servicio ofertado (propuesta o proposición técnica), así como su precio (propuesta económica);

2.28 ***Proveedor, Participante o Licitante adjudicado:*** se refiere a él o los licitantes que participan del presente proceso de licitación y son determinados mediante el fallo como los ganadores del proceso y quienes deberán de proveer al Gobierno del Estado lo solicitado en el anexo técnico;

2.29 ***Reglamento:*** Reglamento de la Ley de Compras, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios;

2.30 ***Secretaría de la Hacienda Pública:*** Dependencia gubernamental del Estado de Jalisco responsable de la gestión, supervisión y control de los recursos financieros, así como de garantizar el cumplimiento de las obligaciones fiscales y la administración eficiente del presupuesto público establecido en las bases de licitación;

2.31 ***Sobre Cerrado:*** Medio de presentación de las propuesta técnica/económica en un procedimiento de licitación pública, restringida o de invitación, en el cual los licitantes entregan la documentación requerida en sobre físico sellado, garantizando la confidencialidad e integridad de la información hasta el momento de su apertura;

2.32 ***Testigo social:*** la persona física o jurídica que participa con voz en los procedimientos de adquisiciones, contrataciones, arrendamientos y contratación de servicios y que emite un testimonio final de conformidad la ley;

2.33 ***Tracto Sucesivo:*** hace referencia a la continuidad en la cadena de transmisiones o actos jurídicos sobre un derecho o bien, garantizando que cada acto se derive legítimamente del anterior sujetándose a los montos establecidos previstos por el decreto de presupuesto de egresos del estado, los cuales podrán ser multianuales siempre y cuando garanticen las mejores condiciones en precios y servicios, hasta por el término de la administración correspondiente y en los términos de la legislación aplicable;

2.34 ***Tipo de contrato:*** La modalidad de abastecimiento: contrato abierto o contrato cerrado;

2.34.1 **Contrato abierto** es cuando se establecerá la cantidad máxima de los bienes, arrendamientos o servicios a contratar; o bien, el presupuesto máximo que podrá ejercerse. La cantidad o presupuesto mínimo no podrá ser inferior al cuarenta por ciento de la cantidad o presupuesto máximo;

2.34.2 **Contrato cerrado** es cuando la convocante establece una cantidad determinada de unidades a licitar;

2.35 ***Visita de campo:*** acto en el cual la dependencia o el licitante realizan una inspección del lugar del licitante donde se llevará a cabo con el fin de aclarar dudas y que los proveedores tengan la información necesaria para realizar una propuesta técnica y económica más adecuada.

3. Objetivo.

Establecer las bases y reglas bajo las cuales se llevará a cabo el proceso de licitación pública de la solicitud de aprovisionamiento establecida en la ***Portada*** de las presentes bases.

4. Etapas del proceso de licitación.

4.1 **Preguntas Junta Aclaratoria.** Cuando el Participante tenga dudas o requiera aclarar alguna cuestión referente

Fundamento Legal:
Art. 2, 59, 62, 64, 79, 83 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 2, 48, 49, 51, 63, 65, 66, 67, 68, 73, 184, 187 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

al contenido de las bases y/o sus anexos, podrá formular sus preguntas que podrán ser presentadas de manera presencial en las oficinas de la Dirección o bien de manera electrónica a los correos que se las presentes bases, cumpliendo con los siguientes requisitos:

4.1.1 Las preguntas deberán ser presentadas y formuladas bajo el formato Anexo 13 – Formato para preguntas de Junta Aclaratoria. Que deberá incluir:

a. Nombre del interesado.
b. Nombre del representante o apoderado.
c. Número de licitación pública.
d. Pregunta.
e. Declaración bajo protesta de decir verdad donde declara su intención de participar.
f. Firma.

4.1.2 Las preguntas deberán ser presentadas dentro del plazo establecido en el Calendario de las presentes bases.

4.1.3 Para su presentación digital será necesario enviar las preguntas vía correo electrónico en formato WORD docx. al correo que se muestra en la convocatoria y en el Calendario de las presentes Bases.

4.1.4 Para su presentación presencial deberá de ser en las oficinas de la dirección ubicada en Av. Fray Antonio Alcalde #1221, Colonia Miraflores, Guadalajara, Jalisco México. C.P. 44270.

4.2 **Junta Aclaratoria.** La junta aclaratoria es aquel acto que se realiza para resolver las preguntas de los Participantes.

4.2.1 La convocante deberá realizar al menos una Junta de Aclaratoria, cuya asistencia será opcional para los participantes la asistencia a la misma, salvo que en la convocatoria se disponga lo contrario.

4.2.2 En el acto de Junta de Aclaratoria, 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 plasmar las respuestas 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.

4.2.3 Con independencia de la asistencia de los interesados a las juntas de aclaraciones que se celebren, las determinaciones que en ellas se acuerden serán de observancia obligatoria para todos aquellos que presenten proposiciones, aún para aquellos que no hayan asistido a las juntas de aclaraciones. En el supuesto de que en la convocatoria se haya señalado como obligatoria la asistencia a las juntas de aclaraciones, el incumplimiento de este requisito será motivo suficiente para que no se tome en consideración la propuesta que llegue a presentar el interesado.

4.2.4 **Lugar, fecha y hora.** El acto de la junta aclaratoria se llevará a cabo en el día, lugar y hora previstos en el Calendario de las presentes bases, el cual será publicado en el SECG.

4.3 **Acto de presentación y apertura de proposiciones.** El acto de apertura es la junta donde se debe presentar las propuestas de los Participantes de acuerdo con los siguientes puntos:

4.3.1 **Presentación de la propuesta.** Se deberán entregar las propuestas en un sobre cerrado, cumpliendo con todos los requisitos establecidos a lo largo de las presentes bases, el día y a la hora establecidos en el calendario, para la celebración del **Acto de presentación y apertura de proposiciones**.

a. **Forma de presentación.** Los Participantes, deberán entregar sus propuestas, el día y la hora establecido en el calendario de las presentes bases.

I. **Propuesta Técnica:** Se deberá presentar dentro del sobre cerrado conforme a las disposiciones técnicas

Fundamento Legal:
Art. 47, 49, 64 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 59, 67, 68, 69 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

establecidas en el Anexo 1 de las presentes bases.

4.3.1.a.I.1 La propuesta técnica deberá ser elaborada por el participante en primera persona ofreciendo los bienes o servicios solicitados y garantizando el cumplimiento de los compromisos requisitados de acuerdo al anexo técnico. No será considerada como válida una propuesta técnica que sea copia textual del anexo técnico del cual no se pueda considerar el cumplimiento de lo antes establecido.

II. **Propuesta económica USB:** para las licitaciones públicas, preferentemente, se deberá agregar a su proposición impresa una USB con la propuesta económica en formato Excel y la propuesta técnica en formato PDF. Lo anterior sin exentar su presentación impresa. Ambos deberán estar dentro del sobre cerrado.

III. **Proposición impresa.** Presentar dentro del sobre cerrado un (1) juego de todos los documentos descritos en el **Anexo 3 – Índice de la Proposición,** en el apartado de proposición impresa, con las características establecidas a lo largo del punto 5.4

IV. Contenido. deberá contener todos los documentos solicitados en el **Anexo 3 – Índice de la Proposición.**

b. **Lugar, fecha y hora.** El Acto de presentación y apertura de proposiciones se llevará a cabo en el día, lugar y hora previstos en el **Calendario** de las presentes bases.

4.3.2 **Apertura del sobre.** Un Servidor Público adscrito a la Contraloría del Estado o del Órgano Interno de Control o en caso de comité un vocal, procederán a abrir cada uno de los sobres para revisar públicamente su contenido.

4.3.3 **Revisión documental.** Un servidor público Adscrito a la Dirección General de Abastecimientos (para procesos sin concurrencia del comité) o en su caso un Vocal del comité (para procesos con concurrencia del comité), procederá a la revisión del contenido de cada una de las proposiciones, haciéndose constar la documentación presentada, sin que ello implique la evaluación de su contenido. Para los procesos de concurrencia del comité A efecto de cumplimentar lo determinado en el artículo 65, numeral 1, fracción II de la Ley, durante este acto se llevará a cabo la revisión conjunta de las propuestas en su totalidad con los participantes que las presenten. De todo lo anterior quedará registro audiovisual en el desarrollo de la sesión, constando además documentalmente en el acta respectiva.

4.3.4 **Levantamiento de acta.** Se levantará acta que servirá de constancia de la celebración del acto de presentación y apertura de las proposiciones, en la que se hará constar la documentación presentada e importe económico de cada uno de los participantes.

4.4 **Fallo.** Para el conocimiento de todos los participantes, el resultado del fallo deberá ocurrir dentro de los veinte (20) días naturales siguientes a la celebración del acto de apertura de proposiciones. Dicho plazo podrá prorrogarse por un plazo excedente de 20 días naturales contados a partir del plazo establecido originalmente.

4.5 **Orden de compra.** Los participantes adjudicados, se obligan a recoger la orden de compra, en un plazo no mayor de diez días hábiles contados a partir de la fecha de la notificación del fallo, previa entrega de la garantía de cumplimiento; de lo contrario, se podrá cancelar la adjudicación y proceder a adjudicar conforme a la ley.

4.5.1 **Firma de contrato.** La firma del contrato se llevará a cabo en las oficinas de la Dirección General Jurídica de la Secretaría de Administración ubicado en Av. Fray Antonio Alcalde #1221, Colonia Miraflores, Guadalajara, Jalisco México. C.P. 44270, dentro de los diez días hábiles posteriores a la notificación del fallo en un horario de 09:00 a 15:00 horas.

4.5.2 El participante adjudicado o su representante que acuda a la firma del contrato deberá presentar original de identificación vigente con validez oficial, pudiendo ser cartilla del servicio militar nacional, pasaporte vigente, credencial de elector o cédula profesional.

Fundamento Legal:
Art. 59, 64, 65, Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 59, 69, 79 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

5. Requisitos.

El licitante deberá de cumplir con todos los requisitos establecidos a lo largo del presente capítulo, el cumplimiento de los requisitos le permitirá al licitante participar en la licitación mediante la evaluación técnica y económica de su propuesta. En caso de incumplimiento en alguno de los requisitos se desechará la propuesta del licitante de conformidad a la Ley.

5.1 **Requisitos de las Muestras (ÚNICAMENTE EN CASO DE SER NECESARIO):** únicamente en caso de que así lo solicite expresamente el Dependencia requirente en el **Anexo 1**, o en **Portada** de estas bases, el licitante deberá entregar muestras físicas del producto o productos con los que participa en la presente licitación pública.

5.1.1 **Entrega de muestras:** en caso de que así lo solicité el Dependencia requirente en el anexo técnico, el participante deberá integrar en su proposición el anexo 12 – Formato de entrega de muestras, sellado o firmado por el Servidor Público Adscrito. Al presentar las muestras el día y lugar que se indique en **Calendario**.

5.1.2 **Formato de entrega de muestras:** las muestras deberán ir acompañadas del **Anexo 12 – "Formato entrega de muestras"**.

5.1.3 **Plazo para recoger las muestras:** el participante cuenta con 10 días hábiles posteriores al fallo de la licitación, para recoger las muestras presentadas, de lo contrario la Dirección General de Abastecimientos no se hace responsable de las mismas, lo anterior a excepción del proveedor adjudicado.

5.2 **Requisitos de la Visita de Campo (ÚNICAMENTE EN CASO DE SER NECESARIO):** únicamente en caso de que así lo solicite expresamente la Dependencia requirente en el **Anexo 1**, o en **La portada** de las presentes bases.

5.2.1 **Sobre la visita de campo:** él o la participante deberá asistir a la fecha y hora determinada por la parte requirente en **Portada** de las presentes bases y/o en la Convocatoria.

5.2.2 **Evidencia de visita de campo:** el participante deberá integrar a su propuesta su constancia de visita de campo**.**

5.3 **Requisitos del registro.**

5.3.1 Previo al acto de presentación de proposiciones, se deberá efectuar el registro de participantes. No se podrá impedir el acceso a quién decida presentar su documentación y proposiciones en la fecha, hora y lugar establecido para la celebración del citado acto.

5.3.2 Previo al registro del acto de presentación y apertura de proposiciones, el participante deberá entregar el manifiesto de personalidad (Anexo 2) en donde declare bajo protesta de decir verdad que cuenta con las facultades suficientes para comprometerse por sí o por su representada, sin que resulte necesario acreditar su personalidad jurídica.

5.3.3 Además del manifiesto (Anexo 2), sí la propuesta es presentada por un tercero, éste deberá entregar carta poder simple en formato libre (anexo 15) otorgada por el representante legal, deberá acreditarse adjuntando copia simple de la identificación oficial vigente de los involucrados.

5.4 **Requisitos de la proposición o propuesta.**

5.4.1 **Listado de documentos obligatorios.** La Proposición deberá contener los documentos establecidos en el **Anexo 3 – Índice de la proposición**, los cuales son (El incumplimiento de cualquiera de estos requisitos pudiera determinar el desechamiento de la proposición):

a. Constancia de situación fiscal.
b. Opinión del cumplimiento de obligaciones fiscales en materia de seguridad social (Ante el IMSS).

Fundamento Legal:
Art. 47, 49, 69 párrafo 2 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 67, 68, 6, Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

c. Acuse de Obligaciones en Materia de Seguridad Social conforme al acuerdo emitido por el Consejo Técnico publicado en el diario oficial de la Federación el 22 de septiembre del 2022.
d. Constancia de Situación Fiscal en Materia de Aportaciones Patronales y Entero de Descuentos ante INFONAVIT
e. Opinión del cumplimiento de obligaciones fiscales (ante el Servicio de Administración Tributaria).
f. Copia de identificación oficial del licitante o en su caso los apoderados o representantes.
g. Propuesta Técnica (Deberá incluir todas las especificaciones, documentos de experiencia, certificaciones, contratos o demás requerimientos establecidos en el Anexo técnico) (Anexo 1).
h. Anexo 3 – Índice de la Proposición
i. Anexo 4 – Acreditación del Participante
j. Anexo 5 – Propuesta Económica
k. Anexo 6 – Declaraciones del Participante
l. Anexo 7 –Aportación 5 al Millar
m. Anexo 8 - Declaración de Estratificación
n. Anexo 9 – Listado de miembros y representantes.
o. Anexo 10 - Manifiesto de cumplimiento de obligaciones fiscales.
p. Anexo 11 - Manifiesto de cumplimiento obligaciones en materia de Seguridad Social
q. Anexo 12 – Muestras Físicas **(Cuando aplique).** Podrá integrarse a la proposición impresa, o en caso de que las muestras se entreguen el día del acto de presentación de propuestas, podrá presentarse en folder separado, lo anterior de acuerdo con el punto 5.1.1, 5.1.2 y 5.1.3
r. Constancia de Visita de Campo ***(Cuando aplique)*** ***Puedes descargar un formato de Constancia de Visita de Campo aquí***.

5.4.2 **Documentos públicos.** El participante deberá incluir los documentos públicos dentro de su proposición considerando las siguientes características:

a) ***Constancia de situación fiscal.***
i. Emitido por el SAT.
ii. Original.
iii. Con una antigüedad no mayor a 30 días naturales a la fecha del acto de presentación y apertura de proposiciones.

b) ***Opinión del cumplimiento de obligaciones fiscales en materia de seguridad social (Ante el IMSS).***
i. Emitido por el IMSS.
ii. En sentido positivo u opinión sin opinión
iii. Original.
iv. La opinión del cumplimiento de obligaciones fiscales en materia de seguridad social se considerará válida durante los plazos de quince días hábiles o de veinte días hábiles tratándose de contrataciones derivadas de procedimientos consolidados.
v. El documento deberá ser legible

c) ***Acuse de Obligaciones en Materia de Seguridad Social conforme al acuerdo emitido por el Consejo Técnico publicado*** **en el diario oficial de la Federación el 22 de septiembre del 2022.**
i. *El "PARTICIPANTE" deberá autorizar al IMSS a hacer público el resultado de la consulta de su opinión del cumplimiento de obligaciones fiscales en materia de seguridad social, según el siguiente procedimiento:*
1) *Ingresar al Buzón IMSS, por la página electrónica del Instituto (www.imss.gob.mx/buzonimss), a través del medio de autenticación correspondiente.*
2) *Del menú, seleccionar la opción "Cobranza".*
3) *Del menú, seleccionar la opción "32D Autorización de Opinión Pública" y después la opción "Autorizo hacer pública mi opinión del cumplimiento".*
4) *Dar clic en el botón "Guardar" y firmar mediante la e. firma.*
5) *El Buzón IMSS generará el acuse correspondiente, mismo que se deberá presentar dentro de la propuesta del participante, como parte del Anexo 11* manifiesto de cumplimiento obligaciones en materia de seguridad social.
ii. Emitido por el IMSS.
iii. En sentido positivo u opinión sin opinión
iv. Original.

Fundamento Legal:
Art. 59, 64, 65, 68, 72, 76 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 67, 68, 69, 79 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

v. El documento deberá ser legible

d) ***Constancia de Situación Fiscal en Materia de Aportaciones Patronales y Entero de Descuentos ante INFONAVIT:***

i. Emitido por el INFONAVIT.
ii. En sentido positivo u opinión sin opinión
iii. Original.
iv. Con una antigüedad no mayor a 30 días naturales a la fecha del acto de presentación y apertura de proposiciones.
v. El documento deberá ser legible

e) ***Opinión del cumplimiento de obligaciones fiscales (ante el Servicio de Administración Tributaria).***

i. Emitido por el SAT.
ii. En sentido positivo
iii. Original.
iv. Con una antigüedad no mayor a 30 días naturales a la fecha del acto de presentación y apertura de proposiciones.
v. El documento deberá ser legible

f) ***Identificación oficial del Licitante o en su caso Representante legal.***

i. Vigente.
ii. Presentar en copia.
iii. El documento deberá ser legible

5.4.3 **Aspectos de Forma de la proposición:** Los documentos descritos en el punto 5.4.1. deberán cumplir con los siguientes requisitos de forma.

a. **Hoja membretada:** la proposición, preferentemente, deberá estar impresa en hoja membretada, con la firma autógrafa del participante y/o su representante, con facultades suficientes, en todas sus hojas.
b. **Sobre cerrado:** la proposición deberá encontrarse dentro un (1) sobre cerrado y firmado por el participante y/o representante.
c. **Plazo de entrega:** La proposición deberá ser entregada dentro del día y la hora establecida en el calendario como "**Acto de Presentación y Apertura de Proposiciones**".
d. **Formato:** la proposición, preferentemente, deberá presentarse en hojas tamaño carta.
e. **Forma de entrega:** la proposición deberá integrar todos los documentos establecidos en el **anexo 3 – Índice de la Proposición** y la USB con el **Anexo 5 - Propuesta Económica** en formato Excel.
f. **Firma:** Todos los documentos que conforman la proposición deberán estar firmados por el participante y/o su representante, preferentemente en tinta azul.
g. **Idioma:** la propuesta, documentación, anexos, declaraciones y cartas, en general toda la proposición deberá ser presentada en español y/o con su debida traducción.
h. **Folio:** la proposición, preferentemente, deberá encontrarse foliadas la totalidad de sus páginas.

5.4.4 **Requisitos de Propuesta Técnica:**

a. **Contenido.**

I. **El nombre del bien o servicio** objeto de la licitación deberá coincidir exacto con lo solicitado por la Dependencia requirente.
II. **No. De Partida:** número de partida de acuerdo con el anexo 1.
III. **Cantidad:** número de piezas o servicios a proveer.
IV. **Descripción detallada:** descripción clara y detallada de las características específicas y características técnicas de los productos o servicios (contenido literal de la solicitud de aprovisionamiento establecida en **Anexo 1.**).

Fundamento Legal:
Art. 47, 49, 69 párrafo 2 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 67, 68, 6, Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

b. **Ficha técnica de los bienes y servicios** deberá presentar ficha técnica de los productos o servicios, incluyendo su marca, modelo, color, tamaño y demás características, garantía y tiempo de entrega ***(siempre y cuando se solicite en los requisitos técnicos del Anexo 1)***.

c. **Propuesta Técnica:** el participante deberá presentar la propuesta técnica de acuerdo con las especificaciones establecidas en el "Anexo 1" para ser evaluado de acuerdo con el mismo y cumplir las especificaciones técnicas mínimas necesarias.

Cuando se desprenda del Anexo Técnico la existencia de validaciones gráficas, el proveedor participante deberá adjuntar la hoja de validación donde se contienen las características de los productos gráficos a ofertar, así como las imágenes que se desprendan de dicha validación.La ausencia de éstos documentos será motivo de desechamiento técnico de la propuesta.

5.4.5 **Requisitos de propuesta económica:**

a. Deberá establecer el precio unitario del bien o servicio y el importe total desglosando el I.V.A.
b. **Tipo de cambio:** deberá ser elaborado en moneda nacional, es decir pesos mexicanos MXN.
c. **Impuestos:** deberá ser elaborada considerando las retenciones de impuestos correspondientes a cada participante conforme al régimen fiscal en el que esté tribute.
d. **Incluir todos los costos:** no se aceptarán aumentos en la cotización, por lo tanto, la misma debe de considerar todos los costos y gastos implicados.
e. **Entregar la propuesta económica de acuerdo** con las presentes bases y **al Anexo 5 – Propuesta Económica.**

5.4.6 **Anexos obligatorios para participar.** Cada uno de los siguientes documentos son obligatorios para la evaluación de la propuesta.

a. **Anexo 2 - Manifiesto de Personalidad** anexo donde el participante declara que cuenta con personalidad jurídica para llevar a cabo el acto. Anexo 2 – Manifiesto de Personalidad**. (necesario para el registro).** Este anexo se entrega de forma independiente a la proposición, al momento del registro en el acto de presentación y apertura de proposiciones, y no debe integrarse al sobre cerrado ni foliarse.
b. **Anexo 3 – Índice de la Proposición** listado de documentos necesarios para presentar una propuesta. Anexo 3 – Índice de la Proposición.
c. **Anexo 4 – Acreditación del Participante** anexo donde el participante declara la información necesaria para acreditar su personalidad**.** Anexo 4 – Acreditación del Participante.
d. **Anexo 5 – Propuesta Económica.** Para generar una propuesta económica, que cumpla con los requisitos establecidos en las presentes bases. Anexo 5 – Propuesta Económica.
e. **Anexo 6 – Declaraciones del Participante.** Anexo en el que el participante manifiesta su aceptación a las bases, declaración de tiempos, calidad y precio fijo de Dependencia requirente, declaración de no colusión, declaración de no conflicto de interés particular y casos del artículo 52 de la ley y su declaración del padrón de proveedores. Anexo 6 – Declaraciones del Participante.
f. **Anexo 7 – Aportación 5 al Millar** formato en el que el participante declara su intención de aportar o no hacerlo al fondo impulso Jalisco **-** Anexo 7 - Aportación 5 al Millar.
g. **Anexo 8 - Declaración de Estratificación** anexo donde el participante identifica su ubicación en la estratificación de empresas de acuerdo con el parámetro de la dirección. Anexo 8 – Declaración de Estratificación
h. **Anexo 9 – Listado de miembros y representantes.** Declaración del listado de miembros, socios y representante legal. Anexo 9 – Listado de miembros y representantes.
i. **Anexo 10 - Manifiesto de cumplimiento de obligaciones fiscales.** Manifiesto de parte de los participantes

Fundamento Legal:
Art. 47, 49, 52, 53, 69 párrafo 2 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 67, 68, 69 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

si se encuentran en algún supuesto del artículo 32-D del código Fiscal de la Federación. ANEXO 10.- Manifestación de Cumplimiento de Obligaciones Fiscales.

j. **Anexo 11 - Manifiesto de cumplimiento obligaciones en materia de Seguridad Social** La presentación de este documento es un requisito legal y administrativo que garantiza que el PARTICIPANTE (proveedor o contratista) cumple con sus obligaciones fiscales y de seguridad social. Anexo 11 - Manifiesto de cumplimiento obligaciones en materia de Seguridad Social

k. **Anexo 12 – Formato de Muestras** formato de registro de entrega de muestras físicas ***(Cuando aplique)***. Anexo 12 Formato de Muestras Físicas.

5.4.7 **Anexos de apoyo:** documentos que no son obligatorios para presentar la propuesta, pero ayudan a ciertos puntos específicos de las bases.

a. **Anexo 13 – Formato de Preguntas Junta Aclaratoria** formato bajo el cual el participante deberá establecer sus preguntas, para ser resueltas en la junta aclaratoria. Anexo 13 - Formato de Pregunta Aclaratoria o llenando el formato.

b. **Anexo 14 – Texto Para Fianza** formato en el que se establece las características que debe contener el contrato de fianza presentado para la firma del contrato. Anexo 14 – Texto para fianza

c. **Anexo 14 A – Texto de la fianza de anticipo** formato en el que se establece las características que debe contener el contrato de fianza presentado para la firma del contrato. Anexo 14 A – Texto de la fianza de anticipo

d. **Anexo 15 – Poder** formato de ejemplo de un poder para la presentación de propuestas por medio de un apoderado. Anexo 15 – Poder. **(En caso de ser necesario)** Este anexo se entrega de forma independiente a la proposición, al momento del registro en el acto de presentación y apertura de proposiciones, y no debe integrarse al sobre cerrado ni foliarse.

5.5 Los tiempos de entrega que se establezcan en la propuesta técnica y/o económica de los participantes deberán de considerarse a partir del día hábil siguiente de aquel en que se realice la notificación del fallo, manifestando que cualquier contravención a dicha premisa podrá ser motivo de la disminución del porcentaje de calificación y/o un objeto a considerar en los criterios de evaluación entre puntos y porcentajes o costo Beneficio.

5.6 Participaciones conjuntas: 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.

5.7 En este supuesto la proposición deberá ser firmada por el representante común que para ese acto haya sido designado por el grupo de personas.

5.8 Cuando la proposición conjunta resulte adjudicada con un contrato, dicho instrumento deberá ser firmado por el representante legal de cada una de las personas participantes en la proposición, a quienes se considerará, para efectos del procedimiento y del contrato, como responsables solidarios o mancomunados, según se establezca en el propio contrato.

5.9 Lo anterior, sin perjuicio de que las personas que integran la proposición conjunta puedan constituirse en una nueva sociedad, para dar cumplimiento a las obligaciones previstas en el convenio de proposición conjunta, siempre y cuando se mantengan en la nueva sociedad las responsabilidades de dicho convenio.

6. Condiciones generales.

6.1 **Criterios de desechamiento.** Aquel participante que incumpla cualquiera de los siguientes criterios podrá ser motivo para desechamiento.

6.1.1 La Dirección o en su caso el comité, podrá desechar las propuestas de los Participantes que incurran en una o

Fundamento Legal: Art. 38 49, 52, 58, 59, 65, 66, 67,68, 71, 78 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 69, 97 Fr. III y IV, 73, 183, 189 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

varias de las siguientes situaciones:

6.1.2 Cuando alguno o algunos de los participantes se encuentren en alguno de los casos previstos por el Artículo 52 de la Ley.

6.1.3 Encontrarse en alguno de los requisitos establecidos en el artículo 32-D del Código Fiscal de la Federación.

6.1.4 Cuando algún Participante se encuentre incumpliendo con otro contrato u orden de compra con el poder ejecutivo del estado de Jalisco.

6.1.5 Si se comprueba que el participante incumplió con entregas, servicios o garantías en el Estado de Jalisco o en otras entidades públicas de los 3 niveles de Gobierno.

6.1.6 Si incumple con los requisitos especificados en las presentes bases, sus anexos y lo derivado de la Junta Aclaratoria, de conformidad a los lineamientos establecidos en el artículo 66 de la Ley.

6.1.7 Si un mismo socio o administrador pertenece a dos o más de las empresas participantes.

6.1.8 Si se comprueba que ha acordado con otro u otros participantes elevar el costo de los trabajos, o cualquier otro acuerdo que tenga como fin obtener una ventaja sobre los demás.

6.1.9 Si presentan datos falsos en la documentación solicitada en estas bases o en la propuesta económica.

6.1.10 Cuando al Participante se le hubieren rescindido dos o más contratos con alguna entidad o dependencia de los tres niveles de Gobierno por causas imputables al proveedor.

6.1.11 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.

6.1.12 De conformidad con la fracción XVI del artículo 59 de la Ley, cuando el participante sea omiso en incluir en su propuesta la declaración por escrito en la que haga constar su postura para la aportación de su aportación de cinco al millar del monto total del contrato adjudicado (antes del IVA), para ser aportado al Fondo Impulso Jalisco.

6.2 **Criterios de adjudicación.**

6.2.1 Se verificará que las proposiciones cumplan con los requisitos solicitados en las presentes bases, quedando a cargo de la Dependencia requirente, la evaluación de los aspectos técnicos.

6.2.2 Sólo debe adjudicarse a quien cumpla los requisitos establecidos en las presentes bases y sus anexos.

6.2.3 De conformidad con lo establecido en el artículo 59, fracción XII de la Ley y 55 del Reglamento, la evaluación de las proposiciones será conforme a lo estipulado en la portada de las presentes bases respecto a los criterios de evaluación.

6.3 **Criterios de evaluación** Se adjudicará al participante cuya oferta resulte solvente y cumpla con los requisitos legales, técnicos y económicos establecidos en estas bases y sus anexos, y, por tanto, garantice el cumplimiento de las obligaciones respectivas, considerando para tal efecto los criterios de evaluación del anexo 1.

6.3.1 La Dirección se reserva la plena facultad para emitir su fallo de adjudicación.

6.3.2 En los casos que aplique el comité se reserva la plena facultad para aprobar el fallo de adjudicación.

6.3.3 Si derivado de la evaluación de las proposiciones y previa consideración de los criterios de preferencia se obtuviera un empate entre dos o más participantes en una misma o más partidas, se establecerá el desempate en conformidad con el establecido en la Ley.

6.3.4 En caso de subsistir el empate entre participantes de la misma estratificación de los sectores señalados en el párrafo anterior, o bien, de no haber empresas de este sector y el empate se diera entre participantes que no tienen el carácter de micro, pequeñas o medianas empresas, se realizará la adjudicación del contrato a favor del participante que resulte ganador del sorteo por insaculación que realice la dirección, el cual consistirá en depositar en una urna o recipiente transparente, las boletas con el nombre de cada participante empatado, acto seguido se extraerá en primer lugar la boleta del participante ganador y posteriormente las demás boletas de los participantes que resultaron empatados en esa partida, con lo cual se determinarán los subsecuentes lugares que

Fundamento Legal:
Art. 47, 59 62, 63, 64, 65, 69, 72, 75, 79, 83 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 21, 48, 49, 51, 63, 65, 66, 67, 68, 73, 183, 184, 185 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

ocuparán tales proposiciones.

6.3.5 Si hubiera más partidas empatadas se llevará a cabo un sorteo por cada una de ellas, hasta concluir con la última que estuviera en ese caso. Cuando se requiera llevar a cabo el sorteo por insaculación, la Dirección deberá girar invitación al órgano de control y al testigo social cuando éste participe en la licitación pública, para que en su presencia se lleve a cabo el sorteo; se levantará acta que firmarán los asistentes, sin que la inasistencia, la negativa o falta de firma en el acta respectiva de los participantes o invitados invalide el acto.

6.3.6 Son principios rectores de adjudicación, los de eficiencia, eficacia, economía, imparcialidad, transparencia y honradez a que alude el primer párrafo del artículo 134 de la Constitución Política de los Estados Unidos Mexicanos; los de economía, legalidad, racionalidad, austeridad, control y rendición de cuentas que se mencionan en el artículo 1 numeral 4 de la Ley y el artículo 1 numeral 3 del Reglamento.

6.4 **Métodos de evaluación.** Revisa el **Anexo 1**, ahí encontrarás los criterios de evaluación. En dicho anexo pudiera establecerse alguno de los siguientes métodos de evaluación:

I. **Puntos y porcentajes.** En este método de evaluación el evaluador considera una rúbrica en la que se establecen puntos o porcentajes por cada uno de los rubros de evaluación.

II. **Costo Beneficio.** Cuando existan más de dos Participantes se evaluará de acuerdo con la que cuente con el precio más bajo y mejore la oferta, siempre y cuando sea un Participante solvente para llevar a cabo el proceso de compra.

III. **Binario.** El cual solo se adjudica al que cumpla con los requisitos y oferte el precio más bajo. Este solo se utilizará cuando no se pueda utilizar ninguno de los anteriores.

6.5 **Declaración de licitación desierta.**

a. Se procederá a declarar desierta una licitación, o determinadas partidas de ésta, cuando ninguna de las proposiciones presentadas reúna los requisitos solicitados o cuando la propuesta más económica que cumpla con todos los requerimientos técnicos solicitados en la convocatoria, resulte superior en un 10% o inferior en un 40% respecto de la media de precios que arroje la investigación de mercado.

b. Cuando ningún participante se hubiese registrado o ninguna proposición sea presentada en el acto de presentación y apertura de propuestas técnicas.

c. Cuando se declare desierta una licitación o alguna partida y persista la necesidad de contratar con el carácter y requisitos solicitados en la primera licitación, el ente podrá emitir una segunda convocatoria, o bien optar por la adjudicación directa, en los términos establecidos por la ley.

6.6 **Sobre el fallo** Se desechará una proposición, cuando no cumpla con los requisitos señalados en la convocatoria; y para el caso de que determinadas partidas de la proposición presentada no cumplan con dichos requisitos, ésta se desechará de forma parcial únicamente por lo que ve a las partidas en que se incumple. Invariablemente, en el fallo deberán exponerse y fundarse las razones que motivan la determinación que se tome.

6.7 El contenido, alcance, especificaciones técnicas y cualquier otra información detallada en el Anexo Técnico de estas bases, es responsabilidad exclusiva del Área Requirente, así como del área que valide técnicamente dicho anexo.

7. Restricciones para participar.

7.1 No podrán participar aquellas empresas o personas que de contratar pudiera existir conflicto de interés.

7.1.1 No podrán participar aquellos Participantes que no cumplan con las declaraciones de no colusión ni conflicto de

Fundamento Legal:
Art., 52 49 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 40, 45, 46, 48, 56, 60 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

interés, descritas en el **Anexo 6 – Declaración del Participante.**

7.1.2 No podrán participar aquellos participantes que no entreguen los documentos y anexos obligatorios.

7.2 No podrán participar aquellos participantes que no cumplan con los requisitos establecidos en el capítulo 5.

7.3 No podrán participar aquellos participantes que se encuentren en alguno de los supuestos establecidos en el artículo 52 de la Ley.

8. Restricciones para firmar contrato.

El licitante adjudicado deberá cumplir con los siguientes requisitos para poder firmar el contrato y obtener la orden de pago.

8.1 **Garantía:** los participantes adjudicados deberán constituir una garantía para el cumplimiento de su orden de compra o contrato, en moneda nacional, por el importe del 10% (diez por ciento) del monto total adjudicado en el fallo, I.V.A incluido, esta garantía podrá ser mediante:

8.1.1 **Fianza** expedida por afianzadora nacional en favor de la Secretaría de la Hacienda Pública.

a. Las personas físicas o jurídicas a quienes se les haya adjudicado contrato para suministrar bienes o servicios deberán garantizar, cuando se les requiera, la correcta aplicación de los anticipos, con la exhibición de póliza de fianza que garantice el monto total de éstos.

8.1.2 **Cheque certificado o de caja** emitido en favor de la Secretaría de la hacienda pública.

8.1.3 La garantía deberá entregarse en las oficinas de la Dirección General de Abastecimientos del Estado de Jalisco, previo a la firma del contrato, dichas oficinas se encuentran ubicadas en la calle de Secretaria de Administración ubicado en Av. Fray Antonio Alcalde #1221, Colonia Miraflores, Guadalajara, Jalisco México. C.P. 44270

8.1.4 La garantía será cancelada o devuelta según sea el caso, una vez cumplidos los compromisos contraídos por el participante adjudicado.

8.2 **Anticipos:**

8.2.1 El proveedor adjudicado tendrá un plazo máximo de 60 días naturales contados a partir de la firma del contrato.

8.2.2 Deberán constituir una garantía equivalente al 100% del o de los anticipos cuando así lo hayan solicitado en su propuesta económica, sin que éste exceda del 50% (cincuenta por ciento) del monto total de la orden de compra o contrato, I.V.A. incluido, a través de los medios antes señalados.

8.3 **Registro en el padrón de Proveedores.**

8.3.1 **Registro al padrón:** El Participante deberá estar registrado y activo ante el Padrón de Proveedores en caso de ganar la licitación.

a. **Evidencia de registro:** El Participante que se encuentre debidamente registrado y activo deberá presentar en su propuesta copia simple de su constancia de inscripción en el Padrón de proveedores.

8.3.2 El participante deberá agregar a su propuesta el **Anexo 6** – Declaración del participante. En la que comparte su número de registro o en su defecto se compromete a registrarse ante el padrón de participantes en caso de ganar la licitación.

8.3.3 **Plazo para registrarte en el padrón**: al caso que se refiere el inciso anterior, de ser ganador de la licitación el participante tendrá 5 días hábiles para realizar el trámite correspondiente para el registro o actualización al Padrón de Proveedores ante la Dirección.

Fundamento Legal:
Art., 52 49 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 40, 45, 46, 48, 56, 60 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

9. Pago al Licitante adjudicado.

9.1 El pago se efectuará una vez que sea realizada la entrega parcial y/o total de los bienes/servicios conforme a lo establecido en las presentes "bases", y dentro de los 30 días naturales posteriores a la recepción de la documentación correspondiente, en la "dependencia requirente", de conformidad con los lineamientos de la Secretaría de la Hacienda Pública y/o "dependencia requirente":

9.1.1 **Documentos para pago de anticipo (cuando aplique)**

a. Original y copia del comprobante fiscal respectivo expedido a favor de la Secretaría de la Hacienda Pública, cuyo domicilio es en la calle Pedro Moreno No. 281, Guadalajara Centro, Guadalajara, Jalisco, C.P. 44100, y su R.F.C. es SPC130227L99, validado por la Dirección de Almacenes.
b. Impresión de la verificación del CFDI de la página del Servicio de Administración Tributaria.
c. Copia del Acta de "resolución" o "fallo"
d. Original del "contrato"
e. Original de la póliza de fianza de anticipo a la que se hace referencia en el numeral 8 de la presente "bases", expedida por una institución mexicana legalmente autorizada a nombre de la Secretaría de la Hacienda Pública, con domicilio en la calle Pedro Moreno No. 281, Colonia Centro, en el municipio de Guadalajara, Jalisco, C.P. 44100, R.F.C. SPC130227L99, en caso de corresponder
f. Copia de la Declaración de aportación del 5 al millar para el Fondo Impulso Jalisco (Anexo 7 de las "bases") en la cual el "proveedor" declara su voluntad de sí o no realizar la retención del 5 al millar del monto total del contrato antes del I.V.A., para su entero al Fondo Impulso Jalisco.

9.1.2 **Documentos para pago parcial o total.**

a. Original del CFDI y XML, a nombre de la Secretaría de la Hacienda Pública, con domicilio en la calle Pedro Moreno No. 281, Colonia Centro, en el municipio de Guadalajara, Jalisco, C.P. 44100, R.F.C. SPC130227L99, validada por la Dependencia y/o Entidad Requirente.
b. Impresión de la verificación del CFDI de la página del Servicio de Administración Tributaria.
c. Copia del Acta de "resolución" o "fallo (solo se requiere para el primer trámite de pago)".
d. 1 copia del "contrato (solo se requiere para el primer trámite de pago)"
e. 1 copia de la garantía de cumplimiento de contrato a nombre de la Secretaría de la Hacienda Pública, con domicilio en la calle Pedro Moreno No. 281, Colonia Centro, en el municipio de Guadalajara, Jalisco, C.P. 44100, R.F.C. SPC130227L99, en caso de corresponder a la que hará referencia el contrato que en su momento suscriba(n) el o los proveedores participantes adjudicados (solo se requiere para el primer trámite de pago).
f. Copia de la Declaración de aportación del 5 al millar para el Fondo Impulso Jalisco (Anexo 7 de las "BASES") en la cual el "proveedor" declara su voluntad de sí o no realizar la retención del 5 al millar del monto total del contrato antes del IVA, para su entero al Fondo Impulso Jalisco. (solo se requiere para el primer trámite de pago).
g. Solicitud de pago emitida a través del Sistema Integral de Información Financiera señalando la(s) clave(s) presupuestal(es) y fuente(s) de financiamiento con la(s) que se solventará el pago del parcial o total
h. Oficio de entera satisfacción.

9.2 El pago se realizará mediante transferencia bancaria electrónica en moneda nacional, conforme se realice cada entrega y en caso de haberse otorgado anticipos haciendo la amortización de este en cada pago y de acuerdo con el plazo estipulado en la propuesta y una vez que se entregue la documentación correspondiente en las oficinas de la Secretaría de la Hacienda Pública del Estado de Jalisco ubicada en la Calle Pedro Moreno 281, Zona Centro, 44100 Guadalajara, Jal.

Fundamento Legal:
Art.24,31, 59, 69, 71, 90 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 36, 44, 59, 61, 84, 88, 89, 107 de Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

10. Patentes, marcas y derechos de autor

10.1 El (los) proveedor (es) adjudicado (s), asumirá (n) la responsabilidad total para el caso de que, al suministrar sus bienes y/o servicios, se infrinjan derechos sobre patentes, marcas o derechos de autor, liberando al Poder Ejecutivo del Estado de Jalisco de toda responsabilidad civil, penal, fiscal o de cualquier índole, obligándose a salir en su defensa si por cualquier motivo, llegase a ser reclamado por éstos y además, a pagar, sin derecho a réplica contra él, cualquier cantidad o prestación que deba ser pagada por dicho motivo, de conformidad con la leyes respectivas, como la Ley de la Propiedad Industrial y la Ley Federal del Derecho de Autor, u otras aplicables.

11. Protección de Datos Personales y Confidencialidad.

11.1 En todas aquellas licitaciones cuyo objeto (bienes o servicios) implique el uso, tratamiento, indexación, almacenamiento o procesamiento de datos personales y/o datos personales sensibles (incluyendo datos biométricos o faciales), el proveedor adjudicado se obliga a garantizar la confidencialidad, integridad y disponibilidad de la información.

11.2 Aceptación de la obligación: Con la sola presentación de su propuesta y la firma de la "Declaración de aceptación de bases" contenida en el Anexo 6, el licitante manifiesta su plena conformidad y se obliga a que, en caso de resultar adjudicado, implementará y mantendrá las medidas de seguridad técnicas, físicas y administrativas necesarias para la protección de dichos datos.

11.3 El proveedor adjudicado deberá informar periódicamente a la Dependencia Requirente acerca de las medidas de seguridad adoptadas. A falta de disposición expresa en el Anexo Técnico sobre la periodicidad de estos informes, el proveedor deberá entregarlos de manera trimestral durante la vigencia del contrato o licenciamiento.

11.4 En caso de que el proveedor adjudicado aplique la subcontratación de servicios de cómputo en la nube para el almacenamiento o procesamiento de la información, asume la obligación ineludible de cumplir irrestrictamente con todas las estipulaciones previstas en el artículo 69 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

11.5 Todo lo anterior tiene como finalidad fortalecer el seguimiento y protección irrestricta de los datos personales, en estricto apego y términos de lo dispuesto por los artículos 29, 64, 65, 67 y 69 de la Ley antes mencionada.

12. Facultades del comité de adquisiciones

12.1 El Comité tendrá respecto de esta licitación, además de aquellas que el Reglamento y la Ley le confieren, las siguientes:

12.1.1 Aprobar adendas a contratos;

12.1.2 Conocer las bases que expida la Dirección para los procedimientos de adquisiciones de bienes o contratación de servicios y presentar las observaciones que considere pertinentes;

Fundamento Legal:
Art., 52 49 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 40, 45, 46, 48, 56, 60 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

12.1.3 Participar en las licitaciones públicas, presentación y apertura de propuestas, y fallo;

12.1.4 Resolver sobre las propuestas presentadas por los Participantes en procedimientos de adquisiciones de bienes o contratación de servicios, con la finalidad de obtener las mejores condiciones de calidad, servicio, precio, pago y tiempo de entrega ofertadas por los proveedores;

12.1.5 Analizar la pertinencia de la justificación del caso fortuito o fuerza mayor cuando sea necesario;

12.1.6 Proponer las bases sobre las cuales habrá de convocarse a procedimiento de adquisiciones de bienes o contratación de servicios para la adquisición de bienes o contratación de servicios, de bienes y servicios;

12.1.7 Dictaminar los proyectos de políticas, bases y lineamientos en materia de adquisiciones, contrataciones, arrendamientos y servicios que le presenten, así como someterlas a la consideración del titular del ente público o de su órgano de gobierno; en su caso, autorizar los supuestos no previstos en las mismas;

12.1.8 Opinar sobre las dudas y controversias que surjan en la aplicación de la Ley y las disposiciones que de ella deriven;

12.1.9 Suspender las sesiones y acordar fecha, hora y condiciones para reanudarlas, en caso de que, por la complejidad del objeto del procedimiento correspondiente, así se haga necesario;

12.1.10 Decidir lo conducente respecto de las situaciones extraordinarias que se presenten en el ejercicio de sus funciones, observando siempre los principios de economía, eficacia, transparencia, imparcialidad, y honradez;

12.1.11 Las demás que sean conferidas por las disposiciones secundarias.

13. Penas convencionales.

13.1.1 Las penas convencionales a cargo del proveedor por incumplimiento en los pedidos o contratos, podrán fluctuar entre el 3% y el 10% del precio pactado, dependiendo del bien o servicio objeto del contrato. Las citadas penas podrán pactarse por incumplimientos en los tiempos convenidos, número de bienes entregados, o por la posible afectación total o parcial de lo contractualmente establecido.

13.1.2 Estas penas se harán efectivas con independencia de que se exija el pago de daños y perjuicios que el incumplimiento haya ocasionado.

14. Sanciones.

14.1 Se podrá cancelar la orden de compra o el contrato y podrá hacerse efectivo el documento de garantía de cumplimiento en los siguientes casos:

14.1.1 Cuando el proveedor adjudicado no cumpla con alguna de las obligaciones estipuladas en la orden de compra o contrato.

14.1.2 Estar suspendido o dado de baja del padrón de proveedores del Gobierno del estado de Jalisco.

14.1.3 En caso de entregar bienes con especificaciones diferentes a las ofertadas, la Dependencia requirente considerará estas variaciones como un acto doloso y será razón suficiente para exigir la aplicación de la garantía del 10% y la cancelación total de la orden de compra o contrato, aun cuando el incumplimiento sea parcial e independientemente de los procesos legales que se originen.

14.1.4 En caso de que el participante ganador, injustificadamente y por causas imputables al mismo incumpliere con sus obligaciones será sancionado conforme a lo señalado en el Título Tercero denominado Procedimientos de Compra, de Enajenación de Bienes y de Contratación de Servicios, en su Capítulo VII denominado SANCIONES de la Ley.

14.1.5 No iniciar o iniciar de forma no oportuna sus obligaciones.

14.1.6 No desarrollar conforme a las bases, orden de compra o contrato, sus anexos y demás documentos relacionados con el procedimiento de adquisiciones de bienes o contratación de servicios de que se trate, las obligaciones a las cuales se comprometió.

14.1.7 Resultar falsas, con o sin intención de falsear la verdad, las declaraciones que haga en cualquier etapa del procedimiento de adquisiciones de bienes o contratación de servicios o las presentes bases, sobremanera, aquellas que tengan que ver con sus facultades y capacidades legales o las de sus representantes, que impidan o

Fundamento Legal:
Art. 17, 58 59, 65, 66, 67, 68, 69, 72, 84 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 40, 45, 46, 48, 56, 60 del Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

limiten su aptitud para obligarse o que por cualquier motivo y en cualquier medida, impidan la celebración o ejecución del mismo.

14.1.8 Resultar falsas, con o sin intención de falsear la verdad legal, sus declaraciones en torno a su personalidad jurídica.

14.1.9 Resultar con o sin declaración de por medio, no apto, por cualquier motivo, para llevar a cabo el presente contrato, en su formulación o cumplimiento.

14.1.10 Proveer su producto o servicio, en menor cantidad a la ofrecida.

14.1.11 Proveer su producto o servicio, en menor calidad a la ofrecida.

14.1.12 Incrementar, por cualquier motivo, el precio establecido en su cotización, sin las condiciones legales requeridas para ello.

14.1.13 No presentar la garantía establecida.

14.1.14 Las demás consideradas a lo largo de este documento.

14.1.15 Las demás que las legislaciones aplicables contemplen.

14.2 La contraloría será competente de sustanciar y resolver los procedimientos que se instauren contra de los particulares que infrinjan las disposiciones previstas en la ley.

15. Inconformidades.

15.1 **Inconformidad**, de acuerdo lo establece el artículo 59 en su fracción XIII El Participante podrá presentar el recurso de inconformidad en contra de los actos de la licitación, solicitar el proceso de conciliación ante cualquier diferencia derivada del cumplimiento de los contratos o pedidos y presentar quejas o denuncias;

15.2 **Lugar:** Las inconformidades se presentan ante la Contraloría del Estado de Jalisco Av. Vallarta No. 1252, esq. Atenas Col. Americana C.P. 44160 Guadalajara, Jalisco. También se pueden presentar en el Órgano interno de control de la Secretaría de Administración ubicado en Av. Fray Antonio Alcalde 1221, Miraflores, 44266 Guadalajara, Jalisco.

16. Relaciones laborales:

16.1 De resultar adjudicado el participante, desde que comience cualquier actividad encaminada al cumplimiento de sus obligaciones como proveedor, será el único responsable de la relación laboral, civil, administrativa, de seguridad social o cualquier otra que exista entre él y su personal, empleados o terceros de quienes se auxilie o sirva para abastecer su producto o servicio, sin que bajo ninguna circunstancia y en ningún caso, se considera al Estado de Jalisco, patrón sustituto, responsable o solidario de dichas relaciones, siendo aquél, el responsable de los actos u omisiones imputables a sus representantes, factores, dependientes o colaboradores en general.

17. Prórrogas

17.1 Si en cualquier momento en el curso de la ejecución de la orden de compra o del contrato, el proveedor se encontrara en una situación que impidiera la oportuna entrega de los bienes por caso fortuito o de fuerza mayor plenamente justificado, éste deberá notificar de inmediato a la Dirección General de Abastecimientos por escrito, dentro de la vigencia del plazo de entrega pactado en la orden de compra o contrato y mínimo 5 días hábiles anteriores al vencimiento de dicho término, justificando las causas de la demora y su duración probable, solicitando en su caso prórroga para su regularización. La Dirección o en caso de procesos con concurrencia, El Comité, procederá a analizar la solicitud de prórroga para determinar si es procedente.

Fundamento Legal:
Art. 16, 17, 71, 80, 84, 86 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 25, 67, 71, 74, 75, 76 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

18. Cesión de derechos:

18.1 De acuerdo con el numeral 54 de la Ley, los derechos y obligaciones que nazcan del proceso en desarrollo serán intransferibles; sin embargo, habrá lugar a subcontratación, cuando quienes deseen usar esta modalidad lo incluyan en la propuesta original y presenten una justificación por escrito en la que fundamenten la imposibilidad de solventar una propuesta sin realizarla y siempre y cuando el Estado de Jalisco así lo consienta expresamente y por escrito.

18.2 Para efectos de las presentes bases, no se considerará subcontratación la adquisición de bienes o contratación de servicios u obtención de los bienes respaldados por parte del participante con fabricantes, distribuidores y/o terceros proveedores.

18.3 El licitante que resulte adjudicado podrá ceder los derechos de cobro del contrato siempre y cuando se cuente con la aceptación expresa por parte del Gobierno del estado.

19. Suspensión y Cancelación.

19.1 El Comité o en su caso la dirección podrá cancelar o suspender bajo las siguientes condiciones:

A. podrá suspender el procedimiento de adquisiciones de bienes o contratación de servicios cuando:
   I. se compruebe que existe arreglo entre los participantes para elevar los precios de las compras objeto de la licitación.
   II. Por orden escrita debidamente fundada y motivada de autoridad.
   III. Si los precios ofertados por los participantes son superiores a los del mercado.
   IV. Por razones de interés del Gobierno del estado.

   En caso que el comité o la dirección así lo decida por los casos anteriores y de no resolver o solventar las condiciones establecidas en la ley se podrá proceder a cancelar.

B. El comité o en su caso la dirección podrá cancelar el presente procedimiento en los siguientes casos:
   I. Si se justifica que ya no se requiere del bien o servicio.
   II. En caso fortuito o fuerza mayor.
   III. Por orden escrita debidamente fundada y motivada de autoridad.
   IV. Por razones de interés del Gobierno del estado.

19.2 Se podrá cancelar una licitación o determinadas partidas de ésta, cuando se extinga la necesidad de adquirir los bienes o servicios correspondientes, o cuando se detecte que, de continuar con el procedimiento, puedan ocasionarse daños o perjuicios a la Convocante, a la Dependencia requirente y/o terceros. El uso de la figura de cancelación será responsabilidad de quien la solicita, podrá llevarse a cabo hasta antes de la firma del contrato, y sus efectos serán que no se adquieran los bienes o servicios correspondientes.

19.3 En caso de que el presente procedimiento sea suspendido o cancelado se notificará a todos los participantes.

20. Anexos.

a. **Anexo 1 – Anexo técnico** Documento técnico que deberá incluir todas las especificaciones, documentos de experiencia, certificaciones, contratos o demás requerimientos de la Licitación.

b. **Anexo 2 - Manifiesto de Personalidad** anexo donde el participante declara que cuenta con personalidad jurídica para llevar a cabo el acto. Anexo 2 – Manifiesto de Personalidad**. (necesario para el registro).** Este anexo se entrega de forma independiente a la proposición, al momento del registro en el acto de presentación y apertura de proposiciones, y no debe integrarse al sobre cerrado ni foliarse.

c. **Anexo 3 – Índice de la Proposición** listado de documentos necesarios para presentar una propuesta. Anexo 3 – Índice de la Proposición.

d. **Anexo 4 – Acreditación del Participante** anexo donde el participante declara la información necesaria para acreditar su personalidad**.** Anexo 4 – Acreditación del Participante.

e. **Anexo 5 – Propuesta Económica.** Para generar una propuesta económica, que cumpla con los requisitos establecidos en las presentes bases. Anexo 5 – Propuesta Económica.

Fundamento Legal:
Art. 16, 17, 80, 84, 86 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 25, 67, 71, 75 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

f. **Anexo 6 – Declaraciones del Participante.** Anexo en el que el participante manifiesta su aceptación a las bases, declaración de tiempos, calidad y precio fijo de Dependencia requirente, declaración de no colusión, declaración de no conflicto de interés particular y casos del artículo 52 de la ley y su declaración del padrón de proveedores. Anexo 6 – Declaraciones del Participante.

g. **Anexo 7 – Aportación 5 al Millar** formato en el que el participante declara su intención de aportar o no hacerlo al fondo impulso Jalisco **-** Anexo 7 - Aportación 5 al Millar.

h. **Anexo 8 - Declaración de Estratificación** anexo donde el participante identifica su ubicación en la estratificación de empresas de acuerdo con el parámetro de la dirección. Anexo 8 – Declaración de Estratificación

i. **Anexo 9 – Listado de miembros y representantes**. Declaración del listado de miembros, socios y representante legal. Anexo 9 – Listado de miembros y representantes.

j. **Anexo 10 - Manifiesto de cumplimiento de obligaciones fiscales.** Manifiesto de parte de los participantes si se encuentran en algún supuesto del artículo 32-D del código Fiscal de la Federación. ANEXO 10.- Manifestación de Cumplimiento de Obligaciones Fiscales.

k. **Anexo 11 - Manifiesto de cumplimiento obligaciones en materia de Seguridad Social** La presentación de este documento es un requisito legal y administrativo que garantiza que el PARTICIPANTE (proveedor o contratista) cumple con sus obligaciones fiscales y de seguridad social. Anexo 11 - Manifiesto de cumplimiento obligaciones en materia de Seguridad Social

l. **Anexo 12 – Formato de Muestras** formato de registro de entrega de muestras físicas ***(Cuando aplique)***. Anexo 12 Formato de Muestras Físicas.

m. **Anexo 13 – Formato de Preguntas Junta Aclaratoria** formato bajo el cual el participante deberá establecer sus preguntas, para ser resueltas en la junta aclaratoria. Anexo 13 - Formato de Pregunta Aclaratoria o llenando el formato.

n. **Anexo 14 – Texto Para Fianza** formato en el que se establece las características que debe contener el contrato de fianza presentado para la firma del contrato. Anexo 14 – Texto para fianza

o. **Anexo 14 A – Texto de la fianza de anticipo** formato en el que se establece las características que debe contener el contrato de fianza presentado para la firma del contrato. Anexo 14 A – Texto de la fianza de anticipo

p. **Anexo 15 – Poder** formato de ejemplo de un poder para la presentación de propuestas por medio de un apoderado. Anexo 15 – Poder. **(En caso de ser necesario)** Este anexo se entrega de forma independiente a la proposición, al momento del registro en el acto de presentación y apertura de proposiciones, y no debe integrarse al sobre cerrado ni foliarse.

Fundamento Legal:
Art. 16, 17, 80, 84, 86 Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.
Art. 25, 67, 71, 75 Reglamento de la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

ANEXO 1 (TECNICO)

PROYECTO TIC

N° o Clave de proyecto: **SECADMON/2026/11**

1. GLOSARIO:

Siglas o palabra	Significado
DIC	*Dirección de Infraestructura y Comunicaciones*
GEJ	*Gobierno del Estado de Jalisco*
DGTI	*Dirección General de Tecnologías de la Información*
RMA	*Autorización de devolución de materiales*
SLA	*Acuerdo de nivel de servicio*

2. ANTECEDENTES

La DGTI a través de la DIC de la Secretaría de Administración del GEJ, es responsable de la gestión, seguridad y correcta operación de los equipos, infraestructura y servicios de Tecnologías de la Información y Comunicaciones (TIC) del Centro de Datos de la Secretaría de Administración del GEJ. Como parte de estas responsabilidades se encuentra la infraestructura de seguridad lógica perimetral que da servicios a las Dependencias del GEJ.

3. JUSTIFICACIÓN

Uno de los principales compromisos de las instituciones de gobierno es salvaguardar la información y datos de carácter confidencial en poder de estas, tanto de la ciudadanía como de los propios servidores públicos y dependencias de gobierno, en su calidad de personas morales. Los riesgos informáticos vinculados a la pérdida, robo, modificación o uso ilícito de información y datos son cada vez más sofisticados y frecuentes, en metodologías y herramientas de ataque, derivado de esto, resulta necesario contar con métodos, infraestructura y servicios de ciberseguridad de última generación que garanticen la seguridad disponibilidad, privacidad y confidencialidad de la información y los datos en dominio del GEJ, haciendo necesario e ineludible la continuidad de la operación de los servicios técnicos profesionales de seguridad lógica perimetral del Centro de Datos de la Secretaria de Administración del GEJ así como del mantenimiento preventivo y correctivo que incluya refacciones, actualizaciones y parches de seguridad.

4. OBJETIVOS

Garantizar la seguridad lógica perimetral del Centro de Datos de la Secretaría de Administración del GEJ mediante de la contratación de una póliza de soporte y mantenimiento por parte de la DIC, cuyo alcance integre la cobertura, soporte técnico y actualizaciones a sistemas y equipos de seguridad lógica perimetral. Además de garantizar la integridad de los sistemas y servicios tecnológicos del GEJ, asegurando las capacidades y conocimientos técnicos sobre la operación de la infraestructura existente.

5. REQUERIMIENTO

Partida: 1

Descripción: Póliza Servicios de Soporte Técnico y Mantenimiento a la Infraestructura de Red Segura del GEJ.

A. Renovación de licenciamiento para equipos de seguridad lógica

Administración Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

1325

El proveedor participante deberá asegurar la renovación de licencias, póliza de soporte y mantenimiento 24X7 y garantía con el fabricante de la infraestructura de seguridad lógica del GEJ incluida en este anexo; esta renovación debe incluir actualizaciones, parches de seguridad, servicios profesionales, así como el reemplazo avanzado de hardware por parte del fabricante de los equipos descritos a continuación cumpliendo con una vigencia de un año a partir de la firma del contrato, los números de serie respectivos a cada uno de los equipos serán proporcionados al proveedor que resulte ganador.

Tabla "A"

Número de parte (ID)	Tipo de licencia Principal	Soporte	Cantidad de dispositivos
Fortigate 80F	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	51
Fortigate 40F	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	158
Fortigate 101F	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	18
Fortigate 201F	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	12
Fortigate 100F	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	8
Fortigate 601E	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	4
Fortigate 201E	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	3
Fortigate 3400E	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	2
Fortigate 200F	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	2
Fortigate 401E	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	2
Fortiweb 3000F	Standard Bundle (Detallado en otra fila)	Forticare 24x7	2
FortiAnalyzer 3000G	Enterprise Protection (Detallado en otra fila)	Forticare 24x7	1
Forti Mail 400F	Enterprise ATP Bundle Contract	Forticare 24x7	1
Forti Manager VM	24x7 FortiCare Contract (1 - 310 devices/Virtual Domains)	Forticare 24x7	1
Fortigate 200E	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	1
		TOTAL	267

Administración Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
Nº 1325

Todos los equipos listados anteriormente deberán contar con contrato de licenciamiento y soporte con el fabricante durante la vigencia señalada en este apartado, considerando lo siguiente:

- El licenciamiento deberá incluir todas las actualizaciones y parches de seguridad publicadas por el fabricante.
- El soporte del fabricante deberá brindarse en modalidad 24x7 con reemplazo de partes al siguiente día hábil.

B. Renovación de infraestructura de seguridad perimetral del GEJ

Como parte de la póliza se deberá considerar la actualización de la infraestructura de seguridad lógica existente del GEJ. El proveedor participante deberá considerar en su propuesta el suministro, diseño, instalación, configuración, puesta a punto y licenciamiento requerido por 12 meses, cumpliendo como mínimo con los lineamientos técnicos y funcionales de cata tipo descrito a continuación.

TIPO	CANTIDAD
A	1
B	2
C	1
D	2
E	2
F	1

1. TIPO A

Como parte de la póliza se deberá considerar la actualización de la infraestructura de seguridad perimetral existente del GEJ. El proveedor participante deberá considerar en su propuesta el suministro, diseño, instalación, configuración, puesta a punto y licenciamiento requerido por 12 meses de un (1) equipo cortafuego de siguiente generación (NGFW), cumpliendo como mínimo con los siguiente lineamientos técnicos y funcionales:

Características de desempeño por equipo:

- El equipo deberá de contar con un FW Throughput (64 bytes) de al menos 27Gbps
- El equipo deberá de soportar al menos 8 milion de sesiones concurridas (TCP)
- El equipo deberá de soportar al menos 450, 000 de New Sessions/Second (TCP)
- El equipo deberá de contar con IPsec VPN Throughput (512 byte) de al menos 20 GB
- El equipo deberá de contar con Gateway-to-Gateway IPsec VPN Tunnels de al Menos 2000
- El equipo deberá de generar de al menos 50, 000 Client-to-Gateway IPsec VPN Tunnels
- El equipo deberá de generar de al menos 7 GB de SSL-VPN Throughput
- El equipo deberá de soportar al menos 10,000 Concurrent SSL-VPN Users
- El equipo deberá de soportar al menos 10 Gbps de IPS Throughput (Enterprise Mix)
- El equipo Debera de soportar al menos 8 Gbps de SSL Inspection Throughput (IPS, avg. HTTPS)
- El equipo deberá de soportar al menos 9.5 Gbps de NGFW Throughput.
- El equipo deberá de soportar al menos 7 Gbps de Threat Protection Throughput
- El equipo Debera de soportar un maximo de 96 FortiSwitches
- El equipo deberá de soportar un máximo de 1024 FortiAPs
- El equipo Debera de generar al menos 10 Virtual Domains (Default)

Dirección General de Innovación Tecnológica Gubernamental
Administración
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
Nº 1325
DIRECCIÓN DE PLANEACIÓN

- El equipo deberá de generar al menos 50 Virtual Domains (Maximum)

Características de Hardware por equipo:

- El equipo deberá de contar con al menos 8 GE RJ45 Interfaces
- El equipo deberá de contar con al menos 8 GE SFP Slots
- El equipo deberá de contar con al menos 2 10GE SFP+ Slots
- El equipo deberá de contar con al menos 2 GE RJ45 Management Ports
- El equipo deberá de contar con al menos 1RU Rack Mount
- El equipo deberá de generar al menos 129W / 244W Power Comsumtion (Average / Maximum)
- El equipo deberá de generar al menos 832 BTU/hr Heat Dissipation
- El equipo deberá de contar con al menos Redundant Power Supplies (Hot Swappable); Optional
- El equipo deberá de contar con al menos Power Supply Efficiency Rating: 80Plus Compliant
- El equipo deberá de contar con al menos Compliance FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
- El equipo deberá de contar con al menos Certifications USGv6/IPv6

Licenciamiento.

Se deberá considerar las licencias necesarias para habilitar los servicios de Protección Unificada contra Amenazas, IPS, protección avanzada contra malware, control de aplicaciones, filtrado de URL, DNS y vídeo, servicio antispam. Soporte técnico 24x7, reemplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Firewall

- Debe soportar controles de zona de seguridad;
- Debe contar con políticas de control por puerto y protocolo;
- 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;
- Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- Debe soportar automatización de situaciones como deteción de equipos comprometidos, estado del sistema, cambios de onfiguración, eventos especificos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- Debe soportar integración de nubes publicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes
- Debe soportar el protocolo estándar de la industria VXLAN;
- La solución debe permitir la implementación sin asistencia de SD-WAN
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;

Dirección General de Administración e Innovación Tecnológica Gubernamental
14 OCT 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

- la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall.

FOLIO
Nº 1325
PLANEACION

APP Control

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- Detección de miles de aplicaciones en 18 categorias, 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;
- 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;
- 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;
- 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;
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- Actualización de la base de firmas de la aplicación de forma automática;
- Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por politica de usuarios y grupos;
- Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- 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;
- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;
- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
- 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);
- Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;
- Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;

Dirección General de Administración Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

PODER EJECUTIVO
1325

- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Threat Prevention

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
- Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
- 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;
- Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
- Debe incluir la protección contra ataques de denegación de servicio;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
- Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;
- Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
- Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;
- Detectar y bloquear los escaneos de puertos de origen;
- Bloquear ataques realizados por gusanos (worms) conocidos;
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
- Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- Identificar y bloquear la comunicación con redes de bots;
- 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;
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- 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;
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;

Dirección General de Innovación Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

- 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;
- 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;
- 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);

URL Filter

- 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);
- 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;
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- 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;
- Tener por lo menos 75 categorías de URL;
- Debe tener la funcionalidad de exclusión de URLs por categoría;
- Permitir página de bloqueo personalizada;
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
- Además del Explicit Web Proxy, soportar proxy web transparente;

User Identity

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

Dirección General de Administración, Innovación Tecnológica y Subdirección
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
No. 1325
DIRECCIÓN DE PLANEACIÓN

- 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;
- 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);
- 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;
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;

QoS & 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 aplicaciones, tanto de audio como de video streaming;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
- Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
- Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
- En QoS debe permitir la definición de tráfico con máximo ancho de banda;
- En QoS debe permitir la definición de colas de prioridad;
- Soportar marcación de paquetes DiffServ, incluso por aplicación;
- Soportar la modificación de los valores de DSCP para Diffserv;
- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

Geo IP

- Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

VPN

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
No 1325
DIRECCIÓN DE PLANEACIÓN

- Soporte VPN de sitio-a-sitio y cliente-a-sitio;
- Soportar VPN IPSec;
- Soportar VPN SSL;
- La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
- La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
- Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
- Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;
- 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;
- 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;
- Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
- Deberá mantener una conexión segura con el portal durante la sesión;
- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

2. TIPO B

Como parte de la póliza se deberá considerar la actualización de la infraestructura de seguridad perimetral existente del GEJ. El proveedor participante deberá considerar en su propuesta el suministro, diseño, instalación, configuración, puesta a punto y licenciamiento requerido por 12 meses de dos (2) equipo cortafuego de siguiente generación (NGFW), cumpliendo como mínimo con los siguiente lineamientos técnicos y funcionales:

Características de desempeño por equipo:

- El equipo deberá de contar con un FW Throughput (64 bytes) de al menos 27Gbps
- El equipo deberá de soportar al menos 8 milion de sesiones concurridas (TCP)
- El equipo deberá de soportar al menos 450, 000 de New Sessions/Second (TCP)
- El equipo deberá de contar con IPsec VPN Throughput (512 byte) de al menos 20 GB
- El equipo deberá de contar con Gateway-to-Gateway IPsec VPN Tunnels de al Menos 2000
- El equipo deberá de generar de al menos 50, 000 Client-to-Gateway IPsec VPN Tunnels
- El equipo deberá de generar de al menos 7 GB de SSL-VPN Throughput
- El equipo deberá de soportar al menos 10,000 Concurrent SSL-VPN Users
- El equipo deberá de soportar al menos 10 Gbps de IPS Throughput (Enterprise Mix)
- El equipo Debera de soportar al menos 8 Gbps de SSL Inspection Throughput (IPS, avg. HTTPS)

Dirección General de Administración, Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
No. 1325
DIRECCIÓN DE PLANEACIÓN TECNOLÓGICA

- El equipo deberá de soportar al menos 9.5 Gbps de NGFW Throughput.
- El equipo deberá de soportar al menos 7 Gbps de Threat Protection Throughput
- El equipo deberá de contar con al menos 2x 240 GB SSD onboard storage
- El equipo Debera de soportar un maximo de 96 FortiSwitches
- El equipo deberá de soportar un máximo de 1024 FortiAPs
- El equipo Debera de generar al menos 10 Virtual Domains (Default)
- El equipo deberá de generar al menos 50 Virtual Domains (Maximum)

Características de Hardware por equipo:

- El equipo deberá de contar con al menos 8 GE RJ45 Interfaces
- El equipo deberá de contar con al menos 8 GE SFP Slots
- El equipo deberá de contar con al menos 2 10GE SFP+ Slots
- El equipo deberá de contar con al menos 2 GE RJ45 Management Ports
- El equipo deberá de contar con al menos 1RU Rack Mount
- El equipo deberá de generar al menos 129W / 244W Power Comsumtion (Average / Maximum)
- El equipo deberá de generar al menos 832 BTU/hr Heat Dissipation
- El equipo deberá de contar con al menos Redundant Power Supplies (Hot Swappable); Optional
- El equipo deberá de contar con al menos Power Supply Efficiency Rating: 80Plus Compliant
- El equipo deberá de contar con al menos Compliance FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
- El equipo deberá de contar con al menos Certifications USGv6/IPv6

Licenciamiento.

Se deberá considerar las licencias necesarias para habilitar los servicios de Protección Unificada contra Amenazas, IPS, protección avanzada contra malware, control de aplicaciones, filtrado de URL, DNS y vídeo, servicio antispam. Soporte técnico 24x7, reemplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Firewall

- Debe soportar controles de zona de seguridad;
- Debe contar con políticas de control por puerto y protocolo;
- 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;
- Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- Debe soportar automatización de situaciones como deteción de equipos comprometidos, estado del sistema, cambios de onfiguración, eventos especificos, y aplicar una acción que puede ser notificación, bloqued de un equipo, ejecución de scripts, o funciones en nube pública.

Dirección General de Administración, Innovación Tecnológica y Modernamiento
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

Nº 1325
DIRECCIÓN DE PLANEACIÓN TECNOLÓGICA

- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- Debe soportar integración de nubes publicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes
- Debe soportar el protocolo estándar de la industria VXLAN;
- La solución debe permitir la implementación sin asistencia de SD-WAN
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;
- la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall.

APP Control

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- Detección de miles de aplicaciones en 18 categorias, 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;
- 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;
- 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;
- 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;
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- Actualización de la base de firmas de la aplicación de forma automática;
- Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por politica de usuarios y grupos;
- Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- 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;
- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;

Dirección General de Innovación Tecnológica
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
Nº 1325
DIRECCIÓN DE PLANEACIÓN TECNOLÓGICA

- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
- 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);
- Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;
- Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Threat Prevention

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
- Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
- 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;
- Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
- Debe incluir la protección contra ataques de denegación de servicio;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
- Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;
- Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
- Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;
- Detectar y bloquear los escaneos de puertos de origen;
- Bloquear ataques realizados por gusanos (worms) conocidos;
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
- Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- Identificar y bloquear la comunicación con redes de bots;

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO
Nº 1325

- 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;
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- 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;
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- 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;
- 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;
- 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);

URL Filter

- 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);
- 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;
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- 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;
- Tener por lo menos 75 categorías de URL;
- Debe tener la funcionalidad de exclusión de URLs por categoría;
- Permitir página de bloqueo personalizada;
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
- Además del Explicit Web Proxy, soportar proxy web transparente;

User Identity

Administración Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
Nº 1325

- 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;
- 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;
- 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 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;
- 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;
- 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;
- 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);
- 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;
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;

QoS & 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 aplicaciones, tanto de audio como de video streaming;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
- Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
- Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
- En QoS debe permitir la definición de tráfico con máximo ancho de banda;
- En QoS debe permitir la definición de colas de prioridad;
- Soportar marcación de paquetes DiffServ, incluso por aplicación;
- Soportar la modificación de los valores de DSCP para Diffserv;

Administración Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

FOLIO INTERNO
Nº 1325

Geo IP

- Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

VPN

- Soporte VPN de sitio-a-sitio y cliente-a-sitio;
- Soportar VPN IPSec;
- Soportar VPN SSL;
- La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
- La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
- Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
- Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;
- 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;
- 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;
- Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
- Deberá mantener una conexión segura con el portal durante la sesión;
- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

3. TIPO C

Como parte de la póliza se deberá considerar la actualización de la infraestructura de seguridad perimetral existente del GEJ. El proveedor participante deberá considerar en su propuesta el suministro, diseño, instalación, configuración, puesta a punto y licenciamiento requerido por 12 meses de un (1) equipo cortafuego de siguiente generación (NGFW), cumpliendo como mínimo con los siguiente lineamientos técnicos y funcionales:

Dirección General de Administración e Innovación Tecnológica
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
Nº 1325

Características de desempeño por equipo:

- El equipo deberá de contar con un FW Throughput (64 bytes) de al menos 28Gbps
- El equipo deberá de soportar al menos 3 millones de sesiones concurridas (TCP)
- El equipo deberá de soportar al menos 140, 000 de New Sessions/Second (TCP)
- El equipo deberá de contar con IPsec VPN Throughput (512 byte) de al menos 35 GB
- El equipo deberá de contar con Gateway-to-Gateway IPsec VPN Tunnels de al Menos 2000
- El equipo deberá de generar de al menos 16,000 Client-to-Gateway IPsec VPN Tunnels
- El equipo deberá de generar de al menos 1.5 GB de SSL-VPN Throughput
- El equipo deberá de soportar al menos 500 Concurrent SSL-VPN Users
- El equipo deberá de soportar al menos 5.3 Gbps de IPS Throughput (Enterprise Mix)
- El equipo deberá de soportar al menos 3 Gbps de SSL Inspection Throughput (IPS, avg. HTTPS)
- El equipo deberá de soportar al menos 3.1 Gbps de NGFW Throughput.
- El equipo deberá de soportar al menos 2.8 Gbps de Threat Protection Throughput
- El equipo deberá de contar con al menos 1x 480 GB SSD onboard storage
- El equipo deberá de soportar un máximo de 48 FortiSwitches
- El equipo deberá de soportar un máximo de 128 FortiAPs
- El equipo deberá de generar al menos 10 Virtual Domains (Default)
- El equipo deberá de generar al menos 10 Virtual Domains (Maximum)

Características de Hardware por equipo:

- El equipo deberá de contar con al menos 16 GE RJ45 Interfaces
- El equipo deberá de contar con al menos 8 GE SFP Slots
- El equipo deberá de contar con al menos 4 10GE SFP+ Slots
- El equipo deberá de contar con al menos 1/1 GE RJ45 Management / HA
- El equipo deberá de contar con al menos 1RU Rack Mount
- El equipo deberá de generar al menos 43W / 47W Power Comsumtion (Average / Maximum)
- El equipo deberá de generar al menos 159 BTU/hr Heat Dissipation
- El equipo deberá de contar con al menos Redundant Power Supplies; Yes (Default dual non-swappable AC PSU for 1+1 Redundancy)
- El equipo deberá de contar con al menos Power Supply Efficiency Rating : N/A
- El equipo deberá de contar con al menos Compliance FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI
- El equipo deberá de contar con al menos Certifications USGv6/IPv6

Licenciamiento.

Se deberá considerar las licencias necesarias para habilitar los servicios de Protección Unificada contra Amenazas, IPS, protección avanzada contra malware, control de aplicaciones, filtrado de URL, DNS y video, servicio antispam. Soporte técnico 24x7, reemplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

No 1325

Firewall

- Debe soportar controles de zona de seguridad;
- Debe contar con políticas de control por puerto y protocolo;
- 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;
- Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- Debe soportar automatización de situaciones como deteción de equipos comprometidos, estado del sistema, cambios de onfiguración, eventos especificos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- Debe soportar integración de nubes publicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes
- Debe soportar el protocolo estándar de la industria VXLAN;
- La solución debe permitir la implementación sin asistencia de SD-WAN
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;
- la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall.

APP Control

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- Detección de miles de aplicaciones en 18 categorias, 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;
- 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;
- 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;
- 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;
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- Actualización de la base de firmas de la aplicación de forma automática;
- Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2020
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
No. 1325
DIRECCIÓN DE PLANEACIÓN TECNOLÓGICA

- Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- 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;
- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;
- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
- 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);
- Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;
- Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Threat Prevention

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
- Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
- 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;
- Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
- Debe incluir la protección contra ataques de denegación de servicio;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
- Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;

Dirección General de Administración Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
No. 1325
DIRECCIÓN DE PLANEACIÓN

- Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
- Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;
- Detectar y bloquear los escaneos de puertos de origen;
- Bloquear ataques realizados por gusanos (worms) conocidos;
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
- Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- Identificar y bloquear la comunicación con redes de bots;
- 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;
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- 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;
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- 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;
- 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;
- 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);

URL Filter

- 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);
- 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;
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- 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;
- Tener por lo menos 75 categorías de URL;

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERN
1325

- Debe tener la funcionalidad de exclusión de URLs por categoría;
- Permitir página de bloqueo personalizada;
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
- Además del Explicit Web Proxy, soportar proxy web transparente;

User Identity

- 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;
- 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;
- 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 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;
- 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;
- 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;
- 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);
- 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;
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;

QoS & 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 aplicaciones, tanto de audio como de video streaming;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
- Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;

Dirección General de Administración e Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

1325
DIRECCIÓN DE PLANEACIÓN TECNOLÓGICA

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

Geo IP

- Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

VPN

- Soporte VPN de sitio-a-sitio y cliente-a-sitio;
- Soportar VPN IPSec;
- Soportar VPN SSL;
- La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
- La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
- Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
- Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;
- 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;
- 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;
- Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
- Deberá mantener una conexión segura con el portal durante la sesión;
- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

Administración Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
Nº 1325
DIRECCIÓN DE PLANEACIÓN TECNOLÓGICA

4. TIPO D

Como parte de la póliza se deberá considerar la actualización de la infraestructura de seguridad perimetral existente del GEJ. El proveedor participante deberá considerar en su propuesta el suministro, diseño, instalación, configuración, puesta a punto y licenciamiento requerido por 12 meses de dos (2) equipos cortafuegos de siguiente generación (NGFW), cumpliendo como mínimo con los siguiente lineamientos técnicos y funcionales:

Características de desempeño por equipo:

- El equipo deberá contar con un Throughput en Firewall tanto en IPv4 como en IPv6 de al menos 28 Gbps para paquetes UDP de 1518, 28 Gbps de 512 bytes y de 27.9 Gbps en paquetes UDP de 64 bytes
- El equipo deberá contar con un Throughput VPN IPSEC de por lo menos 25 Gbps.
- El equipo deberá contar con un Throughput IPS de al menos 4.5 Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad protección ante amenazas de al menos 2.2Gbps.
- El equipo deberá contar con un Throughput en la funcionalidad NGFW de al menos 2.5 Gbps.
- El equipo deberá soportar al menos 3 millones de Sesiones concurrentes.
- El equipo deberá soportar al menos 124,000 nuevas sesiones por segundo.
- El equipo deberá soporta al menos 200 usuarios concurrentes de VPN SSL.
- El equipo deberá generar al menos 2500 VPN's IPSec Client to Gateway.
- El equipo deberá generar al menos 200 VPN's IPSec Gateway to Gateway
- El equipo deberá soportar la configuración de al menos 5,000 políticas de firewall.
- El equipo deberá soportar al menos 10 sistemas virtuales lógicos (contextos) por appliance.

Características de Hardware por equipo:

- El equipo deberá contar con al menos 8 Interfaces GE RJ45
- El equipo deberá contar con al menos 2 10/5/2.5/GE RJ45 o 10GE/GE SFP+/SFP pares de medios compartidos
- El equipo deberá contar con al menos 1 puertos USB.
- El equipo deberá contar con al menos 1 Interfaz RJ45 gestión por consola.
- El equipo deberá contar con al menos 1 x 120 GB SSD Internal Storage.

Licenciamiento.

Se deberá considerar las licencias necesarias para habilitar los servicios de Protección Unificada contra Amenazas, IPS, protección avanzada contra malware, control de aplicaciones, filtrado de URL, DNS y vídeo, servicio antispam. Soporte técnico 24x7, reemplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Firewall

- Debe soportar controles de zona de seguridad;
- Debe contar con políticas de control por puerto y protocolo;
- 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;
- Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;

Dirección General de Administración y Evolución Tecnológica Gubernamental
14 DIC. 2020
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERN
Nº 1325

- Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- Debe soportar automatización de situaciones como deteción de equipos comprometidos, estado del sistema, cambios de onfiguración, eventos especificos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- Debe soportar integración de nubes publicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes
- Debe soportar el protocolo estándar de la industria VXLAN;
- La solución debe permitir la implementación sin asistencia de SD-WAN
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;
- la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall.

APP Control

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- Detección de miles de aplicaciones en 18 categorias, 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;
- 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;
- 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;
- 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;
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- Actualización de la base de firmas de la aplicación de forma automática;
- Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por politica de usuarios y grupos;
- Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- 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;
- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

DESPACHO INTERNO
Nº 1325
DIRECCIÓN DE PLANEACIÓN TECNOLÓGICA

- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;
- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
- 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);
- Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;
- Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Threat Prevention

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
- Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
- 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;
- Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
- Debe incluir la protección contra ataques de denegación de servicio;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
- Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;
- Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
- Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;
- Detectar y bloquear los escaneos de puertos de origen;
- Bloquear ataques realizados por gusanos (worms) conocidos;
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2020
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
Nº 1325

- Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- Identificar y bloquear la comunicación con redes de bots;
- 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;
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- 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;
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- 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;
- 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;
- 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);

URL Filter

- 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);
- 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;
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- 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;
- Tener por lo menos 75 categorías de URL;
- Debe tener la funcionalidad de exclusión de URLs por categoría;
- Permitir página de bloqueo personalizada;
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
- Además del Explicit Web Proxy, soportar proxy web transparente;

User Identity

Dirección General de Innovación Tecnológica Gubernamental
Administración
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
Nº 1325

- 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;
- 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;
- 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 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;
- 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;
- 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;
- 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);
- 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;
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;

QoS & 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 aplicaciones, tanto de audio como de video streaming;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
- Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
- Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
- En QoS debe permitir la definición de tráfico con máximo ancho de banda;
- En QoS debe permitir la definición de colas de prioridad;
- Soportar marcación de paquetes DiffServ, incluso por aplicación;
- Soportar la modificación de los valores de DSCP para Diffserv;

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

HP 1325

Geo IP

- Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

VPN

- Soporte VPN de sitio-a-sitio y cliente-a-sitio;
- Soportar VPN IPSec;
- Soportar VPN SSL;
- La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
- La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
- Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
- Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;
- 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;
- 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;
- Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
- Deberá mantener una conexión segura con el portal durante la sesión;
- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

5. TIPO E

Como parte de la póliza se deberá considerar la actualización de la infraestructura de seguridad perimetral existente del GEJ. El proveedor participante deberá considerar en su propuesta el suministro, diseño, instalación, configuración, puesta a punto y licenciamiento requerido por 12 meses de dos (2) equipo cortafuego de siguiente generación (NGFW), cumpliendo como mínimo con los siguiente lineamientos técnicos y funcionales:

Características de desempeño por equipo:

- El equipo deberá de contar con un FW Throughput (64 bytes) de al menos 4Gbps

14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
Nº 1325
DIRECCIÓN DE PLANEACIÓN

- El equipo deberá de soportar al menos 720,000 de sesiones concurridas (TCP)
- El equipo deberá de soportar al menos 85,000 de New Sessions/Second (TCP)
- El equipo deberá de contar con IPsec VPN Throughput (512 byte) de al menos 4.5 GB
- El equipo deberá de contar con Gateway-to-Gateway IPsec VPN Tunnels de al Menos 2000
- El equipo deberá de generar de al menos 250 Client-to-Gateway IPsec VPN Tunnels
- El equipo deberá de soportar al menos 2.25 Gbps de IPS Throughput (Enterprise Mix)
- El equipo Debera de soportar al menos 1.3 Gbps de SSL Inspection Throughput (IPS, avg. HTTPS)
- El equipo deberá de soportar al menos 1.25 Gbps de NGFW Throughput.
- El equipo deberá de soportar al menos 1.1 Gbps de Threat Protection Throughput
- El equipo deberá de contar con al menos 64 GB SSD onboard storage
- El equipo Debera de soportar un maximo de 8 FortiSwitches
- El equipo deberá de soportar un total de 16 FortiAPs
- El equipo Debera de generar al menos 5 Virtual Domains (Default)
- El equipo deberá de generar al menos 5 Virtual Domains (Maximum)

Características de Hardware por equipo:

- El equipo deberá de contar con al menos 3 GE RJ45 Interfaces
- El equipo deberá de contar con al menos 1 GE WAN Port
- El equipo deberá de contar con al menos 1 GE RJ45 Puerto FortiLink
- El equipo deberá de contar con al menos 1 GE RJ45 Management Port
- El equipo deberá de contar con un factor de forma de escritorio
- El equipo deberá de generar al menos 8.3W / 8.9W Power Comsumtion (Average / Maximum)
- El equipo deberá de generar al menos 30.35 BTU/hr Heat Dissipation
- El equipo deberá de contar con al menos Compliance FCC, ISED, CE, UL/cUL, CB
- El equipo deberá de contar con al menos Certifications USGv6/IPv6

Licenciamiento.

Se deberá considerar las licencias necesarias para habilitar los servicios de Protección Unificada contra Amenazas, IPS, protección avanzada contra malware, control de aplicaciones, filtrado de URL, DNS y vídeo, servicio antispam. Soporte técnico 24x7, reemplazo avanzado de hardware y actualizaciones de firmware.

Funcionalidades.

Firewall

- Debe soportar controles de zona de seguridad;
- Debe contar con políticas de control por puerto y protocolo;
- 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;
- Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;

Dirección de Innovación Tecnológica
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

- Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- Debe soportar automatización de situaciones como deteción de equipos comprometidos, estado del sistema, cambios de onfiguración, eventos especificos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes
- Debe soportar el protocolo estándar de la industria VXLAN;
- La solución debe permitir la implementación sin asistencia de SD-WAN
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;
- la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall.

APP Control

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- Detección de miles de aplicaciones en 18 categorias, 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;
- 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;
- 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;
- 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;
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- Actualización de la base de firmas de la aplicación de forma automática;
- Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por politica de usuarios y grupos;
- Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- 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;
- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;

No 1325

Dirección General de Administración e Innovación Tecnológica Gubernamental
14 OCT. 2025
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
No. 1325
DIRECCIÓN DE PLANEACIÓN TECNOLÓGICA

- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;
- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
- 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);
- Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;
- Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Threat Prevention

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
- Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
- 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;
- Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
- Debe incluir la protección contra ataques de denegación de servicio;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
- Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;
- Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
- Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;
- Detectar y bloquear los escaneos de puertos de origen;
- Bloquear ataques realizados por gusanos (worms) conocidos;
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);

Dirección General de Innovación Tecnológica Gubernamental
Administración
04 OCT. 2020
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
1325

- Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- Identificar y bloquear la comunicación con redes de bots;
- 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;
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- 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;
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- 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;
- 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;
- 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);

URL Filter

- 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);
- 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;
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- 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;
- Tener por lo menos 75 categorías de URL;
- Debe tener la funcionalidad de exclusión de URLs por categoría;
- Permitir página de bloqueo personalizada;
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
- Además del Explicit Web Proxy, soportar proxy web transparente;

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

1325

User Identity

- 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;
- 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;
- 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 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;
- 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;
- 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;
- 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);
- 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;
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;

QoS & 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 aplicaciones, tanto de audio como de video streaming;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
- Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
- Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
- En QoS debe permitir la definición de tráfico con máximo ancho de banda;
- En QoS debe permitir la definición de colas de prioridad;

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2020
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
No. 1325

- Soportar marcación de paquetes DiffServ, incluso por aplicación;
- Soportar la modificación de los valores de DSCP para Diffserv;
- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

Geo IP

- Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

VPN

- Soporte VPN de sitio-a-sitio y cliente-a-sitio;
- Soportar VPN IPSec;
- Soportar VPN SSL;
- La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
- La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
- Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
- Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;
- 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;
- 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;
- Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
- Deberá mantener una conexión segura con el portal durante la sesión;
- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

6. TIPO F

Como parte de la póliza se deberá considerar la actualización de la infraestructura de seguridad existente del GEJ.

El proveedor participante deberá considerar en su propuesta el suministro, diseño, instalación, configuración, puesta a punto y licenciamiento requerido por 12 meses de un (1) dispositivo de gestión de identidad de acceso, cumpliendo como mínimo con los siguiente lineamientos técnicos y funcionales:

Dirección General de Administración y Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

No 1325

Características físicas del equipo:

- El equipo deberá contar con al menos Local + Remote Users (Base / Upper Limit): 1500/ 3500
- El equipo deberá contar con al menos User Groups: 150
- El equipo deberá contar con al menos CA Certificates: 10
- El equipo deberá contar con al menos GE RJ45 Interfaces: 4
- El equipo deberá contar con al menos Storage [TB]: 2 TB Hard Disk Drive
- El equipo deberá contar con al menos Form Factor: Rack Mountable: 1RU

Características General

- Se puede entregar en una única solución o conjunto de soluciones, siempre que cumpla con todos los requisitos
- La solución debe soportar crecimiento adaptativo de usuarios a través de licenciamiento.
- La solución debe soportar administración vía interface gráfica (GUI) por HTTP / HTTPS
- La solución debe soportar administración por línea de comandos (CLI) utilizando Telnet / SSH
- Permite definir perfiles de administradores para una solución, de modo que puede segmentar la responsabilidad de los administradores por tareas operativas
- Incluya un indicador visual centralizado de información crítica (estado de la licencia, versión de firmware, consumo de CPU / memoria / disco, número de usuarios creados y con licencia)
- La solución debe soportar actualización de firmware a través de la interfaz gráfica, mediante un proceso simplificado e intuitivo
- La solución debe soportar la personalización de mensajes de solución estándar como páginas de error, portales de autenticación, autorregistro, restablecimiento de contraseña y otros. También La solución debe soportar la inclusión, alteración y eliminación de imágenes en mensajes / páginas sin la necesidad de recursos o conectividad externa
- La solución debe soportar la configuración de alta disponibilidad (HA), minimizando el tiempo de inactividad
- La solución debe soportar implementaciones de HA como "Active-Passive" o configuraciones de sincronización entre dos unidades activas
- La solución permite la sincronización automática de configuraciones entre todos los equipos que componen la solución HA
- La solución debe soportar la implementación de HA sincronizando configuraciones con dispositivos en ubicaciones geográficamente separadas
- La solución debe soportar la opción de copia de seguridad cifrada
- La solución debe soportar copias de seguridad automatizadas (programadas por criterios predefinidos), no solo bajo demanda
- La solución debe soportar copia de seguridad completa de la configuración, incluida la base de usuarios, grupos, tokens, certificados, configuraciones de inicio de sesión único, etc. La solución también Permite la restauración de toda la configuración directamente desde la interfaz gráfica
- La solución debe soportar NTP (Protocolo de tiempo de red), con el objetivo de sincronización de hora / fecha
- La solución debe soportar ruteo estático

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
1325

- La solución debe soportar SNMP v1, v2 e v3 permitiendo consultar MIBs propias y envío de SMNP Traps
- La solución debe soportar nativo SNMP Trap que indica un cambio de estado en el HA
- La solución debe soportar la captura de paquetes a través de la interfaz gráfica para solucionar problemas avanzados en herramientas de análisis de paquetes (por ejemplo, Wireshark)
- La solución debe soportar el envío de correos electrónicos actuando como su propio servidor (localhost) o integración con servidores externos para enviar mensajes a usuarios o administradores
- El equipo permite el envío de correos electrónicos relacionados con el restablecimiento de la contraseña, la aprobación de nuevos usuarios, el auto registro del usuario y la autenticación de segundo factor (vía token).
- Permita el envío de mensajes SMS a los usuarios a través de gateway SMS de terceros
- La solución debe soportar el registro de todos los eventos que los usuarios de su base de datos local realizan con sus cuentas, como crear un usuario, cambiar la contraseña de un usuario y cambiar la información general

Authentication

- La solución debe realizar la autenticación para la gestión de identidad de los usuarios de la red, siendo un punto central de control de autenticación, donde se pueden consolidar múltiples métodos de autenticación
- La solución debe soportar autenticación de dos factores (two-factor authentication)
- La solución debe soportar autenticación de dos factores en al menos dos tipos diferentes de tokens, el primero es físico (token) y el segundo lógico como software para dispositivos móviles
- La solución debe permitir la definición de un nivel de complejidad mínima para las contraseñas de todos los usuarios registrados en la base de datos local, permitiendo la definición de un número mínimo de letras minúsculas, mayúsculas, caracteres numéricos, caracteres especiales, etc.
- La solución debe permitir la creación de una política de bloqueo automático de usuarios después de una serie de fallas de autenticación, evitando así los ataques de fuerza bruta
- La solución debe soportar la creación de usuarios a nivel local, que se puede utilizar para autenticar dispositivos según sea necesario.
- La solución debe permitir la creación masiva de usuarios en la base de datos local mediante la importación de una lista de usuarios que se creará en archivos externos.
- La solución debe permitir la creación de nuevos usuarios en la base de datos local y que el administrador pueda definir una contraseña al momento de crearlos.
- La solución debe permitir la creación de nuevos usuarios en la base de datos local y que el equipo genere una contraseña aleatoria y la envíe automáticamente al usuario.
- La solución debe permitir la creación de nuevos usuarios en la base de datos local sin la definición de una contraseña, requiriendo que use el token como el único factor de autenticación
- Permite asociar tokens a usuarios creados localmente en la base de datos
- Permite a los propios usuarios registrar sus tokens e informar la pérdida de un token automáticamente, sin la necesidad de involucrar a un administrado
- Eliminación automática masiva de usuarios inactivos, según criterios definidos
- La solución permite a los usuarios locales restablecer sus contraseñas de manera segura, sin la intervención de los administradores, por correo electrónico o preguntas de seguridad en portal de autoservicio.

Dirección General de Administración, Innovación Tecnológica y Gobierno Digital
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
1325

- La solución debe soportar la creación de grupos de usuarios, que pueden usarse para autenticar uno o varios dispositivos.
- Los tokens deben generar códigos con un mínimo de 6 dígitos e intervalos que no excedan los 60 segundos
- La solución debe soportar autenticación de dos factores por hardware dedicado (token)
- La solución debe soportar autenticación de dos factores por aplicación móvil (iPhone y Android)
- La solución debe soportar autenticación de dos factores enviando un mensaje SMS
- La solución debe soportar autenticación de dos factores mediante el envío de correo electrónico.
- La solución debe soportar sincronización de dispositivos en hardware de generación OTP (one time password)
- Permite sincronizar los tokens con el equipo para su correcto funcionamiento.
- Permite desactivar un token cuando es robado o perdido, permitiendo su reactivación posterior cuando / si se recupera
- Permite la disociación de un token a un usuario y asociarlo con otro usuario cuando sea necesario, permitiendo así su reutilización
- Permite la autenticación de doble factor en clientes Windows, incluso con la máquina fuera de línea
- Debe proporcionar un portal web para que los usuarios se registren automáticamente, de modo que puedan acceder, completar sus datos y enviar el registro. Después de que el usuario inicia sesión, el administrador debe ser notificado automáticamente para aprobar o denegar el registro del usuario antes de que el usuario sea activado.
- La solución debe funcionar como un servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticación a dispositivos compatibles con dicho protocolo
- La solución La solución debe soportarr la integración con el servidor RADIUS remoto
- La solución puede funcionar como un servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticación a dispositivos compatibles con ese protocolo
- La solución debe tener un servidor LDAP interno que permita su configuración jerárquica, para la correcta administración por grupos o unidades organizativas de usuarios locales.
- La solución debe soportar la integración con un servidor LDAP remoto (como Microsoft Active Directory)
- La solución debe soportar la autenticación de usuarios con credenciales de redes sociales como Facebook, Twitter y LinkedIn
- La solución debe permitir a los usuarios que no tienen una cuenta local o de redes sociales autenticarse a través de un registro rápido, que garantice una trazabilidad mínima, a través de la validación de direcciones de correo electrónico o números de teléfono.
- La solución debe permitir el inicio de sesión automático de los usuarios visitantes después de que se hayan registrado con éxito
- La solución debe permitirle configurar los parámetros de red (como la configuración de WiFi) en un dispositivo de usuario (laptop, móvil) mediante la descarga de un script o un archivo ejecutable a través del portal de visitantes.
- La solución debe soportar el lenguaje de marcado de aserción de seguridad (SAML), que actúa como un proveedor de identidad (IDP), estableciendo una relación de confianza para la autenticación segura de los usuarios que intentan acceder a un Proveedor de Servicios (SP)

Dirección General de Administración e Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

Port Based Control

- La solución debe soportar de forma nativa (sin redireccionamientos) la integración y autenticación de conmutadores y otros dispositivos compatibles con el estándar 802.1X
- Debe proporcionar de forma nativa (sin redirigir a equipos de terceros) la integración de los clientes finales para ofrecer autenticación 802.1X
- La solución debe soportar los siguientes métodos EAP 802.1X: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS y EAP-GTC
- La solución debe soportar la interoperabilidad con equipos de acceso de terceros (swtiches), para la autenticación de puertos con la solución, a través de los estándares 802.1X
- Debe ser compatible con el bypass de autenticación 802.1X para dispositivos conocidos que no son compatibles con 802.1X, el lanzamiento debe realizarse en función de la dirección MAC del equipo previamente registrado, tendrán acceso a la red sin necesidad de autenticación o acción del usuario o dispositivo.

Certification Authority

- La solución debe actuar como una Autoridad de Certificación (CA)
- Permite la administración de certificados digitales, con emisión y revocación.
- Permite el uso de CAs de confianza, para validar certificados emitidos por CAs externas
- Debe ser compatible con OCSP para proporcionar una lista de revocación de certificados (CRL)
- Debe proporcionar un repositorio para la autenticación VPN site-to-site a través de certificados
- Debe ser compatible con el servidor SCEP (Simple Certificate Enrollment Protocol), lo que permite la firma de solicitudes de certificados digitales (CSR) automáticamente o con interacción del administrador
- Debe crear y firmar certificados X.509 para usar en servidores https y ssh, así como clientes de sericios HTTPS, SSH, VPNs IPSec
- Debe poder importar otros certificados de CA, así como la lista de revocación de certificados
- Permite que el administrador del sistema genere, firme y revoque certificados digitales para los usuarios

SSO

- La solución debe proporcionar la capacidad de servicio SSO (Single Sign-On), con autenticación transparente de usuarios (pasiva) en sistemas compatibles
- Debe poder integrarse con un directorio activo (Windows AD) y poder ofrecer la funcionalidad SSO, donde la autenticación automática / transparente a través de SSO para los servicios necesarios se basa en la autenticación previa del usuario en el dominio
- Permite definir una lista de usuarios de SSO que serán ignorados, evitando así la interferencia de cuentas de servicio como antivirus o scripts a través de GPO
- La solución debe soportar el análisis de archivos syslog enviados desde una fuente remota, para uso del servicio SSO
- La solución debe soportar el Security Assertion Markup Language (SAML), para solicitar información de identidad del usuario a Proveedores de identidad (IDP) de terceros.
- La solución debe soportar SSO basado en radio (RSSO - RADIUS Single Sign-On)
- La solución debe soportar el RSSO RADIUS Accounting Proxy, que permite la recepción de paquetes de radio de búsqueda, la modificación de estos paquetes y el reenvío de ellos a varios otros puntos

Dirección General de Gobierno Digital
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

INTERNO
Nº 1325

Implementación

Como parte del servicio de actualización de infraestructura, se deberá considerar la puesta a punto de la solución propuesta, considerando al menos los siguientes requerimientos:

- El proveedor participante deberá realizar el diseño de la arquitectura de solución.
- El proveedor participante deberá realizar el plan de trabajo para la implementación, el cual deberá contener al menos las tareas a realizar, así como los tiempos de ejecución y rollback.
- El proveedor participante deberá realizar la instalación física en la Secretaría de Administración
- El proveedor participante deberá realizar el respaldo de la configuración de la infraestructura existente.
- El proveedor participante deberá realizar la migración de configuración a la infraestructura propuesta.
- Como parte de la implementación, el proveedor participante deberá realizar al menos una sesión de transferencia de conocimiento de 4 horas como mínimo, durante la cual, se capacitará al personal técnico de la Secretaría de Administración sobre el uso y administración de la infraestructura de seguridad perimetral implementada.
- El proveedor participante deberá realizar la memoria técnica de la implementación la cual deberá contener al menos lo siguiente:
  - Diagrama.
  - Memoria fotográfica.
  - Respaldo de configuración
  - Pruebas de funcionamiento.
  - Evidencia de la transferencia de conocimientos.

C. Servicio de soporte y mantenimiento

El proveedor participante deberá proporcionar un servicio de soporte y mantenimiento 24x7 propio -distinto al del fabricante- cumpliendo con una vigencia de 1 año a partir de la firma del contrato que cubra los siguientes equipos, los números de serie respectivos a cada uno de los equipos serán proporcionados al proveedor que resulte ganador:

Número de parte (ID)	Tipo de licencia Principal	Soporte (Inferido)	Cantidad de dispositivos
Fortigate 80F	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	51
Fortigate 101F	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	18
Fortigate 201F	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	12
Fortigate 100F	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	8
Fortigate 601E	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	7
Fortigate 201E	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	3
Fortigate 3400E	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	2

Dirección General de Administración e Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

Fortigate 200F	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	2
Fortigate 401E	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	2
Fortigate 90G	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	2
Fortiweb 3000F	Standard Bundle (Varias versiones)	Forticare 24x7	2
FAC-VM	FortiCare Premium Support	Forticare 24x7	1
Forti Manager VM	24x7 FortiCare Contract (1 - 310 devices/Virtual Domains)	Forticare 24x7	1
FortiAnalyzer 3000G	Enterprise Protection (Largo)	Forticare 24x7	1
Fortigate 121G	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	1
Fortigate 200E	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	1
Fortigate 51G	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	1
Fortigate 600E	24x7 FortiCare and FortiGuard Unified Threat Protection (UTP)	Forticare 24x7	1
FortiMail 400F	Enterprise ATP BundleContract	Forticare 24x7	1
		TOTAL	118

Adicional, tendrá que cumplir con las características listadas a continuación:

- Contar con una "Mesa de servicios" con atención 24x7 los 365 días del año, siendo esta el conducto para realizar las solicitudes de soporte técnico y seguimiento. El servicio deberá ser brindado en idioma español y sin límites de eventos.
- Facilitar al menos los siguientes medios de contacto hacia la mesa de servicios para el reporte y seguimiento a incidentes:
  - Soporte telefónico.
  - Soporte vía aplicación de acceso remoto brindada por EL proveedor.
  - Soporte vía correo electrónico.
  - Plataforma Web.
- Para generar reportes y dar seguimiento, EL proveedor deberá de proporcionar usuario y contraseña para el acceso vía web a la mesa de servicios.
- 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) deberán ajustarse a los siguientes tiempos de respuesta:

Nivel de Severidad 1	Tiempo de Respuesta

Dirección General de Administración e Innovación Tecnológica Gubernamental
14 OCT 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

PLIEGO INTERNO
Nº 1325

Servicio totalmente degradado, impacto crítico.	
Contacto del Ingeniero Asignado	15 minutos
Análisis y Diagnóstico	30 minutos
Workaround	1 hora
Solución	2 horas

Nivel de Severidad 2 Servicio severamente degradado.	Tiempo de Respuesta
Contacto del Ingeniero Asignado	30 minutos
Análisis y Diagnóstico	1 hora
Workaround	2 horas
Solución	4 horas

Nivel de Severidad 3 Desempeño operativo perjudicado.	Tiempo de Respuesta
Contacto del Ingeniero Asignado	2 horas
Análisis y Diagnóstico	3 horas
Workaround	6 horas
Solución	8 horas

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
Nº 1325
DIRECCIÓN DE PLANEACIÓN

Nivel de Severidad 4 Requerimiento de configuración.	Tiempo de Respuesta
Contacto del Ingeniero Asignado	4 horas
Análisis y Diagnóstico	8 horas
Solución	24 horas

- El soporte podrá ser recibido de manera remota o presencial de acuerdo con lo solicitado por el personal de la DIC.
- En caso de requerir presencia en sitio, El proveedor participante deberá de informar de manera previa el/los nombre(s) del personal técnico designado, mismo que deberá contar con gafete y/o uniforme que lo identifique.
- En caso de requerir soporte técnico por parte del fabricante, EL proveedor será responsable de realizar el reporte de fallas y solicitudes de RMA, así como el seguimiento y en su caso la escalación hasta su solución y cierre.
- Una vez atendido y resuelto el reporte y/o solicitud en su totalidad, EL proveedor participante deberá entregar reporte de servicio que incluya de manera amplia la descripción de la falla o servicio solicitado, diagnóstico y solución, así como las recomendaciones de configuración en apego a las mejores prácticas.
- El proveedor participante deberá proporcionar acceso a la base de conocimientos del fabricante, así como a sus recursos y herramientas.
- EL proveedor participante deberá proporcionar acceso al personal de la DIC al portal de soporte técnico del fabricante de los equipos cubiertos.
- EL proveedor participante deberá dar acceso al personal de la DIC a la descarga de actualizaciones y parches de seguridad del sistema operativo, incluyendo releases menores y mayores, los cuales deberán ser oficiales, y accesibles desde el sitio web del fabricante de los equipos cubiertos.
- La mesa de ayuda deberá apegarse a la metodología ITIL, lo cual deberá ser demostrado mediante copia simple del certificado ITIL 4 Managing Professional Transition del personal que la administra.
- Se deberán entregar reportes mensuales.

D. Plataforma de ciberseguridad para la protección de servidores

El proveedor participante deberá considerar dentro de la propuesta mantener activa una solución de ciberseguridad con capacidad de detección de actividades de explotación y de vulnerabilidades, considerando un análisis de comportamiento con motores que reconocen las actividades y procesos para asegurar la protección de los servidores (en ambiente virtual o físico) que se encuentran hospedados en el Centro de Datos de la Secretaría de Administración del GEJ. EL proveedor participante deberá considerar 1,000 licencias de la solución para cumplir con las características siguientes:

- Tener una vigencia de un año a partir de la firma del contrato
- Brindar los siguientes motores de detección de amenazas:
  - Reputación: Motor de inteligencia artificial para asegurar que no se escriban, ni ejecuten, archivos maliciosos conocidos en el disco.

Administración | Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

- Inspección profunda de archivos: Motor de inteligencia artificial estática preventiva para escanear y buscar archivos maliciosos escritos en el disco.
- Inspección profunda de archivos sospechosos: Motor de búsqueda de archivos sospechosos escritos en el disco cuando está en modo de protección.
- Seguimiento dinámico de comportamiento: motor de inteligencia artificial conductual que deberá implementar herramientas avanzadas de aprendizaje automático. Este motor deberá detectar actividades maliciosas en tiempo real cuando se ejecutan los procesos.
- Movimiento lateral: Motor que deberá detectar ataques iniciados por dispositivos remotos.
- Anti-explotación: Motor que deberá enfocarse en exploits y todos los intentos de ataque sin archivos, como los exploits relacionados con la web y línea de comandos.
- Detección de amenazas interactivas: Deberá estar enfocado en amenazas internas para detectar comandas maliciosas en sesiones interactivas.
- Detección basada en comportamiento de amenazas: Mediante análisis de comportamiento deberá determinar la acción que trata de realizar algún archivo o proceso sobre el sistema. La detección será basada en comportamiento sin necesidad de depender de firmas ni conexión a la nube. Además, se deberá ajustar los resultados al marco MITRE y ATT&CK.
- Deberá incluir el control de dispositivos USB y Bluetooth

- La solución deberá tomar las siguientes acciones contra las amenazas:
  - Deberá matar el proceso.
  - Deberá poner en cuarentena los archivos infectados o las amenazas.
  - Deberá deshacer los cambios realizados por la amenaza sobre el sistema operativo.
  - Deberá realizar Rollback para dejar los archivos tal como estaban originalmente antes de que se ejecutara la amenaza.
  - Deberá brindar al administrador el poder establecer una conexión remota con cualquier sistema y realizar actividades adicionales de remediación.
  - Deberá garantizar una funcionalidad para remediar en tiempo real.
  - Deberá detectar en tiempo real amenazas de día cero, sin necesidad de enviar información adicional a la nube.
- La solución deberá contar con una consola centralizada para detectar amenazas y los agentes deberán ser autónomos, es decir, no deberán requerir estar conectados a internet para su funcionamiento y no deberá afectar sus funcionalidades de protección.
- EL proveedor participante deberá considerar la instalación y configuración de todos los agentes de acuerdo con las recomendaciones del fabricante.
- EL proveedor participante deberá considerar el servicio administrado 24x7 con vigencia de un año a partir de la firma del contrato

E. Programa de Capacitación y Certificación Técnica

El proveedor participante deberá incluir dentro de su propuesta técnica un programa de capacitación y certificación para el personal designado por la Secretaría de Administración, considerando como mínimo los siguientes rubros:

- Se deberá suministrar el curso de capacitación técnica especializada, así como los vauchers correspondientes para la presentación del examen de certificación oficial en el nivel de Fortinet NSE 7 para al menos 2 (dos) personas contando con las siguientes consideraciones:
  - El curso deberá tener una duración mínima de 3 (tres) días.
  - La capacitación podrá ser impartida en modalidad presencial o virtual a elección de la convocante.

1325

Dirección General de Administración e Innovación Tecnológica
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO 1325

- Se deberá suministrar el curso de capacitación, materiales de estudio y el váucher de examen para la certificación Certified Ethical Hacker (CEH) para al menos 5 (cinco) personas, contando con las siguientes consideraciones:
  - El curso deberá contar con una carga horaria total de 40 (cuarenta) horas.
  - Esta capacitación deberá ser impartida exclusivamente en modalidad virtual.

En ambos casos, el proveedor deberá garantizar que los cursos sean impartidos por instructores certificados y en centros de capacitación autorizados por los fabricantes, incluyendo todo el material didáctico y laboratorios necesarios para el aprendizaje y la acreditación de los exámenes correspondientes.

6. GARANTÍAS

Garantía de 1 año a partir de la firma del contrato.

7. OBLIGACIONES DE LOS PARTICIPANTES

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

- EL proveedor participante deberá mencionar marca, modelo y especificaciones técnicas y garantía en su cotización y propuesta técnica.
- EL proveedor participante deberá presentar Datasheet de las soluciones propuestas con link de la página oficial del fabricante, en el cual se corroboró la información de acuerdo con su cotización.
- El proveedor participante deberá demostrar que cuenta con oficinas operativas dentro de la zona Metropolitana de Guadalajara, con el fin de responder a tiempo a las incidencias que requieran atención en sitio
- El proveedor participante podrá ofertar características superiores a las solicitadas, lo cual deberá ser corroborado por el fabricante como superior mediante carta original haciendo mención del número de concurso al cual participa.
- EL proveedor participante deberá presentar carta bajo protesta de decir verdad en la que menciona que está considerando dentro de su propuesta económica cualquier tipo de componente, hardware, software, mano de obra, viático, traslados, costos de importación, etc. Necesarios para la correcta ejecución de la póliza de soporte y mantenimiento, y en ningún caso se deberá generar un costo extra para el GEJ.
- Carta del fabricante de los equipos de seguridad perimetral en la que establezca sobre el Proveedor participante, es un Revendedor Autorizados, además tener un nivel Expert con especializaciones en *SD-WAN, Cloud Security, Secure Networking LAN* y *Security Operations*, al menos
- Con el fin de asegurar que se reúnen las competencias necesarias para prestar los servicios asociados a este proyecto, el Proveedor Participante, deberá proporcionar copia simple y vigente de las certificaciones siguientes:
  - 1 certificado ITIL 4 Managing Professional Transition
  - 2 certificado Especialista en Soluciones de Seguridad de Red (FCSSNS) del fabricante de los equipos de seguridad perimetral
  - 1 certificado Especialista en Soluciones de Seguridad de Nube (FCSSCS) del fabricante de los equipos de seguridad perimetral
  - 1 certificado Especialista en Soluciones de Seguridad de Operaciones (FCSSSO) del fabricante de los equipos de seguridad perimetral

Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

FOLIO INTERNO
Nº 1325

- 1 certificado de Administración de Proyecto (PMP) emitido por el Project Management Institute (PMI)
- Una misma persona con las tres siguientes certificaciones:
  - (1) Un Certificado vigente en Ethical Hacker (CEH)
  - (1) Un Certificado vigente en Ethical Hacker (CEH) Práctico
  - (1) Un Certificado vigente en Ethical Hacker (CEH) Maestro

- El proveedor participante deberá demostrar mediante copia simple de al menos 1 contrato celebrado con algún ente público con antigüedad no mayor a 2 años, que ha ejecutado un proyecto de póliza de mantenimiento y soporte de infraestructura de Red IP de servicios de datos y seguridad.
- El proveedor participante deberá presenta carta digital, mencionando el concurso al cual participa, emitida por el fabricante de los equipos de ciberseguridad que se actualizarán (Tipo A, Tipo B, Tipo C, Tipo D, Tipo E, Tipo F) donde mencione respecto a los equipos incluidos en la oferta del Proveedor participante, haga constar, que son originales de fábrica, se suministrarán nuevos (no remanufacturados) al distribuidor autorizado quien, a su vez, proporcionará al Proveedor participante y se encuentran disponibles para su venta sin que éstos cuenten con fecha de Fin de Orden (End of Order o "EoO" por sus siglas en inglés) ni tampoco fecha de Fin de Soporte (End of Support o "EoS" por sus siglas en inglés)

8. ENTREGABLES

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

- Garantía por escrito de acuerdo con lo especificado en el apartado 6. GARANTÍAS.
- Pólizas de soporte técnico y mantenimiento donde se menciona el alcance, la vigencia, el procedimiento para generar reportes y solicitudes, así como los SLA's, organigrama y procedimiento de escalamiento, debiendo incluir al menos los siguientes datos del personal técnico:
  - Nombre y cargo.
  - Teléfono de contacto (oficina y celular).
  - Correo electrónico.
- Las pólizas deberán ser entregadas de manera individual de acuerdo en las siguientes áreas:
  - **Secretaría de Administración** – Dirección de Infraestructura y Comunicaciones
    - Domicilio: Avenida Alcalde 1221, Col. Miraflores, Guadalajara, Jalisco.
- Documento de suscripción y licenciamiento donde se mencionan los números de contrato, incluyendo el detalle de su cobertura, de los equipos de seguridad perimetral. Dicho documento deberá estar dirigido a la Dirección de Infraestructura y Comunicaciones de la Secretaría de Administración del Gobierno del Estado de Jalisco.

Administración Dirección General de Innovación Tecnológica Gubernamental
14 OCT. 2026
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

Está hoja forma parte del anexo técnico validado por parte de la Dirección General de Innovación Tecnologíca Gubernamental Servicio (35-101-2026 - PÓLIZA DE SOPORTE TÉCNICO Y MANTENIMIENTO A LA INFRAESTRUCTURA DE RED SEGURA DEL GEJ).

Especificaciones del Contrato:

Tipo de Contrato:	Abierto ( ) | Cerrado (X)
Forma de Entrega:	**UNA SOLA EXHIBICIÓN (X)** **PARCIALIDADES ( )**
Tiempo y Lugar de Entrega:	**Tiempo de entrega:** A partir de la firma del contrato **Lugar de Entrega:** Almacen de Parcialidades de la Secretaría de Administración ubicada en Av. Prol. Alcalde 1221, Mirafiores, 44266 Guadalajara, Jal.
Tipo de Adjudicación:	(X) A un Solo Proveedor | ( ) Por Partida | ( ) Abastecimiento Simultaneo
Metodo de evaluación	Binario

FIN ANEXO 1

ANEXO 2 – Manifiesto de Personalidad

Número de Licitación:

Título de la Licitación:

Nombre o denominación del participante:

Nombre del representante o apoderado (si aplica):

Declaro bajo protesta de decir verdad que cuento con las facultades suficientes para comprometerme en el acto de presentación y apertura de proposiciones de la presente licitación Pública.

Atentamente.

Fecha

_____

(Nombre y firma autógrafa del licitante o Representante Legal).

[1]*Este documento no hace las veces de poder.*
[2]*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 lo dispuesto en el artículo 59 numeral 1 fracciones VI y VIII de la Ley de Compras Gubernamentales, Enajenaciones y Contrataciones de Servicios del Estado de Jalisco y sus Municipios.*

ANEXO 3 – ÍNDICE DE LA PROPOSICIÓN

PROPUESTA			
Número	***NOMBRE DEL DOCUMENTO***	INTEGRAR A PROPOSICIÓN IMPRESA	FORMATO DIGITAL
1	Propuesta Técnica	SI	NO
2	ANEXO 3 – Índice de la Proposición	SI	NO
3	ANEXO 4 - Acreditación del Licitante	SI	NO
4	ANEXO 5 – Propuesta Económica	SI	SI (EXCEL)
5	ANEXO 6 – Declaraciones del Licitante	SI	NO
6	ANEXO 7 – Aportación 5 al Millar	SI	NO
7	ANEXO 8 – Declaración de Estratificación	SI	NO
8	ANEXO 9 - Listado de miembros	SI	NO
9	ANEXO 10 - Manifestación de Cumplimiento de Obligaciones Fiscales.	SI	NO
10	ANEXO 11 - Manifiesto de cumplimiento obligaciones en materia de Seguridad Social	SI	NO
11	ANEXO 12 – Formato de Muestras Físicas ***(Cuando aplique)***	SI	NO
12	Constancia de Visita de Campo ***(Cuando aplique).***	SI	NO
DOCUMENTOS PÚBLICOS			
13	Opinión del cumplimiento de obligaciones fiscales en materia de seguridad social (Ante el IMSS)	SI	NO
14	Acuse de autorización al IMSS para hacer público el resultado de la consulta de su opinión del cumplimiento de obligaciones fiscales en materia de seguridad social.	SI	NO
15	Opinión del cumplimiento de obligaciones fiscales (Ante el SAT)	SI	NO
16	Constancia de Situación Fiscal (SAT)	SI	NO
17	Constancia de Situación Fiscal en Materia de Aportaciones Patronales y Entero de Descuentos ante INFONAVIT	SI	NO
18	Copia de INE.	SI	NO

Declaro que acepto íntegramente las Bases y me comprometo a cumplir con sus disposiciones. Reconozco que el incumplimiento de las mismas podrá acarrear las sanciones correspondientes, incluyendo descalificación o exclusión del proceso. Asimismo, eximo a la Dirección de cualquier responsabilidad sobre la veracidad de la información proporcionada por los proveedores.

TOTAL DE PÁGINAS DE LA PROPOSICIÓN_____ Fecha:_____

_____

Nombre y firma del representante o Licitante.

ANEXO 4 – "Acreditación del Participante "

Yo_____, manifiesto **BAJO PROTESTA DE DECIR VERDAD**, que los datos aquí asentados son ciertos, así como que cuento con facultades suficientes para suscribir la proposición de la presente Licitación, a nombre y representación de quien firma el presente documento, por lo que en caso de **falsear** información, datos o documentos a lo largo de la proposición acepto que se apliquen las medidas disciplinarias tanto a mí como a mí representada, en los términos de la ley de la materia, incluyendo el desechamiento de la proposición en la presente licitación y que la sancione a mi representada de acuerdo a los artículos 107 del reglamento y 110, 116, 117 y 118 de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

DATOS DEL PARTICIPANTE	
Nombre del Participante:	
Domicilio: (Calle, Número exterior - interior, Colonia, Municipio, Entidad Federativa, Código Postal)	
RFC:	
Teléfono (s):	
Correo Electrónico:	
Requisitarse este recuadro únicamente por Personas Jurídicas:	
Número de Escritura Pública: _____ **Notario No.** _____ **de** _____.	
Folio Mercantil: _____ **Fecha y lugar de expedición:** _____	**En caso de contar con registro de proveedores Vigente, indicar numero de proveedor y con esto se verifica la acreditación de la empresa:** _____
Requisitarse este recuadro únicamente por Personas Físicas:	
Tipo de Identificación Oficial Vigente:_____ **Número de registro de Identificación Oficial Vigente:** _____	
Para Personas Físicas o Jurídicas que comparezcan a través del Representante	
REPRESENTACIÓN	**Para Personas Físicas o Jurídicas** que comparezcan a través del Representante, con **Facultades Generales o Especiales para Actos de Administración o de Dominio**, que les faculte para comparecer a la presente Licitación y a la firma del contrato que resulte del mismo
Número de Escritura Pública: **Tipo de representación:** **Nombre del Fedatario Público**: **Lugar y fecha de expedición:**	

Nombre del participante:_____ Fecha:_____/_____/_____

Firma:_____ Nombre del representante: _____

ANEXO 5 – Propuesta Económica

Nombre o Razon Social: _____

PARTIDA	CANTIDAD	U.M	DESCRIPCION	MARCA / MODELO	PRECIO UNITARIO	IMPORTE
				SUBTOTAL		
				IVA		
				TOTAL		

Condiciones de pago:
Tiempo de Entrega:
Garantia:

_____
Nombre y firma del representante o Licitante.

Fecha de firma:_____/_____/_____ lugar de firma:_____

"ANEXO 6 – "Declaraciones del Participante"

Declaración de aceptación de bases.

Por medio de la presente, acepto que he leído todo el contenido de las presentes bases de licitación. Entiendo y acepto cada uno de los puntos establecidos en el documento. Declaro que toda la información que proporcionó es verídica y acepto que de mentir o falsear información asumiré lo que la ley determine.

Declaración de tiempos, calidad y precio fijo.

Manifiesto que en caso de ser adjudicado de entregar los servicios solicitados: me comprometo a cumplir de acuerdo con las necesidades y tiempos de la Dependencia solicitante de los mismos. Así como de mantener el precio de los bienes ofertados y en caso de resultar adjudicado cubrir cualquier eventualidad. Y de la calidad de los servicios ofertados contra vicios ocultos del bien o servicio que ofrecen, y me comprometo a responder por ellos.

Declaración de no colusión.

De conformidad con los artículos 59 punto 1 fracción IX de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios, 183 y 187 de su Reglamento; me presentó a realizar la Declaración de Integridad y No Colusión, por tal motivo, manifiesto BAJO PROTESTA DE DECIR VERDAD, que me comprometo de abstenerse de adoptar conductas que induzcan a los servidores públicos a alterar las evaluaciones de las proposiciones técnicas y económicas en el presente proceso de licitación, a alterar el resultado del procedimiento de contratación pública de que se trate, u otros aspectos que otorguen condiciones más ventajosas, en igualdad de circunstancias, a determinada persona en relación con los demás participantes en el procedimiento de mérito o a incitar la celebración de acuerdos colusorios.

Asimismo, me comprometo a no incitar a los servidores públicos a que incumplan con los principios rectores y valores que rigen su actuación en el ejercicio de su empleo, cargo o comisión, tales como disciplina, legalidad, objetividad, profesionalismo, honradez, lealtad, imparcialidad, integridad, rendición de cuentas, eficacia, eficiencia, equidad, transparencia, economía, competencia por mérito, confidencialidad, respeto a la dignidad humana y a la equidad de género, compromiso, cooperación, honestidad, liderazgo, rendición de cuentas, responsabilidad, solidaridad, tolerancia, vocación de servicio e igualdad de trato y oportunidades, inclusión y no discriminación, previstos en el artículo 5 de la Ley General del Sistema Nacional Anticorrupción.

Declaración de no conflicto de interés particular de acuerdo al art. 52. de la Ley

En cumplimiento al artículo 49, fracción IX, de la Ley General de Responsabilidades Administrativas, manifiesto bajo protesta de decir verdad que (el o la) que suscribe, así como los socios o accionistas que ejercen control sobre la sociedad (en caso de que sea persona jurídica), no desempeñar empleo, cargo o comisión en el servicio público y, en caso de desempeñarlo, no se actualiza ningún conflicto de interés con la formalización del contrato en caso de resultar adjudicado.

Además, manifiesto bajo protesta de decir verdad que no me encuentro en alguno 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.

Declaración Constancia de proveedores.

Por medio de la presente declaración, expresó que actualmente (Si/No) _____ Me encuentro registrado ante el padrón de proveedores. En caso de no contar con el registro activo, acepto que tengo 5 días a partir del fallo para registrarme.
En caso de contar con registro, favor de proporcionar el numero: _____

Declaración de Veracidad de Documental y No Edición de Anexos.

Declaro bajo protesta de decir verdad que la totalidad de los documentos presentados en el marco de la Ley, incluyendo propuestas técnicas, documentos públicos y legales, certificaciones, contratos y cualquier otra documentación requerida, son auténticos, veraces, y reflejan fielmente la información original emitida por las autoridades o entidades correspondientes. Asimismo, manifiesto que ninguno de los documentos ni de los anexos presentados ha sido alterado, editado o modificado en su contenido.

Me comprometo a asumir la responsabilidad legal que pudiera derivarse de cualquier falsedad o inexactitud en los documentos proporcionados, en términos de la legislación aplicable.

Nombre o Denominación del Participante: _____

_____

firma del Representante legal o Participante.

ANEXO 7

(NÚMERO Y NOMBRE DEL PROCESO)

CARTA DE ACEPTACIÓN A LA APORTACIÓN CINCO AL MILLAR PARA FONDO IMPULSO JALISCO.

El/La suscrito/a _____**(nombre de persona física o jurídica)**, por mi propio derecho, en mi carácter de _____, en cumplimiento al artículo 59, numeral 1, fracción XVI, y 145 numeral 1 Fracción I de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios, manifiesto mediante la declaración escrita de mi representada, en la cual, hago constar que_____(ACEPTO/NO ACEPTO) la aportación cinco al millar del contrato que sea adjudicado (0.5%) antes de IVA para ser aportado al Fondo Impulso Jalisco.

Atentamente
Lugar y fecha

_____
(Nombre y firma autógrafa de la persona física)

ANEXO No. 8

ESTRATIFICACIÓN

Me refiero al procedimiento de **Licitación Pública**, 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, son infracciones previstas por los artículos 116, 117 y 118 de la Ley y los diversos numerales 155 al 161 de su Reglamento, así como los artículos 69 y 81 de la Ley General de Responsabilidades Administrativas de aplicación supletoria.

_____

A T E N T A M E N T E
Nombre y firma del licitante o representante.

Quien manifiesta bajo protesta de decir verdad, que a esta fecha el mandato con el que se ostenta no le ha sido modificado o revocado, y que por tanto la cotización es cierta y actual.

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.

ANEXO 9. LISTADO DE MIEMBROS Y REPRESENTANTES

Yo, **(Representante Legal)**, manifiesto **BAJO PROTESTA DE DECIR VERDAD,** que los datos aquí asentados son ciertos y actuales a la fecha de la participación y han sido debidamente verificados, así como que ninguno de sus administradores, socios, accionistas, asociados, miembros o apoderados, se han desempeñado, colaborado o representado bajo cualquier modalidad, para alguna de las demás empresas, sociedades, asociaciones, agrupaciones, o proveedores en general, que participan dentro del procedimiento de adquisición de bienes y/o contratación de servicios que nos ocupa, en al menos los 02 dos últimos años a la fecha de comenzar su participación en el mismo, por lo que de incurrir en falsedad. **Se hará acreedor a las penas que las leyes que concurran al caso lo establezcan.**

DATOS DE LA PERSONA FÍSICA		
Nombre:		
Documento que acredita la actividad empresarial		
Domicilio Fiscal:	(Calle, Número exterior e interior, Colonia, Ciudad, Estado, Código Postal).	
Ciudad y Entidad Federativa:		
DATOS DE LA EMPRESA (PERSONA MORAL)		
Nombre de la empresa:		
Registro Federal de Contribuyentes (RFC):		
Domicilio Fiscal:	(Calle, Número exterior e interior, Colonia, Ciudad, Estado, Código Postal).	
Ciudad y Entidad Federativa:		
Número de Escritura Pública y folio mercantil:	(En la que consta su Acta Constitutiva y sus modificaciones si las hubiera)	
Fecha y lugar de expedición:		
Nombre del Fedatario Público		
LISTADO DE MIEMBROS Y REPRESENTANTES ACTUALES		
Administrador(es) de la empresa (1)(2)(3):		
Representante(s) legal(es) de la empresa (1)(2)(3):		
Apoderado(s) legal(es) de la empresa (1)(2)(3):		
Socios y accionistas (1)(2)(3): A efecto de cumplir con los principios constitucionales de máxima publicidad y rendición de cuentas, para el caso que los socios o accionistas de la empresa participante, sean a su vez, personas morales, también se deberá señalar quiénes son los socios y accionistas de esa sociedad, y así indefinidamente.		

(1). Extienda cada celda tantas veces como sea necesario.
(2). Si una misma persona funge como socio y/o administrador y/o apoderado, deberá de establecerse en cada uno de los apartados que así lo amerite.
(3). No deben incluirse aquellos que hubieran sido revocados.

El Gobierno Del Estado De Jalisco, a través de la Dirección de Abastecimiento, con domicilio en la calle Av. Fray Antonio Alcalde 1221, Miraflores, 44266, de la ciudad de Guadalajara, se informa lo siguiente:

El tratamiento de sus datos personales se realiza con fundamento en lo establecido en:

- Constitución Política de los Estados Unidos Mexicanos: artículos 6 apartado A fracción I , 108 y 109 fracción III y 134;
- Ley de Fiscalización y Rendición de Cuentas de la Federación: artículos 17 fracción XVI segundo párrafo, 24, 40 fracción V, 67 fracción II primer párrafo y 73;
- Constitución Política del Estado de Jalisco: artículos 35 Bis, fracción I, último párrafo, 91, fracción II, 106 fracción IV y 107;
- Ley General de Responsabilidades Administrativas: artículos 58 y 59.
- Ley de Responsabilidades Políticas y Administrativas del Estado de Jalisco: artículos 1, 3 fracción IX, 46 fracción II, 51, 52, 53 fracción IV;
- Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios: artículos 37 párrafos segundo y tercero, 38, 90, 107 primer párrafo, 108, 110, 116, 119 primer párrafo, 120, 121 y 123;
- Ley del Gobierno y la Administración Pública Municipal el Estado de Jalisco: artículos 67 quinquies, 67 sexies;
- Código de Gobierno Del Estado De Jalisco: artículos 205, 208 Bis, 210;
- Ley General de Transparencia: artículos 1 primer párrafo, 116, 120, fracción IV,
- Adhesión del Estado Mexicano al Grupo de Acción Financiera [1]
- Ley General de Sociedades Mercantiles: artículos 73 y 129.
- 4° Plan de Acción 2019 – 2021 del Comité Coordinador de la Alianza para el Gobierno Abierto en México: compromiso número 11.
- Acuerdo ACT-PUB/31/08/2022.07 del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Los datos personales que serán recabados son los siguientes:

- Nombre completo de las personas físicas que tengan algún nivel de propiedad o control sobre la entidad moral.
- Registro Federal de Contribuyentes.
- Domicilio fiscal.
- Actividad empresarial.
- Descripción del control y/o propiedad que tienen la parte interesada en la empresa participante.
- Nombre completo de las personas morales que tengan algún nivel de propiedad o control sobre la empresa participante.
- Nombre completo de las personas físicas que tengan algún nivel de propiedad o control sobre la persona moral que tenga algún nivel de propiedad o control sobre la empresa participante.

Los datos mencionados podrán ser recabados, de manera directa o indirectamente, tanto de forma física como electrónica y serán utilizados única y exclusivamente para las siguientes finalidades:

[1] https://www.fatf-gafi.org/content/dam/fatf-gafi/annual-reports/1999%202000%20ENG.pdf

- Impulsar estrategias de rendición de cuentas y combate a la corrupción en los procesos de adjudicación y contratación de obra pública; y contrataciones en procesos de adquisiciones y servicios;
- Publicación de información relacionadas a Actas, aperturas o Fallos en las plataformas de transparencia.

Se le informa que con la aceptación del presente aviso de privacidad, se entiende que otorga su consentimiento tácito para que se transfieran sus datos personales a terceros, los terceros receptores pueden ser: las autoridades jurisdiccionales; otras autoridades administrativas la Auditoría Superior de la Federación y la Auditoría Superior del Estado de Jalisco, la Contraloría del Estado de Jalisco, Fiscalía del Estado de Jalisco, la Fiscalía Especializada en Combate a la Corrupción el Ministerio Público Federal, las Secretarías, Órganos Internos de Control, o Tribunales al Tribunal de Justicia Administrativa, al Comité Coordinador de los Sistemas Nacional y Estatal de Anticorrupción Servicio de Administración Tributaria y la Comisión Nacional Bancaria y de Valores.

Ejercicio de los Derechos Arco

Usted tiene derecho a solicitar en cualquier tiempo el Acceso, Rectificación, Cancelación, Oposición o Revocación del consentimiento del uso de sus datos personales, mediante la presentación de una solicitud de ejercicio de derechos ARCO a esta dirección.

El presente aviso de privacidad puede sufrir modificaciones y/o actualizaciones incluyendo modificaciones a las políticas de privacidad que se susciten. Cualquier cambio en el presente aviso de privacidad se hará del conocimiento de los titulares de la información confidencial.

Fecha de actualización: Diciembre 2024.

Atentamente

_____

Nombre y firma autógrafa del representante legal

Nombre de la empresa participante

ANEXO 10.- Manifestación de Cumplimiento de Obligaciones Fiscales.

_____ con RFC _____, manifiesto bajo protesta de decir verdad que tal como lo señala la opinión de cumplimiento en materia fiscal, adjunto a la presente propuesta, no me encuentro en ninguno de los supuestos de incumplimiento de mis obligaciones fiscales, establecidos por el artículo 32-D del Código Fiscal de la Federación, el cual a la letra señala:

Artículo 32-D. Cualquier autoridad, ente público, entidad, órgano u organismo de los poderes Legislativo, Ejecutivo y Judicial, de la Federación, de las entidades federativas y de los municipios, órganos autónomos, partidos políticos, fideicomisos y fondos, así como cualquier persona física, moral o sindicato, que reciban y ejerzan recursos públicos federales, en ningún caso contratarán adquisiciones, arrendamientos, servicios u obra pública con las personas físicas, morales o entes jurídicos que:

I. Tengan a su cargo créditos fiscales firmes.

II. Tengan a su cargo créditos fiscales determinados, firmes o no, que no se encuentren pagados o garantizados en alguna de las formas permitidas por este Código.

III. No se encuentren inscritos en el Registro Federal de Contribuyentes.

IV. Habiendo vencido el plazo para presentar alguna declaración, provisional o no, así como aquellas declaraciones correspondientes a retenciones y con independencia de que en la misma resulte o no cantidad a pagar, ésta no haya sido presentada. Lo dispuesto en esta fracción también aplicará a la falta de cumplimiento de cualquier otra declaración informativa, que establezca el Servicio de Administración Tributaria mediante reglas de carácter general.

V. Estando inscritos en el registro federal de contribuyentes, se encuentren como no localizados.

VI. Tengan sentencia condenatoria firme por algún delito fiscal. El impedimento para contratar será por un periodo igual al de la pena impuesta, a partir de que cause firmeza la sentencia.

VII. No hayan desvirtuado la presunción de emitir comprobantes fiscales que amparan operaciones inexistentes o transmitir indebidamente pérdidas fiscales y, por tanto, se encuentren en los listados a que se refieren los artículos 69-B, cuarto párrafo o 69-B Bis, noveno párrafo de este Código.

VIII. Hayan manifestado en las declaraciones de pagos provisionales, retenciones, definitivos o anuales, ingresos y retenciones que no concuerden con los comprobantes fiscales digitales por Internet, expedientes, documentos o bases de datos que lleven las autoridades fiscales, tengan en su poder o a las que tengan acceso.

IX. Incumplan con las obligaciones establecidas en los artículos 32-B Ter y 32-B Quinquies de este Código.

La prohibición establecida en este artículo no será aplicable a los particulares que se encuentren en los supuestos de las fracciones I y II de este artículo, siempre que celebren convenio con las autoridades fiscales en los términos que este Código establece para cubrir a plazos, ya sea como pago diferido o en parcialidades, los adeudos fiscales que tengan a su cargo con los recursos que obtengan por enajenación, arrendamiento, servicios u obra pública que se pretendan contratar y que no se ubiquen en algún otro de los supuestos contenidos en este artículo.

Para estos efectos, en el convenio se establecerá que los sujetos a que se refiere el primer párrafo de este artículo retengan una parte de la contraprestación para ser enterada al fisco federal para el pago de los adeudos correspondientes.

Cuando se ubiquen en los supuestos de las fracciones III, IV y VIII, los particulares contarán con un plazo de quince días para corregir su situación fiscal, a partir del día siguiente a aquél en que la autoridad les notifique la irregularidad detectada.

Los proveedores a quienes se adjudique el contrato, para poder subcontratar, deberán solicitar y entregar a la contratante la constancia de cumplimiento de las obligaciones fiscales del subcontratante, que se obtiene a través de la página de Internet del Servicio de Administración Tributaria.

Los contribuyentes que requieran obtener la opinión del cumplimiento de obligaciones fiscales para realizar alguna operación comercial o de servicios, para obtener subsidios y estímulos, para realizar algún trámite fiscal u obtener alguna autorización en materia de impuestos internos, incluyendo los de comercio

exterior, así como para las contrataciones por adquisición de bienes, arrendamiento, prestación de servicio y obra pública que vayan a realizar con los sujetos señalados en el primer párrafo de este artículo, deberán hacerlo mediante el

procedimiento que establezca el Servicio de Administración Tributaria y las autoridades fiscales federales en materia de seguridad social, a través de las reglas de carácter general.

Para participar como proveedores de los sujetos señalados en el primer párrafo de este artículo, los contribuyentes estarán obligados a autorizar al Servicio de Administración Tributaria y a las autoridades fiscales federales en materia de seguridad social, para que hagan público el resultado de la opinión del cumplimiento, a través del procedimiento que establezcan dicho órgano desconcentrado y autoridades fiscales federales, mediante reglas de carácter general, además de cumplir con lo establecido en las fracciones anteriores.

Robusteciendo lo anterior, manifiesto bajo protesta de decir verdad que no me encuentro en ninguno de los supuestos de incumplimiento establecidos en los numerales 5, 6 y 7 de la Regla 2.1.36 de la Resolución Miscelánea para el ejercicio fiscal 2026, o bien, encontrándome dentro de cualquiera de éstos, el contribuyente, con RFC _____, cuento con:

1. Cuento con autorización emitida por la autoridad fiscal para pagar a plazos, sin que esta me haya sido revocada.
2. Me encuentro dentro del plazo para pagar a que se refiere el artículo 65 del Código Fiscal de la Federación.
3. Teniendo un medio de defensa en contra de un crédito fiscal determinado, éste se encuentra debidamente garantizado hasta por el interés fiscal.
4. Me encuentro pagando mis adeudos por periodo o ejercicio, en términos del segundo párrafo de la regla 2.1.49. y además que, entre la fecha de solicitud y la del primer pago, o entre cada pago realizado, no han transcurrido más de sesenta días naturales.

_____

(Nombre y firma autógrafa del licitante o Representante Legal).

ANEXO 11 - Manifiesto de cumplimiento obligaciones en materia de Seguridad Social

Guadalajara Jalisco, a de del 2026.

SECRETARÍA DE ADMINISTRACIÓN
DEL GOBIERNO DEL ESTADO DE JALISCO
PRESENTE.

AT'N: Dirección General de Abastecimientos

(Nombre completo), en mi carácter de Representante Legal de la empresa (Nombre de la Empresa), manifiesto estar al corriente de mis obligaciones fiscales en materia de Seguridad Social, por lo que anexo la Constancia de opinión positiva de cumplimiento/sin opinión de obligaciones en materia de Seguridad Social, documento vigente expedido el IMSS, de conformidad al ACUERDO número ACDO.AS2.HCT.270422/107.P.DIR dictado por el H. Consejo Técnico, en sesión ordinaria de 27 de abril del 2022

Asimismo, se informa que, se autorizó al IMSS a hacer público el resultado de la consulta de opinión del cumplimiento de obligaciones fiscales en materia de seguridad social de (nombre de la empresa/quien suscribe), de conformidad con la regla séptima del ACUERDO número ACDO.AS2.HCT.270422/107.P.DIR dictado por el H. Consejo Técnico, en sesión ordinaria de 27 de abril del 2022. Se adjunta al presente el acuse correspondiente. Dicha autorización se mantendrá activa hasta el momento que se emita resolución en el procedimiento de licitación citado a rubro, y en caso de resultar adjudicado hasta el término del contrato.

De igual manera, por virtud del presente se autoriza a la Secretaría de Administración del Gobierno del Estado de Jalisco, para que, a través de las áreas organizativas que resulten competentes, lleve a cabo la consulta en línea de la opinión del cumplimiento de las obligaciones fiscales en materia de seguridad social de (mi representada/quien suscribe).

ATENTAMENTE

_____
Nombre y firma del Licitante
o Representante Legal.

ANEXO 12 – "Formato de Muestras "

Llenar ambos recuadros con la misma información (original y acuse).

FECHA:	

12 - A - ORIGINAL

CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN DE LA MUESTRA ENTREGADA

FECHA:	

12- B - ACUSE

CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN DE LA MUESTRA ENTREGADA

NOTA: El proveedor cuenta con 10 días hábiles posteriores al fallo de la licitación, para recoger las muestras presentadas, de lo contrario la Dirección General de abastecimientos no se hace responsable de las mismas.

ANEXO 13 – "Formato de Pregunta para Junta Aclaratoria "

1. Nombre del participante:	
2. Nombre del representante legal (en caso):	
3. Número de Licitación Pública:	

BAJO PROTESTA DE DECIR VERDAD DECLARO QUE ES MI INTERÉS PARTICIPAR DEL PROCESO DE LICITACIÓN PÚBLICA EXPRESADO EN EL PUNTO 3. DEL PRESENTE ANEXO.

Preguntas
Página donde encontraste tu duda, punto específico de tu duda y pregunta.

EJEMPLO:
1.
2.
3.
4.
5.
SIN RECUADROS

_____

A T E N T A M E N T E

Nombre y firma del licitante o representante.

ANEXO 14 - Texto para Fianza

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 Y CANTIDAD CON LETRA)*** *IMPUESTOS INCLUIDOS* ***(CUANDO APLIQUE)*****. A FAVOR DE LA SECRETARÍA DE LA HACIENDA PÚBLICA** CON DOMICILIO EN CALLE PEDRO MORENO #281, GUADALAJARA CENTRO, GUADALAJARA, JALISCO CP: 44100., A EFECTO DE:

GARANTIZAR POR **(*NOMBRE DEL "PROVEEDOR"*)** CON DOMICILIO EN **(DOMICILIO COMPLETO DE ACUERDO AL REGISTRO EN PADRÓN DE PROVEEDORES)** FIEL Y EXACTO CUMPLIMIENTO DE TODAS Y CADA UNA DE LAS OBLIGACIONES PACTADAS EN EL CONTRATO **NÚMERO (ANOTAR EL NÚMERO COMPLETO INCLUYENDO LAS SIGLAS), DE FECHA (LA FECHA PLASMADA EN EL PRIMER PÁRRAFO DEL CONTRATO),** CELEBRADO ENTRE NUESTRO FIADO Y EL GOBIERNO DEL ESTADO DE JALISCO, CON UN IMPORTE TOTAL DE $ ***(CANTIDAD CON NÚMERO Y CANTIDAD CON LETRA)*** *IMPUESTOS INCLUIDOS* ***(CUANDO APLIQUE)*****.** ASÍ MISMO, SE ACEPTA SUJETARSE 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 CUMPLIMIENTO O SE CELEBRE CON ÉSTE, CUALQUIER ACUERDO MODIFICATORIO AL CONTRATO PRINCIPAL.

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

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

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

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

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

ANEXO 14 A - Texto para Fianza

TEXTO DE LA FIANZA DE ANTICIPO

(***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 Y CANTIDAD CON LETRA)*** *IMPUESTOS INCLUIDOS* ***(CUANDO APLIQUE)*****. A FAVOR DE LA SECRETARÍA DE LA HACIENDA PÚBLICA** CON DOMICILIO EN CALLE PEDRO MORENO #281, GUADALAJARA CENTRO, GUADALAJARA, JALISCO CP: 44100., A EFECTO DE:

GARANTIZAR POR (***NOMBRE DEL PROVEEDOR***) CON DOMICILIO EN **(DOMICILIO COMPLETO DE ACUERDO AL REGISTRO EN PADRÓN DE PROVEEDORES)** LA DEBIDA INVERSIÓN O DEVOLUCIÓN TOTAL EN SU CASO, DEL ANTICIPO QUE POR IGUAL SUMA RECIBIRÁ DE LA BENEFICIARIA DE ESTA FIANZA, A CUENTA DEL ***(ESTABLECER EL PORCENTAJE SOLICITADO)*** DEL IMPORTE TOTAL DEL CONTRATO **NÚMERO (ANOTAR EL NÚMERO COMPLETO INCLUYENDO LAS SIGLAS), DE FECHA (LA FECHA PLASMADA EN EL PRIMER PÁRRAFO DEL CONTRATO)** CELEBRADO ENTRE NUESTRO FIADO Y EL GOBIERNO DEL ESTADO DE JALISCO, CON UN IMPORTE TOTAL DE ***$ (CANTIDAD CON NÚMERO Y CANTIDAD CON LETRA)*** *IMPUESTOS INCLUIDOS* ***(CUANDO APLIQUE)*****.**

ASÍ MISMO, SE ACEPTA SUJETARSE 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 CUMPLIMIENTO O SE CELEBRE CON ÉSTE, CUALQUIER ACUERDO MODIFICATORIO AL CONTRATO PRINCIPAL, ESTA FIANZA ESTARÁ EN VIGOR A PARTIR DE LA FECHA DEL CONTRATO Y HASTA EN TANTO SE AMORTICE EL ANTICIPO SEÑALADO EN EL MISMO O ESTE SEA DEVUELTO A ENTERA SATISFACCIÓN DE LA SECRETARÍA DE LA HACIENDA PÚBLICA Y SÓLO PODRÁ SER CANCELADA CON LA PRESENTACIÓN POR PARTE DE NUESTRO FIADO, DE LA ORIGINAL DE LA MISMA.

EN EL CASO QUE SE OTORGUE PRÓRROGA AL CONTRATO, ASÍ COMO DURANTE LA SUSTANCIACIÓN DE TODOS LOS RECURSOS LEGALES, JUICIOS QUE SE INTERPONGAN O INCONFORMIDADES DE LOS BIENES Y/O SERVICIOS CONTRATADOS ESTA FIANZA CONTINUARÁ VIGENTE HASTA QUE SE DICTE RESOLUCIÓN DEFINITIVA.

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 ACOMPAÑADO A SU ESCRITO DE RECLAMO LOS DOCUMENTOS QUE COMPRUEBEN LA EXISTENCIA Y EXIGIBILIDAD DE LA OBLIGACIÓN GARANTIZADA EN TÉRMINOS DEL **ARTÍCULO 279** DE LA LEY CON INDEPENDENCIA DE LO ANTERIOR, LA INSTITUCIÓN TENDRÁ DERECHO A SOLICITAR AL BENEFICIARIO TODO TIPO DE INFORMACIÓN O DOCUMENTACIÓN QUE SEAN NECESARIAS RELACIONADAS CON LA FIANZA MOTIVO DE LA RECLAMACIÓN EN TERMINACIÓN DEL MISMO NUMERAL. =FIN DE TEXTO=

"ANEXO 15 – “Poder"

Poderdante (quien concede el poder): _____
Apoderado (quien recibe el poder):

fecha: _____
Lugar: _____

Para Dirección de Abastecimientos.

El suscrito poderdante, bajo protesta de decir verdad, que cuenta con facultades suficientes para comprometerse por sí o por su representada, sin que resulte necesario acreditar su personalidad jurídica; manifiesta mexicano por nacimiento, persona física, con plena capacidad para contratar, suscribo esta carta poder que se otorga en los términos de lo dispuesto por los artículos 2551 y 2554 del Código Civil Federal, así mismo, en favor de la siguiente persona, denominada como apoderado.

El presente poder se otorga de manera amplia y bastante, a fin de que la persona referida previamente, comparezcan de manera individual o conjunta, ante esta honorable autoridad, para que cumplan con el siguiente objeto:

Acudir ante la Dirección de Abastecimientos para presentar la propuesta de Licitación Pública en nombre y representación del poderdante.

PODERDANTE
Quien otorga el poder.

APODERADO
Quien recibe el poder.