LICITACIÓN PÚBLICA ELECTRÓNICA DE CARÁCTER NACIONAL

N° LA-27-514-027000002-N-232-2024

"SUMINISTRO, INSTALACIÓN Y CONFIGURACIÓN DE SOLUCIONES DE SEGURIDAD INFORMÁTICA PARA LA SFP"

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

GLOSARIO

Además de las definiciones contenidas en los artículos 2 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 2 de su Reglamento, se entenderán por:

Secretaría, SFP o Convocante:	Secretaría de la Función Pública.
Acuerdo:	Acuerdo por el que se establecen las Disposiciones que se deberán observar para la Utilización del Sistema Electrónico de Información Pública Gubernamental Denominado CompraNet.
LAASSP o Ley:	Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
POBALINES:	Políticas, bases y lineamientos en materia de adquisiciones, arrendamientos y servicios de la Secretaría de la Función Pública.
RLAASSP o Reglamento:	Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
SAT:	Servicio de Administración Tributaria.
IMSS:	Instituto Mexicano del Seguro Social.
INFONAVIT:	Instituto del Fondo Nacional de la Vivienda para los Trabajadores.
OIC:	Órgano Interno de Control de la Secretaría de la Función Pública.
Proveedor:	La persona que celebre contratos de adquisiciones, arrendamientos o servicios.
Licitante:	La persona que participe en cualquier procedimiento de Licitación Pública o bien de Invitación a Cuando Menos Tres Personas.
SHCP	Secretaría de Hacienda y Crédito Público.
TESOFE	Tesorería de la Federación.
I.V.A.	Impuesto al valor Agregado
MFIJ	Módulo de Formalización de Instrumentos Jurídicos

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

APARTADO I. DATOS GENERALES O DE IDENTIFICACIÓN DE LA LICITACIÓN

1. DATOS GENERALES DE LA LICITACIÓN: Nombre de la Convocante, área contratante y domicilio

La SFP como área convocante, en cumplimiento a las disposiciones que establecen el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos; 26 fracción I, 26 Bis fracción II, 27, 28 fracción I, 29 y 30 de la Ley; así como el 39 del Reglamento, en los numerales V.10., Subnumeral V.10.1, base B. y V.11., Subnumeral V.11.1, lineamiento a. inciso 6 de las POBALINES; y demás disposiciones relativas vigentes aplicables en la materia, a través de la Dirección General de Recursos Materiales y Servicios Generales, por conducto de la Dirección de Planeación y Adquisiciones en su carácter de Área Contratante, con domicilio en Avenida de los Insurgentes Sur número 1735, mezanine, ala sur, colonia Guadalupe Inn, Alcaldía Álvaro Obregón, código postal 01020, Ciudad de México, con número telefónico 55 20003000, convoca a los interesados, a participar en la Licitación Pública Electrónica de carácter Nacional, para la contratación del **"Suministro, Instalación y Configuración de Soluciones de Seguridad para la SFP".**

Ninguna de las condiciones contenidas en la presente Convocatoria, así como en las proposiciones presentadas por los licitantes podrán ser negociadas.

1.2. Medio y carácter de la Licitación

Los Licitantes podrán participar en forma electrónica en la o las juntas de aclaraciones, el Acto de presentación y apertura de proposiciones y el Acto de Fallo, conforme al Acuerdo, publicado en el Diario Oficial de la Federación el 28 de junio del año 2011.

Esta licitación tiene carácter nacional electrónica, por lo que, en la presente Licitación Pública únicamente se permitirá la participación de los licitantes a través de la plataforma integral **CompraNet.**

1.3. Número de la Licitación

El número de la presente Licitación es LA-27-514-027000002-N-232-2024.

El número de control interno es LPN-015/2024.

1.4. Vigencia del contrato

La vigencia del contrato será a partir del día hábil siguiente a la notificación del fallo y hasta el 31 de diciembre 2024.

La vigencia de las licencias para cada solución propuesta será de doce meses contados a partir del día siguiente de la conclusión de la puesta a punto y aprobación por parte de la SFP.

1.5. Ejercicio Fiscal de la contratación

Esta contratación se realizará con recursos del ejercicio 2024.

1.6. Idioma de las proposiciones

Los licitantes deberán elaborar y enviar su proposición en idioma español.

1.7. Disponibilidad Presupuestaria

Para cubrir las erogaciones que se deriven de la presente Licitación, la Convocante cuenta con la suficiencia presupuestal en la **partida 32701 "Suministro, Instalación y Configuración de Soluciones de Seguridad para la SFP"** como se hace constar mediante la **Suficiencia Presupuestal 3100044668** de **fecha 09 de mayo de 2024**, autorizada por la Dirección General de Programación y Presupuesto, de conformidad con los artículos 24 y 25 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

1.8. Contratación financiada con créditos externos

El presente procedimiento de contratación no será financiado con fondos provenientes de créditos externos otorgados al Gobierno Federal, ni con la garantía de organismos financieros regionales o multilaterales.

1.9. Servidores Públicos Responsables del Procedimiento.

Los actos que se deriven del presente procedimiento de Licitación, podrán ser presididos por María de la Luz Padilla Díaz, Directora General de Recursos Materiales y Servicios Generales, o por el servidor público que designe, pudiendo recaer indistintamente, en Ambrosio Rene Oliva Delgado, Director de Planeación y Adquisiciones o en Aída Camacho Guerrero, Subdirectora de Adquisiciones, así como suscribir documentos en los actos inherentes al procedimiento y de aquellos relacionados con el mismo. Lo anterior de conformidad a lo establecido en el numeral V.10., Subnumeral V.10.1 y base C. de las POBALINES.

1.10. Igualdad de género

A fin de dar cumplimiento a la Norma Mexicana para la Igualdad Laboral entre Mujeres y Hombres (NMX-R-025-SCFI-2015), en todos los casos donde se utilice un lenguaje que pudiera interpretarse como excluyente al género femenino, invariablemente deberá interpretarse y entenderse como incluyente e igual tanto para hombres como para mujeres.

APARTADO II. OBJETO Y ALCANCE DE LA LICITACIÓN

DESCRIPCIÓN DEL SERVICIO

1. Objeto de la Licitación

La presente Licitación tiene como objeto llevar a cabo la contratación del **"Suministro, Instalación y Configuración de Soluciones de Seguridad para la SFP",** de acuerdo con lo solicitado en las Especificaciones Técnicas y Alcances del Servicio que se describen en el **ANEXO I** de la presente Convocatoria.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

a. Agrupación de Partidas.

No Aplica.

b. Precio Máximo de Referencia.

No Aplica.

c. Normas Oficiales Vigentes.

No Aplica

d. Pruebas.

El proveedor deberá cumplir con las pruebas descritas en el numeral 4 METODOLOGÍA Y PLAN DE TRABAJO, sección 4.1 Metodología, numeral **4.1.3. Pruebas y validación.**

e. Tipo de Contratación.

La contratación se hará mediante contrato cerrado de acuerdo con los términos establecidos en el artículo 45 de la LAASSP.

f. Modalidad de Contratación.

No Aplica

g. Forma de Adjudicación.

La adjudicación se realizará por partida única **A UN SOLO LICITANTE** que cumpla con todos **los requisitos legales, técnicos y económicos** establecidos en la Convocatoria y garantice el cumplimiento de las obligaciones respectivas, conforme al **ANEXO I**, y además **oferte el precio más bajo.**

h. Modelo de contrato

El modelo de contrato, será de conformidad al **ANEXO III "Modelo de Contrato"** que forma parte integrante de esta Convocatoria, el cual podrá ser modificado y/o adecuado sin limitación alguna por parte de la Convocante, a fin de ser ajustado a las características y especificaciones que considere pertinentes para la formalización del Licitante que resulte adjudicado y cumplirá con lo dispuesto por los artículos 29, fracción XVI y 5 de la LAASSP y 39, fracción II inciso i) y 81 de su Reglamento.

En caso de discrepancia entre el contenido en el modelo de Contrato y el de la presente Convocatoria, prevalecerá lo establecido en la Convocatoria y sus juntas de aclaraciones.

APARTADO III. FORMA Y TÉRMINOS QUE REGIRÁN LOS DIVERSOS ACTOS DEL PROCEDIMIENTO

1. FORMA Y TÉRMINOS QUE REGIRÁN LOS DIVERSOS ACTOS DE ESTE PROCEDIMIENTO

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

Este procedimiento se efectuará de conformidad con lo previsto en el Título Segundo "De Los Procedimientos de Contratación", Capítulo Segundo "de la Licitación Pública" de la Ley, y los correlativos aplicables del Reglamento.

1.1 Reducción de plazos

El plazo que se deberá considerar es el establecido en el segundo párrafo del artículo 32 de la Ley, por lo que en esta licitación **NO** se contempla la reducción de plazos.

1.2 Eventos del procedimiento

Esta Licitación es electrónica por lo que se señala la fecha y hora en las que se llevarán los actos del procedimiento. a través de la plataforma integral CompraNet:

ACTO	FECHA	HUSO HORARIO DE LA CD. DE MÉXICO	LUGAR
Publicación de Convocatoria.	16 de mayo de 2024		Plataforma Integral CompraNet
Recepción de preguntas sobre el contenido de la Convocatoria por CompraNet.	03 de junio de 2024	09:30 HRS.	Se llevarán a cabo sin la presencia de los licitantes en la sala de juntas de la Dirección General de Recursos Materiales y Servicios Generales ubicada en Avenida de los Insurgentes Sur 1735, mezzanine, ala sur, tercer cuadrante, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Código Postal 01020, Ciudad de México
Junta de Aclaraciones	04 de junio de 2024	09:30 HRS.	
Presentación y Apertura de Proposiciones	11 de junio de 2024	10:30 HRS.	
Fallo	13 de junio de 2024	10:00 HRS.	
Firma del Contrato	Dentro de los 15 posteriores a la notificación del fallo	09:00 a 18:00 HRS.	

Todos los actos se realizarán de conformidad con lo establecido en el artículo 26 Bis, fracción II de la LAASSP y el medio a utilizar será a través del sistema electrónico de información pública gubernamental CompraNet, https://upcp-compranet.hacienda.gob.mx.

El horario que regirá a los diferentes actos del procedimiento de licitación pública será de conformidad con la zona horaria de la Ciudad de México (UTC-6).

1.3 Lugar en donde se llevarán a cabo los actos públicos de la Licitación.

Asimismo, se hace del conocimiento de los interesados que los actos del procedimiento de esta Licitación, se llevarán a cabo en la Sala de juntas de la Dirección General de Recursos Materiales y Servicios Generales ubicada en Avenida de los Insurgentes sur 1735, mezzanine, ala sur, tercer cuadrante, colonia Guadalupe Inn, Alcaldía Álvaro Obregón, código postal 01020, Ciudad de México y,

en su caso, de conformidad con el artículo 26, penúltimo párrafo de la LAASSP, a los actos de esta Licitación podrá asistir cualquier persona que manifieste su interés por escrito para estar presente en calidad de observador, bajo la condición de que deberá registrar su asistencia e identificarse a través de identificación oficial vigente (credencial de elector, cartilla del Servicio Militar Nacional, pasaporte o cédula profesional con fotografía) y abstenerse de intervenir en cualquier forma en el desarrollo de los mismos.

Una vez iniciado cualquiera de los distintos eventos en que participen los observadores, no se permitirá el ingreso a cualquier persona, de igual forma, para la debida conducción del proceso se les informa que no podrán hacer uso de cualquier dispositivo electrónico o de comunicación durante los mismos, por lo que se les conmina a que den estricto cumplimiento a este numeral.

Asimismo, si los observadores que se encuentren presentes en el recinto donde se desarrollen los eventos deciden abandonarlo, no se les permitirá nuevamente el acceso.

1.4 . Obtención de la convocatoria.

Las personas interesadas podrán consultar la convocatoria o podrán descargarla de la plataforma integral de CompraNet en la dirección electrónica https://upcp-compranet.hacienda.gob.mx/sitiopublico/#/

1.5 Actos de la Licitación

Los actos que forman parte del procedimiento de esta Licitación Pública, se realizarán puntualmente el día, hora y lugar que se indican en esta Convocatoria, levantándose en cada uno de ellos acta circunstanciada, las cuales serán firmadas por los servidores públicos que hubieran asistido e incorporadas en la plataforma integral CompraNet en la sección de anexos, al concluir dichos actos, como se establece en el Acuerdo.

Por tratarse de un procedimiento electrónico, queda bajo la responsabilidad de los licitantes realizar su registro en la plataforma integral **CompraNet** para poder participar.

1.5.1 Visita a las Instalaciones

No aplica.

1.5.2 Junta de Aclaraciones a la Convocatoria

El primero de los actos públicos será la Junta de Aclaraciones, el cual se desarrollará en los tiempos y conforme lo establecen los artículos 33 y 33 Bis de la Ley, así como los artículos 45 y 46 del Reglamento, tratándose de una Licitación Pública Electrónica de Carácter Nacional.

Los licitantes que pretendan solicitar aclaraciones a los aspectos contenidos en la Convocatoria, deberán expresar su interés en participar en la Licitación Pública por sí o en representación de un tercero, manifestando en todos los casos los datos generales del interesado y, en su caso, del representante ***de acuerdo al FORMATO 1 "ACREDITACIÓN DE LA EXISTENCIA LEGAL Y***

PERSONALIDAD JURÍDICA DEL LICITANTE", a través del sistema CompraNet, firmando de manera electrónica y de conformidad con lo señalado en el artículo 48, fracción V del Reglamento.

Cabe señalar, que en la plataforma integral *CompraNet* emite un escrito de interés en participar, mismo que será válido para poder presentar en su caso las aclaraciones que considere el Licitante.

Las solicitudes de aclaración, deberán enviarse a través de **CompraNet,** a más tardar 24 horas antes de la fecha y hora en que se vaya a realizar la Junta de Aclaraciones, de conformidad con el penúltimo párrafo del artículo 45 del RLAASSP.

Las personas que manifiesten su interés en participar en la Licitación Pública conforme a lo antes mencionado, serán considerados licitantes y tendrán derecho a formular solicitudes de aclaración en relación con la Convocatoria a la Licitación Pública.

La Convocante tomará como hora de recepción de las solicitudes de aclaración del licitante, la que registre la plataforma integral **CompraNet** al momento de su recepción en el sistema.

Las solicitudes de aclaración deberán plantearse de manera concisa y estar directamente vinculadas con los numerales contenidos en la Convocatoria a la Licitación Pública, indicando el numeral específico con el cual se relaciona. Las solicitudes que no cumplan con los requisitos señalados, serán desechadas por la Convocante.

Las solicitudes de aclaración recibidas con posterioridad al plazo arriba señalado no serán contestadas por resultar extemporáneas, de conformidad con el artículo 46 fracción VI del Reglamento de la Ley.

La Convocante procederá a enviar a través de **CompraNet,** las respuestas a las solicitudes de aclaración recibidas a partir de la hora y fecha señaladas. Cuando en razón del número de solicitudes de aclaración recibidas o algún otro factor imputable a la Convocante y que sea acreditable, el servidor público que presida la Junta de Aclaraciones, informará a los licitantes si éstas serán enviadas en ese momento o si se suspenderá la sesión para reanudarla en hora o fecha posterior a efecto de que las respuestas sean remitidas.

Con el envío de las respuestas a que se refiere el párrafo anterior, los licitantes contarán con el plazo que para el efecto señale la Convocante en el Acta de la Junta de Aclaraciones, dicho plazo no podrá ser inferior a seis (6) ni superior a cuarenta y ocho horas (48) para formular las preguntas que consideren necesarias en relación con las respuestas remitidas, las cuales podrán ser realizadas por cualquier licitante, dicho plazo se contabilizará a partir de que se publique el Acta de la Junta de Aclaraciones en **CompraNet**. Una vez recibidas las preguntas en la plataforma integral **CompraNet,** la Convocante informará a los licitantes el plazo máximo en el que enviará las contestaciones correspondientes.

Si derivado de la o las juntas de aclaraciones se determina posponer la fecha de celebración del acto de presentación y apertura de proposiciones, la modificación respectiva será publicada en CompraNet de conformidad con el artículo 46 fracción VI del Reglamento de la Ley.

La Convocante, levantará el Acta de la Junta de Aclaraciones correspondiente, la cual será difundida a través de **CompraNet,** para efectos de notificación a los licitantes participantes. Será responsabilidad

de los licitantes enterarse del contenido de la misma, a través del medio señalado, toda vez que cualquier modificación a la Convocatoria de la Licitación, derivada del resultado de la Junta de Aclaraciones, será considerada como parte integrante de la presente Convocatoria.

1.5.3 Modificaciones a la Convocatoria

Cualquier modificación a la Convocatoria, derivada de la(s) Junta(s) de Aclaraciones, formará parte integrante de la misma y deberá ser considerada por los licitantes en la elaboración de su proposición.

Las modificaciones en ningún caso podrán consistir en la sustitución de los servicios convocados originalmente, adición de otros de distintos rubros o en variación significativa de sus características.

1.5.4 Elaboración de las proposiciones

La proposición deberá ser foliada y elaborada preferentemente en papel membretado de cada licitante. Deberán numerar de manera individual la propuesta técnica y económica, así como el resto de los documentos que entregue el licitante. El licitante deberá verificar que los documentos sean legibles; aquéllos que no lo sean, no serán objeto de análisis por la Convocante.

Las Propuestas Técnica y Económica, deberán presentarse en idioma "español" y contar con **firma autógrafa** en la última hoja de cada documento que la integre, por lo que es indispensable que todas las hojas de la propuesta técnica y económica, así como el resto de los documentos que integran la proposición, estén **foliados** en su totalidad.

Para el envío por medio de la plataforma Integral CompraNet deberá firmarse únicamente el sobre electrónico; utilizando **los medios de identificación electrónica E. FIRMA** (antes FIRMA ELECTRÓNICA) que emite el **SAT**.

La proposición se integra por la Propuesta Técnica **(ANEXO I)**, Propuesta Económica **(ANEXO II)** y la documentación distinta a la proposición **(legal-administrativa).**

La Propuesta técnica deberá contener todos los aspectos técnicos de acuerdo con el **ANEXO I** y la propuesta económica en estricto apego a lo establecido en el **ANEXO II**.

La presentación de la propuesta técnica que no cumpla con todos y cada uno de los requisitos técnicos solicitados de acuerdo con el **ANEXO I**, o con los requisitos solicitados para la elaboración de la propuesta económica conforme a lo establecido en el **ANEXO II**, así como, el incumplimiento en la presentación de alguno de los documentos distintos a la proposición (legal-administrativa) será motivo de desechamiento de la proposición.

La persona licitante sufragará todos los costos relacionados con la preparación de su proposición, por lo que la SFP no asumirá en ningún caso dichos costos, cualquiera que sea la forma en que se realice la licitación o el resultado de ésta, salvo en los casos previstos en la LAASSP.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020, Tel: (55)20-00-30-00 www.gob.mx/sfp

1.5.4.1. Documentación distinta a la proposición (legal-administrativa)

Para considerar todos los escritos debidamente requisitados, deberán contener invariablemente la firma autógrafa del representante o apoderado legal de la persona licitante, debidamente acreditado, y en su caso, cuando así se haya solicitado, la leyenda "Bajo Protesta de Decir Verdad".

1.5.4.2. Propuesta técnica (ANEXO I "ESPECIFICACIONES TÉCNICAS Y ALCANCES DEL SERVICIO").

En la propuesta técnica, se deberá describir la forma y términos en las que se proporcionará el servicio conforme al **ANEXO I "ESPECIFICACIONES TÉCNICAS Y ALCANCES DEL SERVICIO"** de la presente Convocatoria, deberá presentarse conforme a lo siguiente:

1. Deberá ser clara y precisa, detallando las características técnicas que proponga, en concordancia con lo solicitado en el **ANEXO I "ESPECIFICACIONES TÉCNICAS Y ALCANCES DEL SERVICIO"** y sus **REQUISITOS TÉCNICOS** de la presente Convocatoria. **NO** se aceptará que se indique "o similar", "cotizo de acuerdo a lo solicitado", "incluido", "descripciones genéricas", "condicionar la proposición" y/o cualquier aseveración o manifestación como las mencionadas.

2. En todos los casos, deberá ser firmada por el representante o apoderado legal de la persona licitante, debidamente acreditado, en la última hoja del documento que las contenga; por lo que no podrán desecharse cuando las demás hojas que la integran y sus anexos carezcan de firma o rúbrica, no obstante, deberá firmar aquellos documentos en los que aparezca su nombre en el espacio específico para ello.

3. Se presentará en idioma español, así como todos y cada uno de los documentos que la integran.

4. En caso de ser requerido y/o necesario, las personas licitantes deberán incluir en su propuesta técnica los catálogos, folletos, manuales o documentos en los que se aprecie el cumplimiento de las especificaciones solicitadas por la Convocante, éstos podrán ser descargados de Internet, siempre y cuando la información sea clara y legible y deberán de enviarlos en un archivo escaneando los documentos solicitados, en caso de estar en otro idioma estos deberán ir acompañados de una traducción simple al español.

1.5.4.3. Propuesta económica (ANEXO II "PROPUESTA ECONÓMICA").

La propuesta económica (se describe en el **ANEXO II** de la presente Convocatoria), deberá presentarse conforme a lo siguiente:

1. Señalar el costo mensual del servicio en Moneda Nacional, de conformidad con lo indicado en el **Anexo II "Propuesta Económica"**. Asimismo, se deberán considerar dos decimales, indicar la cantidad con número y letra, desglosando el Impuesto al Valor Agregado. En todos los casos, deberá ser firmada por la persona legalmente facultada para ello en la última hoja del documento que las contenga; por lo que no afectará la solvencia de la propuesta cuando las demás hojas que la integran y sus anexos carezcan de firma o rúbrica, por lo que no podrá desecharse por esta causa.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

2. En todos los casos, deberá ser firmada por la persona legalmente facultada para ello en la última hoja del documento que las contenga; por lo que no afectará la solvencia de la propuesta cuando las demás hojas que la integran y sus anexos carezcan de firma o rúbrica, por lo que no podrá desecharse por esta causa.

3. En caso de estar en otro idioma estos deberán ir acompañados de una traducción simple al español, así como todos y cada uno de los documentos que la integran.

4. Deberá ser clara y precisa, en concordancia con lo solicitado en el **ANEXO II** de la presente Convocatoria. **NO** se aceptará que se indique "o similar", "cotizo de acuerdo a lo solicitado", "incluido", "descripciones genéricas", "condicionar la proposición" y/o cualquier aseveración o manifestación como las mencionadas.

LAS PROPUESTAS TÉCNICAS Y ECONÓMICAS QUE NO CONTENGAN CUALQUIERA DE LOS REQUISITOS MENCIONADOS, SE VERÁN AFECTADAS EN SU SOLVENCIA Y SERÁN DESECHADAS.

1.5.4.4. Participación de licitantes de forma electrónica.

La presentación de proposiciones, de conformidad con lo establecido en los artículos 27 y 34 de la Ley, se llevará a cabo a través de medios electrónicos, conforme a las disposiciones administrativas que emita la SFP.

Las proposiciones serán enviadas a través de medios remotos de comunicación electrónica, para lo cual los licitantes deberán utilizar exclusivamente el programa informático que la SFP les proporcione. Dicho programa generará el sobre con las proposiciones mediante el uso de tecnologías que resguardan la confidencialidad de la información, de tal forma que sea inviolable.

El programa informático se encuentra disponible en la página https://upcp-compranet.hacienda.gob.mx

Lo anterior, de conformidad a la fracción II del artículo 26 Bis de la LAASSP y el Acuerdo publicado en el Diario Oficial de la Federación de fecha 28 de junio de 2011.

Las proposiciones deberán elaborarse conforme a lo señalado en esta convocatoria en formatos Word, Excel o PDF.

La proposición deberá ser firmada autógrafamente por la persona facultada para ello en la última hoja de cada uno de los documentos que forman parte de la misma, por lo que es indispensable que todas las hojas de la propuesta técnica y económica, así como el resto de los documentos que integran la proposición, estén foliados en su totalidad.

Para el envío de las proposiciones a través de medios remotos de comunicación electrónica, deberá firmarse únicamente el sobre electrónico, empleándose los medios de identificación electrónica que establezca la SHCP, esto es, por los medios de identificación electrónica **E. FIRMA**, los cuales

producirán los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.

La convocante tendrá como no presentada la proposición del licitante, cuando el archivo electrónico enviado a través de la plataforma integral CompraNet no pueda abrirse por tener algún virus informático o por cualquier causa ajena a la misma.

1.5.5. Acto de Presentación y Apertura de Proposiciones.

En el Acto de Presentación y Apertura de Proposiciones se actuará conforme a lo establecido en los artículos 34 y 35 de la Ley y 47, 48 y 50 del Reglamento, y se llevará a cabo en el día, lugar y hora previstos en la presente Convocatoria a la Licitación. el Acto de presentación y apertura de proposiciones se llevará sin la presencia de los licitantes. Una vez recibidas las proposiciones a través de la plataforma integral **CompraNet**, se procederá a su apertura, haciéndose constar la documentación presentada, sin que ello implique la evaluación de su contenido.

Tomando en consideración que el presente procedimiento se lleva a cabo por medio electrónico, con fundamento en los artículos 26 Bis, fracción II y 35, fracción II de la Ley, la rúbrica de la totalidad de los documentos que integran las proposiciones no se llevará a cabo, ya que las propuestas se encuentran resguardadas en el servidor del sistema **CompraNet**, por lo que únicamente se imprimirá el **Anexo II "Propuesta Económica"**-de la presente convocatoria, presentada por los licitantes, y se levantará acta que servirá de constancia de la celebración del acto, en la que se harán constar el importe de cada una de ellas; se señalará lugar, fecha y hora en que se dará a conocer el Fallo de la Licitación.

Para la evaluación correspondiente, se proporcionará al área requirente en medio electrónico (disco magnético CD o memoria USB) las proposiciones presentadas por los licitantes, a fin de que se realice la evaluación correspondiente, misma que se integrará en el expediente respectivo.

En este acto, no se llevará a cabo la evaluación de las proposiciones, por lo que aún en caso de que algún licitante omitiere la presentación de documentos en su proposición, o les faltare algún requisito, ésta no será desechada en ese momento; la recepción de los documentos se hará constar mediante el acuse de presentación de proposición electrónica a través de **CompraNet** para cada licitante y será integrado al acta de presentación y apertura.

Los licitantes deberán enviar sus proposiciones en formato Word, Excel o PDF.

En el supuesto de que, durante el acto de presentación y apertura de proposiciones, por causas ajenas a la voluntad de la SFP, no sea posible abrir los sobres que contengan las proposiciones enviadas por la plataforma integral **CompraNet**, el acto se reanudará a partir de que se restablezcan las condiciones que permitan continuar con el procedimiento, con base en lo establecido en el Acuerdo.

Para la presentación y firma de proposiciones, o en su caso, de inconformidades a través de **CompraNet**, los licitantes deberán utilizar la **FIRMA ELECTRÓNICA AVANZADA** que emite el SAT para el cumplimiento de sus obligaciones fiscales, conforme a lo establecido en el artículo 50 primer párrafo del Reglamento.

El sistema **CompraNet** emitirá un aviso de la recepción de las proposiciones; una vez iniciado el acto de apertura de presentación de proposiciones, no se aceptará proposición alguna.

La SFP levantará un acta en la que hará constar la documentación enviada a través de **CompraNet** en forma cuantitativa, así como las propuestas y el importe de cada una de ellas para su posterior análisis y evaluación, el acta será firmada por los servidores públicos que asistan al evento, la cual será difundida a través de **CompraNet**-para efectos de notificación. Será responsabilidad de los licitantes enterarse del contenido de la misma, a través del medio señalado.

LA SFP, TENDRÁ COMO NO PRESENTADAS SUS PROPOSICIONES Y, EN SU CASO, LA DOCUMENTACIÓN REQUERIDA POR LA UNIDAD COMPRADORA, CUANDO EL ARCHIVO ELECTRÓNICO EN EL QUE SE CONTENGAN LAS PROPOSICIONES Y/O DEMÁS INFORMACIÓN NO PUEDA ABRIRSE POR TENER ALGÚN VIRUS INFORMÁTICO O POR CUALQUIER OTRA CAUSA AJENA A LA MISMA, EN TÉRMINOS DEL NUMERAL 29 DEL ACUERDO POR EL QUE SE ESTABLECEN LAS DISPOSICIONES QUE SE DEBERÁN OBSERVAR PARA LA UTILIZACIÓN DEL SISTEMA ELECTRÓNICO DE INFORMACIÓN PÚBLICA GUBERNAMENTAL DENOMINADO COMPRANET.

1.5.6. Vigencia de Proposiciones

Una vez recibidas las proposiciones de los licitantes a través de la plataforma integral **CompraNet** en la fecha y hora establecidas para tal efecto, éstas no podrán ser retiradas o dejarse sin efecto por lo que deberán considerarse vigentes dentro del procedimiento de esta Licitación hasta su conclusión.

1.5.7. De las Actas del procedimiento

De conformidad con lo establecido en los artículos 37 Bis de la Ley y 47 del Reglamento, las Actas de las Juntas de Aclaraciones, de Presentación, Apertura de Proposiciones y de Fallo mismas que serán firmadas por las personas que hubieran asistido a dicho acto, sin que la falta de firma de alguno de ellos reste validez o efectos a las mismas.

La Convocante fijará un ejemplar de las Actas de Juntas de Aclaraciones, Presentación y Apertura de Proposiciones y Fallo en los estrados del edificio sede de la SFP, sita en Avenida de los Insurgentes Sur número 1735, Planta Baja, Ala Norte, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Código Postal 01020, Ciudad de México, por un término no menor de cinco días hábiles. Asimismo, se difundirán a través de la plataforma integral **CompraNet** al concluir cada acto para efectos de su notificación.

1.6 Recepción de proposiciones enviadas a través de servicio postal o mensajería

En esta Licitación **no se aceptarán propuestas por medio de servicio postal o mensajería**, toda vez que éste procedimiento es electrónico y únicamente se permitirá la participación de los licitantes a través de la plataforma integral **CompraNet.**

1.7 Requisitos para la presentación de Proposiciones Conjuntas

En esta Licitación se acepta la presentación de proposiciones conjuntas que cumplan con lo dispuesto en los artículos 34, tercer, cuarto y quinto párrafo de la Ley, 44 y 48, fracción VIII del Reglamento.

Los interesados podrán presentar conjuntamente una proposición sin necesidad de constituir una sociedad, o una nueva sociedad en caso de personas morales; 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 exigirá su cumplimiento. En este supuesto la proposición será firmada por el representante común que para ese acto haya sido designado por el grupo de personas, por los medios de identificación electrónica establecidos por conforme al Acuerdo.

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 mantenga en la nueva sociedad las responsabilidades de dicho convenio.

Las personas que integran la agrupación deberán celebrar entre todas, un convenio en los términos de la legislación aplicable, en el que se establecerán con precisión los aspectos siguientes:

a) Nombre, domicilio y Registro Federal de Contribuyentes de las personas integrantes, señalando, en su caso, los datos de los instrumentos públicos con los que se acredita la existencia legal de las personas morales y, de haberlas, sus reformas y modificaciones, así como el nombre de los socios que aparezcan en éstas;
b) Nombre y domicilio de los representantes de cada una de las personas agrupadas, señalando, en su caso, los datos de las escrituras públicas con las que acrediten las facultades de representación;
c) Designación de un representante común, otorgándole poder amplio y suficiente, para atender todo lo relacionado con la proposición y con el procedimiento de Licitación Pública;
d) Descripción de las partes objeto del contrato que corresponderá cumplir a cada persona integrante, así como la manera en que se exigirá el cumplimiento de las obligaciones, y
e) Estipulación expresa de que cada uno de los firmantes quedará obligado junto con los demás integrantes, en forma solidaria, para efectos del procedimiento de contratación y del contrato, en caso de que se les adjudique el mismo.

Dicho convenio deberá apegarse a lo dispuesto por la Ley Federal de Competencia Económica en Materia de Prácticas Monopólicas y Concentraciones.

En el supuesto de que se adjudique a los licitantes que presentaron una proposición conjunta, el convenio indicado y las facultades del apoderado legal de la agrupación que formalizará el contrato respectivo, deberán constar en escritura pública, salvo que el contrato sea firmado por todas las personas que integran la agrupación que formula la proposición conjunta o por sus representantes legales, quienes en lo individual, deberán acreditar su respectiva personalidad, o por el apoderado legal de la nueva sociedad que se constituya por las personas que integran la agrupación que formuló la proposición conjunta, antes de la fecha fijada para la firma del contrato, lo cual deberá comunicarse mediante escrito a la Dependencia por dichas personas o por su apoderado legal, al momento de darse a conocer el Fallo o a más tardar en las veinticuatro horas siguientes, en términos de los artículos 34 de la Ley y 44 del Reglamento.

1.8 Registro de licitantes y revisión previa de documentos

No aplica.

1.9 Acreditación legal en la junta de aclaraciones y Acto de Presentación y Apertura de Proposiciones.

Los licitantes deberán acreditar su personalidad jurídica utilizando el **FORMATO 1 "ACREDITACIÓN DE LA EXISTENCIA LEGAL Y PERSONALIDAD JURÍDICA DEL LICITANTE"**.

1.10 Indicaciones respecto al Fallo y a la firma del Contrato.

1.10.1 Acto de Fallo.

Se levantará el acta respectiva y se publicará a través de la plataforma integral **CompraNet** https://upcp-compranet.hacienda.gob.mx/sitiopublico/#/ el mismo día en que se emita, de conformidad con los artículos 37 y 37 Bis de la Ley.

La Convocante en esta etapa comunicará el resultado de la evaluación legal-administrativa, técnica y económica en el acta, que para ese efecto se levante debidamente fundada y motivada; se señalarán detalladamente las propuestas que fueron desechadas y las que no resultaron aceptadas, indicándose, en su caso, las que hayan cumplido con la totalidad de los requisitos legales-administrativos, técnicos y económicos solicitados en los Requisitos de Participación, al igual que las especificaciones requeridas por la Convocante respecto de los bienes objeto de la presente Licitación, así como el nombre del licitante que ofertó las mejores condiciones y dando a conocer el importe respectivo.

Conforme a lo establecido en el artículo 35 fracción III de la Ley, el acto de fallo podrá ser diferirse, siempre que el nuevo plazo fijado no exceda de 20 días naturales contados a partir del plazo establecido originalmente.

NOTA: El llenado del **FORMATO 15 "ENCUESTA DE TRANSPARENCIA"** es opcional; sin embargo, es importante para la SFP, sea requisitado y transmitido posterior a la emisión del fallo a los correos que se mencionan en el mismo, a fin de mejorar el desarrollo de los procedimientos de contrataciones.

1.10.2 Notificación del Fallo

Para efectos de notificación, a través de la plataforma integral CompraNet, se enviará a los licitantes un aviso informándoles que el acta de fallo se encuentra a su disposición en la plataforma electrónica, conforme a lo establecido en el artículo 37 quinto párrafo de la Ley.

En caso de error aritmético, mecanográfico o de cualquier otra naturaleza en el Fallo, que no afecte el resultado de la evaluación realizada por la Convocante, se procederá a su corrección, en la forma y términos por el penúltimo párrafo del artículo 37 de la Ley.

Con la notificación del Fallo por el que se adjudica el contrato, las obligaciones derivadas de éste serán exigibles, sin perjuicio de la obligación de las partes de firmarlo dentro de los 15 (quince) días naturales siguientes, con fundamento en el artículo 46 de la Ley, para ello el (los) licitante(s) ganador(es)

deberá(n) entregar la documentación detallada en los numerales 1.11.1 y 1.11.2., según corresponda, de lo contrario se reportará al Órgano Interno de Control.

1.11 Firma del contrato

La formalización del contrato será de manera electrónica, a través del MFIJ de CompraNet, en términos del "ACUERDO por el que se incorpora como un módulo de CompraNet la aplicación denominada Formalización de Instrumentos Jurídicos y se emiten las Disposiciones de carácter general que regulan su funcionamiento", publicado en el DOF, el 18 de septiembre del 2020 (ACUERDO), y al "Manual de Operación para la utilización en CompraNet, del Módulo de Formalización de Instrumentos Jurídicos, derivados de los procedimientos de contratación al amparo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y la Ley de Obras Públicas y Servicios Relacionados con las Mismas.", emitido el 21 de julio de 2023, por la Oficial Mayor de la SHCP.

Si el licitante adjudicado no firma el contrato adjudicado por causas imputables al mismo, conforme a lo señalado en el numeral anterior, la Convocante, sin necesidad de un nuevo procedimiento, deberá adjudicar el contrato al participante que haya obtenido el segundo lugar, siempre que la diferencia en precio con respecto a la proposición inicialmente adjudicada no sea superior a un margen del 10% (diez por ciento), de conformidad con lo asentado en el Fallo correspondiente, y así sucesivamente en caso de que este último no acepte la adjudicación.

Con apego en lo dispuesto por el artículo 46 de la Ley, el licitante adjudicado deberá formalizar el contrato de conformidad con las fechas señaladas en el Acta de Fallo y eventualmente dentro del plazo de 15 días naturales contados a partir del día siguiente a la notificación del Fallo en términos del citado artículo, para presentar la siguiente documentación:

1.11.1 Para personas morales:

1. Original para su cotejo y copia simple del acta constitutiva y sus modificaciones estatutarias, en donde acredite su existencia legal y personalidad jurídica, mismas que deberán contener y señalar en el objeto social el cumplimiento con la naturaleza del servicio a contratar.

2. Original para su cotejo y copia simple del instrumento notarial del representante legal, en donde demuestre tener facultades para la firma del instrumento jurídico.

3. Original para su cotejo y copia simple del comprobante de domicilio con una antigüedad no mayor a 3 meses.

4. Original para su cotejo y copia simple de la Cédula de identificación Fiscal.

5. Original para su cotejo y copia simple de Identificación oficial vigente (pasaporte, credencial para votar o cédula profesional) de la persona facultada para suscribir el Contrato.

6. Para dar cumplimiento a lo establecido en el Artículo 32-D del Código Fiscal de la Federación, deberá presentar la opinión positiva, la cual deberá estar vigente a la fecha de formalización del contrato, de cumplimiento de obligaciones fiscales emitida por el SAT, en términos del artículo 32-D del Código Fiscal de la Federación y la Resolución Miscelánea Fiscal para 2024, publicada en el

Diario Oficial de la Federación el 29 de diciembre de 2023 con antigüedad no mayor a 30 días naturales.

En caso de que subcontrate con terceros (obligaciones patronales), adicionalmente, deberá presentar la opinión de cumplimiento de obligaciones fiscales por el SAT en sentido positivo, del tercero que preste el servicio.

7. Opinión positiva y vigente a la fecha de formalización del contrato, de cumplimiento de obligaciones fiscales en materia de seguridad social emitida por el IMSS, en términos del artículo 32-D del Código Fiscal de la Federación y el Acuerdo ACDO.SA1.HCT.101214/281.P.DIR y su Anexo Único, relativo a las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social, publicado en el Diario Oficial de la Federación el 27 de febrero de 2015, reformado mediante ACUERDO ACDO.SA1.HCT.250315/62.P.DJ dictado por el H. Consejo Técnico, relativo a la autorización para modificar la Primera de las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social de fecha 25 de marzo de 2015, y publicado en el Diario Oficial de la Federación el 03 de abril del mismo año.

   Cuando los licitantes no cuenten con trabajadores deberán manifestarlo mediante escrito libre, justificando el motivo y anexando el documento en el que conste que no se puede emitir la constancia de su cumplimiento del IMSS.

   En caso de que subcontrate con terceros (obligaciones patronales), adicionalmente, deberá presentar la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social, en sentido positivo, del tercero que preste el servicio.

8. Constancia positiva y vigente a la fecha de formalización del contrato, de encontrarse al corriente de sus obligaciones fiscales de aportaciones patronales y entero de descuentos a través del documento emitido por el INFONAVIT, conforme lo establece la Resolución RCA-5789-01/17 y su Anexo Único, relativo a las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de amortizaciones, publicado en el Diario Oficial de la Federación el 28 de junio de 2017.

   En caso de que subcontrate con terceros (obligaciones patronales), adicionalmente, deberá presentar la opinión de cumplimiento de obligaciones fiscales en materia de aportaciones patronales, en sentido positivo, del tercero que preste el servicio.

9. En caso de contar con un domicilio diferente al que aparece en el R.F.C., deberá presentar la última actualización vigente de cambio de domicilio fiscal, tramitado ante el SAT.

10. Constancia de la Institución Bancaria sobre la existencia de la cuenta de cheques abierta a nombre de la persona moral que incluya el número de cuenta con 11 posiciones, así como la clave bancaria estandarizada (CLABE) con 18 posiciones o estado de cuenta.

1.11.2 Para personas físicas:

1. Original para su cotejo y copia simple del Acta de Nacimiento (actualizada) o Carta de Naturalización.

2. Original para su cotejo y copia simple de la identificación oficial vigente con fotografía. (pasaporte, credencial para votar o cédula profesional.).

3. Original para su cotejo y copia simple de la Cédula de identificación Fiscal.

4. Original para su cotejo y copia simple de Clave Única de Registro de Población (CURP).

5. Original para su cotejo y copia simple del comprobante de domicilio con una antigüedad no mayor a 3 meses.

6. En su caso, original para su cotejo y copia simple de poder notarial del apoderado legal, en donde demuestre tener facultades para la firma del documento.

7. Para dar cumplimiento a lo establecido en el Artículo 32-D del Código Fiscal de la Federación, deberá presentar la Opinión positiva y vigente de cumplimiento de obligaciones fiscales emitida por el SAT, en términos del artículo 32-D del Código Fiscal de la Federación y la Resolución Miscelánea Fiscal para 2024, la Resolución Miscelánea Fiscal para 2024, publicada en el Diario Oficial de la Federación el 29 de diciembre de 2023, con antigüedad no mayor a 30 días naturales.

   En caso de que subcontrate con terceros (obligaciones patronales), adicionalmente, deberá presentar la opinión de cumplimiento de obligaciones fiscales por el SAT en sentido positivo, del tercero que preste el servicio.

8. Opinión positiva y vigente de cumplimiento de obligaciones fiscales en materia de seguridad social emitida por el IMSS, en términos del artículo 32-D del Código Fiscal de la Federación y el Acuerdo ACDO.SA1.HCT.101214/281.P.DIR y su Anexo Único, relativo a las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social, publicado en el Diario Oficial de la Federación el 27 de febrero de 2015, reformado mediante ACUERDO ACDO.SA1.HCT.250315/62.P.DJ dictado por el H. Consejo Técnico, relativo a la autorización para modificar la Primera de las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social de fecha 25 de marzo de 2015, y publicado en el Diario Oficial de la Federación el 03 de abril del mismo año, con antigüedad no mayor a 30 días naturales.

   En caso de que se subcontrate con terceros, adicionalmente, deberá presentar la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social del tercero que preste los servicios.

9. Constancia positiva y vigente de encontrarse al corriente de sus obligaciones fiscales de aportaciones patronales y entero de descuentos a través del documento emitido por el INFONAVIT, conforme lo establece la Resolución RCA-5789-01/17 y su Anexo Único, relativo a las Reglas para la

obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de amortizaciones, publicado en el Diario Oficial de la Federación el 28 de junio de 2017, con antigüedad no mayor a 30 días naturales.

En caso de que se subcontrate con terceros, adicionalmente, deberá presentar la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social del tercero que preste los servicios.

10. En caso de contar con un domicilio diferente al que aparece en el R.F.C., deberá presentar la última actualización vigente de cambio de domicilio fiscal, tramitado ante el SAT.

11. Constancia de la Institución Bancaria sobre la existencia de la cuenta de cheques abierta a nombre de la persona física que incluya el número de cuenta con 11 posiciones, así como la clave bancaria estandarizada (CLABE) con 18 posiciones o estado de cuenta.

1.12 Garantía de Cumplimiento.

De conformidad con el artículo 48 fracción II y 49 fracción I de la LAASSP, el proveedor se obliga a constituir y entregar a más tardar, dentro de los 10 (diez) días naturales siguientes a la fecha de firma del contrato, garantía de cumplimiento **INDIVISIBLE** por Institución legalmente constituida y apta en la diversificación de las responsabilidades que asuma, a favor de la TESOFE a satisfacción de la SFP, para garantizar el exacto cumplimiento de las obligaciones contraídas, por lo que la Dirección de Abastecimiento y Contratos deberá requerir al licitante Adjudicado, su escrito con el señalamiento de que ofrece y exhibe la Garantía de Cumplimiento.

El importe de la garantía de cumplimiento por la vigencia del contrato será el equivalente al **10%** (diez por ciento) del **MONTO TOTAL DEL CONTRATO**, sin incluir el I.V.A.

Instrucciones para la elaboración y entrega de la garantía de cumplimiento del contrato.

De conformidad a lo establecido en el artículo 48 último párrafo de la LAASSP, el proveedor a fin de garantizar el cumplimiento de las obligaciones derivadas del contrato y para responder en la calidad del servicio prestado, así como de cualquier otra responsabilidad, deberá presentar la garantía en alguna de las siguientes formas:

1. Depósito de dinero constituido a través de certificado o billete de depósito, expedido por institución de crédito autorizada para operar como tal.
2. Fianza otorgada por institución de fianzas o de seguros autorizada para expedirla.
3. Depósito de dinero constituido ante la TESOFE.
4. Carta de crédito irrevocable, expedida por Institución de Crédito autorizada para operar como tal.
5. Seguro de caución otorgada por Institución de seguros autorizada para expedirlo.
6. Cheque certificado o de caja expedido a favor de la TESOFE.
7. Cualquier otro que en su caso autorice la TESOFE.

El proveedor deberá presentar la garantía de cumplimiento a más tardar dentro de los 10 (diez) días naturales siguientes a la fecha de firma establecida en el contrato o el día hábil anterior si el décimo día

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

no lo fuera. De no cumplir con dicha entrega, la SFP podrá determinar la rescisión administrativa del contrato y remitir el asunto al OIC de la SFP, para su consideración y efectos legales a los que haya lugar, de conformidad a lo establecido en el artículo 60, fracción III de la LAASSP.

Dicha garantía deberá ser expedida por la vigencia del periodo de prestación del servicio y la SFP a través de la Dirección de Abastecimiento y Contratos, procederá a su calificación; en términos de lo establecido en las Disposiciones Generales en Materia de Funciones de Tesorería, publicadas en el Diario Oficial de la Federación el 30 de noviembre de 2018; debiendo remitir el original de la aceptación de la garantía (Formato número 1. Uno de la Guía en Materia de Garantías del 22 de febrero de 2019) así como el original de la garantía de cumplimiento para su guarda y custodia, a más tardar dentro de los 5 (cinco) días naturales posteriores a que tenga lugar la aceptación; o en su defecto, dentro de dicho plazo deberá enviar el dictamen para que se rescinda el contrato, marcado copia del mismo al OIC en la Secretaría, para los efectos de su competencia.

En caso de garantizar el cumplimiento con fianza, ésta deberá señalar claramente que se expide para garantizar el fiel y exacto cumplimiento de las especificaciones y obligaciones derivadas de la presente licitación y contraídas mediante contrato que se suscriba, según características, cantidad y calidad que se describen en la proposición presentada por el licitante y de conformidad a la presente convocatoria, los anexos y la Junta de Aclaraciones.

La póliza de fianza para garantizar el cumplimiento del contrato debe otorgarse en estricto apego al **ANEXO VI "FORMATO DE FIANZA PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO"** de esta convocatoria.

La garantía de cumplimiento, de ninguna manera será considerada como una limitación de la responsabilidad de la persona licitante adjudicada, derivada de sus obligaciones y garantías estipuladas en el contrato y sus anexos, y no impedirá que la SFP reclame la indemnización o el reembolso por cualquier incumplimiento que pueda exceder el valor de dicha garantía.

En el supuesto de que la Secretaría y por así convenir a sus intereses, decidiera modificar o ampliar la prestación de los servicios pactados en el contrato, el proveedor se obliga a garantizar dicha prestación, mediante el endoso, en donde consten las modificaciones o cambios en la respectiva garantía de cumplimiento y entregarla a más tardar dentro los 10 (diez) días naturales posteriores a la firma del Convenio respectivo.

La SFP, a través de la Dirección de Abastecimiento y Contratos, previa solicitud por escrito por parte del administrador del contrato, procederá a cancelar la garantía de cumplimiento correspondiente, siempre y cuando se cuente con la constancia de cumplimiento de obligaciones contractuales a nombre del proveedor.

El proveedor acepta expresamente que la garantía de cumplimiento se hará efectiva independientemente de que se interponga cualquier tipo de recurso ante instancias del orden administrativo o judicial.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

Será necesaria la manifestación expresa y por escrito del proveedor, de su conformidad para que la garantía de cumplimiento del contrato adjudicado, permanezca vigente durante toda la substanciación de las demandas civiles, laborales o recursos legales que interponga con relación a dicho contrato, hasta que sea pronunciada resolución o laudo definitivo que cause ejecutoria por la autoridad competente, de conformidad a lo establecido por el artículo 48 de la LAASSP.

La entrega de la garantía de cumplimiento será en la Dirección de Abastecimiento y Contratos, sita en Avenida Insurgentes Sur número 1735, mezzanine ala sur, colonia Guadalupe Inn, Alcaldía Álvaro Obregón, código postal 01020, Ciudad de México.

1.13 Póliza de Responsabilidad Civil.

La SFP no solicitará la presentación de Póliza de Responsabilidad Civil.

APARTADO IV. REQUISITOS QUE DEBERÁN CUMPLIR QUIENES DESEEN PARTICIPAR.

Documentación obligatoria (indispensables cuyo incumplimiento afecta la solvencia de la proposición):

1. Propuesta Técnica.

Deberá describir la forma y términos en las que se proporcionará el servicio conforme al **ANEXO I "ESPECIFICACIONES TÉCNICAS Y ALCANCES DEL SERVICIO"** de esta convocatoria, así como presentar **todos y cada uno de los documentos que la integren.**

2. Propuesta económica.

Los licitantes deberán presentar su propuesta económica indicando el precio unitario y total de la partida única, conforme a lo señalado en el **ANEXO II "PROPUESTA ECONÓMICA"** de esta convocatoria.

3. Formato de acreditación.

Conforme a lo señalado en la **fracción V del artículo 48 del RLAASSP**, las personas licitantes que participen ya sea por sí mismas, o a través de un representante, para acreditar su personalidad, deberán presentar un escrito (preferentemente en papel membretado de la persona licitante) firmado por su propio derecho o a través de su representante o apoderado legal, mediante el cual manifieste bajo protesta de decir verdad, que cuenta con facultades suficientes para suscribir en nombre de su representada la propuesta correspondiente, el cual deberá contener los siguientes datos (**FORMATO 1 "ACREDITACIÓN DE LA EXISTENCIA LEGAL Y PERSONALIDAD JURÍDICA DEL LICITANTE"**). En caso de proposición conjunta, deberá ser presentado por cada una de las personas participantes en la proposición conjunta, de conformidad con lo establecido en el Artículo 48 fracción VIII segundo párrafo del RLAASSP:

A) Del procedimiento, nombre y número.

B) De la persona licitante:

- Nombre completo o Razón Social,
- Clave del Registro Federal de Contribuyentes,
- Clave Única de Registro de Población, CURP (personas físicas),
- Datos de las escrituras públicas con las que se acredita la existencia legal de las personas morales, y de haberlas, sus reformas y modificaciones.
- Domicilio (calle y número exterior e interior, si lo tiene, colonia, código postal, Alcaldía de la Ciudad de México o municipio, entidad federativa, teléfono, fax y correo electrónico),
- Relación de los accionistas o socios con su RFC y homoclave. En el caso de ser personas morales deberá incluir la siguiente información:

Nombre completo o Razón Social	Clave del Registro Federal de Contribuyentes	Datos de las escrituras públicas	Domicilio	Descripción del objeto social.	Relación de los accionistas

- Descripción del objeto social.

C) Del representante o apoderado legal de la persona licitante (en su caso):

- Nombre completo.
- Para acreditar que cuenta con facultades suficientes para suscribir la propuesta, mencionar número y fecha de la escritura pública en el documento que lo acredite la personalidad con la que comparezca, señalando el nombre, número y el lugar o circunscripción del fedatario público que las protocolizó, así como fecha y datos de su inscripción en el Registro Público de Comercio.

D) Tratándose de **personas morales** deberá acompañar al escrito, fotocopia de una **identificación oficial vigente con fotografía** (Cédula Profesional, Cartilla del Servicio Militar Nacional, Pasaporte, Credencial de elector.) de su representante legal. En caso de **personas físicas** acompañar copia de su **identificación oficial vigente y de su Registro Federal de Contribuyentes (RFC).**

En el caso de proposiciones conjuntas únicamente el representante común deberá presentar copia simple por ambos lados de la identificación oficial vigente con fotografía (pasaporte, cartilla, credencial del INE o cédula profesional).

E) Acompañar este formato con su **acta constitutiva y, en su caso, la última modificación** a la misma. La falta de presentación del acta constitutiva acompañando este formato afectará la solvencia de la proposición.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

En el caso de proposiciones conjuntas deberá presentar las Actas constitutivas y en su caso modificaciones de cada uno de las personas participantes en la proposición conjunta.

4. Carta del artículo 50 y 60 de la LAASSP.

Carta en papel (preferentemente en papel membretado de la persona licitante) firmada por su propio derecho o a través de su representante o apoderado legal, mediante la cual manifieste **bajo protesta de decir verdad**, que la persona licitante no se encuentra en ninguno de los supuestos del artículo **50 y 60 de la LAASSP** (**FORMATO 2 "MANIFESTACIÓN DE QUE EL LICITANTE NO SE UBICA EN LOS SUPUESTOS ESTABLECIDOS EN LOS ARTÍCULOS 50 Y 60 DE LA LEY"**).

En caso de proposición conjunta, deberá de ser presentado por cada una de las personas participantes en la proposición conjunta, de conformidad con lo establecido en el Artículo 48 fracción VIII segundo párrafo del RLAASSP.

5. Declaración de integridad.

Declaración de integridad, mediante carta en papel (preferentemente en papel membretado de la persona licitante) firmada por su propio derecho o a través de su representante o apoderado legal, mediante la cual manifieste **bajo protesta de decir verdad** que por sí mismos o través de interpósita persona, se abstendrá de adoptar conductas, para que los servidores públicos de la SFP, induzcan o alteren las evaluaciones de las propuestas, el resultado del procedimiento, u otros aspectos que otorguen condiciones más ventajosas con relación a los demás participantes (**FORMATO 3 "DECLARACIÓN DE INTEGRIDAD"**).

En caso de proposición conjunta, deberá de ser presentado por cada una de las personas participantes en la proposición conjunta, de conformidad con lo establecido en el Artículo 48 fracción VIII segundo párrafo del RLAASSP.

6. Manifestación de Nacionalidad.

Declaración que deberán presentar las personas licitantes donde manifiesten que es originario de los Estados Unidos Mexicanos y en el caso de personas morales, que se encuentran debidamente constituidos de acuerdo a la legislación aplicable. (**FORMATO 4 "MANIFESTACIÓN DE NACIONALIDAD"**).

En caso de proposición conjunta, deberá de ser presentado por cada una de las personas participantes en la proposición conjunta, de conformidad con lo establecido en el Artículo 48 fracción VIII segundo párrafo del RLAASSP.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

7. Cumplimiento de normas.

Declaración de conocer que existen normas oficiales mexicanas que cubran los requerimientos del presente procedimiento, conforme a las especificaciones indicadas en el **ANEXO I "ESPECIFICACIONES TÉCNICAS Y ALCANCES DEL SERVICIO"** de la convocatoria. **(FORMATO 5 "CUMPLIMIENTO DE NORMAS")**:

8. Uso de medios.

La persona licitante deberá presentar escrito original firmado por el representante legal, en papel preferentemente membretado de la persona licitante, dirigido a la SFP, en el que se manifieste que se tendrá como no presentada su proposición y, en su caso, la documentación requerida por la Unidad compradora, cuando el archivo electrónico en el que contenga la proposición y/o demás información no pueda abrirse por tener algún virus informático o por cualquier otra causa ajena a la dependencia o entidad **(FORMATO 6 "MANIFESTACIÓN CON RELACIÓN AL PUNTO 29 DEL ACUERDO POR EL QUE SE ESTABLECEN LAS DISPOSICIONES QUE SE DEBERÁN OBSERVAR PARA LA UTILIZACIÓN DEL SISTEMA ELECTRÓNICO DE INFORMACIÓN PÚBLICA GUBERNAMENTAL DENOMINADO COMPRANET")**.

9. Manifestación MIPYME.

Escrito en formato libre en el cual se manifieste **bajo protesta de decir verdad**, si la empresa se encuentra clasificada como MIPYME de acuerdo a la Secretaría de Economía, conforme al formato adjunto a la presente convocatoria como **(FORMATO 7 "MANIFESTACIÓN MIPYME")**.

En caso de proposición conjunta, deberá de ser presentado por cada una de las personas participantes en la proposición conjunta, de conformidad con lo establecido en el Artículo 48 fracción VIII segundo párrafo del RLAASSP.

10. Carta de los artículos 49 fracción IX y 72 de la Ley General de Responsabilidades Administrativas.

Carta en papel (preferentemente en papel membretado de la persona licitante) firmada por su propio derecho o a través de su representante o apoderado legal, mediante la cual manifiesta **bajo protesta de decir verdad**, que la persona licitante no se encuentra en ninguno de los supuestos de los artículos 49 fracción IX y 72 de la Ley General de Responsabilidades Administrativas **(FORMATO 8 "CARTA DE LOS ARTÍCULOS 49 FRACCIÓN IX Y 72 DE LA LEY GENERAL DE RESPONSABILIDADES ADMINISTRATIVAS").**

En caso de proposición conjunta, deberá de ser presentado por cada una de las personas participantes en la proposición conjunta, de conformidad con lo establecido en el Artículo 48 fracción VIII segundo párrafo del RLAASSP.

11. Declaración de conocer el Protocolo de actuación.

Declaración escrita en papel membretado que conoce el contenido del Protocolo de Actuación en Materia de Contrataciones Públicas, Otorgamiento y Prórroga de Licencias, Permisos, Autorizaciones y Concesiones **(FORMATO 9 "DECLARACIÓN DE CONOCER EL PROTOCOLO DE ACTUACIÓN")**.

En caso de proposición conjunta, deberá de ser presentado por cada una de las personas participantes en la proposición conjunta, de conformidad con lo establecido en el Artículo 48 fracción VIII segundo párrafo del RLAASSP.

12. Acuse del manifiesto de Ausencia de Conflicto de Interés.

Acuse del manifiesto en el que el licitante afirme o niegue los vínculos o relaciones de negocios, laborales, profesionales, personales o de parentesco con consanguinidad o afinidad hasta el cuarto grado que tengan las personas con servidores públicos.

Este deberá ser tramitado en la página de internet https://manifiesto.funcionpublica.gob.mx de conformidad con lo establecido en los numerales 3, 4, 5 y 6 del Anexo Segundo del Protocolo de actuación en materia de contrataciones públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones.

En caso de proposición conjunta, deberá de ser presentado por cada una de las personas participantes en la proposición conjunta, de conformidad con lo establecido en el Artículo 48 fracción VIII segundo párrafo del RLAASSP.

13. Escrito de confidencialidad.

Manifestación en la que el licitante se obliga durante la presente licitación y en caso de ser adjudicado, a mantener la más estricta confidencialidad de toda la información y documentación que la Convocante le proporcione, por lo que se compromete a no divulgar ni a utilizar la información que conozca en el desarrollo y cumplimiento de este servicio, así como, cuidar los documentos y sistemas de información a que tuviere acceso, garantizando la confidencialidad de la información que reciba, resguarde, registre o genere derivado de los servicios requeridos, durante la vigencia del servicio. **(FORMATO 12 "ESCRITO DE CONFIDENCIALIDAD").**

En caso de proposición conjunta, deberá de ser presentado por cada una de las personas participantes en la proposición conjunta, de conformidad con lo establecido en el Artículo 48 fracción VIII segundo párrafo del RLAASSP.

EL CUMPLIMIENTO DE LOS REQUISITOS ANTERIORES (1 AL 13) ES INDISPENSABLE, POR LO QUE SU OMISIÓN AFECTARÁ LA SOLVENCIA DE LA PROPOSICIÓN PRESENTADA Y SERÁ MOTIVO PARA DESECHAR LAS PROPOSICIONES PRESENTADAS.

Obligatorios adicionales, aplicables únicamente para proposiciones conjuntas:

14. Participación Conjunta (Formato Libre).

- Para las personas licitantes que presenten proposición conjunta, de conformidad a lo establecido en los artículos 34 de la LAASSP y 44 del RLAASSP, deberán formalizar un convenio, en el cual deberá indicar las obligaciones específicas del contrato que corresponderá a cada una de ellas, observando lo establecido en los referidos ordenamientos legales anteriormente invocados, mismo que deberá incluir en su proposición.
- El representante común de la agrupación deberá presentar escrito en el que manifieste, que la proposición que presenta es en forma conjunta.
- Escrito de cada uno de los integrantes de la proposición conjunta manifestando de forma individual, los documentos señalados en el numerales 3, 4, 5, 6, 9, 10, 11, 12, 13, 14, 15 y 16 del Apartado IV.

El cumplimiento del requisito anterior (14) únicamente es aplicable para proposiciones conjuntas, y la falta de cualquiera de los documentos mencionados en este requisito afectará la solvencia de la proposición presentada y será motivo para desechar las proposiciones presentadas.
Documentación optativa.

15. Manifiesto de información reservada y/o confidencial.

Escrito firmado de forma autógrafa y en original por el representante legal del licitante, que con fundamento en lo establecido por los artículos 113 y 116 de la Ley General de Transparencia y Acceso a la Información Pública, manifieste cuáles son los documentos de su proposición, que contienen información reservada y/o confidencial, siempre que tengan el derecho de reservarse la información, de conformidad con las disposiciones aplicables, explicando los motivos de la clasificación. **(FORMATO 10 "MANIFIESTO DE INFORMACIÓN RESERVADA Y/O CONFIDENCIAL").**

En caso de que los licitantes no lo manifiesten y/o no determinen qué parte de su documentación, propuesta técnica y económica son consideradas reservadas y/o confidenciales, la convocante asumirá que la información proporcionada en su totalidad es información pública.

16. Domicilio Convencional.

En caso de que el domicilio fiscal del Licitante no se encuentre dentro de la Ciudad de México o su área metropolitana, éste deberá informar por escrito algún domicilio convencional para oír y recibir todo tipo de notificaciones relacionadas con el procedimiento o en caso de resultar adjudicado lo relativo a la contratación. **(FORMATO 11 "DOMICILIO CONVENCIONAL")**

17. Correo electrónico del licitante.

Escrito en el que el licitante manifieste una dirección de correo electrónico, de conformidad con lo establecido en el Artículo 39 fracción VI inciso d) del RLAASSP, en caso contrario, deberá indicar en el escrito que no cuenta con el mismo. **(FORMATO 14 "CORREO ELECTRÓNICO DEL LICITANTE")**

18. Consentimiento para uso de datos personales (aviso de privacidad).

Consentimiento por parte del Representante Legal (El Titular), donde reconoce que la DGRMSG a través de la Dirección de Planeación y Adquisiciones hizo de su conocimiento el Aviso de Privacidad Integral previo a proporcionar sus datos personales; de igual manera, consiente expresamente que la DGRMSG trate sus datos personales, así como los de su representada, con sujeción a las finalidades, términos y demás condiciones establecidas en dicho Aviso de Privacidad Integral. **(FORMATO 13 "CONSENTIMIENTO POR PARTE DEL REPRESENTANTE LEGAL (EL TITULAR) PARA EL USO DE DATOS PERSONALES")**

El Aviso de Privacidad Integral se encuentra a disposición en el portal web https://www.gob.mx/sfp/documentos/avisos-de-privacidad apartado de -**Avisos de Privacidad-** de la -**Dirección General de Recursos Materiales, y Servicios Generales.**

19. Opinión positiva sobre el cumplimiento de obligaciones fiscales emitida por la autoridad fiscal competente.

Para dar cumplimiento al artículo 32-D del Código Fiscal de la Federación, deberá presentar la opinión positiva de encontrarse al corriente en sus obligaciones fiscales a través del documento expedido por el SAT, conforme lo establece la regla 2.1.28 de la Resolución Miscelánea Fiscal para 2024, publicada en el Diario Oficial de la Federación el 29 de diciembre de 2023.

En caso de que subcontrate con terceros (obligaciones patronales), adicionalmente, deberá presentar la opinión de cumplimiento de obligaciones fiscales por el SAT en sentido positivo, del tercero que preste el servicio.

20. Opinión positiva de cumplimiento de obligaciones fiscales en materia de seguridad social emitida por autoridad competente.

Para dar cumplimiento al artículo 32-D del Código Fiscal de la Federación, deberá presentar la opinión positiva de encontrarse al corriente de sus obligaciones fiscales en materia de seguridad social a través del documento emitido por el IMSS, conforme lo establece el Acuerdo ACDO.SA1.HCT.101214/281.P.DIR y su Anexo Único, relativo a las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social, publicado en el Diario Oficial de la Federación el 27 de febrero de 2015; reformado mediante ACUERDO ACDO.SA1.HCT.250315/62.P.DJ dictado por el H. Consejo Técnico, relativo a la autorización para modificar la Primera de las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social de fecha 25 de marzo de 2015 y publicado en el Diario Oficial de la Federación el 03 de abril del mismo año.

Los licitantes deberán acreditar que están al corriente en el pago de sus cuotas patronales, así como en sus obligaciones patronales para lo cual deberán presentar Dictamen del IMSS del ejercicio Fiscal 2023 sin salvedades, lo anterior de conformidad al Artículo 16 de la Ley del Seguro Social.

En caso de que subcontrate con terceros (obligaciones patronales), adicionalmente, deberá presentar la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social, en sentido positivo, del tercero que preste el servicio.

21. Constancia de cumplimiento de obligaciones fiscales en materia de aportaciones patronales y entero de descuentos emitida por el Instituto del Fondo Nacional de la Vivienda para los trabajadores (INFONAVIT).

Para dar cumplimiento al artículo 32-D del Código Fiscal de la Federación, deberá presentar la constancia de situación fiscal de no adeudos en materia de aportaciones patronales y entero de descuentos a través del documento emitido por el INFONAVIT, conforme lo establece la Resolución RCA-5789-01/17 y su Anexo Único, relativo a las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de amortizaciones, publicado en el Diario Oficial de la Federación el 28 de junio de 2017.

En caso de que subcontrate con terceros (obligaciones patronales), adicionalmente, deberá presentar la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social, en sentido positivo, del tercero que preste el servicio.

EL CUMPLIMIENTO DE LOS REQUISITOS ANTERIORES (15 AL 21) ES OPTATIVO, POR LO QUE SU OMISIÓN NO AFECTARÁ LA SOLVENCIA DE LA PROPOSICIÓN PRESENTADA Y NO SERÁ MOTIVO PARA DESECHAR LAS PROPOSICIONES PRESENTADAS.

APARTADO V. CRITERIOS ESPECÍFICOS PARA LA EVALUACIÓN DE PROPOSICIONES Y ADJUDICACIÓN DEL CONTRATO.

El acreditar alguna o algunas de las causas establecidas en los incisos del numeral 1 del presente apartado, afectará la solvencia de la proposición y motivará su desechamiento, independientemente de otros requisitos señalados en la presente convocatoria.

1. Causas de desechamiento de proposiciones.

De conformidad con el artículo 29, fracción XV de la Ley, serán causa de desechamiento de las proposiciones que incurran en una o varias de las siguientes situaciones:

a) Cuando se compruebe que algún licitante ha acordado con otro u otros elevar el costo del servicio solicitado en la presente convocatoria, o cualquier otro acuerdo que tenga como fin obtener una ventaja sobre los demás licitantes; o existan elementos de los que sea posible desprender que existe una relación o vinculación entre dos o más licitantes.

b) Cuando presenten la propuesta económica en moneda extranjera.

c) Cuando presenten proposiciones en idioma diferente al español.

d) Cuando presenten documentos alterados, tachados o con enmendaduras.

e) Cuando presenten más de una propuesta técnica y/o económica

f) Cuando no cotice todos y cada uno de los conceptos que integran la partida única.

g) Cuando exista discrepancia entre lo ofertado en la propuesta técnica y económica en lo referente a la descripción del servicio.

h) Cuando el licitante se encuentre en alguno de los supuestos establecidos por los artículos 50 y 60 de la Ley.

i) Cuando el licitante se encuentra en alguno de los supuestos de los artículos 49 fracción IX y 72 de la Ley General de Responsabilidades Administrativas.

j) Cuando se solicite una manifestación "bajo protesta de decir verdad" y esta leyenda sea omitida en el documento correspondiente.

k) La presentación de la propuesta técnica que no cumpla con todos y cada uno de los requisitos técnicos solicitados de acuerdo con el **ANEXO I,** o con los requisitos solicitados para la elaboración de la propuesta económica conforme a lo establecido en el **ANEXO II.**

l) Cuando el o los archivo (s) electrónico (s) que contengan la proposición de los licitantes enviado (s) a través de CompraNet no puedan abrirse por tener algún virus informático o por cualquier causa ajena a la Convocante.

m) Cuando se omita la presentación de cualquier otro requisito que deba cumplir y que se considere indispensable para evaluar la proposición y que afecte directamente su solvencia.

n) Cuando las proposiciones técnicas y/o económicas presentadas a través de CompraNet carezcan de la firma electrónica (sin archivo adjunto) o el sistema CompraNet la identifique como Archivo con Firma Digital No Valido, de acuerdo a lo solicitado por dicho Sistema; o los archivos presentados en su proposición técnica y/o económica, hayan sido firmados de manera individual con la extensión p7m, ya que no podrán ser abiertas por el sistema CompraNet.

o) Si se determina que los precios propuestos no son aceptables ni convenientes.

p) Cuando el monto de la propuesta económica exceda la suficiencia presupuestal con la que se cuenta para esta contratación, y en concepto del área requirente no sea posible ni conveniente la reasignación de recursos económicos para cubrir el faltante; o bien, por la naturaleza del servicio a

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

contratar no sea posible la reducción del servicio.

q) Cuando en la propuesta técnica y/o económica recibida a través de la plataforma integral CompraNet, se desprenda que el nombre del Licitante difiere al nombre del registro en el citado sistema de quien presente la propuesta.

r) La falta de cualquiera de los documentos y/o requisitos obligatorios, solicitados en la convocatoria a la presente licitación.

s) El incumplimiento en el contenido de los documentos o requisitos establecidos en la convocatoria a la presente licitación.

t) Si la proposición técnica o la proposición económica presentadas no son firmadas **Autógrafamente** por la persona facultada para ello en la última hoja de cada una de ellas o no es firmado algún documento en los que aparezca su nombre en el espacio específico para ello.

u) En el caso de personas morales, si el objeto social del acta constitutiva de la persona licitante, no corresponde al objeto de contratación que se requiere en la presente licitación. En el caso de personas físicas, si no acredita que cuenta con la capacidad jurídica y que la actividad económica registrada en el SAT corresponde al objeto que se requiere en la presente licitación.

v) Si la persona licitante no presenta copia simple por ambos lados de la identificación oficial vigente con fotografía (pasaporte, cartilla, credencial del INE o cédula profesional), de la persona que firma la proposición.

w) Si la persona licitante no presenta Acta constitutiva y, en su caso, la última modificación a la misma

x) Si cada uno de los documentos que integren la proposición y aquéllos distintos a ésta, no están foliados en todas y cada una de las hojas que los integren y no se actualiza alguno de los supuestos establecidos en el tercer párrafo del artículo 50 del RLAASSP.

y) En su caso, cuando la persona licitante no acepte las correcciones previstas en el primer párrafo del artículo 55 del RLAASSP.

z) Única y exclusivamente para el caso de proposiciones conjuntas, si no presenta cualquiera de los siguientes documentos:

I. Escrito en el que el representante común de la agrupación manifieste, que la proposición se presenta en forma conjunta.
II. Convenio debidamente formalizado por las personas licitantes que presenten la proposición conjunta, de conformidad a lo establecido en los artículos 34 de la LAASSP y 44 del RLAASSP.
III. Escrito de cada uno de los integrantes de la proposición conjunta manifestando de forma

individual, los documentos señalados en los numerales 3, 4, 5, 6, 9, 10, 11, 12, 13, 14, 15 y 16 del Apartado IV.

2. Criterios de evaluación y adjudicación.

Los criterios de evaluación que la SFP tomará en consideración para la adjudicación son los siguientes:

a) Cumplir con todos los puntos requeridos en el **ANEXO I "ESPECIFICACIONES TÉCNICAS Y ALCANCES DEL SERVICIO"**.

b) El cumplimiento de los requisitos indispensables y que afectan la solvencia de la misma, solicitados e indicados en el **APARTADO IV "REQUISITOS QUE LOS LICITANTES DEBEN CUMPLIR"**, Subapartado denominado **"Documentación Obligatoria" (Indispensables cuyo incumplimiento afecta la solvencia de la proposición), numeral del 1 al 13, así como el 14, únicamente aplicable para proposiciones conjuntas.**

c) El cumplimiento de los documentos y/o requisitos solicitados en la convocatoria a la presente licitación.

d) El cumplimiento en el contenido de los documentos y/o requisitos establecidos en la convocatoria a la presente licitación.

e) Si la proposición técnica y la proposición económica presentadas fueron firmadas por la persona facultada para ello por lo menos en la última hoja de cada una de ellas y fueron firmados los documentos en los que aparezca su nombre en el espacio específico para ello.

f) En el caso de personas morales, que el objeto social del acta constitutiva de la persona licitante, corresponda a la prestación del servicio que se requiere en la presente licitación. en el caso de personas físicas, acredite que cuente con la capacidad jurídica y que la actividad económica registrada en el SAT corresponde al objeto que se requiere en la presente licitación.

g) Si el licitante presenta copia simple por ambos lados de la identificación oficial vigente con fotografía (pasaporte, cartilla, credencial del INE o cédula profesional con fotografía), de la persona que firma la proposición, en el caso de proposiciones conjuntas únicamente el representante común deberá presentar copia simple por ambos lados de la identificación oficial vigente con fotografía (pasaporte, cartilla, credencial del INE o cédula profesional con fotografía).

h) No se acredita que la persona ha acordado con uno u otros elevar el costo del servicio, o cualquier otro acuerdo que tengo como fin obtener una ventaja sobre las demás personas licitantes.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México. C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

i) No presenta más de una proposición, o alternativas de propuestas técnicas o económicas y ninguna propuesta es condicionada.

j) La proposición presentada no contiene virus informático y pudo abrirse, conforme al Acuerdo para el uso de medios remotos de comunicación electrónica, en el envío de proposiciones dentro de las licitaciones públicas que celebren las dependencias y entidades de la Administración Pública Federal, así como en la presentación de las inconformidades por la misma vía. D.O.F. 28/06/2011.

k) Se encuentra la totalidad de los documentos que integren la proposición con folio. De ser el caso la convocante aplicará lo establecido en el tercer párrafo del artículo 50 del RLAASSP.

l) Única y exclusivamente para el caso de proposiciones conjuntas, presenta los siguientes documentos:

- Escrito en el que el representante común de la agrupación manifieste, que la proposición se presenta en forma conjunta.
- Convenio debidamente formalizado por las personas licitantes que presenten la proposición conjunta, de conformidad a lo establecido en los artículos 34 de la LAASSP y 44 del RLAASSP.
- Escrito de cada uno de los integrantes de la proposición conjunta manifestando de forma individual, los documentos señalados en el apartado IV, numerales 3, 4, 5, 6, 9, 10, 11, 12, 13, 14, 15 y 16.

m) En su caso, que la persona licitante acepte las correcciones previstas en el primer párrafo del artículo 55 del RLAASSP.

n) Cotizar todos y cada uno de los conceptos correspondientes a la partida única.

o) Se verificará que exista concordancia entre lo ofertado en la propuesta técnica y económica.

p) El criterio de evaluación será **BINARIO.**

q) Las proposiciones presentadas en el acto de presentación y apertura de proposiciones, se evaluarán de conformidad con el artículo 36 de la LAASSP.

r) La adjudicación se hará al licitante que haya presentado la proposición solvente, porque cumple con los requisitos legales y/o administrativos, técnicos y económicos establecidos en la presente convocatoria, y oferta el precio más bajo, y por tanto garantiza el cumplimiento de las obligaciones respectivas.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020 Tel: (55)20-00-30-00 www.gob.mx/sfp

s) La **Dirección General de Tecnologías de Información** será la responsable de la evaluación de las propuestas técnicas. La evaluación de las propuestas económicas y la evaluación legal-administrativa la llevará a cabo el titular de la **Dirección de Planeación y Adquisiciones** o el superior jerárquico, conforme a lo establecido en el numeral V.11.5. de las POBALINES en materia de Adquisiciones, Arrendamientos y Servicios de la Secretaría de la Función Pública. Dichas evaluaciones servirán como base para la emisión del fallo por parte de la Dirección de Planeación y Adquisiciones.

t) De conformidad con lo establecido en los artículos 36 bis de la LAASSP y 54 del RLAASSP, si derivado de la evaluación de las proposiciones se obtuviera un empate entre dos o más proposiciones solventes, de conformidad con el criterio de desempate, se adjudicará el contrato en primer término a las micro empresas, a continuación, se considerará a las pequeñas empresas y en caso de no contarse con alguna de las anteriores, se adjudicará a la que tenga el carácter de mediana empresa. Para obtener este beneficio las personas licitantes deberán incluir la manifestación correspondiente conforme al **FORMATO 7 "MANIFESTACIÓN DE MIPYME"**.

u) Si derivado de la evaluación de las proposiciones se obtuviera un empate en el precio de dos o más proposiciones solventes y ninguna persona licitante manifiesta encontrarse en el supuesto señalado en el inciso anterior, la adjudicación se efectuará a favor de la persona licitante que resulte adjudicada del sorteo manual por insaculación que la SFP celebrará, en su caso, en el acto de fallo, el cual consistirá en la participación de un boleto por cada proposición que resulte empatada y depositados en una urna, de la que se extraerá el boleto de la persona licitante.

v) Cuando el licitante no se encuentre en alguno de los supuestos de los artículos 50 y 60 de la LAASSP.

w) Cuando el licitante no se encuentra en ninguno de los supuestos de los artículos 49 fracción IX y 72 de la Ley General de Responsabilidades Administrativas

2.1 Criterio de evaluación binario.

Con apego en lo dispuesto por los artículos 26 fracción I, 36, 36 Bis de la Ley, 51 del Reglamento, la evaluación de las proposiciones se realizará utilizando el criterio de evaluación binario, es decir Cumple o No cumple, considerando exclusivamente los requisitos y condiciones establecidos en la presente Convocatoria y en las respuestas proporcionadas en la Junta de Aclaraciones, así como en las "Especificaciones Técnicas y alcances del Servicio " descritas en el **ANEXO I** y en el **ANEXO II**, a efecto de que se garantice satisfactoriamente el cumplimiento de las obligaciones respectivas.

Los requisitos de forma que se señalan en la presente Convocatoria y que no afectan la solvencia de la proposición, se entenderán que, si bien para efectos de descalificación no es indispensable su cumplimiento, si lo es para la mejor conducción del procedimiento.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

Ninguna de las condiciones contenidas en la presente Convocatoria podrán ser modificadas una vez proporcionadas las respuestas en la Junta de Aclaraciones; así como ninguna de las proposiciones presentadas por los licitantes podrán ser negociadas.

Se verificará que las proposiciones cumplan con todo lo señalado en la presente convocatoria.

2.1.1 Evaluación de la documentación distinta a la proposición (legal-administrativa).

A) Se verificará si la proposición fue debidamente firmada electrónicamente.

B) Después de constatar que el licitante firmó adecuadamente su(s) proposición(es), se procederá a la evaluación de la documentación distinta a la proposición a que se refieren el **APARTADO IV** de la Convocatoria bajo el título **"REQUISITOS QUE DEBERÁN CUMPLIR QUIENES DESEEN PARTICIPAR"** apartado **Documentación obligatoria (indispensables cuyo incumplimiento afecta la solvencia de la proposición)** a fin de verificar el cumplimiento de los extremos exigidos tanto en la Ley, el Reglamento, así como las condiciones establecidas en la Convocatoria.

El análisis correspondiente a la documentación distinta (legal – administrativa) se realizará por el área contratante, la Dirección de Planeación y Adquisiciones de la Dirección General de Recursos Materiales y Recursos Generales de la SFP.

2.1.2 Evaluación técnica.

Asimismo, se evaluará la PROPUESTA TÉCNICA de los licitantes, para tal efecto, se procederá a revisar el cumplimiento de los REQUERIMIENTOS TÉCNICOS de conformidad con lo previsto en el ANEXO I de la Convocatoria y el resultado de la (las) Junta (s) de aclaraciones respectivas.

A) Para que una proposición sea aceptada, deberá cumplir en su totalidad con las Especificaciones Técnicas, señaladas en el ANEXO I y lo correspondiente a la (las) Junta (s) de aclaraciones.

El análisis correspondiente a las propuestas técnicas se realizará por el área requirente la **Dirección General de Tecnologías de Información.**

2.1.3 Evaluación económica.

De advertirse que la(s) propuesta(s) técnica(s) evaluada(s) cumplen en su totalidad con las Especificaciones Técnicas y Alcances del Servicio señaladas en el Anexo I y el resultado de la (las) Junta (s) de aclaraciones, se procederá a realizar la evaluación de la(s) PROPUESTA(S) ECONÓMICA(S).

Para que una proposición sea aceptada, deberá cumplir en su totalidad con los aspectos económicos solicitados en el **ANEXO II** y el resultado de la (las) Junta (s) de aclaraciones; así como lo establecido en la Convocatoria a la Licitación.

Se verificará que las propuestas presentadas correspondan a las características y especificaciones del servicio solicitado, emitiendo la evaluación correspondiente, en caso de que no se presente conforme a lo solicitado o no sea lo requerido, la proposición será desechada.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

Cuando la Convocante detecte un error de cálculo en alguna proposición podrá llevar a cabo su rectificación sin modificar los precios unitarios. Si la Propuesta Económica del licitante a quien se le adjudiquen los contratos específicos fuera objeto de correcciones y éste no las aceptase, se aplicará lo dispuesto en el segundo párrafo del artículo 46 de la Ley respecto del contrato.

En su caso, se verificará que los precios de las proposiciones presentadas por los licitantes sean aceptables y/o convenientes de conformidad al artículo 51, del RLAASSP.

El análisis correspondiente a la Propuesta Económica, se realizará por el área contratante, es decir, la Dirección de Planeación y Adquisiciones de la Dirección General de Recursos Materiales y Servicios Generales de la SFP.

2.1.4 Evaluación final.

De acuerdo con la evaluación realizada bajo el criterio de evaluación binario, el contrato **se adjudicará al licitante** cuya proposición resulte solvente, porque cumple con todos los requisitos legales-administrativos, técnicos y económicos establecidos en la Convocatoria, y garantiza el cumplimiento de las obligaciones respectivas, presentado conforme al ANEXO I; y además sea el precio más bajo y éste, de ser el caso, resulte conveniente y aceptable.

En caso de empate derivado de la evaluación de las proposiciones entre dos o más proposiciones solventes, se procederá conforme a lo dispuesto por los artículos 36 Bis segundo y tercer párrafo de la Ley y 54 del Reglamento, y se adjudicará el contrato en primer término a las micro empresas, a continuación, se considerará a las pequeñas empresas y en caso de no contarse con alguna de las anteriores, se adjudicará a la que tenga el carácter de mediana empresa. Para obtener este beneficio las personas licitantes deberán incluir la manifestación correspondiente conforme al **FORMATO 7 "MANIFESTACIÓN DE MIPYME".**

Si derivado de la evaluación de las proposiciones se obtuviera un empate en el precio de dos o más proposiciones solventes y ninguna persona licitante manifiesta encontrarse en el supuesto señalado en el párrafo anterior, la adjudicación se efectuará a favor de la persona licitante que resulte adjudicada del sorteo manual por insaculación que la SFP celebrará, en su caso, en el acto de fallo, el cual consistirá en la participación de un boleto por cada proposición que resulte empatada y depositados en una urna, de la que se extraerá el boleto de la persona licitante.

Finalmente, de conformidad con lo previsto en el **numeral 1.10. del apartado III. "Indicaciones respecto al Fallo y a la firma del Contrato"**, se procederá en su caso, a adjudicar el contrato al licitante que corresponde, y a establecer las condiciones para la firma del mismo.

3 Requisitos cuyo incumplimiento no afectan la solvencia de la proposición.

a) El omitir aspectos que puedan ser cubiertos con información contenida en la propia proposición.

b) El no presentar la información en los formatos establecidos en esta licitación, siempre y cuando la información requerida en ellos sea proporcionada de manera clara y en su totalidad.

c) El no enviar su proposición requerida en papel membretado del licitante.

d) El no enviar formato de entrega de documentación.

e) Y los demás que de manera expresa se señalen en la presente convocatoria a la licitación.

En el Acto de Presentación y Apertura de Proposiciones, no habrá revisión de la documentación recibida; el análisis detallado de su contenido, se efectuará durante el proceso de evaluación de las proposiciones.

Se verificará que las proposiciones cumplan con todo lo señalado en el **ANEXO I** de la presente licitación, así como en el resultado en la Junta de Aclaraciones.

Cuando la Convocante detecte un error de cálculo en alguna proposición, podrá llevar a cabo su rectificación cuando la corrección no implique la modificación del importe especificado por el licitante en el **ANEXO II.**

Si la propuesta económica del licitante a quien se le adjudica el contrato fue objeto de correcciones y éste no acepta las mismas, se aplicará lo dispuesto en el segundo párrafo del artículo 46 de la Ley.

APARTADO VI. DOMICILIO DE LAS OFICINAS Y LA DIRECCIÓN ELECTRÓNICA DE COMPRANET, EN QUE PODRÁN PRESENTARSE INCONFORMIDADES.

1. Presentación de inconformidades.

En términos del artículo 65 y 66 de la Ley, los licitantes podrán presentar escrito de inconformidad directamente en el Órgano Interno de la Secretaría de la Función Pública ubicadas en Avenida de los Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México.

Asimismo, se señala que tales inconformidades podrán presentarse mediante el Sistema CompraNet en la dirección electrónica https://upcp-compranet.hacienda.gob.mx/
Atención a usuarios: 55-3688-1977.
Correo electrónico: cnet_inconformidades@hacienda.gob.mx

Lo anterior, contra actos del procedimiento de contratación que contravengan las disposiciones que rigen las materias objeto del mencionado ordenamiento antes citado, en las inconformidades que se presenten a través de CompraNet, deberán utilizarse medios de identificación electrónica en sustitución de la firma autógrafa.

La SFP conocerá de las inconformidades que se promuevan contra los actos de los procedimientos de la Licitación que se indican a continuación:

A. La Convocatoria, y las Juntas de Aclaraciones.

   En este supuesto, la inconformidad sólo podrá presentarse por el interesado que haya manifestado su interés por participar en el procedimiento según lo establecido en el artículo 33 bis de la Ley, dentro de los seis días hábiles siguientes a la celebración de la última Junta de Aclaraciones.

B. El Acto de Presentación y Apertura de Proposiciones, y el Fallo.

En este caso, la inconformidad sólo podrá presentarse por quien hubiere presentado proposición dentro de los seis días hábiles siguientes a la celebración de la junta pública en la que se dé a conocer el fallo, o de que se le haya notificado al licitante en los casos en que no se celebre junta pública.

C. La cancelación de la licitación.

En este supuesto, la inconformidad sólo podrá presentarse por la persona licitante que hubiere presentado proposición, dentro de los seis días hábiles siguientes a su notificación, y

D. Los actos y omisiones por parte de la dependencia que impidan la formalización del contrato en los términos establecidos en la convocatoria o en la Ley.

En esta hipótesis, la inconformidad sólo podrá presentarse por quien haya resultado adjudicado, dentro de los seis días hábiles posteriores a aquél en que hubiere vencido el plazo establecido en el fallo para la formalización del contrato o, en su defecto, el plazo legal.

En todos los casos en que se trate de licitantes que hayan presentado proposición conjunta, la inconformidad sólo será procedente si se promueve conjuntamente por todos los integrantes de la misma.

La interposición de la inconformidad en forma o ante autoridad diversa a la señalada en este Apartado, según cada caso, no interrumpirá el plazo para su oportuna presentación.

Confidencialidad.

El proveedor se obliga a no divulgar por escrito, verbalmente o por cualquier otro medio la información que obtenga para el cumplimiento del contrato y mantener en la más estricta confidencialidad, los resultados parciales y finales del mismo, absteniéndose de dar a conocer cualquier información al respecto.

La información contenida en el contrato que derive de esta convocatoria es pública de conformidad con lo dispuesto en el artículo 1, 24 fracción VI y 70 fracción XXVIII, de la Ley General de Transparencia y Acceso a la Información Pública; sin embargo la información que proporcione la Dependencia al proveedor para el cumplimiento del objeto materia del mismo, será considerada como confidencial en términos del artículo 116 último párrafo del citado ordenamiento jurídico, por lo que el proveedor se compromete a recibir, proteger y guardar la información confidencial proporcionada por la Dependencia con el mismo empeño y cuidado que tiene respecto de su propia información confidencial, así como hacer cumplir a todos y cada uno de los usuarios autorizados a los que les entregue o permita acceso a la información confidencial, en los términos del mencionado contrato.

El proveedor se compromete a que la información considerada como confidencial no será utilizada para fines diversos a los autorizados en el contrato; asimismo, dicha información no podrá ser copiada o duplicada total o parcialmente en ninguna forma o por ningún medio, ni podrá ser divulgada a terceros que no sean usuarios autorizados. De esta forma, el proveedor se obliga a no divulgar o

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

publicar informes, datos y resultados obtenidos de la prestación de los servicios objeto del contrato, toda vez que son propiedad de la Dependencia.

Cuando concluya la vigencia del contrato, subsistirá la obligación de confidencialidad sobre los servicios solicitados en este instrumento legal y de los insumos utilizados para prestar los servicios.

En caso de incumplimiento a lo establecido, el proveedor tiene conocimiento de que la Dependencia podrá ejecutar o tramitar las sanciones.

Protocolo de actuación en materia de contrataciones públicas.

Se informa a los particulares, lo siguiente:

1) Los servidores públicos en el contacto con particulares deben observar el Protocolo de Actuación en Materia de Contrataciones Públicas, Otorgamiento y Prórroga de Licencias, Permisos, Autorizaciones y Concesiones, publicado mediante acuerdo en el Diario Oficial de la Federación el 20 de agosto de 2015 y sus modificaciones, las cuales pueden ser consultadas en la sección de la Secretaría de la Función Pública, que se encuentra en el Portal de la Ventanilla Única Nacional, a través de la liga www.gob.mx/sfp.

2) Los datos personales que se recaben con motivo del contacto con particulares serán protegidos y tratados conforme a las disposiciones jurídicas aplicables.

3) En caso de que se advierta algún incumplimiento de las obligaciones establecidas en el protocolo podrá presentar queja o denuncia, ante el Órgano Interno de Control de la Secretaría de la Función Pública con domicilio ubicado en Avenida de los Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México.

2. Denuncias.

En términos de lo dispuesto en el artículo 92 de la Ley General de Responsabilidades Administrativas, las autoridades investigadoras establecerán áreas de fácil acceso, para que cualquier interesado pueda presentar denuncias por presuntas faltas administrativas; mismas que deberán contener conforme al artículo 93 los datos o indicios que permitan advertir la presunta responsabilidad administrativa por la comisión de faltas administrativas, y podrán ser presentadas de manera electrónica a través de los mecanismos que para tal efecto establezcan las autoridades investigadoras, lo anterior sin menoscabo de la plataforma digital que determine, para tal efecto, el Sistema Nacional Anticorrupción, de conformidad con los criterios establecidos en la citada Ley. Para este fin, podrá presentar la denuncia ante el Órgano Interno de Control de la Secretaría de la Función Pública con domicilio ubicado en Avenida de los Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México. Asimismo, podrá presentarla en el Sistema Integral de Denuncias Ciudadanas (SIDEC) en la siguiente liga https://sidec.funcionpublica.gob.mx/

3. Sanciones.

Se hace del conocimiento a los licitantes que podrán ser sancionados en caso de encontrarse en alguno de los supuestos previstos en los artículos 50 y 60 de la Ley, o incurrir en alguna de las hipótesis previstas en los artículos 65 al 72 de la Ley General de Responsabilidades Administrativas.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020, Tel: (55)20-00-30-00 www.gob.mx/sfp

Las sanciones que podrían imponerse son las establecidas en el artículo 81 fracciones I y II del mismo ordenamiento.

4. Ley General de Responsabilidades Administrativas.

Asimismo, la Convocante informa a los particulares, lo siguiente:

Que son actos de particulares vinculados con faltas administrativas graves, conforme a los artículos del 65 al 72 de Ley General de Responsabilidades Administrativas: el soborno, la colusión, la obstrucción de facultades de investigación, el uso indebido de recursos públicos, el tráfico de influencias, la participación ilícita en procedimientos administrativos, la utilización de información falsa y la contratación indebida de ex servidores públicos.

En caso de acreditarse la falta grave de algún particular ya sea persona física o moral, las sanciones que podrían imponerse previo desahogo del procedimiento correspondiente, de acuerdo con el artículo 81 fracciones I y II de la Ley General de Responsabilidades Administrativas, son: la sanción económica, la inhabilitación temporal para participar en contrataciones, la indemnización por daños y perjuicios ocasionados a la Hacienda Pública (federal, local o municipal), la suspensión de actividades y la disolución de la sociedad respectiva.

APARTADO VII. FORMATOS QUE FACILITEN Y AGILICEN LA PRESENTACIÓN Y RECEPCIÓN DE LAS PROPOSICIONES

La relación de los documentos que deben presentar los participantes en el procedimiento de Licitación Pública Electrónica de Carácter Nacional, será verificada en el Acto de Presentación y Apertura de Proposiciones, de acuerdo al "acuse de presentación de proposición electrónica a través de CompraNet", mismo que emite el sistema de forma automática al cargar la proposición.

Los formatos que se incluyen en esta Licitación deben considerarse solo como una guía, por lo que la adecuada presentación de las proposiciones es responsabilidad exclusiva de los licitantes.

FORMAN PARTE INTEGRANTE DE LA PRESENTE CONVOCATORIA LOS SIGUIENTES ANEXOS Y FORMATOS

RELACIÓN DE ANEXOS

ANEXO I.	ESPECIFICACIONES TÉCNICAS Y ALCANCES DEL SERVICIO.
ANEXO II.	FORMATO DE PROPUESTA ECONÓMICA
ANEXO III.	MODELO DE CONTRATO
ANEXO IV.	SOLICITUD DE AFILIACIÓN A CADENAS PRODUCTIVAS DE NAFIN

ANEXO V. NOTA INFORMATIVA PARA PARTICIPANTES DE PAÍSES MIEMBROS DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OCDE).

ANEXO VI. FORMATO DE FIANZA PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO.

RELACIÓN DE FORMATOS

FORMATO 1. ACREDITACIÓN DE LA EXISTENCIA LEGAL Y PERSONALIDAD JURÍDICA DEL LICITANTE

FORMATO 2. MANIFESTACIÓN DE QUE EL LICITANTE NO SE UBICA EN LOS SUPUESTOS ESTABLECIDOS EN LOS ARTÍCULOS 50 Y 60 DE LA LEY.

FORMATO 3. DECLARACIÓN DE INTEGRIDAD.

FORMATO 4. MANIFESTACIÓN DE NACIONALIDAD.

FORMATO 5. CUMPLIMIENTO DE NORMAS.

FORMATO 6. MANIFESTACIÓN CON RELACIÓN AL PUNTO 29 DEL ACUERDO POR EL QUE SE ESTABLECEN LAS DISPOSICIONES QUE SE DEBERÁN OBSERVAR PARA LA UTILIZACIÓN DEL SISTEMA ELECTRÓNICO DE INFORMACIÓN PÚBLICA GUBERNAMENTAL DENOMINADO COMPRANET.

FORMATO 7. MANIFESTACIÓN MIPYME.

FORMATO 8. CARTA DE LOS ARTÍCULOS 49 FRACCIÓN IX Y 72 DE LA LEY GENERAL DE RESPONSABILIDADES ADMINISTRATIVAS.

FORMATO 9. DECLARACIÓN DE CONOCER EL PROTOCOLO DE ACTUACIÓN.

FORMATO 10. MANIFESTACIÓN DE INFORMACIÓN RESERVADA Y/O CONFIDENCIAL

FORMATO 11. DOMICILIO CONVENCIONAL

FORMATO 12. ESCRITO DE CONFIDENCIALIDAD

FORMATO 13. CONSENTIMIENTO POR PARTE DEL REPRESENTANTE LEGAL (EL TITULAR) PARA EL USO DE DATOS PERSONALES.

FORMATO 14 CORREO ELECTRÓNICO DEL LICITANTE

FORMATO 15. ENCUESTA DE TRANSPARENCIA

APARTADO VIII. INFORMACIÓN ESPECÍFICA DE LA PRESTACIÓN DEL SERVICIO

1. Cantidades adicionales que podrán contratarse.

De conformidad con el artículo 52 de la LAASSP, la SFP, dentro de su presupuesto aprobado y disponible, y por razones fundadas y explicitas, podrá incrementar el monto del contrato mediante modificaciones al contrato vigente derivado del presente procedimiento, sin tener que recurrir a la celebración de un nuevo procedimiento, siempre que las modificaciones no rebasen, en conjunto, el veinte por ciento del monto o cantidad de los conceptos o volúmenes establecidos originalmente en el mismo y el precio del servicio sea igual al pactado originalmente.

APARTADO IX. SUSPENSIÓN O CANCELACIÓN DEL PROCEDIMIENTO

1. Suspensión del Procedimiento.

Se podrá suspender el procedimiento cuando el OIC de la SFP así lo determine con motivo de su intervención y de acuerdo a sus facultades, conforme a lo dispuesto por el artículo 70 de la LAASSP, dicha suspensión se hará del conocimiento de las personas licitantes mediante aviso vía correo electrónico.

Una vez que desaparezcan las causas que motivaron la suspensión, se reanudará la misma, previo aviso a las personas licitantes.

2. Cancelación del procedimiento, partidas o conceptos.

Se procederá a la cancelación del procedimiento, partidas o conceptos incluidos en este procedimiento de contratación:

a) Por caso fortuito;

b) Por causa de fuerza mayor;

c) Cuando existan circunstancias, debidamente justificadas, que provoquen la extinción de la necesidad para continuar con la prestación del servicio, y que de continuarse con el procedimiento de contratación se pudiera ocasionar un daño o perjuicio a la propia SFP.

En el acta correspondiente, se asentarán las causas que motivaron la suspensión o cancelación del procedimiento.

En caso de ser cancelado este procedimiento, se notificará a los participantes de la misma manera como fueron convocados.

La SFP cancelará la Licitación por la pérdida del mecanismo de seguridad del sistema CompraNet.

APARTADO X. PROCEDIMIENTO DESIERTO.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

La Convocante procederá a declarar desierto el presente procedimiento de contratación en los siguientes casos:

a) Al revisar la plataforma CompraNet, no se encuentra proposición alguna enviada por medios remotos de comunicación electrónica.

b) Cuando la totalidad de las proposiciones presentadas no reúnan los requisitos solicitados en la presente licitación.

c) Si las proposiciones recibidas exceden la suficiencia presupuestal asignada para este procedimiento y el área requirente determina que no es posible la asignación de recursos.

APARTADO XI. SANCIONES.

Los licitantes o proveedores que infrinjan las disposiciones de la LAASSP, serán sancionados por la Secretaría de la Función Pública de conformidad a lo establecido en los artículos 59 y 60 de la Ley.

APARTADO XII. PENAS CONVENCIONALES.

De conformidad con lo establecido en el artículo 53 de la LAASSP, la SFP a través de los Titulares de las áreas requirentes, aplicará al proveedor las penas convencionales a las que se haga acreedor por atraso en el cumplimiento de las fechas pactadas para la prestación del servicio, establecidos en el **numeral 11. PENAS CONVENCIONALES** del **ANEXO I "ESPECIFICACIONES TÉCNICAS Y ALCANCES DEL SERVICIO".**

En el caso de incumplimiento en el tiempo para la prestación del servicio, el administrador del contrato procederá a notificar al PROVEEDOR o a su representante legal la pena respectiva, dentro de los 30 (treinta) días hábiles siguientes a la fecha en que se hayan generado las penas convencionales, notificando, igualmente a la DGPyP, para que ésta reciba de parte del PROVEEDOR, el comprobante que acredite el pago de la pena convencional.

Las penas convencionales se deberán pagar a la TESOFE directamente por el proveedor, lo cual podrá realizar en cualquier institución bancaria definida para el efecto por la TESOFE mediante la presentación del formato mencionado anteriormente.

En caso de que sea rescindido el contrato correspondiente, no procederá el cobro de las penas convencionales o de las deducciones al pago.

La SFP podrá aplicar las sanciones, en caso de que el PROVEEDOR incurra en cualquiera de los supuestos establecidos en el **ANEXO I "ESPECIFICACIONES TÉCNICAS Y ALCANCES DEL SERVICIO"**.

APARTADO XIII. DEDUCCIONES AL PAGO.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

De conformidad con lo establecido en el artículo 53 Bis de la LAASSP y 97 del RLAASSP, la SFP a través del Titular del área requirente, establece que no aplican deducciones al pago.

APARTADO XIV. CAUSALES DE RESCISIÓN

De conformidad con el artículo 54 de la Ley, y 98 de su Reglamento, la SFP podrá en cualquier momento rescindir el contrato, cuando el proveedor incurra en incumplimiento de cualquiera de los siguientes supuestos:

Cuando el importe de las penas convencionales alcance el monto máximo aplicable, y la causa de la pena persista.

a. Si el proveedor adjudicado no entrega la garantía de cumplimiento conforme al plazo estipulado en la normatividad vigente y la cláusula denominada Garantía de Cumplimiento.
b. Cuando el importe de las penas convencionales alcance el monto de la garantía de cumplimiento.
c. Si el proveedor es declarado por autoridad competente, en concurso mercantil o de acreedores o en cualquier situación análoga que afecte su patrimonio.
d. Si el proveedor cede, vende, traspasa o subcontrata en forma total o parcial los derechos y obligaciones derivados del contrato; o transfiere los derechos de cobro derivados del contrato, sin contar con el consentimiento de la dependencia, a través del(a) administrador (a) del contrato correspondiente.
e. Si el proveedor no da a la dependencia o a quien éste designe por escrito, las facilidades o datos necesarios para la supervisión o inspección en la prestación del servicio.
f. Por presentar una garantía apócrifa.
g. Si el proveedor incurriera en falta de veracidad, total o parcialmente respecto a la información proporcionada para la celebración de este contrato.

En general, por el incumplimiento por parte del proveedor a cualquiera de las obligaciones derivadas del contrato y sus anexos o a las leyes y reglamentos aplicables, además de las señaladas en el **ANEXO I "ESPECIFICACIONES TÉCNICAS Y ALCANCES DEL SERVICIO"**.

En caso de incumplimiento del proveedor a cualquiera de las obligaciones del contrato, la SFP podrá optar entre exigir el cumplimiento del mismo y el pago de las penas convencionales por el atraso, o declarar la rescisión administrativa conforme al procedimiento que se señala en la Cláusula denominada Rescisión y hacer efectiva la garantía de cumplimiento, en forma proporcional al incumplimiento, sin menoscabo de que la SFP pueda ejercer las acciones judiciales que procedan.

En este caso, la aplicación de la garantía de cumplimiento será proporcional al monto de las obligaciones incumplidas, salvo que, por las características del servicio, éstos no puedan ser utilizados por la Dependencia por estar incompletos, en cuyo caso, la aplicación de la garantía correspondiente será total.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

En caso de que sea rescindido el contrato, no procederá el cobro de las penas por atraso ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento si la hubiere.

Si el proveedor es quien decide rescindirlo, será necesario que acuda ante la autoridad judicial y obtenga a declaración o resolución correspondiente.

APARTADO XV. SOLICITUD DE PRÓRROGAS.

Conforme a lo establecido en el artículo 91 del RLAASSP, solo en caso fortuito, fuerza mayor o causas atribuibles a la convocante, se considerará el otorgamiento de prórrogas.

APARTADO XVI. TERMINACIÓN ANTICIPADA DEL CONTRATO.

Conforme a lo establecido en el artículo 54 Bis de la LAASSP, la SFP podrá dar por terminado anticipadamente el(los) Contrato(s) que se suscriba(n) sin que medie resolución judicial, en los siguientes casos:

a) Cuando concurran razones de interés general.
b) Cuando por causa justificada se extinga la necesidad de continuar con la prestación del servicio originalmente requerido y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas se ocasionaría algún daño o perjuicio al Estado.
c) Cuando se determine la nulidad total o parcial de los actos que dieron origen al contrato, con motivo de la resolución de una inconformidad emitida por la Secretaría de la Función Pública.

La determinación de dar por terminado anticipadamente el Contrato deberá constar por escrito mediante resolución emitida por la Coordinación Consultiva de la Unidad de Asuntos Jurídicos de la SFP, previo dictamen emitido por el área requirente, en el cual se precisen las razones o las causas justificadas que den origen a la misma y bajo su responsabilidad, siendo el Titular de la Dirección General de Recursos Materiales y Servicios Generales el encargado de notificarlo al proveedor.

Derivado de lo anterior, se procederá a la formalización de la terminación respectiva y del Finiquito que elabore el Titular designado de la SFP, en el que se detallarán en forma pormenorizada los importes a cubrir, el servicio entregado y los que estén pendientes de pago.

Asimismo, la SFP reembolsará al proveedor los gastos no recuperables en que haya incurrido, siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con el contrato correspondiente.

APARTADO XVII. CONDICIONES DE PAGO.

1. Anticipos.

La SFP no otorgará anticipos.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

2. Del pago.

El pago será por la prestación del servicio de acuerdo al artículo 51 de la LAASSP, dentro de los 20 (veinte) días naturales siguientes, previa presentación y autorización a satisfacción del administrador del contrato, de la factura correspondiente.

En términos de lo dispuesto en el artículo 90 del Reglamento de la LAASSP, en caso de que los Comprobantes Fiscales Digitales por Internet (CFDI) entregados por el proveedor para su pago, presenten errores o deficiencias, la SFP a través del responsable de administrar el contrato, deberá indicarlo por escrito dentro de los tres días hábiles siguientes al de su recepción. El periodo que transcurre a partir de la entrega del citado escrito y hasta que el proveedor presente las correcciones, no se computará para efectos del plazo de pago señalado en el párrafo anterior.

Para efecto de lo anterior, la persona licitante adjudicada deberá presentar la siguiente documentación:

Facturar a: **Secretaría de la Función Pública.**
Avenida de los Insurgentes Sur No. 1735, Col. Guadalupe Inn,
Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México.
R.F.C. SFP941229 IMA

La factura electrónica deberá enviarse al correo electrónico **envio_factura_sfp@funcionpublica.gob.mx**

Los CFDI deberán contener entre otros, la información relativa al nombre y número de la licitación mediante la que se adjudicó el contrato, el número de contrato correspondiente, así como la descripción del servicio facturado, asimismo deberá cumplir con los requisitos establecidos en el artículo 29-A del Código Fiscal de la Federación.

- Para el trámite de las transferencias electrónicas a las cuentas bancarias de las solicitudes de pago a favor de la (las) persona licitante (s) adjudicada (s), es indispensable se proporcione copia de los siguientes documentos:

SISTEMA INTEGRAL DE ADMINISTRACIÓN FINANCIERA FEDERAL (SIAFF)

Para el trámite de las transferencias electrónicas a las cuentas bancarias de las solicitudes de pago a favor de los prestadores de bienes y/o servicios, es indispensable se proporcione copia de los siguientes documentos:

PERSONAS FÍSICAS:

- Registro Federal de Contribuyentes (R.F.C.).

- Número de CLABE (Clave Bancaria Estandarizada), la cual consta de 18 posiciones, para lo cual deberá enviarse copia de la carátula del Estado de Cuenta Bancaria aperturada por el beneficiario, donde se demuestre el nombre, domicilio fiscal y número de cuenta.
- Comprobante de domicilio fiscal reciente (preferentemente telefónico).
- CURP.
- Copia de la identificación oficial.

PERSONAS MORALES:

- Registro Federal de Contribuyentes (R.F.C.).
- Número de CLABE (Clave Bancaria Estandarizada), la cual consta de 18 posiciones, para lo cual deberá enviarse copia de la carátula del Estado de Cuenta Bancaria aperturada por el beneficiario, donde se demuestre el nombre, domicilio fiscal y número de cuenta.
- Comprobante de domicilio fiscal reciente (preferentemente telefónico).

La SFP no pagará los servicios que no hayan sido prestados por la (las) persona licitante (s) adjudicada (s), el importe de la factura se determinará de acuerdo a los servicios prestados.

Cabe hacer mención que el pago quedará condicionado proporcionalmente al pago que el proveedor deba efectuar por concepto de penas convencionales.

3. Pagos progresivos.

Para el presente procedimiento, no habrá pagos progresivos.

4. Programa de Cadenas Productivas.

El proveedor podrá solicitar la realización de la cesión de los derechos de cobro a favor de un intermediario financiero de su elección, en virtud del acuerdo que la SFP tiene concertado con Nacional Financiera, S.N.C. denominado "Programa de Cadenas Productivas", a efecto de apoyar a los proveedores, contratistas o prestadores de servicios de la SFP, a través de operaciones de factoraje y descuento electrónico de hasta el 100% del importe de los títulos de crédito y/o documentos en que se consignen derechos de crédito expedidos por la SFP, incluyendo los intereses correspondientes, por lo que será la misma Nacional Financiera, el canal para la recepción de los poderes, actas constitutivas y carta de adhesión que firmen los proveedores y contratistas. **(ANEXO IV)**

APARTADO XVIII. CALIDAD DEL SERVICIO

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

El licitante quedará obligado ante la SFP a responder por la calidad del servicio, así como de cualquier otra responsabilidad en que incurra en los términos señalados en la Convocatoria de la presente licitación, sus anexos, la Junta de Aclaraciones, el contrato respectivo y la Legislación vigente y aplicable en la materia.

Facultad de supervisión en la entrega-recepción del servicio.

La Convocante a través del área responsable del seguimiento a los contratos, podrá realizar supervisiones aleatorias o continuas durante la vigencia del contrato por sí mismo o por conducto de cualquier otra persona.

En caso de considerarse oportuno, se dará vista al OIC de la SFP para que proceda conforme a la legislación aplicable.

APARTADO XIX. REGISTRO DE DERECHOS.

La (las) persona licitante (s) adjudicada (s) asumirá (n) la responsabilidad total en caso de que la prestación del servicio objeto de este procedimiento, viole el registro de derechos a nivel nacional o internacional, derechos de autor, propiedad intelectual o industrial, marcas o patentes.

APARTADO XX. DERECHOS DE AUTOR U OTROS DERECHOS.

De acuerdo a lo establecido en el artículo 45 fracción XX del de la LAASSP, en caso de violaciones en materia de derechos inherentes a la propiedad intelectual, la responsabilidad estará a cargo de la (las) persona licitante (s) adjudicada (s) según sea el caso.

Las personas licitantes deberán respetar los derechos de autor y propiedad intelectual de los logotipos, que son propiedad de la SFP, quedando prohibido el hacer uso de ellos sin que medie autorización expresa de la misma.

APARTADO XXI. IMPUESTOS.

Todo impuesto y/o derecho causado por la prestación del servicio objeto de este procedimiento, será a cargo de la (las) persona licitante (s) adjudicada (s), la SFP retendrá y enterará únicamente el importe correspondiente al Impuesto al Valor Agregado I.V.A.

APARTADO XXII. PROHIBICIÓN DE NEGOCIACIÓN DE LA CONVOCATORIA Y PROPUESTAS.

Ninguna de las condiciones contenidas en la presente convocatoria y sus anexos, así como en las proposiciones presentadas por las personas licitantes, podrán ser negociadas.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

APARTADO XXIII. OBLIGACIONES DE LOS PARTICIPANTES.

Para el presente procedimiento de contratación, se da por hecho que las personas licitantes que presenten ofertas se obligan a cumplir todos los requerimientos incluidos en el presente documento y que éstos han sido comprendidos en su totalidad. En consecuencia, las personas licitantes no podrán argumentar que en su propuesta técnica no incluyeron algún requerimiento solicitado por desconocimiento del mismo.

El participante deberá examinar todas las instrucciones, formularios, condiciones y especificaciones que figuren en la convocatoria del presente procedimiento de contratación ya que si omite alguna parte de información indispensable requerida o presenta una propuesta que no cumpla con los requerimientos solicitados en la convocatoria, la SFP rechazará dicha propuesta.

APARTADO XXIV. CONTROVERSIAS ADMINISTRATIVAS.

Las controversias que se susciten con motivo del presente procedimiento de contratación se resolverán con apego a lo previsto en la LAASSP, su RLAASSP vigente y las demás disposiciones legales aplicables.

APARTADO XXV. LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

En concordancia con lo dispuesto en el artículo 113 de la Ley Federal de Transparencia y Acceso a la Información Pública, las personas licitantes participantes podrán señalar aquella información contenida en su propuesta que deba considerarse como confidencial, siempre que tengan el derecho de reservarse la información, de conformidad con las disposiciones aplicables.

APARTADO XXVI. NOTA INFORMATIVA PARA PARTICIPANTES DE PAÍSES DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OCDE)

Al ser México miembro de la Organización para la Cooperación y el Desarrollo Económico y firmante de la ***Convención para combatir el cohecho de servidores públicos extranjeros en transacciones comerciales internacionales, es compromiso de nuestro país general prácticas para eliminar*** la competencia desleal y crear igualdad de oportunidades para las empresas que compiten por las contrataciones gubernamentales.

En tal sentido y para conocimiento de los licitantes, se incluye como parte integral de la presente convocatoria, el **ANEXO V "NOTA INFORMATIVA PARA PARA PARTICIPANTES DE PAÍSES MIEMBROS DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OCDE)".**

APARTADO XXVII. RELACIONES LABORALES.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

El contrato que se suscriba será de naturaleza estrictamente civil por lo que, el proveedor será el único responsable de las obligaciones derivadas de las disposiciones legales y demás ordenamientos en materia de trabajo y seguridad social para con su personal; por tanto, se obligará a que los recursos humanos que utilice para la prestación del servicio no tendrán con esta Dependencia ninguna relación laboral y que él será el único obligado a afrontar las obligaciones laborales, fiscales, de seguridad social o de cualquier otra naturaleza que pudieran surgir con motivo de los pactos y/o contratos que celebre con sus empleados y a responder de todas las demandas y reclamaciones que sus trabajadores presenten en contra de la SFP, en relación con el objeto del contrato, aún, cuando se le reclame a ésta última alguna responsabilidad solidaria.

Asimismo, el proveedor se obliga a que para el caso de que alguna de las personas designadas para la prestación del servicio entable demanda laboral en contra de la SFP, dentro del término legal concedido para la contestación de la demanda comparecerá ante la autoridad competente a deslindar de toda responsabilidad y prestaciones reclamadas a la Dependencia; lo que deberá comprobar a la SFP con la entrega del acuse de recibo original del escrito que hubiese presentado ante la autoridad competente para asumir toda la responsabilidad, o con la actuación de la autoridad laboral de la que así se desprenda. Para el caso de que no lo haga dentro del término o etapa referidos, ni dentro de los 15 días naturales siguientes a su vencimiento o verificación, la SFP podrá rescindir el contrato, sin perjuicio de que también pueda reclamar en la vía jurisdiccional el pago del total de las prestaciones reclamadas que se lleguen a ocasionar por este motivo.

De igual forma, se obliga a responsabilizarse de las consecuencias jurídicas que pudieran derivarse de la interposición de alguna demanda de cualquier índole que sus empleados pudiesen llegar a interponer en contra de la SFP y que resarcirá a la Dependencia de todo daño o perjuicio que ésta pudiera sufrir por tal situación.

En este sentido, el proveedor se obliga a restituir a la SFP el pago que por cualquier concepto se reclame a ésta en la vía jurisdiccional, efectuado en cualquier etapa del juicio; sin que sea necesario que espere a una sentencia ejecutoriada en su perjuicio.

ATENTAMENTE
EL DIRECTOR

AMBROSIO RENE OLIVA DELGADO

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

ANEXO I

ESPECIFICACIONES TÉCNICAS Y ALCANCES DEL SERVICIO

Nota: Se adjunta en versión editable.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

ANEXO II
FORMATO DE PROPUESTA ECONÓMICA

Nota: Se adjunta en versión editable.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

ANEXO III
MODELO DE CONTRATO

Nota: Se adjunta en versión editable.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

ANEXO IV
"SOLICITUD DE AFILIACIÓN A CADENAS PRODUCTIVAS DE NAFIN"

¿Cadenas Productivas?

Es un programa que promueve el desarrollo de las Pequeñas y Medianas Empresas, a través de otorgarle a los proveedores afiliados liquidez sobre sus cuentas por cobrar derivadas de la proveeduría de bienes ó servicios, contribuyendo así a dar mayor certidumbre, transparencia y eficiencia en los pagos, así como financiamiento, capacitación y asistencia técnica.

¿Afiliarse?

Afiliarse a Cadenas Productivas no tiene ningún costo, consiste en la entrega de un expediente, hecho que se realiza una sola vez independientemente de que usted sea proveedor de una o más Dependencias o Entidades de la Administración Pública Federal.

Una vez afiliado, recibirá una clave de consulta para el Sistema de Cadenas Productivas que corre en internet. A través de Cadenas Productivas podrá consultar la fecha programada de sus cuentas por cobrar, a fin de contar con la opción de realizar el cobro de manera anticipada, permitiendo con ello planear de manera eficiente sus flujos de efectivo, realizar compras de oportunidad o cumplir con sus compromisos.

Cadenas Productivas ofrece:

- Adelantar el cobro de las facturas mediante el *descuento electrónico*
- Obtener liquidez para realizar más negocios
- Mejorar la eficiencia del capital de trabajo
- Agilizar y reducir los costos de cobranza
- Realizar en caso necesario, operaciones vía telefónica a través del Call Center 50 89 61 07 o al 01800 NAFINSA (62 34 672)
- Acceder a capacitación y asistencia técnica gratuita
- Recibir información
- Formar parte del *Directorio de compras del Gobierno Federal*

Características descuento ó factoraje electrónico:

- Anticipar la totalidad de su cuenta por cobrar (documento)
- Descuento aplicable a tasas preferenciales
- Sin garantías, ni otros costos o comisiones adicionales
- Contar con la disposición de los recursos en un plazo no mayor a 24 horas, en forma electrónica y eligiendo al intermediario financiero de su preferencia

DIRECTORIO DE COMPRAS DEL GOBIERNO FEDERAL

¿Qué es el directorio de compras?

Es una base de información de empresas como la suya que venden o desean vender a todas las Dependencias y Entidades del Gobierno Federal. A través de esta herramienta los compradores del Gobierno Federal tendrán acceso a la información de los productos y servicios que su empresa ofrece para la adquisición de bienes y contratación de servicios.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

¿Qué beneficios brinda pertenecer al Directorio?

Incrementar las oportunidades de negocio, ya que a través del directorio las Dependencias y Entidades de la Administración Pública Federal buscarán a proveedores que cuenten con capacidad de respuesta inmediata, con recursos técnicos, financieros y demás que sean necesarios, y cuyas actividades comerciales o profesionales estén relacionadas con los bienes o servicios, objeto del contrato a celebrarse.

Recibirá boletines electrónicos con los requerimientos de las Dependencias y Entidades que se interesen en sus productos y/o servicios para que de un modo ágil, sencillo y transparente pueda enviar sus cotizaciones.

Dudas y comentarios vía telefónica,

Llámenos al teléfono 5089 6107 ó al 01 800 NAFINSA (62 34 672) de lunes a viernes de 9:00 a 17:00 horas.

Dirección Oficina Matriz de Nacional Financiera, S.N.C. Av. Insurgentes Sur 1971 – Col. Guadalupe Inn Alcaldía Álvaro Obregón, C.P. 01020, México, D.F.

LISTA DE DOCUMENTOS PARA LA INTEGRACIÓN DEL EXPEDIENTE DE AFILIACIÓN AL PROGRAMA DE CADENAS PRODUCTIVAS.

1.- Carta Requerimiento de Afiliación.
Debidamente firmada por el área requirente compradora

2.- ** Acta Constitutiva (escritura con la que se constituye o crea la empresa).
Esta escritura debe estar debidamente inscrita en el Registro Público de la Propiedad y de Comercio.
Debe anexarse completa y legible en todas las hojas.

3.- ** Escritura de Reformas (modificaciones a los estatutos de la empresa)
Cambios de razón social, fusiones, cambios de administración, etc.
Estar debidamente inscrita en el Registro Público de la Propiedad y de Comercio.
Completa y legible en todas las hojas.

4.- **Escritura pública mediante la cual se haga constar los Poderes y Facultades del Representante Legal para Actos de Dominio.
Esta escritura debe estar debidamente inscrita en el Registro Público de la Propiedad y de Comercio.
Debe anexarse completa y legible en todas las hojas.

5.- Comprobante de domicilio Fiscal
Vigencia no mayor a 2 meses
Comprobante de domicilio oficial (Recibo de Agua, Luz, Teléfono fijo, Predial)
Debe estar a nombre de la empresa, en caso de no ser así, adjuntar contrato de arrendamiento o comodato.

6.- Identificación Oficial vigente del (los) representante(es) legal(es), con actos de dominio
Credencial de elector; pasaporte vigente o FM2 (para extranjeros)
La firma deberá coincidir con la del convenio

7.- Alta en Hacienda y sus modificaciones
Formato R-1 ó R-2 en caso de haber cambios de situación fiscal (razón social o domicilio fiscal)
En caso de no tener las actualizaciones, pondrán obtenerlas de la página del SAT.

8.- Cédula del Registro Federal de Contribuyentes (RFC, Hoja Azul)

9.- Estado de Cuenta Bancario (entregado por SEPOMEX no internet) donde se depositarán los recursos
Sucursal, plaza, CLABE interbancaria
Vigencia no mayor a 2 meses
Estado de cuenta que emite la Institución Financiera y llega su domicilio.

La documentación arriba descrita, es necesaria para que la promotoría genere los contratos que le permitirán terminar el proceso de afiliación una vez firmados, los cuales constituyen una parte fundamental del expediente:

Contrato de descuento automático Cadenas Productivas
Firmado por el representante legal con poderes de dominio.
2 convenios con firmas originales
Contratos originales de cada Intermediario Financiero.
Firmado por el representante legal con poderes de dominio.

(** Únicamente, para personas morales)

Usted podrá contactarse con la Promotoría que va a afiliarlo llamando al 01-800- NAFINSA (01-800-6234672) o al 50-89-61-07; o acudir a las oficinas de Nacional Financiera, S.N.C. en:

Av. Insurgentes Sur No. 1971, Col Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, México D.F., en el Edificio Anexo, nivel Jardín, área de Atención a Clientes.

Estimado Proveedor del Gobierno Federal:
Con el propósito de iniciar su proceso de afiliación a la Cadena Productiva, es importante que nos proporcione la información abajo indicada; con lo anterior, estaremos en posibilidad de generar los contratos y convenios, mismos que a la brevedad le enviaremos vía correo electrónico.

Información requerida para Afiliación a la Cadena Productiva.

1. **Cadena(s) a la que desea afiliarse:**

*
*
*

Número(s) de proveedor (opcional):
*

2. **Datos generales de la empresa o persona física.**

Razón Social:
Fecha de alta SHCP:
R.F.C.:
Domicilio Fiscal: Calle:
No.:
C.P.:
Colonia:
Ciudad:
Teléfono (incluir clave LADA):
Fax (incluir clave LADA):
e-mail:
Nacionalidad:

3. Datos de constitución de la sociedad: (Acta Constitutiva / Persona Moral)

No. de la Escritura:
Fecha de la Escritura:

4. Datos del Registro Público de la Propiedad y de Comercio (Persona Física)

Fecha de Inscripción:
Entidad Federativa:
Alcaldía o municipio:
Folio:
Fecha del folio :
Libro:
Partida:
Fojas:
Nombre del Notario Público:
No. de Notaria:
Entidad del Corredor o Notario:
Alcaldía o municipio del corredor o Notario:

5. Datos de inscripción y registro de poderes para actos de dominio (Persona Moral):

(Acta de poderes y/o acta constitutiva)
No. de la Escritura:
Fecha de la Escritura:
Tipo de Poder: Único ( ) Mancomunado ( ) Consejo ( )

6. Datos del Registro Público de la Propiedad y de Comercio (Persona Moral):

Fecha de inscripción:
Entidad Federativa:
Alcaldía ó municipio:
Folio:
Fecha del folio :
Libro:
:_____
Fojas:
Nombre del Notario Público:
No. de Notaría:
Entidad del Corredor o Notario:
Alcaldía o municipio del corredor o Notario:

7. Datos del representante legal con actos de administración o dominio:

Nombre:
Estado civil:
Fecha de nacimiento:
R.F.C.:
Fecha de alta SHCP:
Teléfono:
Fax (incluir clave LADA):
e-mail:
Nacionalidad:

Tipo de identificación oficial: Credencial IFE ( ) Pasaporte Vigente ( ) FM2 o FM3 extranjeros ( )
No. de la identificación (si es IFE poner el No. que está en la parte donde está su firma):
Domicilio Fiscal: Calle:
No.:
C.P.:
Colonia:
Ciudad:

8. Datos del banco donde se depositarán recursos:

Moneda: pesos (X) dólares ( )
Nombre del banco:
No. de cuenta (11 dígitos):
Plaza:
No. de sucursal:
CLABE bancaria:(18 dígitos):
Régimen: Mancomunada ( )
Individual ( )
Indistinta ( )
Órgano colegiado ( )

9. Persona(s) autorizada(s) por la PyME para la entrega y uso de claves:

Nombre:
Puesto:
Teléfono (incluir clave LADA):
Fax:
e-mail:

10. Actividad empresarial:

Fecha de inicio de operaciones:
Personal ocupado:
Actividad ó giro:
Empleos a generar:
Principales productos:
Ventas (último ejercicio) anuales:
Netas exportación:
Activo total (aprox.):
Capital contable (aprox.)
Requiere Financiamiento SI NO

LISTA DE DOCUMENTOS PARA LA INTEGRACIÓN DEL EXPEDIENTE DE AFILIACIÓN AL PROGRAMA DE CADENAS PRODUCTIVAS

1.- Carta Requerimiento de Afiliación.
- Debidamente firmada por el área usuaria compradora

2.- **Copia simple del Acta Constitutiva (Escritura con la que se constituye o crea la empresa).

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

- Esta escritura debe estar debidamente inscrita en el Registro Público de la Propiedad y de Comercio.
- Debe anexarse completa y legible en todas las hojas.

3.- **Copia simple de la Escritura de Reformas (modificaciones a los estatutos de la empresa)
- Cambios de razón social, fusiones, cambios de administración, etc.,
- Estar debidamente inscrita en el Registro Público de la Propiedad y del Comercio.
- Completa y legible en todas las hojas.

4.- **Copia simple de la escritura pública mediante la cual se haga constar los Poderes y Facultades del Representante Legal para Actos de Dominio.
- Esta escritura debe estar debidamente inscrita en el Registro Público de la Propiedad y de Comercio.
- Debe anexarse completa y legible en todas las hojas.

5.- Comprobante de domicilio Fiscal
- Vigencia no mayor a 2 meses
- Comprobante de domicilio oficial (Recibo de agua, Luz, Teléfono fijo, predio)
- Debe estar a nombre de la empresa, en caso de no ser así, adjuntar contrato de arrendamiento, comodato.

6.- Identificación Oficial Vigente del (los) representante(es) legal(es), con actos de dominio
- Credencial de elector; pasaporte vigente o FM2 (para extranjeros)
- La firma deberá coincidir con la del convenio

7.- Alta en Hacienda y sus modificaciones
- Formato R-1 o R-2 en caso de haber cambios de situación fiscal (razón social o domicilio fiscal)
- En caso de no tener las actualizaciones, pondrán obtenerlas de la página del SAT.

8.- Cédula del Registro Federal de Contribuyentes (RFC, Hoja Azul)

9.- Estado de Cuenta Bancario donde se depositarán los recursos
- Sucursal, plaza, CLABE interbancaria
- Vigencia no mayor a 2 meses
- Estado de cuenta que emite la Institución Financiera y llega su domicilio.

La documentación arriba descrita, es necesaria para que la promotoría genere los contratos que le permitirán terminar el proceso de afiliación una vez firmados, los cuales constituyen una parte fundamental del expediente:

A) Contrato de descuento automático Cadenas Productivas
- Firmado por el representante legal con poderes de dominio.
- 2 convenios con firmas originales

B) Contratos Originales de cada Intermediario Financiero.
- Firmado por el representante legal con poderes de dominio.

(** Únicamente, para personas Morales)
Usted podrá contactarse con la Promotora que va a afiliarlo llamando al 01-800- NAFINSA (01-800-6234672) o al 50-89-61-07; o acudir a las oficinas de Nacional Financiera en:

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

Av. Insurgentes Sur no. 1971, Colonia Guadalupe Inn. C.P. 01020, Alcaldía Álvaro Obregón, en el Edificio Anexo, nivel Jardín, área de Atención a Clientes.

ANEXO V "NOTA INFORMATIVA PARA PARTICIPANTES DE PAÍSES MIEMBROS DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OCDE)".

El compromiso de México en el combate a la corrupción ha transcendido nuestras fronteras y el ámbito de acción del gobierno federal. En el plano internacional y como miembro de la Organización para la Cooperación y el Desarrollo Económico y firmante de la ***Convención para combatir el cohecho de servidores públicos extranjeros en transacciones comerciales internacionales,*** hemos adquirido responsabilidades que involucran a los sectores público y privado.

Esta Convención busca establecer medidas para prevenir y penalizar a las personas y a las empresas que prometan o den gratificaciones a funcionarios públicos extranjeros que participan en transacciones comerciales internacionales. Su objetivo es eliminar la competencia desleal y crear igualdad de oportunidades para las empresas que compiten por las contrataciones gubernamentales.

La OCDE ha establecido mecanismos muy claros para que los países firmantes de la Convención cumplan con las recomendaciones emitidas por ésta y en el caso de México, inició en **noviembre de 2003** una segunda fase de **evaluación** –la primera ya fue aprobada– en donde un grupo de expertos verificó, entre otros:

- La compatibilidad de nuestro marco jurídico con las disposiciones de la Convención.
- El conocimiento que tengan los sectores público y privado de las recomendaciones de la Convención.

El resultado de esta evaluación **impactó** el grado de inversión otorgado a México por las agencias calificadoras y la atracción de inversión extranjera.

Las **responsabilidades** del **sector público** se centran en:

- Profundizar las reformas legales que inició en 1999.
- Difundir las recomendaciones de la Convención y las obligaciones de cada uno de los actores comprometidos en su cumplimiento.
- Presentar casos de cohecho en proceso y concluidos (incluyendo aquellos relacionados con lavado de dinero y extradición).

Las responsabilidades del sector privado contemplan:

- **Las empresas:** adoptar esquemas preventivos como el establecimiento de códigos de conducta, de mejores prácticas corporativas (controles internos, monitoreo, información financiera pública, auditorías externas) y de mecanismos que prevengan el ofrecimiento y otorgamiento de recursos o bienes a servidores públicos, para obtener beneficios particulares o para la empresa.
- **Los contadores públicos:** realizar auditorías; no encubrir actividades ilícitas (doble contabilidad y transacciones indebidas, como asientos contables falsificados, informes financieros fraudulentos, transferencias sin autorización, acceso a los activos sin consentimiento de la gerencia); utilizar registros contables precisos; informar a los directivos sobre conductas ilegales.
- **Los abogados:** promover el cumplimiento y revisión de la Convención (imprimir el carácter vinculatorio entre ésta y la legislación nacional); impulsar los esquemas preventivos que deben adoptar las empresas.

Las **sanciones** impuestas a las personas físicas o morales (privados) y a los servidores públicos que incumplan las recomendaciones de la Convención, implican entre otras, privación de la libertad, extradición, decomiso y/o embargo de dinero o bienes.

Asimismo, es importante conocer que el pago realizado a servidores públicos extranjeros es perseguido y castigado independientemente de que el funcionario sea acusado o no. Las investigaciones pueden iniciarse por denuncia, pero también por otros medios, como la revisión de la situación patrimonial de los servidores públicos o la identificación de transacciones ilícitas, en el caso de las empresas.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

El culpable puede ser perseguido en cualquier país firmante de la Convención, independientemente del lugar donde el acto de cohecho haya sido cometido.

En la medida que estos lineamientos sean conocidos por las empresas y los servidores públicos del país, estaremos contribuyendo a construir estructuras preventivas que impidan el incumplimiento de las recomendaciones de la Convención y por tanto la comisión de actos de corrupción.

Por otra parte, es de señalar que el Código Penal Federal sanciona el cohecho en los siguientes términos:

"Artículo 222
Cometen el delito de cohecho:

I. El servidor público que, por sí o por interpósita persona solicite o reciba indebidamente para sí o para otro, dinero o cualquiera otra dádiva, o acepte una promesa, para hacer o dejar de hacer algo justo o injusto relacionado con sus funciones, y
II. El que de manera espontánea dé u ofrezca dinero o cualquier otra dádiva a alguna de las personas que se mencionan en la fracción anterior, para que cualquier servidor público haga u omita un acto justo o injusto relacionado con sus funciones.

Al que comete el delito de cohecho se le impondrán las siguientes sanciones:

Cuando la cantidad o el valor de la dádiva o promesa no exceda del equivalente de quinientas veces el salario mínimo diario vigente en el Distrito Federal en el momento de cometerse el delito, o no sea evaluable, se impondrán de tres meses a dos años de prisión, multa de treinta a trescientas veces el salario mínimo diario vigente en el Distrito Federal en el momento de cometerse el delito y destitución e inhabilitación de tres meses a dos años para desempeñar otro empleo, cargo o comisión públicos.

Cuando la cantidad o el valor de la dádiva, promesa o prestación exceda de quinientas veces el salario mínimo diario vigente en el Distrito Federal en el momento de cometerse el delito, se impondrán de dos años a catorce años de prisión, multa de trescientas a quinientas veces el salario mínimo diario vigente en el Distrito Federal en el momento de cometerse el delito y destitución e inhabilitación de dos años a catorce años para desempeñar otro empleo, cargo o comisión públicos.

En ningún caso se devolverá a los responsables del delito de cohecho, el dinero o dádivas entregadas, las mismas se aplicarán en beneficio del Estado.

Capítulo XI
Cohecho a servidores públicos extranjeros

Artículo 222 bis
Se impondrán las penas previstas en el artículo anterior al que con el propósito de obtener o retener para sí o para otra persona ventajas indebidas en el desarrollo o conducción de transacciones comerciales internacionales, ofrezca, prometa o dé, por sí o por interpósita persona, dinero o cualquiera otra dádiva, ya sea en bienes o servicios:

I. A un servidor público extranjero para que gestione o se abstenga de gestionar la tramitación o resolución de asuntos relacionados con las funciones inherentes a su empleo, cargo o comisión;
II. A un servidor público extranjero para llevar a cabo la tramitación o resolución de cualquier asunto que se encuentre fuera del ámbito de las funciones inherentes a su empleo.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

ANEXO VI "FORMATO DE FIANZA PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO DE "NOMBRE DEL SERVICIO"

----------INICIA EL TEXTO----------

(Fecha de Emisión)

Fianza a favor de la Tesorería de la Federación (TESOFE), y a satisfacción de la Secretaría de la Función Pública, esta última con domicilio Avenida Insurgentes Sur No. 1735 Col. Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, Código Postal 01020.

Para garantizar por _____, _____. con domicilio en _____ el fiel y exacto cumplimiento de todas y cada una las obligaciones a su cargo derivadas del contrato _____ no. _____, de fecha de firma _____, relativo a la prestación del servicio de _____, a partir del inicio de la vigencia del citado contrato, en los términos y condiciones establecidos en el mencionado contrato y en sus anexos; por un monto total de $_____ (_____ pesos 00/100 m.n.), incluido el Impuesto al Valor Agregado. La Institución Afianzadora garantiza por su fiado hasta por la cantidad de $_____ (_____ pesos 00/100 m.n.), sin incluir el Impuesto al Valor Agregado. La vigencia de la presente fianza se otorga a partir de la vigencia del contrato, y queda abierta para permitir que cumpla su objetivo, de forma tal que no podrá establecerse o estipularse plazo alguno que limite su vigencia, lo cual no debe confundirse con el plazo para el cumplimiento de las obligaciones previsto en el contrato y actos administrativos. Esta garantía estará vigente en los casos en que la SFP otorgue prórrogas o esperas al proveedor o fiado para el cumplimiento de sus obligaciones, así como durante la substanciación de todos los recursos legales o juicios que se interpongan en relación con este contrato, hasta que se pronuncie resolución definitiva por autoridad competente que quede firme, salvo que las partes se otorguen el finiquito, de forma tal que su vigencia no podrá acotarse en razón del plazo de ejecución del contrato principal o fuente de las obligaciones, o cualquier otra circunstancia y en caso de defectos o vicios ocultos de los servicios o de incumplimiento de las obligaciones continuará vigente hasta que aquellos se corrijan o estas sean satisfechas en la calidad de los servicios objeto de dicho contrato, con las especificaciones y alcances establecidos en el mismo. De igual forma, quedan garantizados los daños y perjuicios que, en su caso, se ocasionen por incumplimiento a las obligaciones de confidencialidad previstas en el citado instrumento jurídico. Para la cancelación de esta fianza es requisito indispensable la autorización expresa y por escrito de la SFP. La Institución de Fianzas acepta expresamente someterse, para la efectividad de la presente garantía, al procedimiento de ejecución establecido en el artículo 282 de la Ley de Instituciones de Seguros y de Fianzas, para la efectividad de las fianzas, procedimiento al que también se sujetará para el caso de cobro de indemnización por mora que prevé el artículo 283 del mismo ordenamiento legal, por pago extemporáneo del importe de la póliza de fianza requerida. La presente fianza se expide en cumplimiento de todas las estipulaciones contenidas en el contrato. =Fin de texto="

Fecha de expedición ____ de _____ 2024

----------TERMINA EL TEXTO----------

FORMATO 1

ACREDITACIÓN DE LA EXISTENCIA LEGAL Y PERSONALIDAD JURÍDICA DEL LICITANTE

DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA
P R E S E N T E

En cumplimiento al artículo 48, fracción V del **Reglamento de la Ley**, (**nombre del representante legal o apoderado**) manifiesto bajo protesta de decir verdad, que cuento con las facultades suficientes para comprometerme por sí o por mi representada en la Licitación Pública Electrónica de Carácter Nacional, _____, denominada _____ y que los datos aquí asentados, son ciertos y han sido debidamente verificados, conforme a lo siguiente:

Razón o Denominación social de la Empresa.
Registro Federal de Contribuyentes:
Domicilio:
Calle y número:
Colonia: Alcaldía o Municipio:
Código Postal: Entidad Federativa:
Teléfonos: Fax:
Correo Electrónico
No. de Escritura Pública en la que consta el Acta Constitutiva: Fecha:
Nombre, número y lugar del Notario Público ante el cual se dio fe de la misma:
No. de folio mercantil y fecha de su inscripción en el Registro Público de la Propiedad y del Comercio:
Relación de accionistas
Apellido Paterno Apellido Materno Nombre (s)

En caso de que los socios o accionistas sean personas morales deberá incluir la siguiente información:

Nombre completo o Razón Social	Clave del Registro Federal de Contribuyentes	Datos de las escrituras públicas	Domicilio	Descripción del objeto social.	Relación de los accionistas

Descripción del objeto social:
Reformas al acta constitutiva en su caso:
Nombre del apoderado o representante:
Datos del documento mediante el cual acredita su personalidad y facultades:
Nombre, número y lugar del Notario Público ante el cual se otorgó:

Lugar y fecha

Protesto lo necesario

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

NOTAS:

1. El presente formato podrá ser reproducido por cada participante, debiendo respetar su contenido preferentemente, en el orden incluido.
2. En el caso de tratarse de persona física con actividad empresarial suscribo por propio derecho.
3. El licitante deberá presentar acta constitutiva, y en su caso las modificaciones, en las que se constate que el objeto social es acorde con los servicios que se pretenden contratar.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

FORMATO 2

MANIFESTACIÓN DE QUE EL LICITANTE NO SE UBICA EN LOS SUPUESTOS ESTABLECIDOS EN LOS ARTÍCULOS 50 Y 60 DE LA LEY.

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SECRETARÍA DE LA PÚBLICA

Relativa a la Licitación Pública Electrónica Nacional N° de CompraNet LA-27-514-027000002-N-X-2024, relativa a la contratación del **"XXXXXXXXXXXXXXXXX".**

Yo **nombre del representante o apoderado legal** como representante o apoderado legal de la empresa **nombre de la empresa manifiesto bajo protesta de decir verdad** lo siguiente:

Que en la empresa que represento no participan personas físicas o morales inhabilitadas por resolución de la Secretaría de la Función Pública, en los términos de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Publico.

Asimismo, manifiesto por mi conducto, que no participan en el presente procedimiento de contratación, personas físicas o morales que se encuentren inhabilitadas en los términos del párrafo anterior, con el propósito de evadir los efectos de la inhabilitación, tomando en consideración, entre otros, los supuestos siguientes:

- **a.** Que no participan personas físicas o morales que se encuentren inhabilitadas en términos del segundo párrafo de este escrito;
- **b.** Que en el capital social de mi representada no participan personas morales en cuyo capital social, a su vez, participen personas físicas o morales que se encuentren inhabilitadas en términos del segundo párrafo de este escrito, y
- **c.** Personas físicas que participen en el capital social de personas morales que se encuentren inhabilitadas.

Asimismo, que mi representada no se encuentra dentro de los supuestos de los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Publico.

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

Nota.- Cuando se presente una propuesta conjunta, este escrito deberá de ser presentado por cada persona física o moral que participe en el convenio correspondiente.

FORMATO 3

DECLARACIÓN DE INTEGRIDAD

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA

En cumplimiento a lo ordenado por el artículo 29 fracción IX de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, fracción VI, inciso f y penúltimo párrafo del 39 de su Reglamento; y para efectos de presentar proposición y en su caso poder celebrar el contrato respectivo con este Instituto en relación a Licitación Pública Electrónica de Carácter Nacional: _____

- Me permito manifestar **BAJO PROTESTA DE DECIR VERDAD** que la empresa que represento se abstendrá por si misma o a través de interpósita persona, de adoptar conductas para que los servidores públicos, induzcan o alteren las evaluaciones de las proposiciones, el resultado del procedimiento, u otros aspectos que le otorguen condiciones más ventajosas con relación a los demás participantes; asimismo que dicha empresa por sí misma o por interpósita persona, se abstendrá de llevar a cabo cualquier acto que implique trasgresión a las disposiciones de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento; así como a lo dispuesto en general por la Ley Federal de Competencia Económica.

- ***(EN CASO DE SER PERSONA FÍSICA, DEBERÁ SUSTITUIR EL PÁRRAFO ANTERIOR POR LO SIGUIENTE:*** *"Me permito manifestar BAJO PROTESTA DE DECIR VERDAD que me abstendré por sí mismo o a través de interpósita persona, de adoptar conductas para que los servidores públicos, induzcan o alteren las evaluaciones de las proposiciones, el resultado del procedimiento, u otros aspectos que le otorguen condiciones más ventajosas con relación a los demás participantes; asimismo me abstendré por sí mismo o por interpósita persona, de llevar a cabo cualquier acto que implique trasgresión a las disposiciones de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento; así como a lo dispuesto en general por la Ley Federal de Competencia Económica.")* ***EN CASO DE NO SER PERSONA FÍSICA PODRÁ ELIMINAR ESTE PÁRRAFO.***

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

FORMATO 4

MANIFESTACIÓN DE NACIONALIDAD

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA
P R E S E N T E

Por medio del presente, manifiesto bajo protesta de decir verdad que mi representado nombre *del licitante* es de nacionalidad mexicana mi representada es de nacionalidad mexicana y fue constituida mediante Escritura Pública No. lo anterior para efectos de lo que establece el artículo 35 párrafo primero del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

ATENTAMENTE

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

FORMATO 5

CUMPLIMIENTO DE NORMAS

DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

Relativa a la Licitación Pública Electrónica Nacional N° de CompraNet No. LA-27-514-027000002-N-X-2024, relativa a la contratación del **"XXXXXXXXXXXXXXXXXX".**

(Nombre representante legal), manifiesto:

Opción 1
Que mi representada, la persona_____, que para la prestación del servicio que oferta **SÍ** existen normas de referencia, por lo tanto, la contratación de la prestación del servicio se llevará a cabo conforme a las especificaciones establecidas en el **Anexo 1 "Especificaciones Técnicas y alcances del Servicio".**
Enlistar las normas que cumple.

Opción 2
Que mi representada, la persona_____, que para la prestación del servicio que oferta **NO** existen normas de referencia, por lo tanto, la contratación de la prestación del servicio se llevará a cabo conforme a las especificaciones establecidas en el **Anexo 1 "Especificaciones Técnicas y alcances del Servicio".**
Enlistar las normas que cumple.

DEJA SOLO LA OPCIÓN QUE CORRESPONDA.

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

Nota: El presente formato podrá ser reproducido por cada participante en el modo que estime conveniente, debiendo respetar su contenido.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

FORMATO 6

"MANIFESTACIÓN CON RELACIÓN AL PUNTO 29 DEL ACUERDO POR EL QUE SE ESTABLECEN LAS DISPOSICIONES QUE SE DEBERÁN OBSERVAR PARA LA UTILIZACIÓN DEL SISTEMA ELECTRÓNICO DE INFORMACIÓN PÚBLICA GUBERNAMENTAL DENOMINADO COMPRANET"

DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

Relativa a la Licitación Pública Electrónica Nacional N° de CompraNet No. LA-27-514-027000002-N-X-2024 relativa a la contratación del **"XXXXXXXXXXXXXXXXXX".**

(Nombre representante legal), manifiesto que se tendrá como no presentada mi proposición y, en su caso, la documentación requerida por la Unidad compradora, cuando el archivo electrónico en el que contenga la proposición y/o demás información no pueda abrirse por tener algún virus informático o por cualquier otra causa ajena a la dependencia o entidad.

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE (NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

Nota: El presente formato podrá ser reproducido por cada participante en el modo que estime conveniente, debiendo respetar su contenido.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

FORMATO 7:

MANIFESTACIÓN BAJO PROTESTA DE DECIR VERDAD DE LA ESTRATIFICACIÓN DE MICRO, PEQUEÑA O MEDIANA EMPRESA (MIPYMES)

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA
P R E S E N T E

Me refiero al procedimiento de _____**(3)**_____ No. _____**(4)** _____ en el que mi representada, la empresa_____**(5)**_____, participa a través de la presente proposición.

Al respecto y de conformidad con lo dispuesto por el artículo 34 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **MANIFIESTO BAJO PROTESTA DE DECIR VERDAD** que mi representada está constituida conforme a las leyes mexicanas, con Registro Federal de Contribuyentes _____**(6)**_____, 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 _____**(7)**_____, con base en lo cual se estatifica como una empresa _____**(8)**_____.

A T E N T A M E N T E

_____**(9)**_____

INSTRUCTIVO

FO-CON-14 **Estratificación de las Micro, Pequeña o Mediana Empresa (Mipymes)**

Descripción

Formato para que los licitantes manifiesten, bajo protesta de decir verdad, la estratificación que les corresponde como Mipymes, de conformidad con el Acuerdo de Estratificación de las Mipymes, publicado en el Diario Oficial de la Federación el 30 de junio de 2009.

Instructivo de llenado

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 de la convocante.
3. Precisar el procedimiento de contratación de que se trate (licitación pública o invitación a cuando menos tres personas).
4. Indicar el número de procedimiento de contratación asignado por CompraNet.
5. Anotar el nombre, razón social o denominación del licitante.
6. Indicar el Registro Federal de Contribuyentes del licitante.
7. 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 MIPYME 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.
8. Señalar el tamaño de la empresa (Micro, Pequeña o Mediana), conforme al resultado de la operación señalada en el numeral anterior.
9. Anotar el nombre y firma del apoderado o representante legal del licitante.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

FORMATO 8 "
CARTA DE LOS ARTÍCULOS 49 FRACCIÓN IX y 72 DE LA LEY GENERAL DE RESPONSABILIDADES ADMINISTRATIVAS"
(Aplica para personas físicas o morales)

DIRECCIÓN GENERAL DE RECURSOS MATERIALES
Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA

Lugar y fecha de expedición: .....
Licitación Pública Nacional Electrónica: .....

Relativa a la Licitación Pública Electrónica Nacional N° de CompraNet No. LA-27-514-027000002-N-X-2024, relativa a la contratación del **"XXXXXXXXXXXXXXXX".**

Yo **nombre del representante o apoderado legal** como representante o apoderado legal de la empresa **nombre de la empresa** manifiesto bajo protesta de decir verdad lo siguiente:

EN CASO DE SER PERSONA FÍSICA:

Que no desempeño empleo, cargo o comisión en el servicio público o, en su caso que, a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un Conflicto de Interés.

Asimismo, manifiesto que mi representada no cuenta con personal que haya sido servidor público durante el año previo.

EN CASO DE SER PERSONA MORAL:

Que no desempeño, ni mis socios o accionistas que ejerzan control sobre la sociedad, empleo, cargo o comisión en el servicio público o, en su caso que, a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un Conflicto de Interés.

Asimismo, manifiesto que mi representada, ni mis socios o accionistas que ejerzan control sobre la sociedad, no cuentan con personal que haya sido servidor público durante el año previo.

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

Nota: El presente formato podrá ser reproducido por cada participante en el modo que estime conveniente, debiendo respetar su contenido

FORMATO 9
DECLARACIÓN DE CONOCER EL PROTOCOLO DE ACTUACIÓN
(Aplica para personas físicas o morales)

DIRECCIÓN GENERAL DE RECURSOS MATERIALES
Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

Me refiero al procedimiento No. _____relativo a _____ en el que mi representada, la empresa_____, participa a través de la presente proposición.

El que suscribe, C. (NOMBRE DEL REPRESENTANTE LEGAL O APODERADO DE LA EMPRESA), manifiesto bajo protesta de decir verdad que mi representada la empresa (NOMBRE DE LA EMPRESA), el suscrito y los socios integrantes de la empresa que represento, conocen el contenido del Protocolo de Actuación en Materia de Contrataciones Públicas, Otorgamiento y Prórroga de Licencias, Permisos, Autorizaciones y Concesiones.

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

Nota: El presente formato podrá ser reproducido por cada participante en el modo que estime conveniente, debiendo respetar su contenido.

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

FORMATO 10

"MANIFESTACIÓN DE INFORMACIÓN RESERVADA Y/O CONFIDENCIAL"

Dirección General de Recursos Materiales
y Servicios Generales
Secretaría de la Función Pública

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

Relativa a la Licitación Pública Electrónica Nacional N° de CompraNet LA-27-514-027000002-N-X-2024 relativa a la contratación del **"XXXXXXXXXXXXX".**

Nombre del representante legal en mi carácter de _____(cargo)_____ y con las facultades conferidas conforme a derecho, manifiesto que la documentación, propuesta técnica y económica que se acompañan al presente procedimiento cumplen con lo siguiente:

Párrafo 1
Que para los efectos de los artículos 113 y 116 de la Ley General de Transparencia y Acceso a la Información Pública, los documentos que se entregan en nuestra proposición **NO SON** de naturaleza reservada y/o confidencial.

Párrafo 2
Que para los efectos de los artículos 113 y 116 de la Ley General de Transparencia y Acceso a la Información Pública, los documentos que se enlistan a continuación y que se anexan a nuestra proposición **SON** de naturaleza reservada y/o confidencial.

1.- Información _____ FOLIOS_____
MOTIVO _____
2.- Información_____ FOLIOS_____
MOTIVO _____

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

Nota: El presente formato podrá ser reproducido por cada participante en el modo que estime conveniente, debiendo respetar su contenido. **Solo utilizar el párrafo que corresponda, en ningún caso pueden incluirse los 2 párrafos.**

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

FORMATO 11

ESCRITO DOMICILIO CONVENCIONAL

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA
P R E S E N T E

Nombre o Razón Social manifiesto que la empresa que represento, cuenta con el domicilio convencional para oír y recibir todo tipo de notificaciones relacionadas con el procedimiento o en caso de resultar adjudicado lo relativo a la contratación de la Licitación Pública Electrónica de Carácter Nacional N° _____, denominada _____, siguiente:

DOMICILIO PARA OÍR Y RECIBIR NOTIFICACIONES	
Calle y Número:	
Colonia:	
Alcaldía o Municipio:	
Entidad Federativa:	
Código Postal:	
Número Telefónico	

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

Nota: Este formato únicamente aplicará en caso de que el domicilio fiscal del Licitante se encuentre fuera de la Ciudad de México.

FORMATO 12.

ESCRITO DE CONFIDENCIALIDAD

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA

El que suscribe C. _____ en mi carácter de _____manifiesto, que durante la presente licitación y en caso de ser adjudicado me obligo a mantener la más estricta confidencialidad de toda la información y documentación que la Convocante me proporcione, por lo que me comprometo a no divulgar ni a utilizar la información que conozca en el desarrollo y cumplimiento de este servicio, así como, cuidar los documentos y sistemas de información a que tuviere acceso, garantizando la confidencialidad de la información que reciba, resguarde, registre o genere derivado de la puesta en operación y entrega de los servicios requeridos, durante la vigencia del servicio.

En el entendido de que, de no manifestarme con veracidad, en caso de que resulte adjudicado en el presente procedimiento acepto que ello sea causa de rescisión del contrato celebrado con la Secretaría.

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020, Tel: (55)20-00-30-00 www.gob.mx/sfp

FORMATO 13

CONSENTIMIENTO POR PARTE DEL REPRESENTANTE LEGAL O APODERADO (EL TITULAR) PARA EL USO DE DATOS PERSONALES

(ESCRITO, PREFERENTEMENTE EN PAPEL MEMBRETADO Y FIRMA AUTÓGRAFA DEL PARTICIPANTE O REPRESENTANTE LEGAL O APODERADO)

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA
P R E S E N T E

Me refiero al procedimiento No. _____relativo al _____ en el que mi representada, la empresa_____, participa a través de la presente proposición.

Yo. (ESCRIBIR EL NOMBRE DEL REPRESENTANTE LEGAL O APODERADO), representante legal o apoderado de la empresa (ESCRIBIR EL NOMBRE DE LA EMPRESA), reconozco que la Dirección General de Recursos Materiales (DGRMSG) a través de la Dirección de Planeación y Adquisiciones (DPyA) hizo de mi conocimiento el **Aviso de Privacidad Integral** a través del portal web https://www.gob.mx/sfp/documentos/avisos-de-privacidad apartado de -**Avisos de Privacidad-**de la-**Dirección General de Recursos Materiales y Servicios Generales-**, previo a proporcionar mis datos personales; de igual manera, consiento expresamente que la DGRMSG trate mis datos personales con sujeción a las finalidades, términos y demás condiciones establecidas en Aviso de Privacidad Integral.

Acepto y reconozco que la DGRMSG utilice la información recabada de conformidad con las disposiciones legales aplicables.

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

FORMATO 14

CORREO ELECTRÓNICO DEL LICITANTE

Lugar y fecha de expedición: .....
Licitación Pública Electrónica de Carácter Nacional: .....

DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS GENERALES
SECRETARÍA DE LA FUNCIÓN PÚBLICA
P R E S E N T E

Me refiero al procedimiento de No. _____relativo a la contratación de _____ en el que mi representada, la empresa_____, participa a través de la presente proposición.

Sobre el particular, y en los términos de lo previsto en el Artículo 39 fracción VI inciso d) del RLAASSP, manifiesto que mi correo electrónico para recibir notificaciones por parte de la convocante es: _____.

ATENTAMENTE

_____

NOMBRE, CARGO Y FIRMA DEL REPRESENTANTE LEGAL O APODERADO DEL LICITANTE
(NOMBRE O RAZÓN SOCIAL DE LA EMPRESA)

FORMATO 15:

ENCUESTA DE TRANSPARENCIA

Encuesta de transparencia del procedimiento de la Licitación Pública Electrónica de Carácter Nacional No. LA-27-514-027000002-N-X-2024 relativa a la contratación de "_____". Instrucciones: favor de calificar los supuestos planteados en esta encuesta según considere.

Elija la opción que más se ajuste a su respuesta:

Junta de Aclaración a la Convocatoria ☑

1.- ¿LA CONVOCATORIA SE PUBLICÓ EN FORMA ADECUADA?

Totalmente de acuerdo		En general de acuerdo		En general en desacuerdo		Totalmente en Desacuerdo	

2.- ¿EL CONTENIDO DE LOS REQUISITOS DE PARTICIPACIÓN DE LA CONVOCATORIA ES CLARO PARA LA CONTRATACIÓN QUE SE PRETENDE REALIZAR?

Totalmente de acuerdo		En general de acuerdo		En general en desacuerdo		Totalmente en desacuerdo	

Presentación de Proposiciones y Apertura de Propuestas Técnicas y Económicas

3.- ¿EL EVENTO SE DESARROLLÓ CON OPORTUNIDAD, EN RAZÓN DE LA CANTIDAD DE DOCUMENTOS QUE PRESENTARON LOS PARTICIPANTES?

Totalmente de acuerdo		En general de acuerdo		En general en desacuerdo		Totalmente en desacuerdo	

4.- ¿LA EVALUACIÓN DE LAS PROPUESTAS TÉCNICAS FUE REALIZADA CONFORME A LA CONVOCATORIA?

Totalmente de acuerdo		En general de acuerdo		En general en desacuerdo		Totalmente en desacuerdo	

Fallo

5.- ¿EN EL FALLO SE ESPECIFICARON LOS MOTIVOS Y EL FUNDAMENTO QUE SUSTENTA LA DETERMINACIÓN DE LOS PROVEEDORES ADJUDICADOS Y LOS QUE NO RESULTARON ADJUDICADOS?

Totalmente de acuerdo		En general de acuerdo		En general en desacuerdo		Totalmente en desacuerdo	

6.- ¿TUVO FÁCIL EL ACCESO AL LUGAR DONDE SE DESARROLLARON LOS EVENTOS?

Totalmente de acuerdo		En general de acuerdo		En general en desacuerdo		Totalmente en desacuerdo	

7.- ¿TODOS LOS EVENTOS DIERON INICIO EN LA HORA Y LUGAR ESTABLECIDOS EN LA CONVOCATORIA?

Totalmente de acuerdo		En general de acuerdo		En general en desacuerdo		Totalmente en desacuerdo	

8.- ¿EL TRATO QUE LE DIERON LOS SERVIDORES PÚBLICOS DE LA SECRETARÍA DE LA FUNCIÓN PÚBLICA DURANTE EL PROCEDIMIENTO FUE RESPETUOSO Y AMABLE?

Totalmente de acuerdo		En general de acuerdo		En general en desacuerdo		Totalmente en desacuerdo	

9.- ¿VOLVERÍA A PARTICIPAR EN OTRO PROCEDIMIENTO QUE CONVOQUE LA SECRETARÍA DE LA FUNCIÓN PÚBLICA?

Totalmente de acuerdo		En general de acuerdo		En general en desacuerdo		Totalmente en desacuerdo	

10.- ¿EL PROCEDIMIENTO EN EL QUE PARTICIPÓ, SE APEGÓ A LA NORMATIVIDAD APLICABLE?

Totalmente de acuerdo		En general de acuerdo		En general en desacuerdo		Totalmente en desacuerdo	

11.- SI DESEA AGREGAR ALGÚN COMENTARIO RESPECTO AL PROCEDIMIENTO DE LICITACIÓN PÚBLICA DE CARÁCTER NACIONAL ELECTRÓNICA NÚMERO _____, FAVOR DE ANOTARLO A CONTINUACIÓN:

_____

_____

La presente encuesta podrá ser o enviada a los siguientes correos electrónicos: ambrosio.oliva@funcionpublica.gob.mx aida.camacho@funciopublica.gob.mx y/o monica.nunez@funcionpublica.gob.mx

Avenida Insurgentes Sur No. 1735, Colonia Guadalupe Inn, Alcaldía Álvaro Obregón, Ciudad de México, C.P. 01020. Tel: (55)20-00-30-00 www.gob.mx/sfp

SECRETARÍA DE LA FUNCIÓN PÚBLICA

Especificaciones Técnicas

Suministro, Instalación y Configuración de Soluciones de Seguridad Informática

1 OBJETIVOS:

Garantizar la seguridad, confidencialidad, integridad, disponibilidad y recuperación de la información de las Unidades que integran la SFP, previniendo el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada.

Proporcionar a la Secretaría de la Función Pública (SFP) soluciones integrales de Seguridad de la Información. Esto incluye el suministro, instalación, configuración y puesta a punto de las mismas, así como el soporte técnico continuo.

Fortalecer la seguridad de la información mediante la implementación de herramientas de última generación para la prevención, detección, visualización, protección, mitigación y eliminación de ciber-amenazas, asegurando así la protección efectiva de la información y los sistemas institucionales.

2 SOLUCIONES REQUERIDAS

Suministro, instalación, configuración y puesta a punto de los licenciamientos en el siguiente orden:

1. Correlación de Eventos Security Information and Event Management (SIEM)
2. Protección del Sistema de Nombres de Dominio (DNS)
3. Detección y Prevención de Correo Electrónico no deseado (Antispam)
4. Protección Antimalware para estaciones de trabajo y servidores (Endpoint)
5. Administración de Cuentas Privilegiadas (PAM)
6. Puntos de Decepción de Ataque (Trampas de seguridad)

3 REQUERIMIENTOS GENERALES PARA LAS SOLUCIONES PROPUESTAS

- Se deberá privilegiar el aprovisionamiento de soluciones con dispositivos virtuales (**máquinas virtuales**) las cuales quedarán hospedadas sobre la plataforma de virtualización VMware 7.0 o superior, infraestructura propiedad de la SFP. En caso de que la solución contemple maquinas físicas deberán ser equipos ranqueables, considerar los elementos necesarios para su instalación misma que deberá llevarse a cabo en el Site de servidores de la SFP.
- Todas las soluciones deberán contar con garantía y actualizaciones por doce meses.
- Todos los costos de implementación, instalación, gestión, soporte, mantenimiento y aprovisionamiento relacionados con las soluciones estarán a cargo del proveedor garantizando su buen funcionamiento.
- El proveedor proporcionará la transferencia de conocimiento de todas las soluciones implementadas a través del fabricante, de al menos 5 personas designadas por el Administrador del Contrato, la cual deberá estar orientada a la administración, operación y gestión de cada solución, de acuerdo al programa y ubicación definido por la SFP.

- La transferencia de conocimiento de cada solución no deberá significar un costo adicional para la SFP.
- Todas las soluciones deberán cumplir con objetivo específico, no se aceptarán soluciones de software libre o código abierto.
- Toda la infraestructura que sea instalada deberá tener capacidad de trabajar en IPv4, IPv6 o en dual-stack.
- Todas las soluciones deberán mantener los registros (logs) por al menos 30 días.
- Se deberán entregar credenciales de acceso de administración para los elementos de las plataformas tecnológicas de seguridad suministradas.
- El proveedor deberá tomar las medidas que considere necesarias para que antes, durante y posterior a la implementación, las operaciones tecnológicas de la SFP no sean interrumpidas en ningún momento.
- Todas las soluciones deberán ser de última generación, así como, no encontrarse dentro de las fechas establecidas de EOFS (End of Full Support) por cada fabricante y se deberán presentar las fichas técnicas, manuales, folletos y/o páginas web donde se pueda validar el cumplimiento técnico. Las fichas técnicas deberán estar en idioma inglés con su traducción comprensible al español.
- Cada solución deberá incluir soporte técnico por doce meses, que pueda ser atendido por correo electrónico o vía telefónica. El soporte técnico deberá proporcionare en un tiempo no mayor a 60 minutos, desde que el o los eventos sean reportados al proveedor. Éste deberá emitir el folio o acuse de la solicitud del requerimiento, mediante correo electrónico. La atención a la solicitud de soporte no considerará cerrada hasta que la parte requirente otorgue su visto bueno. El servicio de soporte técnico deberá ser 24x7x365.

4 METODOLOGÍA Y PLAN DE TRABAJO

4.1 METODOLOGÍA

Se realizará una reunión a más tardar al quinto día hábil posterior a la notificación del fallo entre el personal designado por el proveedor y el Administrador del contrato, con la finalidad de definir acciones y tiempos de cumplimiento; así como todas aquellas tareas que el proveedor y la SFP consideren necesarias para la elaboración del plan de trabajo de las soluciones requeridas.

Para la puesta en operación de las soluciones descritas en este documento se deben considerar los siguientes puntos, así como sus respectivas actividades listadas en cada uno de estos:

4.1.1 PLANEACIÓN

- El proveedor deberá elaborar un plan de trabajo que incluya todas las etapas necesarias para el suministro, instalación, configuración y puesta a punto de las soluciones.
- El proveedor deberá proporcionar una matriz de escalamiento para garantizar la instalación, configuración y puesta a punto de las soluciones en tiempo y forma.

4.1.2 IMPLEMENTACIÓN

El proveedor deberá realizar y ejecutar la implementación de las soluciones ofertadas de acuerdo con el plan de trabajo:

- Instalación de la solución
- Instalación del licenciamiento
- Actualización de firmas o patrones de protección
- Configuración de protocolos
- Configuración de reglas
- Configuración para protección de ataques conocidos.

Y todas aquellas tareas que el proveedor y la SFP consideren necesarias.

4.1.3 PRUEBAS Y VALIDACIÓN

- El proveedor deberá elaborar y ejecutar el protocolo de pruebas de funcionalidad de las soluciones para demostrar el funcionamiento correcto de las configuraciones realizadas.
- Inspeccionar que todos los componentes se encuentren operando correctamente.
- Validar que ningún componente de las soluciones presente alarmas.
- Simular ataques controlados para validar el objetivo tecnológico de las soluciones.

Y todas aquellas tareas que el proveedor y la SFP consideren necesarias.

4.1.4 TRANSFERENCIA DE CONOCIMIENTO

- El proveedor deberá proporcionar el material necesario en electrónico (manuales, presentaciones, folletos, fichas técnicas, entre otros), para llevar a cabo la transferencia de conocimientos de cada una de las soluciones.

4.2 PLAN DE TRABAJO

El proveedor deberá integrar en el plan de trabajo, todas las actividades necesarias para la correcta instalación, configuración y puesta a punto de las soluciones propuestas, y cualquier actividad que no hubiera sido considera, la cual deberá ser cubierta por el proveedor, sin que ello genere cargos extras para la SFP.

El proveedor deberá entregar la propuesta de plan de trabajo detallado ocho días hábiles posteriores a la notificación del fallo, con base en la metodología propuesta en este apartado, el cual deberá considerar las actividades, recursos y fechas para la instalación, configuración y puesta a punto de las soluciones.

Cronograma de actividades	Días naturales			
	5	10	15	20
1.- Planeación				
2.- Implementación				

3.- Pruebas y validación del servicio				
4.-Transferencia de conocimiento				
Días totales para el inicio de operaciones.				

5 EL PERSONAL

Todo personal que el proveedor proponga para participar en la instalación, configuración, puesta a punto y transferencia de conocimiento y que se relaciona en puntos subsecuentes, deberá contar con experiencia probada en las áreas de tecnología y de seguridad de la información.

Es deseable que el líder técnico, cuente con algunas de las siguientes certificaciones:

- CISM
- CEH Master
- CISA o CISSP

El proveedor debe incluir como parte de su propuesta técnica un escrito firmado por el representante legal en papel membretado donde indique el nombre del personal y el perfil asignado, acompañado del currículum vitae.

No se permite que una persona pueda realizar o cubrir 2 o más perfiles.

El currículum vitae de cada una de las personas se deberá indicar al menos:

- Experiencia profesional: bajo este rubro se considerarán todos los cargos que cada integrante haya desempeñado, con fecha, nombre de los empleadores y contacto para verificar la información, nombre de los cargos que ha ejercido y el tipo de funciones bajo su responsabilidad.
- Experiencia en proyectos de su especialidad en Seguridad de la Información: bajo este rubro se citarán y describirán todos los proyectos que el integrante ha participado.
- Estudios: bajo este rubro se anotarán todos los estudios en materia de tecnología y de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica.

5.1 SUSTITUCIÓN DE PERSONAL

El proveedor no podrá llevar a cabo la sustitución ni cambiar a ningún integrante del personal propuesto para la instalación, configuración, puesta a punto y transferencia de conocimiento, hasta obtener la aceptación del reemplazo por parte de la SFP dentro de los primeros 5 días hábiles a partir del comunicado de reemplazo.

La SFP se reserva el derecho de veto, si considera que algún integrante del personal propuesto no reúne los requisitos solicitados o no cumple con las funciones asignadas, situación que el proveedor deberá solucionar en un plazo de 5 (cinco) días hábiles a partir

del comunicado de rechazo para proponer el personal sustituto. La sustitución deberá ser aprobada por la SFP dentro de los primeros 5 (cinco) días hábiles.

6 ESPECIFICACIONES TÉCNICAS

Las siguientes especificaciones describen las características con las que deberán de contar cada una de las soluciones requeridas por la SFP.

6.1 SOLUCIÓN DE CORRELACIÓN DE EVENTOS (SIEM)

La SFP establece la necesidad para que el proveedor configure y afine una solución de correlación de eventos de seguridad.

El proveedor proporcionará una solución de SIEM de nueva generación que permita la visibilidad de eventos y proporcione la información necesaria para el análisis, administración y generación de reportes. La solución debe permitir identificar en tiempo real las amenazas, y flujos de trabajo para la contención de ataques, identificación de incidentes y riesgos potenciales para la infraestructura y los servicios tecnológicos, el SIEM debe cumplir con al menos las siguientes especificaciones técnicas:

- Debe proveer una solución de propósito específico.
- El software deberá incluir todos los componentes del mismo fabricante, la consola Web, así como el repositorio para almacenar la información.
- La solución no deberá depender de una base de datos de tipo relacional, los eventos deberán ser almacenados en el mismo formato que la fuente original y no deberá realizarse ningún proceso de reducción o transformación de datos.
- Deberá ser capaz de leer eventos en diferentes formatos sin importar la fuente, deberá ser capaz de identificar eventos multilínea y separar los eventos de manera correcta.
- Deberá permitir la creación de usuarios con diferentes roles, estos roles deberán permitir definir esquemas de acceso a los datos por rol, así como la definición de políticas de retención por tipo de dato.
- Deberá permitir almacenar históricos de datos por al menos 1 año en línea y el tiempo restante debe permitir guardar los eventos en cinta o VTL (Virtual Tape Library).
- Deberá ser capaz de recibir eventos a una tasa de al menos 50K EPS (Eventos por Segundo).
- Los componentes no deberán tener costo adicional, de modo que se podrán instalar equipos en alta disponibilidad sin tener costos adicionales por licenciamiento.
- Deberá incluir un lenguaje de búsqueda flexible que permita identificar eventos que contengan una palabra, un código de error o una frase. Esta búsqueda deberá permitir operadores lógicos que permitan definir mejores criterios de búsqueda.
- Deberá permitir la búsqueda de los datos en tiempo real, con rangos de tiempo definidos incluyendo búsquedas históricas. Estas búsquedas deberán regresar los datos en segundos para no afectar la respuesta del manejo de los incidentes.

- Deberá ser capaz de transformar los eventos en gráficas, reportes y vistas que permitan monitorear las métricas importantes para la organización. Estás vistas deberán ser completamente personalizables.
- Deberá permitir la creación de reglas de correlación que puedan adaptarse a los requerimientos de la SFP. Estas reglas deberán combinar múltiples fuentes de datos para tener un mejor entendimiento de los incidentes de seguridad.
- Deberá ser capaz de enriquecer los datos colectados con catálogos que describan los errores o con direcciones IP maliciosas para identificar comunicaciones riesgosas. Los catálogos pueden ser estáticos o dinámicos en una tabla dentro de una base de datos.
- Deberá incluir los siguientes mecanismos de colección: colección de datos sin agente usando WMI o recursos compartidos, recibir eventos por syslog, SNMP, http, conectándose a bases de datos y ejecutando QUERIES, así como leyendo datos directamente de la red en puertos espejo.
- Deberá ser capaz de capturar el tráfico de protocolos directamente desde la red. Se deben poder definir qué tipo de campos extraer de las tramas de red, por ejemplo: dirección IP origen y destino, puerto origen y destino, tiempo de la transacción (time taken) entre otros.
- Se requiere reconocimiento de al menos los siguientes protocolos: http, https, ftp, dns, y dhcp.
- Deberá ser capaz de crecer de manera lineal tan solo instalando nuevos componentes, separando el proceso de captura del proceso de consulta.
- Deberá ser capaz de integrar diferentes roles de usuario, estos roles deben estar integrados con directorio activo o LDAP. Algunos de los usuarios deberán poder crear búsquedas y otros que solo realicen consultas.
- Deberá contener mecanismos para identificar campos dentro de eventos no estándares, estos mecanismos para identificación de campos deberá ser gráfico y además permitir el uso de expresiones regulares para la creación de nuevos campos.
- Deberá permitir la integración con listas de inteligencia de seguridad, como IP maliciosas de SANS, por mencionar algunas, estas listas de direcciones IP y dominios maliciosos deberá compararse con el tráfico generado en la institución para identificar tráfico hacia/desde sitios maliciosos. La solución deberá poder integrarse con listas gratuitas o con listas de pago definidas por la SFP.
- Deberá tener integradas al menos 50 reglas de correlación y por lo menos 20 casos de uso con hasta 10 casos de uso con respuesta automatizada, así como mecanismos para generar nuevas vistas para el monitoreo de incidentes de seguridad agrupado por domino con la capacidad de definir nuevas vistas que se adecuen a los requerimientos de la SFP.
- Deberá tener integrado un sistema para el manejo de incidentes que permita registrar analistas, asignar casos de manera automática por tipo de perfil, así como tener una bitácora que registre las actividades del analista realizadas para cerrar el caso.
- Deberá ser capaz de analizar eventos de alta fidelidad producidos por herramientas antimalware de endpoint, además de leer eventos de sysmon de

Microsoft que permitan identificar procesos con sus identificadores, así como el proceso padre que ejecutó el anterior, todo esto deberá ser reportado y analizado por las reglas de correlación.

- Deberá permitir el acceso de hasta 10 usuarios para la SFP, en caso de requerir licenciamiento por usuario para su gestión deberá ser considerado.
- Deberá ser capaz de analizar peticiones de DNS por medio de logs o de tráfico en puerto 53. Con esta información deberá ser capaz de reconocer conexiones a dominios nuevos o recién creados.
- Deberá ser capaz de incluir una vista que permita analizar todos los eventos generados por una sola dirección IP reportados desde las herramientas de seguridad como: antivirus, proxy, firewall, logs de punto final, etc.
- Deberá permitir un análisis forense que permita ir hasta el evento en su formato original.
- Deberá incluir mecanismos para eliminación de falsos positivos, así como la creación de tareas de remediación automáticas usando scripts.
- Deberá incluir scripts de remediación de ejemplo.
- Deberá ser capaz de correr búsquedas que contengan eventos de al menos 3 meses atrás que no demoren más de 5 minutos en presentar los eventos en su formato original (eventos tipo raw).
- Permitir la correlación de eventos de al menos los siguientes dispositivos:
    - 4 (cuatro) Firewall,
    - 4 (cuatro) servidores WAF,
    - 1 (una) Controladora de Wireless,
    - 3 (tres) Servidores de respaldo,
    - 1(un) Servidor Radius,
    - 5 (cinco) Servidores de Directorio Activo,
    - 1 (un) Servidor de DHCP y
    - 5 (cinco) Servidores de DNS interno,
    - 2 (dos) Servidores de DNS externo,
    - 3 (tres) Servidores de correo
    - 5 (cinco) Antispam
    - 11 (once) File Server
    - 1 (un) VMWare Aria Operations Logs.
    - 1 (un) CarbonBlack

El proveedor otorgará a la SFP (cinco) usuarios de acceso con permisos de administración.

6.2 SOLUCIÓN DE PROTECCIÓN DE DNS

Se requiere que el proveedor implemente una solución para la protección de los DNS internos y externos y que bloquee las peticiones de DNS a dominios maliciosos antes de establecer una conexión. Dicha solución deberá considerar las máquinas virtuales (MV) necesarias para cubrir las necesidades de DNS, DHCP y DNS público.

La solución deberá contar con al menos las siguientes características:

- El licenciamiento de la solución deberá considerar que actualmente se cuenta con un total de hasta 2800 usuarios internos con navegación a Internet.
- Los dispositivos serán distribuidos y funcionarán como un sistema unificado y administrado centralmente, es decir, deberán manejar un sistema de administración centralizado a través de una consola de administración.
- La consola de administración puede ser virtual o en la nube.
- Las actualizaciones de software del sistema se deberán cargar en el punto central de administración.
- La tecnología utilizada debe incluir como mínimo los siguientes módulos de servicio DNS, DNSSEC, DHCP, TFTP y NTP.
- El punto central de administración de la solución debe sincronizar datos entre todos los dispositivos.
- Capacidad de trabajar en IPv4, IPv6 o en dual-stack.
- Detendrá automáticamente las comunicaciones del dispositivo con C&C/botnets.
- Detectar malware, ransomware, phishing, kits de explotación, filtración de datos basada en DNS.
- Contar con filtros por contenido específico como: drogas, juegos, violencia, pornografía, fraude, entre otros.
- La protección de DNS debe contar con herramientas de investigación de indicadores de amenazas.
- Permitir búsquedas de indicadores como: dominios, URLs, hashes, hostnames y direcciones IP.
- Debe soportar la administración de registros de DNS como: A, AAAA, ALIAS, NS, SOA, MX, TXT, SRV, CNAME, PTR.

6.2.1 RESPECTO AL MÓDULO DE DHCP

- Deberá automatizar y centralizar todos los aspectos del aprovisionamiento de direcciones IP.
- Deberá identificar el sistema operativo y el tipo de dispositivo.
- Deberá correlacionar los usuarios de Active Directory con las direcciones IP y MAC para identificar a los usuarios por equipo.
- Deberá permitir actualizar los scope.

6.2.2 RESPECTO A LA PROTECCIÓN DE LOS DNS PÚBLICOS

La solución para protección de los DNS públicos para la SFP debe contar con 2 máquinas virtuales en alta disponibilidad en cada centro de datos. Un total de 4 (cuatro) máquinas virtuales con las siguientes características:

- Debe detectar y mitigar ataques basados en DNS.
- Actualización automática contra amenazas nuevas.
- Detectar y mitigar los siguientes tipos de ataques: Reflexión y Reflexión de DNS, DDoS dirigidos al DNS, NXDOMAIN, Random sub-domain, ataques basados en expolits de DNS, ataques de reconocimiento.
- Descargar respaldos de configuración y poder restaurarse utilizando los mismos.

6.3 SOLUCIÓN DE DETECCIÓN Y PREVENCIÓN EN CORREO ELECTRÓNICO (Antispam)

La solución permitirá a la SFP establecer la entrega y recepción de correo electrónico institucional en Microsoft Exchange de forma segura, libre de contenido malicioso, libre de phishing e identificar y detener correo basura, así como, contener el correo que provenga de dominios con mala reputación, debe proteger los buzones del personal de la SFP.

La SFP requiere una solución que deberá contar con al menos las siguientes características tecnológicas:

- Protección contra spam y phishing para el servicio de correo electrónico.
- Licenciamiento para proteger hasta 4500 buzones.
- La solución debe ser proporcionada mediante Imagen de Software en formato ISO para el despliegue sobre plataforma virtualizada acorde a modalidad gateway virtual.
- Los módulos y/o componentes de la solución deben estar basados en software/appliance de uso específico, con sistema operativo, base de datos y servicios configurados para óptimo rendimiento y securización por el fabricante de la solución.
- Es deseable brindar la opción de separar la consola de administración del motor de revisión antivirus y antispam;
- Debe brindar la opción de analizar el correo entrante y saliente en el mismo Gateway virtual/appliance o separar cada flujo en equipos diferentes;
  Se debe proporcionar la imagen a ser cargada para habilitar el Gateway virtual y debe incluir el sistema operativo y la aplicación de filtro de correo. No se aceptará la instalación manual del sistema operativo y la posterior instalación del producto de filtro antivirus;
- La plataforma de virtualización será responsabilidad de la SFP;
- Debe ser compatible con Exchange Server 2016 y 2019;
- Debe ser compatible con servidores de correo de código abierto que soporten el estándar SMTP;
- Debe brindar al menos las siguientes funciones básicas:
  - Antimalware;
  - Antispam;
  - Filtrado de contenido;
  - Cuarentena local;
  - Validación de autenticidad del remitente;
  - Validación de reputación;
  - Lista blanca y lista negra para recepción de correo;
  - Desarticulación de archivos para eliminar contenido no deseado;
- Debe tener la capacidad de archivar cualquier mensaje que viole las políticas corporativas, reenviándolos a la estructura de archivo de la SFP;
- Es deseable poder integrarse con un servidor de cifrado de mensajes de correo, para cifrar mensajes y archivos adjuntos;

- Debe tener la capacidad de permitir o no permitir direcciones de correo electrónico con caracteres especiales, por lo menos un porcentaje (%), guión (-) y caracteres de 8 bits;
- Debe tener la capacidad de rechazar conexiones que intenten ser abiertas por los comandos "HELO" y "EHLO", sin tener sus direcciones "MX" y "A" registradas en los servidores DNS;
- Debe ser capaz de escanear en tiempo real los mensajes salientes hacia Internet y los entrantes desde Internet hacia el servidor de correo interno;
- Debe permitir incluir mensajes de descargo de responsabilidad a los mensajes salientes;
- Debe contar con mecanismos de validación de remitente:
    - SPF
    - DMARC
    - DKIM
    - Sender ID

6.3.1 CONSOLA DE ADMINISTRACIÓN

- La solución debe ser implementada on premise y debe disponer de una consola de gestión centralizada, 100% Web
- Debe tener la capacidad de administrar centralmente múltiples appliances de la misma solución de filtro de correo;
- La solución debe proveer un procedimiento por el cual se pueda realizar un upgrade de todos y cada uno de los dispositivos que la componen, sin la necesidad de realizar un corte de servicio y sin afectar al resto de los componentes;
- Es deseable que la solución permita definir una lista de control de acceso, es decir, especificar que las estaciones de trabajo de los administradores sean las únicas que pueden acceder a ella;
- Debe brindar información de estado de los appliances, tal como uso de CPU, memoria y espacio en disco;
- Debe permitir validar el estado de los servicios de la solución, brindando además opción de detenerlos, iniciarlos o reiniciarlos;
- Debe permitir aplicar parches o nuevas versiones de manera centralizada;
- Debe permitir realizar respaldos y restaurarlos;
- Debe permitir definir si el respaldo será total o personalizado por el administrador;
- Los respaldos deben poder programarse para ser ejecutados de manera automática;
- Los respaldos deben poder almacenarse fuera del appliance;
- Debe permitir reiniciar o apagar los appliances de la solución, de forma centralizada;
- Debe ofrecer controles de contraseña para administradores locales;
- La consola de administración Web, deberá proporcionar capacidades de acceso basado en roles y perfiles de usuario. Role Based Access Control (RBAC)
- Debe integrarse con algún sistema de almacenamiento de registros vía Syslog;

- Debe mostrar las colas de correo, separando el correo entrante y el saliente, con opción a forzar el reintento de entrega o borrar la cola, según decida el administrador;
- Debe permitir definir más de un dominio de correo electrónico para proteger;
- Debe permitir definir políticas individuales por puerta de enlace o servidor global, desde la misma consola;
- Debe tener la posibilidad de acceso individual al dispositivo a través de SSH, para ejecutar comandos a través de CLI (línea de comando);
- Debe contar con una función de seguimiento de mensajes en la propia consola de administración con la capacidad de buscar por asunto, remitente y destinatario, verificando la acción realizada para un mensaje específico, sin necesidad de integración con productos de terceros;
- Debe tener la funcionalidad de alias y enmascaramiento de direcciones;
- Debe ser posible notificar al administrador por correo electrónico si los filtros antispam no reciben actualizaciones durante un cierto período de tiempo;
- Debe poder integrarse con LDAP Microsoft Active Directory 2019 o superior para sincronización y autenticación a la consola de administración;
- Debe permitir la creación de políticas diferenciadas para el tratamiento de spam, virus, Filtrado de Contenidos y Control de Reputación (traffic shaping), según el destinatario del mensaje y la reputación de origen;
- Debe ser capaz de sincronizar usuarios y grupos LDAP para reconocer usuarios válidos y acciones de filtrado de contenido, spam y virus diferenciadas por grupo LDAP;
- Debe poder utilizar la integración de usuarios LDAP, validando su existencia, posibilitando su descarte y rechazo, no enviando mensajes al servidor de correo electrónico, sin destinatario propio dentro de la base LDAP, evitando procesamientos innecesarios por parte del servidor de correo electrónico;
- Debe ser capaz de procesar el tráfico de mensajes entrantes y salientes, con políticas diferentes para cada dirección de tráfico.
- La solución debe de permitir la configuración de los modos de cifrado TLS a aplicar a los correos en situaciones donde el sistema acepté mensajes de otro servidor, o actué reenviando los mensajes, así como también debe de permitir la configuración de los parámetros TLS para dominios individuales.

6.3.2 FUNCIONES ANTISPAM

- Debe permitir la ejecución de múltiples acciones para un mismo mensaje que sea categorizado como SPAM o violación de filtros de contenido, entre ellas:
  - Borrar mensaje;
  - Enviar a Cuarentena;
  - Reenviar mensaje;
  - Modificar el asunto;
  - Agregar encabezado;
  - Rechazar el mensaje;
  - Entregar normalmente el mensaje;

- La solución debe proporcionar capacidades de detección y protección ante ataques del tipo Business Email Compromise (BEC);
- Debe tener la capacidad de notificar al remitente, destinatario, administrador y otros correos electrónicos simultáneamente;
- La solución debe de contar con asistencia de servicios de reputación en la nube;
- Debe permitir la actualización automática de filtros, sin interrupción de los servicios;
- Debe admitir listas negras y listas blancas con opción por dominio, dirección de correo electrónico y dirección IP;
- Debe tener la capacidad de bloquear mensajes considerados como SPAM en base al uso de listas DNSBL (DNS BlackHole) o RBL (Real Time Black List);
- Debe ser capaz de utilizar al menos las siguientes tecnologías de detección de spam:
    - Firmas para el cuerpo del mensaje y los archivos adjuntos;
    - Análisis heurístico, a través del análisis de encabezados, contenido y estructura del mensaje;
    - Filtros de reputación local (creados automáticamente a través del análisis de los mensajes recibidos) y global (creados por la red de monitoreo del proveedor de la solución);
    - Identificación de idioma;
    - Filtros de URL;
    - Filtros anti-phishing;
- Debe tener la capacidad de crear filtros basados en el encabezado, remitente, tipos y contenido de los archivos adjuntos, diccionarios de palabras, asunto y cuerpo del mensaje, incluyendo el uso de expresiones regulares;
- Debe permitir la creación de "carpetas de cumplimiento", para almacenar mensajes (entrantes/salientes) que violen cualquier política de contenido creada por el Administrador;
- Debe contar con tecnología para detectar Spam, Virus y ataques a Directorios (Usuarios Inválidos);
- La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0.
- La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo Ransomware.
- Es deseable poder ser integrada con tecnologías de Sandboxing.
- Debe contar con tecnología para prevenir ataques de “Mensajes Rebotados”;
- Debe tener la capacidad de crear reglas basadas en el tipo de archivo adjunto;
- Debe tener la capacidad de crear reglas basadas en la detección por "Comodín" (*);
- Debe tener la capacidad de crear reglas basadas en la detección por expresiones regulares;
- Debe tener la capacidad de implementar una comunicación segura a través de TLS (Seguridad de la capa de transporte);
- Debe poder configurar el cifrado TLS por dominio y por política;

- Debe ser capaz de detectar varios idiomas, permitiendo bloquear mensajes escritos en idiomas no deseados;
- Debe tener la capacidad de crear una lista de IP confiables en función del comportamiento de la IP de origen del mensaje, para minimizar el impacto en el rendimiento en entornos grandes;
- La totalidad del análisis y operación de la solución debe realizarse en forma local, solo permitiéndose el envío de hashes cuando sea necesario. La solución no debe enviar ninguna información sensible fuera de la institución.

6.3.3 FUNCIONES ANTIMALWARE

- Debe tener la capacidad de identificar y borrar completamente los mensajes enviados por gusanos de envío masivo, con la opción de acciones diferenciadas por tráfico entrante y saliente;
- Debe ser capaz de reconocer Spyware y Adware y aplicar una acción correctiva diferente a la que se aplica cuando se encuentra virus;
- En caso de objetos infectados, la solución debe poder configurar la realización de las siguientes acciones:
  - Desinfectar
  - Eliminar Anexo
  - Borrar mensaje
  - Rechazar mensaje
  - Ignorar
- Debe contar con una función de detección de ataques en dos escalas para Virus y Directorio (LDAP), capaz de diferir la conexión SMTP si la fuente emisora ha enviado un porcentaje de mensajes considerados como usuarios no válidos o infectados con virus, en un período de tiempo determinado, ambos configurables por el administrador;
- Debe contar con un módulo antivirus para la detección de contenido malicioso en los mensajes.
- Debe tener la capacidad de bloquear archivos adjuntos por extensión, tipo de archivo real (True Type File), Tipo Mime y nombre de archivo;
- Debe ser capaz de desactivar/desarticular componentes maliciosos en al menos archivos de Office y PDF;
- Es deseable permitir definir límites para evitar bloqueo del servicio al analizar archivos comprimidos dentro de archivos comprimidos, pudiendo definirlos por tamaño o tiempo;
- Debe permitir definir el nivel de agresividad para la detección de virus no conocidos;
- Debe contar con una cuarentena diferente de la de spam para almacenar correos sospechosos de virus.
- Debe permitir la trazabilidad de las actividades de los usuarios y bloquear el acceso a enlaces maliciosos.

6.3.4 CUARENTENA

- Eliminación automática de mensajes almacenados en cuarentena según la configuración definida por el administrador;
- Debe permitir al usuario registrar direcciones de correo electrónico en listas negras/listas blancas personales;

6.3.5 FUNCIONES DE FILTRADO DE CONTENIDO

- La solución debe disponer de capacidad de filtrado de contenido de los mensajes mínimamente acorde al nombre, tamaño y tipo de anexo, determinando el formato indiferentemente de su extensión, así como eliminar mensajes o sus anexos;
- En caso de detectar actividad en el módulo de filtrado de contenido, la solución debe poder configurar la realización de las siguientes acciones:
    - Desinfectar
    - Eliminar anexo
    - Borrar mensaje
    - Rechazar mensaje
    - Ignorar

6.3.6 REPORTES DE ESTA SOLUCIÓN

- Debe de incluir la funcionalidad de creación de reportes que sea parte de la misma consola, sin depender de soluciones adicionales;
- Debe incluir al menos los siguientes reportes:
    - Reporte ejecutivo
    - Reporte de virus
    - Reporte de spam
- Los reportes deberán poder generarse por periodos de tiempo específicos según defina el administrador;
- Los reportes deberán poder enviarse por correo electrónico;
- Los reportes deberán poder calendarizarse para su generación y envío periódico;
- Los reportes deberán poder exportarse a PDF, HTML o CSV.

6.4 PROTECCIÓN ANTIMALWARE PARA ESTACIONES DE TRABAJO Y SERVIDORES (Endpoint)

El servicio de protección antimalware de estaciones de trabajo y servidores debe combinar Antivirus con prevención avanzada de amenazas, IPS, Firewall, reputación y comportamiento, así como control de dispositivos y aplicaciones, para proporcionar una defensa contra malware para computadoras portátiles, de escritorio y servidores, integrando tecnologías de seguridad esenciales en un solo agente y una única consola de administración.

6.4.1 Funcionalidades requeridas

- Considerarse para un total de 2000 equipos de escritorio/laptops y 80 servidores.
- Reputación de archivos, sean locales o descargados de la web.

- IPS de próxima generación.
- Protección del navegador (browser).
- Aprendizaje automático (Machine Learning).
- Análisis de Comportamiento.
- Mitigación de explotación de memoria.
- Control de aplicaciones.
- Control de dispositivos.
- Proveer detección y respuesta de amenazas automatizadas contra una variedad de amenazas de malware avanzadas.
- El cliente para instalación en estaciones de trabajo debe ser compatible con al menos los siguientes sistemas operativos:
    - Debian 10;
    - Mac OS X 11.x, 12.x y 13;
    - Oracle Linux 7 y 8;
    - Red Hat Enterprise Linux 8.x y 9.x;
    - Ubuntu 20.04 y superiores;
    - Windows 10 y 11;
    - Windows Server 2008 R2;
    - Windows Server 2012, 2012 R2;
    - Windows Server 2016, 2019 y 2022;
- Soporte para protocolos TCP, UDP e ICMP;
- Reconocimiento de tráfico DNS, DHCP y WINS con opción de bloqueo;
- Proporcionar protección contra la explotación del desbordamiento de buffer;
- Tener protección contra ataques de Denegación de Servicio (DoS), Port-Scan y MAC Spoofing;
- Posibilidad de crear reglas diferenciadas por aplicaciones;

6.4.2 Requisitos técnicos

- Debe contar con administración centralizada a través de una única consola de gestión.
- Acceso a la consola de administración basado en Roles y perfiles de acceso, con capacidades granulares de definición de restricciones y capacidades funcionales.
- Segundo factor de autentificación (2FA) para el acceso a la consola de administración compatible con Microsoft Authenticator y Google Authenticator.
- La consola de administración puede ser virtual o en la nube.
- Debe tener acceso a la consola de administración vía tecnología Web (HTTPS).
- Admitir la instalación del agente en sistemas operativos Windows 10 y 11, así como MAC OS.
- Deberá de instalar clientes en servidores, estaciones de trabajo y máquinas virtualizadas de forma remota a través de la consola de administración con la opción de eliminar las soluciones antimalware instaladas previamente.
- El proveedor deberá ser responsable de la desinstalación del agente actual.
- Integrarse con Active Directory y permitir hacer inicio de sesión a la consola de administración utilizando las credenciales de la red con sus respectivos permisos.
- Contar con los mecanismos de protección para no poder ser desinstalado o desactivado por el usuario.

- Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.;
- Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos;
- La configuración de antivirus, antispyware, firewall, protección contra intrusos, control de dispositivos y control de aplicaciones debe realizarse para máquinas físicas y virtuales a través de la misma consola.
- Toda la solución debe funcionar con un solo agente en la estación de trabajo y servidores físicos y virtuales para reducir el impacto en el usuario final.
- Tener compatibilidad con IPv6.
- El fabricante de la solución debe proporcionar actualizaciones de productos, firmas de virus y de protección contra intrusiones.
- La consola de administración debe permitir bloquear las configuraciones por contraseña en los clientes, servidores y estaciones físicas y virtuales, definiendo permisos para que solo el administrador pueda cambiar las configuraciones, desinstalar o detener el servicio del cliente.
- Reconocimiento de tráfico DNS, DHCP y WINS con opción de bloqueo.
- Proporcionar protección contra la explotación del desbordamiento de buffer.
- Tener protección contra ataques de Denegación de Servicio (DoS), Port-Scan y MAC Spoofing.
- Posibilidad de crear reglas diferenciadas por aplicaciones.
- La funcionalidad del cortafuegos debe ser compatible al menos con Windows y Mac.
- Gestión integrada en la consola de gestión de la solución.
- Funcionalidad antivirus y antispyware.
- Protección en tiempo real contra virus, troyanos, gusanos, spyware, adware y otros tipos de códigos maliciosos.
- La protección antispyware debe ser nativa del propio antivirus, es decir, no depender de un plugin o módulo adicional.
- La configuración antispyware debe realizarse a través de la misma consola que todos los elementos de la solución.
- Permitir la configuración de acciones diferenciadas para cada subcategoría de riesgos de seguridad (Adware, Dialers, Hacking Tools, Spyware, Trackware y otros).
- Permitir la configuración de dos acciones, primaria y secundaria, realizadas automáticamente para cada amenaza, con las opciones: solo alertar, limpiar automáticamente, eliminar automáticamente y poner en cuarentena.
- Permitir la creación de listados de exclusiones con información sobre la severidad, impacto y grado de remoción de la amenaza en niveles bajo, medio o alto, donde los riesgos excluidos no serán verificados por el producto.
- Permitir la verificación de amenazas de forma manual, programada y en Tiempo Real.
- Implementar intervalos de tiempo para iniciar análisis programados con el fin de reducir el impacto en los entornos virtuales.
- Contar con funcionalidades que permitan el aislamiento (área de cuarentena) de archivos contaminados por códigos maliciosos que no se conocen o que no pueden ser reparados en el cliente.
- Tener características que permitan la inclusión manual en aislamiento (área de cuarentena).

- Control de virus de mensajes de correo electrónico, utilizando el antivirus de la estación de trabajo, soportando al menos clientes Outlook y POP3/SMTP.
- Contar con funcionalidades que permitan la detección y reparación de archivos contaminados por códigos maliciosos, aunque estén comprimidos por ZIP, LHA y ARJ, cubriendo al menos hasta el octavo nivel de compresión;
- Capacidad de detección en tiempo real de nuevos virus, desconocidos por la vacuna, con opción de sensibilidad de detección (baja, media y alta).
- Capaz de eliminar de forma totalmente automática los daños causados por spyware, adware y gusanos, como limpiar el registro y los puntos de carga, con la opción de finalizar el proceso y finalizar el servicio de amenazas en el momento de la detección.
- La eliminación automática de los daños causados debe ser nativa del propio antivirus, es decir, no depender de un complemento, ejecución de archivos o módulo adicional.
- Capacidad de identificar el origen de la infección, para virus que utilizan el intercambio de archivos como medio de propagación, informando el nombre o la IP del origen con una opción para bloquear la comunicación a través de la red.
- Posibilidad de bloquear escaneos de virus en recursos de red mapeados, por contraseña.
- Opción a crear una copia de seguridad del archivo sospechoso antes de limpiarlo.
- Gestión integrada en la consola de gestión de la solución.
- Capacidad para proteger contra ataques dirigidos al navegador.
- Administrar el uso de dispositivos USB y CD/DVD, a través de controles para leer/escribir/ejecutar el contenido de estos dispositivos y también sobre el tipo de dispositivo permitido (por ejemplo, permitir mouse USB y bloquear disco USB).
- Permitir bloquear el uso de aplicaciones en función del nombre, directorio y hash de la aplicación.
- Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red
- La solución debe proporcionar la siguiente información de los puntos finales:
    - Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora en que el software fue instalado o removido.
    - Actualizaciones de Windows Updates instaladas
    - Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD
    - Vulnerabilidades de aplicativos instalados en la máquina
- Capacidad de reportar vulnerabilidades de software presentes en las computadoras.
- Capacidad de realizar inventario de hardware de todas las máquinas clientes;
- Capacidad de realizar inventario de aplicativos de todas las máquinas clientes;
- Capacidad de diferenciar máquinas virtuales de máquinas físicas;

6.4.3 Soporte al cliente de Mac OS

- Debe proporcionar protección residente para archivos (antispyware, anti-troyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
- Capacidad de elegir de qué módulos se instalarán, tanto en la instalación local como en la instalación remota;

- La instalación y primera ejecución del producto debe ser realizada sin necesidad de reiniciar la computadora, de modo que el producto funcione con toda su capacidad
- Métodos de detección basados en: Firmas, Heurística, asistido por Nube de seguridad del proveedor.
- La solución deberá contar con medidas de seguridad para el usuario de la estación de trabajo, sea este el administrador de la red o de la pc no deje sin efecto la política de seguridad corporativa.
- La solución deberá contar con tecnologías de detección proactiva de amenazas basadas en la nube del mismo fabricante.
- El cliente para la instalación en estaciones de trabajo debe ser compatible con el sistema operativo Mac OS X para la funcionalidad antivirus, antispyware y firewall.
- Gestión integrada en la consola de gestión de la solución.
- Protección en tiempo real contra virus, troyanos, gusanos, troyanos, spyware, adware y otros tipos de códigos maliciosos.
- Permitir el análisis de amenazas tanto de forma manual como programada.
- Permitir la creación de listas de exclusiones para carpetas y archivos que no serán escaneados por el antivirus.
- Permitir acciones de reparación o cuarentena de archivos en caso de infecciones de archivos.

6.4.4 Funcionalidades de control de acceso a la red

- Debe tener la posibilidad de la puesta en cuarentena de equipos, restringiendo el acceso a la red a aquellos equipos que no cumplan con las políticas, al menos con las siguientes premisas:
    - La computadora debe tener antivirus, actualizado y activo;
    - La computadora debe tener un firewall activo;
    - La computadora debe tener parches instalados, activos y actualizados;
- Debe tener la capacidad de iniciar la auto remediación del equipo que falló la auditoría, es decir, corregir los puntos donde falló la verificación especificada por el administrador.
- Debería tener la posibilidad de notificación personalizada para el usuario.

6.4.5 Funcionalidades de cifrado

- El acceso al recurso cifrado (archivo, carpeta o disco) debe ser garantizado aún en caso de que el usuario haya olvidado la contraseña, a través de procedimientos de recuperación.
- Utilizar, como mínimo, un algoritmo AES con clave de 256 bits.
- Capacidad de cifrar completamente el disco duro de la máquina, agregando un ambiente de preboot para autenticación del usuario.
- Capacidad de utilizar Single Sign-On para la autenticación de preboot.
- Permitir crear varios usuarios de autenticación preboot.
- Capacidad de crear un usuario de autenticación preboot común con una contraseña igual para todas las máquinas a partir de la consola de manejo.
- Capacidad de cifrar drives extraíbles de acuerdo con una regla creada por el administrador, con las opciones:
    - Cifrar solamente los archivos nuevos que sean copiados para el disco extraíble, sin modificar los archivos ya existentes.
    - Cifrar todos los archivos individualmente.

- Cifrar el dispositivo entero, de manera que no sea posible listar los archivos y carpetas almacenadas.
- Cifrar el dispositivo en modo portátil, permitiendo acceder a los archivos en máquinas de terceros a través de una contraseña.

- Capacidad de seleccionar carpetas y archivos (por tipo, o extensión) para ser cifradas automáticamente. En esta modalidad, los archivos deben estar accesibles para todas las máquinas gestionadas por la misma consola de manera transparente para los usuarios.
- Capacidad de crear reglas de exclusiones para que ciertos archivos o carpetas nunca sean cifrados.
- Capacidad de seleccionar aplicaciones que pueden o no tener acceso a los archivos cifrados.

6.5 ADMINISTRACIÓN DE CUENTAS PRIVILEGIADAS

El proveedor deberá de proponer una solución de Seguridad que se encargue de gestionar las Identidades Privilegiadas y que asegure, supervise, audite, genere y controle el acceso a sistemas privilegiados y de carácter sensible para la Secretaría, con el propósito de reducir riesgos de seguridad otorgando protección total contra amenazas avanzadas externas e internas a 50 cuentas y/o usuarios.

Dicha plataforma de Seguridad de Identidades deberá de brindar acceso seguro en todas partes, combinando capacidades para la integración de un inicio de sesión único (Single Sign On), la autenticación multifactorial (MFA) adaptable, el manejo de flujos de trabajo, gestión del ciclo de vida de la identidad y el análisis del comportamiento del usuario.

El proveedor deberá de contemplar dentro de su solución:

- El software necesario para la operación de todos los componentes de la plataforma.

Administración y resguardo de cuentas privilegiadas, incluyendo:

- Descubrimiento automático de cuentas privilegiadas y sus dependencias en servicios de Windows y tareas programadas.
- Centralización y almacenamiento seguro de las cuentas privilegiadas.
- Rotación automática de contraseñas y llaves SSH.
- Flujos de trabajo automatizados para solicitud de cuentas privilegiadas.
- Controles para la solicitud de contraseñas con registros de auditoría y reportes sobre el uso.

Administración de Sesiones Privilegiadas, incluyendo:

- Entrega de sesión privilegiada autenticada al dispositivo destino al usuario solicitante.
- Monitoreo y grabación de todas las actividades realizadas con las cuentas privilegiadas en sistemas críticos como Sistemas Operativos, Bases de Datos, Sitios Web, Dispositivos de Seguridad, Dispositivos de Red, Aplicaciones, etc.
- Evitar mostrar las contraseñas privilegiadas a los usuarios.
- Grabación en video de las sesiones gráficas.

- Monitoreo en tiempo real de las sesiones activas
- Suspensión y Terminación de sesiones activas.
- Registro de comandos o teclas presionadas por el usuario en las sesiones.
- Prevenir el acceso directo a los sistemas críticos, ofreciendo un puente entre los usuarios y los dispositivos (aislamiento), sin utilizar agentes.

La solución propuesta por el proveedor deberá tener la capacidad de detección y respuesta a amenazas que abusen de las cuentas privilegiadas en base a analíticos ofreciendo:

- La capacidad de detectar, alertar y responder a ciberataques intentando explotar las cuentas privilegiadas utilizando algoritmos inteligentes y analíticos.
- Integración bidireccional con soluciones SIEM
- Definición, manual de reglas y autoaprendizaje de la solución para detectar amenazas automáticamente.
- Tablero de alertas y reportes.
- Reglas de respuesta automática a incidentes (rotación automática de cuentas comprometidas)

Control de Acceso a las Identidades privilegiadas (MFA y SSO):

- La plataforma debe ser capaz de autenticar a los usuarios utilizando múltiples factores de autenticación, incluyendo:
    - Contraseñas de Active Directory
    - Código QR propio
    - Código OTP vía SMS enviado por la propia solución
    - Código OTP vía E-mail enviado por la propia solución
    - Notificaciones push a dispositivos móviles enviado por la propia solución
    - OTP de terceros que soporten OATH
    - Tokens de terceros en cumplimiento con FID02
    - Autenticación biométrica de dispositivos como Windows Helio y Apple Touch ID
- Análisis de comportamiento de usuario y uso de Machine Learning para determinar el riesgo durante un inicio de sesión.
- Autenticación adaptable al contexto y riesgo calculado por la plataforma para cada usuario.
- Capacidad de incluir al portal de usuario otras aplicaciones para su protección con MFAy SSO.

Integración con otras soluciones de autenticación que soporten:

- Web SSO.
- RADIUS.
- PKI.
- SAML.
- OpenID Connect (OIDe).

6.5.1 Dispositivos para administrar

La solución de Seguridad de Cuentas Privilegiadas propuesta por el proveedor deberá tener la capacidad de administrar diferentes orígenes o plataformas que estén certificadas y soportadas tanto por la solución propuesta como por la marca de la integración, entre las cuales deberán encontrarse por lo menos las plataformas:

- Sistemas Operativos como: Windows, *NIX, MAC OS, ESXi, Linux RedHat, Oracle Linux, Solaris.
- Aplicaciones de Windows como: Cuentas de servicio, tareas programadas.
- Bases de datos como: Oracle, MSSQL, SAP MongoDB, MySQL.
- Aplicaciones como: SAP, VMWare vSphere.
- Directorios como: Microsoft.
- Interfaces genéricas como: SSH, Web, PuTTY, RDP.
- ODBC- Contraseñas almacenadas en tablas de base de datos.

La solución de seguridad de Cuentas Privilegiadas deberá poder establecer la integración de plataformas adicionales a través de scripts o frameworks de integración ofrecidos por la misma marca.

6.5.2 Descripción técnica

Suministro de la solución de seguridad de cuentas privilegiadas con al menos, las características y especificaciones técnicas siguientes:

- La solución de Seguridad de Cuentas Privilegiadas propuesta por el proveedor deberá tener la capacidad de administrar la plataforma de forma centralizada a través de un portal web y capacidad para restringir accesos a través de zonas de red confiables.
- El acceso a la solución deberá estar protegido por múltiples factores de autenticación adaptable al contexto, basado en el riesgo determinado por geolocalización y horarios de autenticación; esta funcionalidad debe ser nativa y proporcionada por el mismo fabricante, al menos considerando, contraseña, código QR, OTP, Notificación Push al móvil con validación biométrica, código enviado al correo electrónico, código enviado por SMS, Fid02.
- Deberá tener la capacidad de manejar los controles de acceso basado en roles mediante la administración de grupos de usuarios de Directorio Activo o LDAP, además de aprovisionar usuarios en forma automática a partir del Directorio Activo de la Secretaría o LDAP, para así contar con aprovisionamiento automático y transparente de cuentas que reflejen los cambios en dichos directorios.
- Deberá tener la capacidad de ejecutar operaciones de forma masiva (bulk operations) sobre las cuentas privilegiadas, como altas y modificaciones.
- Deberá soportar el español e inglés como lenguajes disponibles en sus interfaces de usuario.
- Deberá contar con una interfaz para programadores (API) y de esta forma permitir la automatización de actividades administrativas, como alta de cuentas, rotación de contraseñas, salud de los componentes instalados y obtener eventos de seguridad.

6.5.3 Seguridad

- La solución propuesta por el proveedor deberá tener la capacidad de cifrar, en reposo y en tránsito todos los datos que utilice para garantizar la máxima seguridad posible. Incluyendo contraseñas, reportes almacenados, grabaciones y registros de usuarios.
- La solución propuesta por el proveedor deberá tener la capacidad de cifrar la comunicación entre todos los componentes de la solución, esto incluye los componentes que residan en un mismo servidor o en los componentes instalados en otros servidores, utilizando algoritmos AES-256, RSA-2048 y que cumplan con FIPS 140-2.
- La solución deberá de poder realizar la Integración de HSM externo para almacenar las llaves de cifrado.
- La solución propuesta por el proveedor deberá tener la capacidad de permitir que ciertos administradores no puedan visualizar las contraseñas que son controladas por otros departamentos de la Secretaría, como por ejemplo que los administradores de Windows Server no puedan visualizar las contraseñas ni accesos a instancias de bases de datos SQL Server. Esto es para garantizar la segmentación de roles lo más apegado a los procesos establecidos de la Secretaría, con el fin de evitar el uso indebido de las cuentas privilegiadas protegidas por la solución.
- La solución propuesta debe permitir que los administradores de la solución no tengan acceso a las contraseñas almacenadas si así se define por el negocio.
- La solución propuesta deberá contar con un repositorio seguro y a prueba de falsificaciones (tamper-proof) de credenciales privilegiadas, políticas, grabaciones, permisos, registros de auditorías separado del resto de los componentes que conformen la solución.

6.5.4 Arquitectura

- La solución de Seguridad de Cuentas Privilegiadas deberá soportar su instalación como solución basada en Servidores Físicos, en ambientes on-prem.
- La solución propuesta deberá ser capaz de realizar las tareas de gestión de cuentas privilegiadas sin la necesidad de que se instalen agentes en los dispositivos del centro de datos.
- La solución deberá ser modular y escalable para adaptarse a crecimientos de utilización o expansión de funcionalidades, evitando Appliances all-in-one que complique la instalación de un solo componente para cubrir necesidades específicas como la concurrencia de sesiones o cobertura a diferentes segmentos de red o regiones.
- El componente que almacene las contraseñas deberá estar separado del servidor que contenga la interfaz de usuario final y no deberá exponer protocolos innecesarios como HTTPS.
- La solución propuesta deberá contar con un repositorio propietario para los datos y ofrecer esquemas de alta disponibilidad (Activo-Activo, Activo-Pasivo) sin necesidad de integrar bases de datos de terceros.
- La solución propuesta No deberá requerir licencias adicionales para su Base de Datos en ninguno de sus esquemas de Alta Disponibilidad (Activo-Activo, Activo-Pasivo).
- La solución propuesta deberá contar por lo menos con un firewall, hardening del sistema, acceso remoto de forma limitada y restringida a los servidores que resguardan las contraseñas.

6.5.5 Alta disponibilidad y redundancia

- La solución propuesta por el proveedor deberá contar con un mecanismo propietario de generación de respaldos cifrados para los datos de la aplicación y no depender de soluciones de respaldo de terceros.
- Soporte para instalar repositorio en Clúster.
- Sitio de recuperación de desastres.
- Integración con respaldos de seguridad del sistema.
- Todos los componentes de la solución deberán soportar esquemas activo-activo o activo-pasivo.
- La solución debe permitir tener acceso fuera de línea a las credenciales privilegiadas desde una aplicación móvil protegida por múltiples factores de autenticación y autenticación biométrica inclusive cuando la solución de PAM no se encuentre disponible.

6.5.6 Integraciones necesarias con otros sistemas

- Directorios LDAP para administración de usuarios (Active Directory).
- Soluciones SIEM para envió de eventos, alertas y recepción de eventos como inicio de sesión, cambios de contraseñas y asignación de perfiles administrativos, que ocurren en los sistemas administrados.
- Integración con Sistemas de Tickets para gestión de solicitudes de sesiones y contraseñas.
- Soluciones de monitoreo para el envío de Tramas SNMP.
- Servidores de correo SMTP para envío de notificaciones por correo electrónico.
- Integración con soluciones de Gobierno de Identidades a través del protocolo SCIM.

6.5.7 Requerimientos de Descubrimiento de Cuentas, Escaneo de Máquinas

- El escaneo debe poderse ejecutar sin haber instalado aún la solución de manejo de cuentas privilegiadas, como primer paso para la detección de riesgos asociados a las cuentas en los ambientes escaneados.
- La solución propuesta por el proveedor deberá tener la capacidad escanear máquinas Windows, Linux y mapear los usuarios que pueden accederlas, incluyendo usuarios locales y de dominio.
- El escaneo debe reportar las cuentas encontradas que no se adhieren a la política corporativa de contraseñas.
- El escaneo debe considerar el descubrimiento de las cuentas de Windows que se utilicen en servicios de Windows y Tareas Programadas de Windows.
- El escaneo debe ser capaz de encontrar credenciales que se encuentren en texto claro de servidores de aplicaciones WebLogic, Websphere y I/S.
- El escaneo debe ser capaz de encontrar credenciales en texto claro que se encuentren en Playbooks de Ansible para los servidores Linux.
- El escaneo debe descubrir llaves privadas y públicas de SSH en Linux/Unix y correlacionarlas con las cuentas descubiertas.
- La solución propuesta deberá tener la capacidad de mostrar en una gráfica los riesgos relacionados a los ataques de Kerberos como Pass-The-Hash y Golden ticket, sin tener que haber implementado la solución de manejo de cuentas privilegiadas.

Características de Administración de Sesiones Privilegiadas

6.5.8 Monitoreo y Auditoría de Sesiones Privilegiadas

- La solución deberá tener la capacidad de asegurar responsabilidad personal cuando se abre una sesión privilegiada con una cuenta compartida, de forma que se pueda diferenciar qué persona hace uso de una cuenta compartida o genérica, cuándo la utiliza y las actividades que realiza.
- La solución deberá tener la capacidad de integrarse a sistemas de Ticketing/HelDesk/Change Management y permitir la validación de tickets antes de establecer la sesión.
- La solución deberá tener la capacidad de hacer búsquedas de comandos privilegiados dentro de las grabaciones de video.
- La solución deberá tener la capacidad de visualizar las sesiones activas en un momento determinado en vivo/tiempo real.
- La solución deberá tener la capacidad de suspender o terminar remotamente una sesión en tiempo real manualmente.
- La solución deberá tener la capacidad de que las actividades de sesiones a nivel granular puedan enviarse a la solución SIEM solicitada en este anexo técnico.
- La solución deberá tener la capacidad de generar videos de toda la sesión y no solo capturas de pantallas.
- La solución deberá tener la capacidad de comprimir las sesiones y sin impactar en la calidad de video.
- La solución deberá tener la capacidad de reproducir los videos de las sesiones desde el mismo portal de administración y con la opción de saltar la inactividad en las sesiones, de modo que solo se visualicen los momentos de actividad en una sesión grabada.

6.6 PUNTOS DE DECEPCIÓN DE ATAQUE (TRAMPAS DE SEGURIDAD)

El proveedor deberá de proponer una solución de alertamiento preventivo para detectar ataques cibernéticos y responder de manera anticipada, estos puntos de decepción de ataque (trampas de seguridad) apoyará principalmente a contar con la capacidad para descubrir amenazas latentes y silenciosas en el ambiente, contener y limitar las ventanas de exposición, e incluso alertar de ransomware antes de que se produzca una fuga, filtración, robo o daño de los datos. , contribuyendo a cumplir con los controles de seguridad que minimicen los riesgos de infección de virus y malware, en cumplimiento a la normatividad aplicable en materia de seguridad de la información.

6.6.1 Funciones Requeridas:

La solución propuesta por el proveedor deberá estar basada en plataforma de propósito específico.

La solución deberá de ser capaz de detectar malware de día cero, polimórfico y exploits dentro de la red, así como comunicación de tipo comando y control (C&C) hacia el exterior de la red de la Secretaría. La arquitectura deberá estar basada en el concepto del despliegue de trampas al interior de la red de la Secretaría en los ambientes definidos, que permitan identificar el movimiento lateral y primeros signos de las amenazas, se puede incluir una solución de honeypots, sensores o trampas.

Cada localidad geográfica relevante de la Secretaría (Centro de datos principal y Centro de datos alterno) deberá contar con su propio equipo virtual de amenazas avanzadas.

Se deberá de contar con un sistema de consola virtual centralizada que reciba la información de todas las localidades geográficas.

La solución deberá cumplir con lo siguiente:

- La solución debe incluir el licenciamiento para publicar 200 emulaciones o trampas, dependiendo de la necesidad de la Secretaría.
- El licenciamiento por trampa debe soportar, sin costo adicional, que éstas puedan ser implementadas en ambientes virtualizados sobre VMWare ESX, Microsoft Hyper-V o Linux KVM.
- La solución debe estar basada en la red y sin utilización de agentes.
- La solución propuesta debe de integrar un appliance virtual por cada localidad geográfica o lógica donde se implemente la solución de engaño.
- La solución debe de emplear trampas o honeypots que deberán ser desplegados estratégicos al interior de la red para la identificación de amenazas.
- La solución debe tener la capacidad de monitorear comunicaciones en VLANs y el tráfico de salida a Internet.
- La solución en sus diversos componentes debe estar basada en un sistema operativo endurecido y cerrado.
- No se aceptan soluciones que publican trampas en servidores en una localidad central y que a través de conectores o componentes de software que proyecten las trampas. la Secretaría podrá decidir el número de trampas a utilizar.
- La solución no debe requerir licencias de sistemas operativos para las emulaciones, trampas o honeypots.
- La solución debe apoyar la mezcla de trampas o emulaciones falsas con los activos del entorno productivo de la entidad bajo el concepto del uso del engaño.
- La solución debe integrar un mecanismo para evaluar la cobertura que ofrecen las trampas implementadas en cada segmento de red en base a las técnicas y tácticas de MITRE ATT&CK. Esto con el objetivo de proveer una visibilidad clara del nivel de exposición actual de la Secretaría, además de permitir, en caso de ser necesario, agregar más trampas para incrementar la cobertura.
- Con el objetivo de incrementar la cobertura de la plataforma del engaño, la solución debe soportar la capacidad de construir trampas personalizadas utilizando la interfaz gráfica de la plataforma de administración, de cualquier dispositivo conectado a la red de la organización.
- La solución debe poder adaptarse a cambios en el entorno productivo mediante la ejecución de escaneos para identificar nuevos activos o plataformas operativas en la red de la entidad.
- La solución deberá soportar el acceso basado en roles para segregar funciones y capacidades de la plataforma por usuario.
- La arquitectura de la solución debe contar e incluir el software, licenciamiento o subscripción requerida para una gestión centralizada en la infraestructura de TI en la

Secretaría o basada en nube para la gestión de múltiples Appliances de la solución en todos los sitios o localidades requeridas por la Secretaría.
- La solución debe tener la capacidad de integrarse con el sistema SIEM solicitado en este anexo técnico.
- La solución debe permitir generar reportes al menos de Top de direcciones IP destino, Top de IP fuentes maliciosas, Ataques de Alto Riesgo Diarios y Semanales.

6.6.2 Inteligencia y Detección de Amenazas

- La solución debe de incluir la capacidad, licencias y componentes requeridos para monitorear el tráfico generado del interior de la red hacia Internet, para poder identificar comportamiento basado en botnets, comando y control (C2) y responder rápidamente ante la identificación de equipos comprometidos.
- La solución no debe estar basada en firmas para detectar el malware o la actividad maliciosa.
- La solución debe soportar al menos los siguientes mecanismos para la detección de malware o ataques:
    - Cajas de arena (sandboxing)
    - Análisis estático
    - Integración con VirusTotal.
- La solución debe de ser capaz de capturar el código malicioso y payloads asociados para su análisis, a pesar de no ser una amenaza conocida previamente.
- La solución debe generar notificaciones después de la detección de posibles amenazas internas o de malware.
- La solución puede utilizar un análisis dinámico descentralizado basado en la nube para realizar un análisis forense y controlado del malware capturado desde los sensores o trampas.
- La solución debe de ser capaz de identificar no solo ataques o comportamientos basados en malware, sino cualquier comportamiento malicioso de interacción humana o automatizado que haga contacto con los sensores desplegados.
- La solución debe de permitir la integración nativa a la plataforma de administración de la tecnología del engaño sin necesidad de licenciamiento o productos adicionales de la misma marca.
- La solución debe permitir la integración con al menos las tecnologías que apoyen la respuesta ante un evento de manera automática o bajo demanda.
- La solución debe permitir incluir datos falsos independientes en cada una de las hasta 200 trampas soportadas por Appliance físico para hacer más creíble el engaño hacia el atacante.
- La solución debe incluir por lo menos la siguiente información relacionada con el ataque:

    - IP del atacante y el objetivo
    - Análisis preliminar
    - Captura de la sesión en la red (PCAP)
    - Servicios utilizados durante los ataques o interacción con la trampa.

- La solución debe permitir la extracción del malware original para realizar un análisis forense externo o una retención legal de ser necesario.
- La plataforma debe de permitir identificar y asociar los eventos generados desde las trampas o sensores en base a la táctica de MITRE ATT&CK correspondiente. Además, debe permitir filtrar los eventos en base a la naturaleza de su actividad:
    - Conexión
    - Reconocimiento
    - Interacción
    - Infección

- La solución debe tener la capacidad de proporcionar información ficticia configurable e independiente por trampa, como puertos, mensajes de bienvenida (banners), credenciales de acceso sobre cada servicio (ftp, smb, etc.) para hacer más factible engañar al atacante.
- La solución debe tener la capacidad de agregar etiquetas personalizables a cada trampa de forma independiente. Esto con el objetivo de simplificar la operación de las trampas desde la interfaz gráfica de la plataforma.
- La solución debe integrar de forma nativa en sus Appliances físicos, sin necesidad de realizar configuraciones personalizadas o por medio de servicios profesionales, un sistema operativo Linux completo que contenga y publique el servicio de SSH.
- La solución deberá permitir visualizar estadísticas de los eventos o amenazas basado en la naturaleza de esta dentro de la entidad.

7 ENTREGABLES

- La documentación en digital deberá ser enviada al correo electrónico del administrador y del supervisor del contrato por parte de la SFP y como un documento adjunto y nunca como liga de descarga.
- Queda estrictamente prohibido que el proveedor utilice plataformas en la nube pública (Dropbox, Google Drive, OneDrive, etc.) para almacenar cualquier entregable descrito en el presente Anexo Técnico.
- El proveedor deberá cumplir con la entrega de la documentación y apegarse a los tiempos requeridos.
- El proveedor debe considerar que los entregables expuestos en los diferentes apartados de este anexo no son limitativos, en caso de que la SFP requiera algún reporte adicional serán analizados y establecidos de común acuerdo durante la vigencia del contrato.
- Cada entregable estará perfectamente identificado con su ID y nombre, el formato de los entregables podrá ser ajustado a los requerimientos de la SFP.

La documentación impresa se deberá entregar los tiempos señalados en la siguiente tabla:

ID	ENTREGABLE	TIEMPO DE ENTREGA	MEDIO
E-01	Plan de Trabajo	Ocho días hábiles posteriores a la notificación del fallo de la contratación.	En formato Impreso y electrónico
E-02	Documento que avale el licenciamiento o suscripción de las soluciones	Cinco días hábiles posteriores a la implementación.	En formato Impreso y electrónico
E-03	Manuales de usuario	Diez días hábiles posteriores a la implementación.	En formato Impreso y electrónico
E-04	Manuales de instalación		
E-05	Credenciales de acceso para la administración de las soluciones.	Dos días hábiles posteriores a la implementación.	En formato Impreso y electrónico
E-06	Protocolo de pruebas de funcionalidad de soluciones	Al día siguiente después de concluir la instalación.	En formato Impreso y electrónico
E-07	Memoria Técnica de la Implementación que incluya, entre otros, diagramas de interconexión.	5 días hábiles posteriores a la conclusión del protocolo de pruebas de funcionalidad soluciones.	En formato Impreso y electrónico
E-08	Taller de transferencia de conocimientos	5 días hábiles posteriores a la conclusión de la fase de pruebas y validación (E-06)	En formato Impreso y electrónico

8 VIGENCIAS

La vigencia del contrato será a partir del día hábil siguiente a la notificación del fallo y hasta el 31 de diciembre del 2024.

La vigencia de las licencias para cada solución propuesta será de doce meses contados a partir del día siguiente de la conclusión de la puesta a punto y aprobación por parte de la SFP.

9 SUFICIENCIA PRESUPUESTAL ESTIMADA DE LA CONTRATACIÓN

Se cuenta con la disponibilidad presupuestaria para llevar a cabo la contratación de las soluciones requeridas.

10 FORMA DE PAGO

El pago se hará en una sola exhibición en moneda nacional, mediante transferencia electrónica a la cuenta del proveedor, previa liberación del servicio por parte de la Dirección General de Tecnologías de Información de la SFP, tras revisar y aceptar los entregables a satisfacción de la SFP

De conformidad a lo establecido en el artículo 51 de la LAASSP, los pagos se realizarán dentro de los veinte días naturales posteriores a la aceptación de la(s) factura(s) y una vez aceptadas las soluciones y la factura a satisfacción de la Dirección General de Tecnologías de Información de la SFP, en su calidad de área requirente, de conformidad con lo dispuesto en los artículos 89 y 90 del Reglamento de la LAASSP.

El pago quedará condicionado proporcionalmente, al pago que el proveedor deba efectuar por concepto de penas convencionales de la factura con motivo del incumplimiento parcial o deficiente en que pudiera incurrir el proveedor respecto al contrato.

Tratándose de pagos en exceso que haya recibido el proveedor, éste deberá integrar las cantidades pagadas en exceso, más las cargas financieras correspondientes, conforme a la tasa que será igual a la establecida en la Ley de Ingresos de la Federación, en los casos de prórroga para el pago de créditos fiscales, los cargos se calculan sobre las cantidades pagadas en exceso en cada caso y considerando días naturales desde la fecha del pago, hasta la fecha en que se pongan efectivamente las cantidades a disposición de la SFP.

11 PENAS CONVENCIONALES.

De conformidad con lo establecido en el artículo 53 de la LAASSP y 96 de su reglamento, la SFP a través del Titular del área requirente, aplicará al proveedor las penas convencionales a las que se haga acreedor por cada día hábil de atraso en el cumplimiento de las fechas pactadas para la entrega de las soluciones, por el 1% antes del IVA del total por concepto no entregado a tiempo.

NUMERAL DEL ANEXO	RUBRO	PENALIZACIÓN
6.1 6.2 6.3 6.4 6.5	Implementación fuera del tiempo establecido en la reunión de inicio entre el proveedor y la SFP.	1% antes del IVA del total por concepto no entregado a tiempo por cada día hábil de atraso.

NUMERAL DEL ANEXO	RUBRO	PENALIZACIÓN
6.6	Entregables con deficiencia o fuera del tiempo establecido.	

Las penas convencionales serán cubiertas por el proveedor mediante el "Pago electrónico de Derechos, Producto y Aprovechamiento, esquema cinco", ante alguna de las Instituciones Bancarias autorizadas, acreditando dicho pago con la entrega del recibo bancario a la Dirección General de Programación y Presupuesto.

La suma de todas las penas convencionales aplicadas al proveedor no deberá exceder el importe de la garantía de cumplimiento del contrato.

Cuando los servicios no se presten en la fecha o plazo convenido y la pena convencional por atraso rebase el monto de la garantía de cumplimiento del contrato, la SFP a través del Administrador del Contrato, previa notificación al proveedor podrá rescindir el contrato, en términos de la Cláusula denominada Rescisión.

El límite de incumplimiento por la aplicación de penas convencionales, a partir del cual se procederá a rescindir el contrato será del 10% (diez por ciento) del importe total del contrato, sin incluir el Impuesto al Valor Agregado.

Para determinar la aplicación de las penas convencionales, no se tomarán en cuenta las demoras motivadas por caso fortuito o causa de fuerza mayor o cualquier otra causa no imputable al proveedor.

En caso de adjudicarse a un ente público, no se aplicarán las penas convencionales de conformidad con lo establecido en el último párrafo del artículo 96 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASSP).

12 DEDUCCIONES AL PAGO.

No aplica.

13 PÓLIZA DE RESPONSABILIDAD CIVIL.

La SFP no solicitará la presentación de Póliza de Responsabilidad Civil.

14 LUGAR Y PLAZO DE LA PRESTACIÓN DEL SERVICIO.

La implementación y soporte deberá realizarse en Avenida de los Insurgentes Sur 1735, Mezanine, Ala Norte y Barranca del Muerto #234 ambos en Col. Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México. En horario de 9:00 a 18:00 hrs. en días hábiles y remotamente en horario 24x7.

15 ANTICIPOS

La SFP no otorgará anticipos.

16 PRÓRROGAS

De conformidad con lo dispuesto en el segundo párrafo del artículo 91 del RLAASSP, la modificación del plazo para la entrega de la prestación del servicio sólo procederá por caso fortuito, fuerza mayor o causas atribuibles a la SFP.

17 FORMA Y TÉRMINOS EN LOS QUE SE REALIZARÁ LA ACEPTACIÓN DE LAS SOLUCIONES.

La aceptación será posterior a la entrega y aceptación de la documentación establecida en el apartado 7. Y conforme a la puesta en operación y validación de la entrega de cada solución descrita en cada partida, correspondiente a los numerales:

- 6.1 SOLUCIÓN DE CORRELACIÓN DE EVENTOS (SIEM).
- 6.2 SOLUCIÓN DE PROTECCIÓN DE DNS.
- 6.3 SOLUCIÓN DE DETECCIÓN Y PREVENCIÓN EN CORREO ELECTRÓNICO (ANTISPAM).
- 6.4PROTECCIÓN ANTIMALWARE PARA ESTACIONES DE TRABAJO Y SERVIDORES (Endpoint)
- 6.5 ADMINISTRACIÓN DE CUENTAS PRIVILEGIADAS
- 6.6 PUNTOS DE DECEPCIÓN DE ATAQUE (TRAMPAS DE SEGURIDAD)

En caso de incumplimiento del proveedor a cualquiera de las obligaciones del contrato, la SFP podrá optar entre exigir el cumplimiento de este y el pago de las penas convencionales por el atraso, o declarar la rescisión administrativa y hacer efectiva la garantía de cumplimiento, en forma proporcional al cumplimiento, sin menoscabo de que la SFP pueda ejercer las acciones judiciales procedentes.

En este caso, la aplicación de la garantía de cumplimiento será proporcional al monto de las obligaciones incumplidas.

En el supuesto de que sea rescindido el contrato, no procederá el cobro de las penas por atraso ni la contabilización de estas al hacer efectiva la garantía de cumplimiento.

Si el proveedor es quien decide rescindirlo, será necesario que acuda ante autoridad judicial y obtenga la declaración o resolución correspondiente.

18 PRUEBAS DE LOS SERVICIOS

El proveedor deberá cumplir con las pruebas descritas en el numeral 4 METODOLOGÍA Y PLAN DE TRABAJO, sección 4.1 Metodología, numeral **4.1.3. Pruebas y validación.**

19 GARANTÍA DE CUMPLIMIENTO

De conformidad a lo establecido en el artículo 48 último párrafo de la LAASSP, (a fin de garantizar el cumplimiento de las obligaciones derivadas del contrato y para responder

en la calidad del servicio prestado, así como de cualquier otra responsabilidad, deberá presentar la garantía ***INDIVISIBLE*** en alguna de las siguientes formas:

1. Depósito de dinero constituido a través de certificado o billete de depósito, expedido por institución de crédito autorizada para operar como tal.
2. Fianza otorgada por institución de fianzas o de seguros autorizada para expedirla.
3. Depósito de dinero constituido ante la TESOFE.
4. Carta de crédito irrevocable, expedida por Institución de Crédito autorizada para operar como tal.
5. Seguro de caución otorgada por Institución de seguros autorizada para expedirlo.
6. Cheque certificado o de caja expedido a favor de la TESOFE
7. Cualquier otro que en su caso autorice la TESOFE.

Dicha garantía deberá ser expedida por institución autorizada para ello; a favor de la TESOFE y a satisfacción de la SFP, **por un monto equivalente al 10% (diez por ciento) del *MONTO TOTAL*** del contrato adjudicado, sin incluir el I.V.A., por la vigencia del periodo de prestación del servicio.

Deberá presentar la garantía de cumplimiento en la Dirección de Abastecimiento y Contratos, sita en Avenida de los Insurgentes Sur 1735, Mezanine Ala Sur, Col. Guadalupe Inn, Alcaldía Álvaro Obregón, C.P. 01020, Ciudad de México, a más tardar dentro de los 10 (diez) días naturales siguientes a la fecha de firma del contrato o el día hábil anterior si el décimo día no lo fuera. De no cumplir con dicha entrega, la SFP podrá determinar la rescisión administrativa del contrato y remitir el asunto al Órgano Interno de Control, para su consideración y efectos legales a los que haya lugar, de conformidad a lo establecido en el artículo 60, fracción III de la LAASSP.

En caso de que sea necesario llevar a cabo la rescisión administrativa del contrato, la aplicación de la garantía de cumplimiento será proporcional al monto de las obligaciones incumplidas.

En caso de adjudicarse a un ente público, no se solicitará garantía de cumplimiento, de conformidad con lo establecido en el artículo 56 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.

19.1 GARANTÍA DEL CORRECTO FUNCIONAMIENTO DE LA SOLUCIÓN PROPUESTA

El personal de la DGTI verificará el correcto funcionamiento de la solución propuesta por el proveedor, cumpliendo con todos los puntos señalado en este anexo técnico.

20 SERVIDOR PÚBLICO DEL ÁREA RESPONSABLE DE ADMINISTRAR Y SUPERVISAR EL CUMPLIMIENTO DE LOS SERVICIOS

De conformidad con lo dispuesto en el artículo 84 del RLAASSP, el servidor público que fungirá como administrador del contrato por parte de la SFP, será **Carlos Raúl Ramírez Orozco, Director General de Tecnologías de Información** o quien lo sustituya en el cargo y/o funciones, asimismo fungirán como Supervisores del contrato por parte de la SFP de la siguiente forma para los servicios:

Numeral del anexo	Supervisor	
• 6.1	**José Luis Maldonado Maldonado, Subdirector de Servicios de Seguridad Lógica Perimetral,** o quien la sustituya en el cargo y funciones	
• 6.2 • 6.3	**Edgar Galicia Barraza** **Subdirector de Soporte a Servidores y Sistemas,** o quien la sustituya en el cargo y funciones	
• 6.4	Para Antivirus en Equipos de Cómputo de Escritorio	**Angélica Chávez Anaya, Directora de Servicios de Computo de Escritorio,** o quien la sustituya en el cargo y funciones
	Para antivirus en Servidores	**Edgar Galicia Barraza, Subdirector de Soporte a Servidores y Sistemas,** o quien la sustituya en el cargo y funciones

Numeral del anexo	Supervisor
• 6.5 • 6.6	**Heriberto López Ramírez Subdirector(a) de Seguridad de Tecnologías de Información,** o quien la sustituya en el cargo y funciones

NORMAS OFICIALES MEXICANAS Y/O INTERNACIONALES

- No aplica

21 CAUSALES DE RESCISIÓN

El proveedor está de acuerdo en que, en cualquier momento, por causas imputables a él, la SFP podrá rescindir administrativamente el contrato, cuando se incumpla con cualquiera de las obligaciones estipuladas en el mismo. Dicha rescisión operará de pleno derecho, sin necesidad de declaración o resolución judicial, bastando que se cumpla con el procedimiento señalado en el artículo 54 de la LAASSP y en la cláusula Rescisión del Contrato.

Las causas que pudieren dar a lugar a que la SFP inicie el procedimiento de rescisión administrativa del contrato, son el incumplimiento en los siguientes apartados:

- 6.1 SOLUCIÓN DE CORRELACIÓN DE EVENTOS (SIEM).
- 6.2 SOLUCIÓN DE PROTECCIÓN DE DNS.
- 6.3 SOLUCIÓN DE DETECCIÓN Y PREVENCIÓN EN CORREO ELECTRÓNICO (ANTISPAM).
- 6.4PROTECCIÓN ANTIMALWARE PARA ESTACIONES DE TRABAJO Y SERVIDORES (Endpoint)
- 6.5 ADMINISTRACIÓN DE CUENTAS PRIVILEGIADAS
- 6.6 PUNTOS DE DECEPCIÓN DE ATAQUE (TRAMPAS DE SEGURIDAD)

En caso de incumplimiento del proveedor a cualquiera de las obligaciones del contrato, la SFP podrá optar entre exigir el cumplimiento de este y el pago de las penas convencionales por el atraso, o declarar la rescisión administrativa y hacer efectiva la garantía de cumplimiento, en forma proporcional al cumplimiento, sin menoscabo de que la SFP pueda ejercer las acciones judiciales procedentes.

En este caso, la aplicación de la garantía de cumplimiento será proporcional al monto de las obligaciones incumplidas.

En el supuesto de que sea rescindido el contrato, no procederá el cobro de las penas por atraso ni la contabilización de estas al hacer efectiva la garantía de cumplimiento.

Si el proveedor es quien decide rescindirlo, será necesario que acuda ante autoridad judicial y obtenga la declaración o resolución correspondiente.

22 CONFIDENCIALIDAD

El proveedor se obliga por escrito firmando una carta de confidencialidad para no divulgar por ningún medio la información que obtenga o a la que tenga acceso por virtud de la prestación objeto de estas Especificaciones Técnicas, sin la autorización expresa y por escrito de la SFP, así como, no divulgar la información que pudiera surgir de la implementación de la solución propuesta.

23 PROPUESTA ECONÓMICA

Es necesario que el proveedor establezca en su propuesta:

- El costo del servicio solicitado bajo el formato referido en el ANEXO 1 Propuesta económica 1.

Autorizó
Ing. Carlos Raúl Ramírez Orozco Director General de Tecnologías de Información

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
1	6.1	SOLUCIÓN DE CORRELACIÓN DE EVENTOS (SIEM)	Debe proveer una solución de propósito específico.		
2	6.1		El software deberá incluir todos los componentes del mismo fabricante, la consola Web, así como el repositorio para almacenar la información.		
3	6.1		La solución no deberá depender de una base de datos de tipo relacional, los eventos deberán ser almacenados en el mismo formato que la fuente original y no deberá realizarse ningún proceso de reducción o transformación de datos.		
4	6.1		Deberá ser capaz de leer eventos en diferentes formatos sin importar la fuente, deberá ser capaz de identificar eventos multilínea y separar los eventos de manera correcta.		
5	6.1		Deberá permitir la creación de usuarios con diferentes roles, estos roles deberán permitir definir esquemas de acceso a los datos por rol, así como la definición de políticas de retención por tipo de dato.		
6	6.1		Deberá permitir almacenar históricos de datos por al menos 1 año en línea y el tiempo restante debe permitir guardar los eventos en cinta o VTL (Virtual Tape Library).		
7	6.1		Deberá ser capaz de recibir eventos a una tasa de al menos 50K EPS (Eventos por Segundo).		
8	6.1		Los componentes no deberán tener costo adicional, de modo que se podrán instalar equipos en alta disponibilidad sin tener costos adicionales por licenciamiento.		
9	6.1		Deberá incluir un lenguaje de búsqueda flexible que permita identificar eventos que contengan una palabra, un código de error o una frase. Esta búsqueda deberá permitir operadores lógicos que permitan definir mejores criterios de búsqueda.		
10	6.1		Deberá permitir la búsqueda de los datos en tiempo real, con rangos de tiempo definidos incluyendo búsquedas históricas. Estas búsquedas deberán regresar los datos en segundos para no afectar la respuesta del manejo de los incidentes.		
11	6.1		Deberá ser capaz de transformar los eventos en gráficas, reportes y vistas que permitan monitorear las métricas importantes para la organización. Estás vistas deberán ser completamente personalizables.		
12	6.1		Deberá permitir la creación de reglas de correlación que puedan adaptarse a los requerimientos de la SFP. Estas reglas deberán combinar múltiples fuentes de datos para tener un mejor entendimiento de los incidentes de seguridad.		
13	6.1		Deberá ser capaz de enriquecer los datos colectados con catálogos que describan los errores o con direcciones IP maliciosas para identificar comunicaciones riesgosas. Los catálogos pueden ser estáticos o dinámicos en una tabla dentro de una base de datos.		
14	6.1		Deberá incluir los siguientes mecanismos de colección: colección de datos sin agente usando WMI o recursos compartidos, recibir eventos por syslog, SNMP, http, conectándose a bases de datos y ejecutando QUERIES, así como leyendo datos directamente de la red en puertos espejo.		
15	6.1		Deberá ser capaz de capturar el tráfico de protocolos directamente desde la red. Se deben poder definir qué tipo de campos extraer de las tramas de red, por ejemplo: dirección IP origen y destino, puerto orígen y destino, tiempo de la transacción (time taken) entre otros.		
16	6.1		Se requiere reconocimiento de al menos los siguientes protocolos: http, https, ftp, dns, y dhcp.		
17	6.1		Deberá ser capaz de crecer de manera lineal tan solo instalando nuevos componentes, separando el proceso de captura del proceso de consulta.		
18	6.1		Deberá ser capaz de integrar diferentes roles de usuario, estos roles deben estar integrados con directorio activo o LDAP. Algunos de los usuarios deberán poder crear búsquedas y otros que solo realicen consultas.		
19	6.1		Deberá contener mecanismos para identificar campos dentro de eventos no estándares, estos mecanismos para identificación de campos deberá ser gráfico y además permitir el uso de expresiones regulares para la creación de nuevos campos.		
20	6.1		Deberá permitir la integración con listas de inteligencia de seguridad, como IP maliciosas de SANS, por mencionar algunas, estas listas de direcciones IP y dominios maliciosos deberá compararse con el tráfico generado en la institución para identificar tráfico hacia/desde sitios maliciosos. La solución deberá poder integrarse con listas gratuitas o con listas de pago definidas por la SFP.		
21	6.1		Deberá tener integradas al menos 50 reglas de correlación y por lo menos 20 casos de uso con hasta 10 casos de uso con respuesta automatizada, así como mecanismos para generar nuevas vistas para el monitoreo de incidentes de seguridad agrupado por domino con la capacidad de definir nuevas vistas que se adecuen a los requerimientos de la SFP.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
22	6.1	SOLUCIÓN DE CORRELACIÓN DE EVENTOS (SIEM)	Deberá tener integrado un sistema para el manejo de incidentes que permita registrar analistas, asignar casos de manera automática por tipo de perfil, así como tener una bitácora que registre las actividades del analista realizadas para cerrar el caso.		
23	6.1		Deberá ser capaz de analizar eventos de alta fidelidad producidos por herramientas antimalware de endpoint, además de leer eventos de sysmon de Microsoft que permitan identificar procesos con sus identificadores, así como el proceso padre que ejecutó el anterior, todo esto deberá ser reportado y analizado por las reglas de correlación.		
24	6.1		Deberá permitir el acceso de hasta 10 usuarios para la SFP, en caso de requerir licenciamiento por usuario para su gestión deberá ser considerado.		
25	6.1		Deberá ser capaz de analizar peticiones de DNS por medio de logs o de tráfico en puerto 53. Con esta información deberá ser capaz de reconocer conexiones a dominios nuevos o recién creados.		
26	6.1		Deberá ser capaz de incluir una vista que permita analizar todos los eventos generados por una sola dirección IP reportados desde las herramientas de seguridad como: antivirus, proxy, firewall, logs de punto final, etc.		
27	6.1		Deberá permitir un análisis forense que permita ir hasta el evento en su formato original.		
28	6.1		Deberá incluir mecanismos para eliminación de falsos positivos, así como la creación de tareas de remediación automáticas usando scripts.		
29	6.1		Deberá incluir scripts de remediación de ejemplo.		
30	6.1		Deberá ser capaz de correr búsquedas que contengan eventos de al menos 3 meses atrás que no demoren más de 5 minutos en presentar los eventos en su formato original (eventos tipo raw).		
	6.1		Permitir la correlación de eventos de al menos los siguientes dispositivos:		
31	6.1		4 (cuatro) Firewall,		
32	6.1		4 (cuatro) servidores WAF,		
33	6.1		1 (una) Controladora de Wireless,		
34	6.1		3 (tres) Servidores de respaldo,		
35	6.1		1(un) Servidor Radius,		
36	6.1		5 (cinco) Servidores de Directorio Activo,		
37	6.1		1 (un) Servidor de DHCP y		
38	6.1		5 (cinco) Servidores de DNS interno,		
39	6.1		2 (dos) Servidores de DNS externo,		
40	6.1		3 (tres) Servidores de correo		
41	6.1		5 (cinco) Antispam		
42	6.1		11 (once) File Server		
43	6.1		1 (un) VMWare Aria Operations Logs.		
44	6.1		1 (un) CarbonBlack		
45	6.1		El proveedor otorgará a la SFP (cinco) usuarios de acceso con permisos de administración.		
46	6.2	SOLUCIÓN DE PROTECCIÓN DE DNS	El licenciamiento de la solución deberá considerar que actualmente se cuenta con un total de hasta 2800 usuarios internos con navegación a Internet.		
47	6.2		Los dispositivos serán distribuidos y funcionarán como un sistema unificado y administrado centralmente, es decir, deberán manejar un sistema de administración centralizado a través de una consola de administración.		
48	6.2		La consola de administración puede ser virtual o en la nube.		
49	6.2		Las actualizaciones de software del sistema se deberán cargar en el punto central de administración.		
50	6.2		La tecnología utilizada debe incluir como mínimo los siguientes módulos de servicio DNS, DNSSEC, DHCP, TFTP y NTP.		
51	6.2		El punto central de administración de la solución debe sincronizar datos entre todos los dispositivos.		
52	6.2		Capacidad de trabajar en IPv4, IPv6 o en dual-stack.		
53	6.2		Detendrá automáticamente las comunicaciones del dispositivo con C&C/botnets.		
54	6.2		Detectar malware, ransomware, phishing, kits de explotación, filtración de datos basada en DNS.		
55	6.2		Contar con filtros por contenido específico como: drogas, juegos, violencia, pornografía, fraude, entre otros.		
56	6.2		La protección de DNS debe contar con herramientas de investigación de indicadores de amenazas.		
57	6.2		Permitir búsquedas de indicadores como: dominios, URLs, hashes, hostnames y direcciones IP.		
58	6.2		Debe soportar la administración de registros de DNS como: A, AAAA, ALIAS, NS, SOA, MX, TXT, SRV, CNAME, PTR.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
59	6.2.1	RESPECTO AL MÓDULO DE DHCP	Deberá automatizar y centralizar todos los aspectos del aprovisionamiento de direcciones IP.		
60	6.2.1		Deberá identificar el sistema operativo y el tipo de dispositivo.		
61	6.2.1		Deberá correlacionar los usuarios de Active Directory con las direcciones IP y MAC para identificar a los usuarios por equipo.		
62	6.2.1		Deberá permitir actualizar los scope.		
63	6.2.2	RESPECTO A LA PROTECCIÓN DE DNS PÚBLICOS	Debe detectar y mitigar ataques basados en DNS.		
64	6.2.2		Actualización automática contra amenazas nuevas.		
65	6.2.2		Detectar y mitigar los siguientes tipos de ataques: Reflexión y Reflexión de DNS, DDoS dirigidos al DNS, NXDOMAIN, Random sub-domain, ataques basados en expolits de DNS, ataques de reconocimiento.		
66	6.2.2		Descargar respaldos de configuración y poder restaurarse utilizando los mismos.		
67	6.3	SOLUCIÓN DE DETECCIÓN Y PREVENCIÓN EN CORREO ELECTRÓNICO (Antispam)	Protección contra spam y phishing para el servicio de correo electrónico.		
68	6.3		Licenciamiento para proteger hasta 4500 buzones.		
69	6.3		La solución debe ser proporcionada mediante Imagen de Software en formato ISO para el despliegue sobre plataforma virtualizada acorde a modalidad gateway virtual.		
70	6.3		Los módulos y/o componentes de la solución deben estar basados en software/appliance de uso específico, con sistema operativo, base de datos y servicios configurados para óptimo rendimiento y securización por el fabricante de la solución.		
71	6.3		Es deseable brindar la opción de separar la consola de administración del motor de revisión antivirus y antispam;		
72	6.3		Debe brindar la opción de analizar el correo entrante y saliente en el mismo Gateway virtual/appliance o separar cada flujo en equipos diferentes;		
73	6.3		Se debe proporcionar la imagen a ser cargada para habilitar el Gateway virtual y debe incluir el sistema operativo y la aplicación de filtro de correo. No se aceptará la instalación manual del sistema operativo y la posterior instalación del producto de filtro antivirus;		
74	6.3		La plataforma de virtualización será responsabilidad de la SFP;		
75	6.3		Debe ser compatible con Exchange Server 2016 y 2019;		
76	6.3		Debe ser compatible con servidores de correo de código abierto que soporten el estándar SMTP;		
	6.3		Debe brindar al menos las siguientes funciones básicas:		
77	6.3		Antimalware;		
78	6.3		Antispam;		
79	6.3		Filtrado de contenido;		
80	6.3		Cuarentena local;		
81	6.3		Validación de autenticidad del remitente;		
82	6.3		Validación de reputación;		
83	6.3		Lista blanca y lista negra para recepción de correo;		
84	6.3		Desarticulación de archivos para eliminar contenido no deseado;		
85	6.3		Debe tener la capacidad de archivar cualquier mensaje que viole las políticas corporativas, reenviándolos a la estructura de archivo de la SFP;		
86	6.3		Es deseable poder integrarse con un servidor de cifrado de mensajes de correo, para cifrar mensajes y archivos adjuntos;		
87	6.3		Debe tener la capacidad de permitir o no permitir direcciones de correo electrónico con caracteres especiales, por lo menos un porcentaje (%), guión (-) y caracteres de 8 bits;		
88	6.3		Debe tener la capacidad de rechazar conexiones que intenten ser abiertas por los comandos "HELO" y "EHLO", sin tener sus direcciones "MX" y "A" registradas en los servidores DNS;		
89	6.3		Debe ser capaz de escanear en tiempo real los mensajes salientes hacia Internet y los entrantes desde Internet hacia el servidor de correo interno;		
90	6.3		Debe permitir incluir mensajes de descargo de responsabilidad a los mensajes salientes;		
	6.3		Debe contar con mecanismos de validación de remitente:		
91	6.3		SPF		
92	6.3		DMARC		
93	6.3		DKIM		
94	6.3		Sender ID		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
95	6.3.1	CONSOLA DE ADMINISTRACIÓN	La solución debe ser implementada on premise y debe disponer de una consola de gestión centralizada, 100% Web		
96	6.3.1		Debe tener la capacidad de administrar centralmente múltiples appliances de la misma solución de filtro de correo;		
97	6.3.1		La solución debe proveer un procedimiento por el cual se pueda realizar un upgrade de todos y cada uno de los dispositivos que la componen, sin la necesidad de realizar un corte de servicio y sin afectar al resto de los componentes;		
98	6.3.1		Es deseable que la solución permita definir una lista de control de acceso, es decir, especificar que las estaciones de trabajo de los administradores sean las únicas que pueden acceder a ella;		
99	6.3.1		Debe brindar información de estado de los appliances, tal como uso de CPU, memoria y espacio en disco;		
100	6.3.1		Debe permitir validar el estado de los servicios de la solución, brindando además opción de detenerlos, iniciarlos o reiniciarlos;		
101	6.3.1		Debe permitir aplicar parches o nuevas versiones de manera centralizada;		
102	6.3.1		Debe permitir realizar respaldos y restaurarlos;		
103	6.3.1		Debe permitir definir si el respaldo será total o personalizado por el administrador;		
104	6.3.1		Los respaldos deben poder programarse para ser ejecutados de manera automática;		
105	6.3.1		Los respaldos deben poder almacenarse fuera del appliance;		
106	6.3.1		Debe permitir reiniciar o apagar los appliances de la solución, de forma centralizada;		
107	6.3.1		Debe ofrecer controles de contraseña para administradores locales;		
108	6.3.1		La consola de administración Web, deberá proporcionar capacidades de acceso basado en roles y perfiles de usuario. Role Based Access Control (RBAC)		
109	6.3.1		Debe integrarse con algún sistema de almacenamiento de registros vía Syslog;		
110	6.3.1		Debe mostrar las colas de correo, separando el correo entrante y el saliente, con opción a forzar el reintento de entrega o borrar la cola, según decida el administrador;		
111	6.3.1		Debe permitir definir más de un dominio de correo electrónico para proteger;		
112	6.3.1		Debe permitir definir políticas individuales por puerta de enlace o servidor global, desde la misma consola;		
113	6.3.1		Debe tener la posibilidad de acceso individual al dispositivo a través de SSH, para ejecutar comandos a través de CLI (línea de comando);		
114	6.3.1		Debe contar con una función de seguimiento de mensajes en la propia consola de administración con la capacidad de buscar por asunto, remitente y destinatario, verificando la acción realizada para un mensaje específico, sin necesidad de integración con productos de terceros;		
115	6.3.1		Debe tener la funcionalidad de alias y enmascaramiento de direcciones;		
116	6.3.1		Debe ser posible notificar al administrador por correo electrónico si los filtros antispam no reciben actualizaciones durante un cierto período de tiempo;		
117	6.3.1		Debe poder integrarse con LDAP Microsoft Active Directory 2019 o superior para sincronización y autenticación a la consola de administración;		
118	6.3.1		Debe permitir la creación de políticas diferenciadas para el tratamiento de spam, virus, Filtrado de Contenidos y Control de Reputación (traffic shaping), según el destinatario del mensaje y la reputación de origen;		
119	6.3.1		Debe ser capaz de sincronizar usuarios y grupos LDAP para reconocer usuarios válidos y acciones de filtrado de contenido, spam y virus diferenciadas por grupo LDAP;		
120	6.3.1		Debe poder utilizar la integración de usuarios LDAP, validando su existencia, posibilitando su descarte y rechazo, no enviando mensajes al servidor de correo electrónico, sin destinatario propio dentro de la base LDAP, evitando procesamientos innecesarios por parte del servidor de correo electrónico;		
121	6.3.1		Debe ser capaz de procesar el tráfico de mensajes entrantes y salientes, con políticas diferentes para cada dirección de tráfico.		
122	6.3.1		La solución debe de permitir la configuración de los modos de cifrado TLS a aplicar a los correos en situaciones donde el sistema acepté mensajes de otro servidor, o actué reenviando los mensajes, así como también debe de permitir la configuración de los parámetros TLS para dominios individuales.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
	6.3.2	FUNCIONES ANTISPAM	Debe permitir la ejecución de múltiples acciones para un mismo mensaje que sea categorizado como SPAM o violación de filtros de contenido, entre ellas:		
123	6.3.2		Borrar mensaje;		
124	6.3.2		Enviar a Cuarentena;		
125	6.3.2		Reenviar mensaje;		
126	6.3.2		Modificar el asunto;		
127	6.3.2		Agregar encabezado;		
128	6.3.2		Rechazar el mensaje;		
129	6.3.2		Entregar normalmente el mensaje;		
130	6.3.2		La solución debe proporcionar capacidades de detección y protección ante ataques del tipo Business Email		
131	6.3.2		Debe tener la capacidad de notificar al remitente, destinatario, administrador y otros correos electrónicos simultáneamente;		
132	6.3.2		La solución debe de contar con asistencia de servicios de reputación en la nube;		
133	6.3.2		Debe permitir la actualización automática de filtros, sin interrupción de los servicios;		
134	6.3.2		Debe admitir listas negras y listas blancas con opción por dominio, dirección de correo electrónico y dirección IP;		
135	6.3.2		Debe tener la capacidad de bloquear mensajes considerados como SPAM en base al uso de listas DNSBL (DNS BlackHole) o RBL (Real Time Black List);		
	6.3.2		Debe ser capaz de utilizar al menos las siguientes tecnologías de detección de spam:		
136	6.3.2		Firmas para el cuerpo del mensaje y los archivos adjuntos;		
137	6.3.2		Análisis heurístico, a través del análisis de encabezados, contenido y estructura del mensaje;		
138	6.3.2		Filtros de reputación local (creados automáticamente a través del análisis de los mensajes recibidos) y global (creados por la red de monitoreo del proveedor de la solución);		
139	6.3.2		Identificación de idioma;		
140	6.3.2		Filtros de URL;		
141	6.3.2		Filtros anti-phishing;		
142	6.3.2		Debe tener la capacidad de crear filtros basados en el encabezado, remitente, tipos y contenido de los archivos adjuntos, diccionarios de palabras, asunto y cuerpo del mensaje, incluyendo el uso de expresiones regulares;		
143	6.3.2		Debe permitir la creación de "carpetas de cumplimiento", para almacenar mensajes (entrantes/salientes) que violen cualquier política de contenido creada por el Administrador;		
144	6.3.2		Debe contar con tecnología para detectar Spam, Virus y ataques a Directorios (Usuarios Inválidos);		
145	6.3.2		La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0.		
146	6.3.2		La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo Ransomware.		
147	6.3.2		Es deseable poder ser integrada con tecnologías de Sandboxing.		
148	6.3.2		Debe contar con tecnología para prevenir ataques de "Mensajes Rebotados";		
149	6.3.2		Debe tener la capacidad de crear reglas basadas en el tipo de archivo adjunto;		
150	6.3.2		Debe tener la capacidad de crear reglas basadas en la detección por "Comodín" (*);		
151	6.3.2		Debe tener la capacidad de crear reglas basadas en la detección por expresiones regulares;		
152	6.3.2		Debe tener la capacidad de implementar una comunicación segura a través de TLS (Seguridad de la capa de transporte);		
153	6.3.2		Debe poder configurar el cifrado TLS por dominio y por política;		
154	6.3.2		Debe ser capaz de detectar varios idiomas, permitiendo bloquear mensajes escritos en idiomas no deseados;		
155	6.3.2		Debe tener la capacidad de crear una lista de IP confiables en función del comportamiento de la IP de origen del mensaje, para minimizar el impacto en el rendimiento en entornos grandes;		
156	6.3.2		La totalidad del análisis y operación de la solución debe realizarse en forma local, solo permitiéndose el envío de hashes cuando sea necesario. La solución no debe enviar ninguna información sensible fuera de la institución.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
157	6.3.3	FUNCIONES ANTIMALWARE	Debe tener la capacidad de identificar y borrar completamente los mensajes enviados por gusanos de envío masivo, con la opción de acciones diferenciadas por tráfico entrante y saliente;		
158	6.3.3		Debe ser capaz de reconocer Spyware y Adware y aplicar una acción correctiva diferente a la que se aplica cuando se encuentra virus;		
	6.3.3		En caso de objetos infectados, la solución debe poder configurar la realización de las siguientes acciones:		
159	6.3.3		Desinfectar		
160	6.3.3		Eliminar Anexo		
161	6.3.3		Borrar mensaje		
162	6.3.3		Rechazar mensaje		
163	6.3.3		Ignorar		
164	6.3.3		Debe contar con una función de detección de ataques en dos escalas para Virus y Directorio (LDAP), capaz de diferir la conexión SMTP si la fuente emisora ha enviado un porcentaje de mensajes considerados como usuarios no válidos o infectados con virus, en un período de tiempo determinado, ambos configurables por el administrador;		
165	6.3.3		Debe contar con un módulo antivirus para la detección de contenido malicioso en los mensajes.		
166	6.3.3		Debe tener la capacidad de bloquear archivos adjuntos por extensión, tipo de archivo real (True Type File), Tipo Mime y nombre de archivo;		
167	6.3.3		Debe ser capaz de desactivar/desarticular componentes maliciosos en al menos archivos de Office y PDF;		
168	6.3.3		Es deseable permitir definir límites para evitar bloqueo del servicio al analizar archivos comprimidos dentro de archivos comprimidos, pudiendo definirlos por tamaño o tiempo;		
169	6.3.3		Debe permitir definir el nivel de agresividad para la detección de virus no conocidos;		
170	6.3.3		Debe contar con una cuarentena diferente de la de spam para almacenar correos sospechosos de virus.		
171	6.3.3		Debe permitir la trazabilidad de las actividades de los usuarios y bloquear el acceso a enlaces maliciosos.		
172	6.3.4	CUARENTENA	Eliminación automática de mensajes almacenados en cuarentena según la configuración definida por el administrador;		
173	6.3.4		Debe permitir al usuario registrar direcciones de correo electrónico en listas negras/listas blancas personales;		
174	6.3.5	FUNCIONES DE FILTRADO DE CONTENIDO	La solución debe disponer de capacidad de filtrado de contenido de los mensajes mínimamente acorde al nombre, tamaño y tipo de anexo, determinando el formato indiferentemente de su extensión, así como eliminar mensajes o sus anexos;		
	6.3.5		En caso de detectar actividad en el módulo de filtrado de contenido, la solución debe poder configurar la realización de las siguientes acciones:		
175	6.3.5		Desinfectar		
176	6.3.5		Eliminar anexo		
177	6.3.5		Borrar mensaje		
178	6.3.5		Rechazar mensaje		
179	6.3.5		Ignorar		
180	6.3.6	REPORTES DE ESTA SOLUCIÓN	Debe de incluir la funcionalidad de creación de reportes que sea parte de la misma consola, sin depender de soluciones adicionales;		
	6.3.6		Debe incluir al menos los siguientes reportes:		
181	6.3.6		Reporte ejecutivo		
182	6.3.6		Reporte de virus		
183	6.3.6		Reporte de spam		
184	6.3.6		Los reportes deberán poder generarse por periodos de tiempo específicos según defina el administrador;		
185	6.3.6		Los reportes deberán poder enviarse por correo electrónico;		
186	6.3.6		Los reportes deberán poder calendarizarse para su generación y envío periódico;		
187	6.3.6		Los reportes deberán poder exportarse a PDF, HTML o CSV.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
188	6.4	PROTECCIÓN ANTIMALWARE PARA ESTACIONES DE TRABAJO Y SERVIDORES (Endpoint)	Considerarse para un total de 2000 equipos de escritorio/laptops y 80 servidores.		
189	6.4.1		Reputación de archivos, sean locales o descargados de la web.		
190	6.4.1		IPS de próxima generación.		
191	6.4.1		Protección del navegador (browser).		
192	6.4.1		Aprendizaje automático (Machine Learning).		
193	6.4.1		Análisis de Comportamiento.		
194	6.4.1		Mitigación de explotación de memoria.		
195	6.4.1		Control de aplicaciones.		
196	6.4.1		Control de dispositivos.		
197	6.4.1		Proveer detección y respuesta de amenazas automatizadas contra una variedad de amenazas de malware avanzadas.		
	6.4.1		El cliente para instalación en estaciones de trabajo debe ser compatible con al menos los siguientes sistemas operativos:		
198	6.4.1		Debian 10;		
199	6.4.1		Mac OS X 11.x, 12.x y 13;		
200	6.4.1		Oracle Linux 7 y 8;		
201	6.4.1		Red Hat Enterprise Linux 8.x y 9.x;		
202	6.4.1		Ubuntu 20.04 y superiores;		
203	6.4.1		Windows 10 y 11;		
204	6.4.1		Windows Server 2008 R2;		
205	6.4.1		Windows Server 2012, 2012 R2;		
206	6.4.1		Windows Server 2016, 2019 y 2022;		
207	6.4.1		Soporte para protocolos TCP, UDP e ICMP;		
208	6.4.1		Reconocimiento de tráfico DNS, DHCP y WINS con opción de bloqueo;		
209	6.4.1		Proporcionar protección contra la explotación del desbordamiento de buffer;		
210	6.4.1		Tener protección contra ataques de Denegación de Servicio (DoS), Port-Scan y MAC Spoofing;		
211	6.4.1		Posibilidad de crear reglas diferenciadas por aplicaciones;		
212	6.4.2	REQUISITOS TÉCNICOS	Debe contar con administración centralizada a través de una única consola de gestión.		
213	6.4.2		Acceso a la consola de administración basado en Roles y perfiles de acceso, con capacidades granulares de definición de restricciones y capacidades funcionales.		
214	6.4.2		Segundo factor de autentificación (2FA) para el acceso a la consola de administración compatible con Microsoft Authenticator y Google Authenticator.		
215	6.4.2		La consola de administración puede ser virtual o en la nube.		
216	6.4.2		Debe tener acceso a la consola de administración vía tecnología Web (HTTPS).		
217	6.4.2		Admitir la instalación del agente en sistemas operativos Windows 10 y 11, así como MAC OS.		
218	6.4.2		Deberá de instalar clientes en servidores, estaciones de trabajo y máquinas virtualizadas de forma remota a través de la consola de administración con la opción de eliminar las soluciones antimalware instaladas previamente		
219	6.4.2		El proveedor deberá ser responsable de la desinstalación del agente actual.		
220	6.4.2		Integrarse con Active Directory y permitir hacer inicio de sesión a la consola de administración utilizando las credenciales de la red con sus respectivos permisos.		
221	6.4.2		Contar con los mecanismos de protección para no poder ser desinstalado o desactivado por el usuario.		
222	6.4.2		Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.;		
223	6.4.2		Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos;		
224	6.4.2		La configuración de antivirus, antispyware, firewall, protección contra intrusos, control de dispositivos y control de aplicaciones debe realizarse para máquinas físicas y virtuales a través de la misma consola.		
225	6.4.2		Toda la solución debe funcionar con un solo agente en la estación de trabajo y servidores físicos y virtuales para reducir el impacto en el usuario final.		
226	6.4.2		Tener compatibilidad con IPv6.		
227	6.4.2		El fabricante de la solución debe proporcionar actualizaciones de productos, firmas de virus y de protección contra intrusiones.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
228	6.4.2	REQUISITOS TÉCNICOS	La consola de administración debe permitir bloquear las configuraciones por contraseña en los clientes, servidores y estaciones físicas y virtuales, definiendo permisos para que solo el administrador pueda cambiar las configuraciones, desinstalar o detener el servicio del cliente.		
229	6.4.2		Reconocimiento de tráfico DNS, DHCP y WINS con opción de bloqueo.		
230	6.4.2		Proporcionar protección contra la explotación del desbordamiento de buffer.		
231	6.4.2		Tener protección contra ataques de Denegación de Servicio (DoS), Port-Scan y MAC Spoofing.		
232	6.4.2		Posibilidad de crear reglas diferenciadas por aplicaciones.		
233	6.4.2		La funcionalidad del cortafuegos debe ser compatible al menos con Windows y Mac.		
234	6.4.2		Gestión integrada en la consola de gestión de la solución.		
235	6.4.2		Funcionalidad antivirus y antispyware.		
236	6.4.2		Protección en tiempo real contra virus, troyanos, gusanos, spyware, adware y otros tipos de códigos maliciosos.		
237	6.4.2		La protección antispyware debe ser nativa del propio antivirus, es decir, no depender de un plugin o módulo adicional.		
238	6.4.2		La configuración antispyware debe realizarse a través de la misma consola que todos los elementos de la solución.		
239	6.4.2		Permitir la configuración de acciones diferenciadas para cada subcategoría de riesgos de seguridad (Adware, Dialers, Hacking Tools, Spyware, Trackware y otros).		
240	6.4.2		Permitir la configuración de dos acciones, primaria y secundaria, realizadas automáticamente para cada amenaza, con las opciones: solo alertar, limpiar automáticamente, eliminar automáticamente y poner en cuarentena.		
241	6.4.2		Permitir la creación de listados de exclusiones con información sobre la severidad, impacto y grado de remoción de la amenaza en niveles bajo, medio o alto, donde los riesgos excluidos no serán verificados por el producto.		
242	6.4.2		Permitir la verificación de amenazas de forma manual, programada y en Tiempo Real.		
243	6.4.2		Implementar intervalos de tiempo para iniciar análisis programados con el fin de reducir el impacto en los entornos virtuales.		
244	6.4.2		Contar con funcionalidades que permitan el aislamiento (área de cuarentena) de archivos contaminados por códigos maliciosos que no se conocen o que no pueden ser reparados en el cliente.		
245	6.4.2		Tener características que permitan la inclusión manual en aislamiento (área de cuarentena).		
246	6.4.2		Control de virus de mensajes de correo electrónico, utilizando el antivirus de la estación de trabajo, soportando al menos clientes Outlook y POP3/SMTP.		
247	6.4.2		Contar con funcionalidades que permitan la detección y reparación de archivos contaminados por códigos maliciosos, aunque estén comprimidos por ZIP, LHA y ARJ, cubriendo al menos hasta el octavo nivel de compresión;		
248	6.4.2		Capacidad de detección en tiempo real de nuevos virus, desconocidos por la vacuna, con opción de sensibilidad de detección (baja, media y alta).		
249	6.4.2		Capaz de eliminar de forma totalmente automática los daños causados por spyware, adware y gusanos, como limpiar el registro y los puntos de carga, con la opción de finalizar el proceso y finalizar el servicio de amenazas en el momento de la detección.		
250	6.4.2		La eliminación automática de los daños causados debe ser nativa del propio antivirus, es decir, no depender de un complemento, ejecución de archivos o módulo adicional.		
251	6.4.2		Capacidad de identificar el origen de la infección, para virus que utilizan el intercambio de archivos como medio de propagación, informando el nombre o la IP del origen con una opción para bloquear la comunicación a través de la red.		
252	6.4.2		Posibilidad de bloquear escaneos de virus en recursos de red mapeados, por contraseña.		
253	6.4.2		Opción a crear una copia de seguridad del archivo sospechoso antes de limpiarlo.		
254	6.4.2		Gestión integrada en la consola de gestión de la solución.		
255	6.4.2		Capacidad para proteger contra ataques dirigidos al navegador.		
256	6.4.2		Administrar el uso de dispositivos USB y CD/DVD, a través de controles para leer/escribir/ejecutar el contenido de estos dispositivos y también sobre el tipo de dispositivo permitido (por ejemplo, permitir mouse USB y bloquear disco USB).		
257	6.4.2		Permitir bloquear el uso de aplicaciones en función del nombre, directorio y hash de la aplicación.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
258	6.4.2	REQUISITOS TÉCNICOS	Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red		
	6.4.2		La solución debe proporcionar la siguiente información de los puntos finales:		
259	6.4.2		Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora en que el software fue instalado o removido.		
260	6.4.2		Actualizaciones de Windows Updates instaladas		
261	6.4.2		Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD		
262	6.4.2		Vulnerabilidades de aplicativos instalados en la máquina		
263	6.4.2		Capacidad de reportar vulnerabilidades de software presentes en las computadoras.		
264	6.4.2		Capacidad de realizar inventario de hardware de todas las máquinas clientes;		
265	6.4.2		Capacidad de realizar inventario de aplicativos de todas las máquinas clientes;		
266	6.4.2		Capacidad de diferenciar máquinas virtuales de máquinas físicas;		
267	6.4.3	SOPORTE AL CLIENTE DE MAC OS	Debe proporcionar protección residente para archivos (antispyware, anti-troyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;		
268	6.4.3		Capacidad de elegir de qué módulos se instalarán, tanto en la instalación local como en la instalación remota;		
269	6.4.3		La instalación y primera ejecución del producto debe ser realizada sin necesidad de reiniciar la computadora, de modo que el producto funcione con toda su capacidad		
270	6.4.3		Métodos de detección basados en: Firmas, Heurística, asistido por Nube de seguridad del proveedor.		
271	6.4.3		La solución deberá contar con medidas de seguridad para el usuario de la estación de trabajo, sea este el administrador de la red o de la pc no deje sin efecto la política de seguridad corporativa.		
272	6.4.3		La solución deberá contar con tecnologías de detección proactiva de amenazas basadas en la nube del mismo fabricante.		
273	6.4.3		El cliente para la instalación en estaciones de trabajo debe ser compatible con el sistema operativo Mac OS X para la funcionalidad antivirus, antispyware y firewall.		
274	6.4.3		Gestión integrada en la consola de gestión de la solución.		
275	6.4.3		Protección en tiempo real contra virus, troyanos, gusanos, troyanos, spyware, adware y otros tipos de códigos maliciosos.		
276	6.4.3		Permitir el análisis de amenazas tanto de forma manual como programada.		
277	6.4.3		Permitir la creación de listas de exclusiones para carpetas y archivos que no serán escaneados por el antivirus.		
278	6.4.3		Permitir acciones de reparación o cuarentena de archivos en caso de infecciones de archivos.		
	6.4.4	FUNCIONALIDADES DE CONTROL DE ACCESO A LA RED	Debe tener la posibilidad de la puesta en cuarentena de equipos, restringiendo el acceso a la red a aquellos equipos que no cumplan con las políticas, al menos con las siguientes premisas:		
279	6.4.4		La computadora debe tener antivirus, actualizado y activo;		
280	6.4.4		La computadora debe tener un firewall activo;		
281	6.4.4		La computadora debe tener parches instalados, activos y actualizados;		
282	6.4.4		Debe tener la capacidad de iniciar la auto remediación del equipo que falló la auditoría, es decir, corregir los puntos donde falló la verificación especificada por el administrador.		
283	6.4.4		Debería tener la posibilidad de notificación personalizada para el usuario.		
284	6.4.5	FUNCIONALIDADES DE CIFRADO	El acceso al recurso cifrado (archivo, carpeta o disco) debe ser garantizado aún en caso de que el usuario haya olvidado la contraseña, a través de procedimientos de recuperación.		
285	6.4.5		Utilizar, como mínimo, un algoritmo AES con clave de 256 bits.		
286	6.4.5		Capacidad de cifrar completamente el disco duro de la máquina, agregando un ambiente de preboot para autenticación del usuario.		
287	6.4.5		Capacidad de utilizar Single Sign-On para la autenticación de preboot.		
288	6.4.5		Permitir crear varios usuarios de autenticación preboot.		
289	6.4.5		Capacidad de crear un usuario de autenticación preboot común con una contraseña igual para todas las máquinas a partir de la consola de manejo.		
290	6.4.5		Capacidad de cifrar drives extraíbles de acuerdo con una regla creada por el administrador, con las opciones:		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
291	6.4.5	FUNCIONALIDADES DE CIFRADO	Cifrar solamente los archivos nuevos que sean copiados para el disco extraíble, sin modificar los archivos ya existentes.		
292	6.4.5		Cifrar todos los archivos individualmente.		
293	6.4.5		Cifrar el dispositivo entero, de manera que no sea posible listar los archivos y carpetas almacenadas.		
294	6.4.5		Cifrar el dispositivo en modo portátil, permitiendo acceder a los archivos en máquinas de terceros a través de una contraseña.		
295	6.4.5		Capacidad de seleccionar carpetas y archivos (por tipo, o extensión) para ser cifradas automáticamente. En esta modalidad, los archivos deben estar accesibles para todas las máquinas gestionadas por la misma consola de manera transparente para los usuarios.		
296	6.4.5		Capacidad de crear reglas de exclusiones para que ciertos archivos o carpetas nunca sean cifrados.		
297	6.4.5		Capacidad de seleccionar aplicaciones que pueden o no tener acceso a los archivos cifrados.		
298	6.5	ADMINISTRACIÓN DE CUENTAS PRIVILEGIADAS	El software necesario para la operación de todos los componentes de la plataforma.		
299	6.5		Administración y resguardo de cuentas privilegiadas, incluyendo:		
300	6.5		Descubrimiento automático de cuentas privilegiadas y sus dependencias en servicios de Windows y tareas programadas.		
301	6.5		Centralización y almacenamiento seguro de las cuentas privilegiadas.		
302	6.5		Rotación automática de contraseñas y llaves SSH.		
303	6.5		Flujos de trabajo automatizados para solicitud de cuentas privilegiadas.		
304	6.5		Controles para la solicitud de contraseñas con registros de auditoría y reportes sobre el uso.		
305	6.5		Administración de Sesiones Privilegiadas, incluyendo:		
306	6.5		Entrega de sesión privilegiada autenticada al dispositivo destino al usuario solicitante.		
307	6.5		Monitoreo y grabación de todas las actividades realizadas con las cuentas privilegiadas en sistemas críticos como Sistemas Operativos, Bases de Datos, Sitios Web, Dispositivos de Seguridad, Dispositivos de Red, Aplicaciones; etc.		
308	6.5		Evitar mostrar las contraseñas privilegiadas a los usuarios.		
309	6.5		Grabación en video de las sesiones gráficas.		
310	6.5		Monitoreo en tiempo real de las sesiones activas		
311	6.5		Suspensión y Terminación de sesiones activas.		
312	6.5		Registro de comandos o teclas presionadas por el usuario en las sesiones.		
313	6.5		Prevenir el acceso directo a los sistemas críticos, ofreciendo un puente entre los usuarios y los dispositivos (aislamiento), sin utilizar agentes.		
314	6.5		La solución propuesta por el proveedor deberá tener la capacidad de detección y respuesta a amenazas que abusen de las cuentas privilegiadas en base a analíticos ofreciendo:		
315	6.5		La capacidad de detectar, alertar y responder a ciberataques intentando explotar las cuentas privilegiadas utilizando algoritmos inteligentes y analíticos.		
316	6.5		Integración bidireccional con soluciones SIEM		
317	6.5		Definición, manual de reglas y autoaprendizaje de la solución para detectar amenazas automáticamente.		
318	6.5		Tablero de alertas y reportes.		
319	6.5		Reglas de respuesta automática a incidentes (rotación automática de cuentas comprometidas)		
320	6.5		Control de Acceso a las Identidades privilegiadas (MFA y SSO):		
	6.5		La plataforma debe ser capaz de autenticar a los usuarios utilizando múltiples factores de autenticación, incluyendo:		
321	6.5		Contraseñas de Active Directory		
322	6.5		Código QR propio		
323	6.5		Código OTP vía SMS enviado por la propia solución		
324	6.5		Código OTP vía E-mail enviado por la propia solución		
325	6.5		Notificaciones push a dispositivos móviles enviado por la propia solución		
326	6.5		OTP de terceros que soporten OATH		
327	6.5		Tokens de terceros en cumplimiento con FID02		
328	6.5		Autenticación biométrica de dispositivos como Windows Helio y Apple Touch ID		
329	6.5		Análisis de comportamiento de usuario y uso de Machine Learning para determinar el riesgo durante un inicio de sesión.		
330	6.5		Autenticación adaptable al contexto y riesgo calculado por la plataforma para cada usuario.		
331	6.5		Capacidad de incluir al portal de usuario otras aplicaciones para su protección con MFAy SSO.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
	6.5	ADMINISTRACIÓN DE CUENTAS PRIVILEGIADAS	Integración con otras soluciones de autenticación que soporten:		
332	6.5		Web SSO.		
333	6.5		RADIUS.		
334	6.5		PKI.		
335	6.5		SAML.		
336	6.5		OpenID Connect (OIDe).		
337	6.5.1	DISPOSITIVOS PARA ADMINISTRAR	Sistemas Operativos como: Windows, *NIX, MAC OS, ESXi, Linux RedHat, Oracle Linux, Solaris.		
338	6.5.1		Aplicaciones de Windows como: Cuentas de servicio, tareas programadas.		
339	6.5.1		Bases de datos como: Oracle, MSSQL, SAP MongoDB, MySQL.		
340	6.5.1		Aplicaciones como: SAP, VMWare vSphere.		
341	6.5.1		Directorios como: Microsoft.		
342	6.5.1		Interfaces genéricas como: SSH, Web, PuTTY, RDP.		
343	6.5.1		ODBC- Contraseñas almacenadas en tablas de base de datos		
344	6.5.2	DESCRIPCIÓN TÉCNICA	La solución de Seguridad de Cuentas Privilegiadas propuesta por el proveedor deberá tener la capacidad de administrar la plataforma de forma centralizada a través de un portal web y capacidad para restringir accesos a través de zonas de red confiables.		
345	6.5.2		El acceso a la solución deberá estar protegido por múltiples factores de autenticación adaptable al contexto, basado en el riesgo determinado por geolocalización y horarios de autenticación; esta funcionalidad debe ser nativa y proporcionada por el mismo fabricante, al menos considerando, contraseña, código QR, OTP, Notificación Push al móvil con validación biométrica, código enviado al correo electrónico, código enviado por SMS, Fid02.		
346	6.5.2		Deberá tener la capacidad de manejar los controles de acceso basado en roles mediante la administración de grupos de usuarios de Directorio Activo o LDAP, además de aprovisionar usuarios en forma automática a partir del Directorio Activo de la Secretaría o LDAP, para así contar con aprovisionamiento automático y transparente de cuentas que reflejen los cambios en dichos directorios.		
347	6.5.2		Deberá tener la capacidad de ejecutar operaciones de forma masiva (bulk operations) sobre las cuentas privilegiadas, como altas y modificaciones.		
348	6.5.2		Deberá soportar el español e inglés como lenguajes disponibles en sus interfaces de usuario.		
349	6.5.2		Deberá contar con una interfaz para programadores (API) y de esta forma permitir la automatización de actividades administrativas, como alta de cuentas, rotación de contraseñas, salud de los componentes instalados y obtener eventos de seguridad.		
350	6.5.3	SEGURIDAD	La solución propuesta por el proveedor deberá tener la capacidad de cifrar, en reposo y en tránsito todos los datos que utilice para garantizar la máxima seguridad posible. Incluyendo contraseñas, reportes almacenados, grabaciones y registros de usuarios.		
351	6.5.3		La solución propuesta por el proveedor deberá tener la capacidad de cifrar la comunicación entre todos los componentes de la solución, esto incluye los componentes que residan en un mismo servidor o en los componentes instalados en otros servidores, utilizando algoritmos AES-256, RSA-2048 y que cumplan con FIPS 140-2.		
352	6.5.3		La solución deberá de poder realizar la integración de HSM externo para almacenar las llaves de cifrado.		
353	6.5.3		La solución propuesta por el proveedor deberá tener la capacidad de permitir que ciertos administradores no puedan visualizar las contraseñas que son controladas por otros departamentos de la Secretaría, como por ejemplo que los administradores de Windows Server no puedan visualizar las contraseñas ni accesos a instancias de bases de datos SQL Server. Esto es para garantizar la segmentación de roles lo más apegado a los procesos establecidos de la Secretaría, con el fin de evitar el uso indebido de las cuentas privilegiadas protegidas por la solución.		
354	6.5.3		La solución propuesta debe permitir que los administradores de la solución no tengan acceso a las contraseñas almacenadas si así se define por el negocio.		
355	6.5.3		La solución propuesta deberá contar con un repositorio seguro y a prueba de falsificaciones (tamper-proof) de credenciales privilegiadas, políticas, grabaciones, permisos, registros de auditorías separado del resto de los componentes que conformen la solución.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
356	6.5.4	ARQUITECTURA	La solución de Seguridad de Cuentas Privilegiadas deberá soportar su instalación como solución basada en Servidores Físicos, en ambientes on-prem.		
357	6.5.4		La solución propuesta deberá ser capaz de realizar las tareas de gestión de cuentas privilegiadas sin la necesidad de que se instalen agentes en los dispositivos del centro de datos.		
358	6.5.4		La solución deberá ser modular y escalable para adaptarse a crecimientos de utilización o expansión de funcionalidades, evitando Appliances all-in-one que complique la instalación de un solo componente para cubrir necesidades específicas como la concurrencia de sesiones o cobertura a diferentes segmentos de red o regiones.		
359	6.5.4		El componente que almacene las contraseñas deberá estar separado del servidor que contenga la interfaz de usuario final y no deberá exponer protocolos innecesarios como HTTPS.		
360	6.5.4		La solución propuesta deberá contar con un repositorio propietario para los datos y ofrecer esquemas de alta disponibilidad (Activo-Activo, Activo-Pasivo) sin necesidad de integrar bases de datos de terceros.		
361	6.5.4		La solución propuesta No deberá requerir licencias adicionales para su Base de Datos en ninguno de sus esquemas de Alta Disponibilidad (Activo-Activo, Activo-Pasivo).		
362	6.5.4		La solución propuesta deberá contar por lo menos con un firewall, hardening del sistema, acceso remoto de forma limitada y restringida a los servidores que resguardan las contraseñas.		
363	6.5.5	ALTA DISPONIBILIDAD Y REDUNDANCIA	La solución propuesta por el proveedor deberá contar con un mecanismo propietario de generación de respaldos cifrados para los datos de la aplicación y no depender de soluciones de respaldo de terceros.		
364	6.5.5		Soporte para instalar repositorio en Clúster.		
365	6.5.5		Sitio de recuperación de desastres.		
366	6.5.5		Integración con respaldos de seguridad del sistema.		
367	6.5.5		Todos los componentes de la solución deberán soportar esquemas activo-activo o activo-pasivo.		
368	6.5.5		móvil protegida por múltiples factores de autenticación y autenticación biométrica inclusive cuando la solución de PAM no se encuentre disponible.		
369	6.5.6	INTEGRACIONES NECESARIAS CON OTROS SISTEMAS	Directorios LDAP para administración de usuarios (Active Directory).		
370	6.5.6		Soluciones SIEM para envió de eventos, alertas y recepción de eventos como inicio de sesión, cambios de contraseñas y asignación de perfiles administrativos, que ocurren en los sistemas administrados.		
371	6.5.6		Integración con Sistemas de Tickets para gestión de solicitudes de sesiones y contraseñas.		
372	6.5.6		Soluciones de monitoreo para el envío de Tramas SNMP.		
373	6.5.6		Servidores de correo SMTP para envío de notificaciones por correo electrónico.		
374	6.5.6		Integración con soluciones de Gobierno de Identidades a través del protocolo SCIM.		
375	6.5.7	REQUERIMIENTOS DE DESCUBRIMIENTO DE CUENTAS, ESCANEO DE MÁQUINAS	El escaneo debe poderse ejecutar sin haber instalado aún la solución de manejo de cuentas privilegiadas, como primer paso para la detección de riesgos asociados a las cuentas en los ambientes escaneados.		
376	6.5.7		La solución propuesta por el proveedor deberá tener la capacidad escanear máquinas Windows, Linux y mapear los usuarios que pueden accederlas, incluyendo usuarios locales y de dominio.		
377	6.5.7		El escaneo debe reportar las cuentas encontradas que no se adhieren a la política corporativa de contraseñas.		
378	6.5.7		El escaneo debe considerar el descubrimiento de las cuentas de Windows que se utilicen en servicios de Windows y Tareas Programadas de Windows.		
379	6.5.7		El escaneo debe ser capaz de encontrar credenciales que se encuentren en texto claro de servidores de aplicaciones WebLogic, Websphere y I/S.		
380	6.5.7		El escaneo debe ser capaz de encontrar credenciales en texto claro que se encuentren en Playbooks de Ansible para los servidores Linux.		
381	6.5.7		El escaneo debe descubrir llaves privadas y públicas de SSH en Linux/Unix y correlacionarlas con las cuentas descubiertas.		
382	6.5.7		La solución propuesta deberá tener la capacidad de mostrar en una gráfica los riesgos relacionados a los ataques de Kerberos como Pass-The-Hash y Golden ticket, sin tener que haber implementado la solución de manejo de cuentas privilegiadas.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
383	6.5.8	MONITOREO Y AUDITORÍA DE SESIONES PRIVILEGIADAS	La solución deberá tener la capacidad de asegurar responsabilidad personal cuando se abre una sesión privilegiada con una cuenta compartida, de forma que se pueda diferenciar qué persona hace uso de una cuenta compartida o genérica, cuándo la utiliza y las actividades que realiza.		
384	6.5.8		La solución deberá tener la capacidad de integrarse a sistemas de Ticketing/HelDesk/Change Management y permitir la validación de tickets antes de establecer la sesión.		
385	6.5.8		La solución deberá tener la capacidad de hacer búsquedas de comandos privilegiados dentro de las grabaciones de video.		
386	6.5.8		La solución deberá tener la capacidad de visualizar las sesiones activas en un momento determinado en vivo/tiempo real.		
387	6.5.8		La solución deberá tener la capacidad de suspender o terminar remotamente una sesión en tiempo real manualmente.		
388	6.5.8		La solución deberá tener la capacidad de que las actividades de sesiones a nivel granular puedan enviarse a la solución SIEM solicitada en este anexo técnico.		
389	6.5.8		La solución deberá tener la capacidad de generar videos de toda la sesión y no solo capturas de pantallas.		
390	6.5.8		La solución deberá tener la capacidad de comprimir las sesiones y sin impactar en la calidad de video.		
391	6.5.8		La solución deberá tener la capacidad de reproducir los videos de las sesiones desde el mismo portal de administración y con la opción de saltar la inactividad en las sesiones, de modo que solo se visualicen los momentos de actividad en una sesión grabada.		
392	6.6	PUNTOS DE DECEPCIÓN DE ATAQUE (TRAMPAS DE SEGURIDAD)	El proveedor deberá de proponer una solución de alertamiento preventivo para detectar ataques cibernéticos y responder de manera anticipada, estos puntos de decepción de ataque (trampas de seguridad) apoyará principalmente a contar con la capacidad para descubrir amenazas latentes y silenciosas en el ambiente, contener y limitar las ventanas de exposición, e incluso alertar de ransomware antes de que se produzca una fuga, filtración, robo o daño de los datos. , contribuyendo a cumplir con los controles de seguridad que minimicen los riesgos de infección de virus y malware, en cumplimiento a la normatividad aplicable en materia de seguridad de la información.		
393	6.6.1	FUNCIONES REQUERIDAS	La solución propuesta por el proveedor deberá estar basada en plataforma de propósito específico.		
394	6.6.1		La solución deberá de ser capaz de detectar malware de día cero, polimórfico y exploits dentro de la red, así como comunicación de tipo comando y control (C&C) hacia el exterior de la red de la Secretaría. La arquitectura deberá estar basada en el concepto del despliegue de trampas al interior de la red de la Secretaría en los ambientes definidos, que permitan identificar el movimiento lateral y primeros signos de las amenazas, se puede incluir una solución de honeypots, sensores o trampas.		
395	6.6.1		Cada localidad geográfica relevante de la Secretaría (Centro de datos principal y Centro de datos alterno) deberá contar con su propio equipo virtual de amenazas avanzadas.		
396	6.6.1		Se deberá de contar con un sistema de consola virtual centralizada que reciba la información de todas las localidades geográficas.		
	6.6.1		La solución deberá cumplir con lo siguiente:		
397	6.6.1		La solución debe incluir el licenciamiento para publicar 200 emulaciones o trampas, dependiendo de la necesidad de la Secretaría.		
398	6.6.1		El licenciamiento por trampa debe soportar, sin costo adicional, que éstas puedan ser implementadas en ambientes virtualizados sobre VMWare ESX, Microsoft Hyper-V o Linux KVM.		
399	6.6.1		La solución debe estar basada en la red y sin utilización de agentes.		
400	6.6.1		La solución propuesta debe de integrar un appliance virtual por cada localidad geográfica o lógica donde se implemente la solución de engaño.		
401	6.6.1		La solución debe de emplear trampas o honeypots que deberán ser desplegados estratégicos al interior de la red para la identificación de amenazas.		
402	6.6.1		La solución debe tener la capacidad de monitorear comunicaciones en VLANs y el tráfico de salida a Internet.		
403	6.6.1		La solución en sus diversos componentes debe estar basada en un sistema operativo endurecido y cerrado.		
404	6.6.1		No se aceptan soluciones que publican trampas en servidores en una localidad central y que a través de conectores o componentes de software que proyecten las trampas. la Secretaría podrá decidir el número de trampas a utilizar.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
405	6.6.1	FUNCIONES REQUERIDAS	La solución no debe requerir licencias de sistemas operativos para las emulaciones, trampas o honeypots.		
406	6.6.1		La solución debe apoyar la mezcla de trampas o emulaciones falsas con los activos del entorno productivo de la entidad bajo el concepto del uso del engaño.		
407	6.6.1		La solución debe integrar un mecanismo para evaluar la cobertura que ofrecen las trampas implementadas en cada segmento de red en base a las técnicas y tácticas de MITRE ATT&CK. Esto con el objetivo de proveer una visibilidad clara del nivel de exposición actual de la Secretaría, además de permitir, en caso de ser necesario, agregar más trampas para incrementar la cobertura.		
408	6.6.1		Con el objetivo de incrementar la cobertura de la plataforma del engaño, la solución debe soportar la capacidad de construir trampas personalizadas utilizando la interfaz gráfica de la plataforma de administración, de cualquier dispositivo conectado a la red de la organización.		
409	6.6.1		La solución debe poder adaptarse a cambios en el entorno productivo mediante la ejecución de escaneos para identificar nuevos activos o plataformas operativas en la red de la entidad.		
410	6.6.1		La solución deberá soportar el acceso basado en roles para segregar funciones y capacidades de la plataforma por usuario.		
411	6.6.1		La arquitectura de la solución debe contar e incluir el software, licenciamiento o subscripción requerida para una gestión centralizada en la infraestructura de TI en la Secretaría o basada en nube para la gestión de múltiples Appliances de la solución en todos los sitios o localidades requeridas por la Secretaría.		
412	6.6.1		La solución debe tener la capacidad de integrarse con el sistema SIEM solicitado en este anexo técnico.		
413	6.6.1		La solución debe permitir generar reportes al menos de Top de direcciones IP destino, Top de IP fuentes maliciosas, Ataques de Alto Riesgo Diarios y Semanales.		
414	6.6.2	INTELIGENCIA Y DETECCIÓN DE AMENAZAS	La solución debe de incluir la capacidad, licencias y componentes requeridos para monitorear el tráfico generado del interior de la red hacia Internet, para poder identificar comportamiento basado en botnets, comando y control (C2) y responder rápidamente ante la identificación de equipos comprometidos.		
415	6.6.2		La solución no debe estar basada en firmas para detectar el malware o la actividad maliciosa.		
	6.6.2		La solución debe soportar al menos los siguientes mecanismos para la detección de malware o ataques:		
416	6.6.2		Cajas de arena (sandboxing)		
417	6.6.2		Análisis estático		
418	6.6.2		Integración con VirusTotal.		
419	6.6.2		La solución debe de ser capaz de capturar el código malicioso y payloads asociados para su análisis, a pesar de no ser una amenaza conocida previamente.		
420	6.6.2		La solución debe generar notificaciones después de la detección de posibles amenazas internas o de malware.		
421	6.6.2		La solución puede utilizar un análisis dinámico descentralizado basado en la nube para realizar un análisis forense y controlado del malware capturado desde los sensores o trampas.		
422	6.6.2		La solución debe de ser capaz de identificar no solo ataques o comportamientos basados en malware, sino cualquier comportamiento malicioso de interacción humana o automatizado que haga contacto con los sensores desplegados.		
423	6.6.2		La solución debe de permitir la integración nativa a la plataforma de administración de la tecnología del engaño sin necesidad de licenciamiento o productos adicionales de la misma marca.		
424	6.6.2		La solución debe permitir la integración con al menos las tecnologías que apoyen la respuesta ante un evento de manera automática o bajo demanda.		
425	6.6.2		La solución debe permitir incluir datos falsos independientes en cada una de las hasta 200 trampas soportadas por Appliance físico para hacer más creíble el engaño hacia el atacante.		
	6.6.2		La solución debe incluir por lo menos la siguiente información relacionada con el ataque:		
426	6.6.2		IP del atacante y el objetivo		
427	6.6.2		Análisis preliminar		
428	6.6.2		Captura de la sesión en la red (PCAP)		
429	6.6.2		Servicios utilizados durante los ataques o interacción con la trampa.		
430	6.6.2		La solución debe permitir la extracción del malware original para realizar un análisis forense externo o una retención legal de ser necesario.		

EVALUACIÓN TÉCNICA
Suministro, Instalación y Configuración de Soluciones de Seguridad Informática.

No. Cons	Punto	Solución	Descripción	Cumple	NO Cumple
	6.6.2	INTELIGENCIA Y DETECCIÓN DE AMENAZAS	La plataforma debe de permitir identificar y asociar los eventos generados desde las trampas o sensores en base a la táctica de MITRE ATT&CK correspondiente. Además, debe permitir filtrar los eventos en base a la naturaleza de su actividad:		
431	6.6.2		Conexión		
432	6.6.2		Reconocimiento		
433	6.6.2		Interacción		
434	6.6.2		Infección		
435	6.6.2		La solución debe tener la capacidad de proporcionar información ficticia configurable e independiente por trampa, como puertos, mensajes de bienvenida (banners), credenciales de acceso sobre cada servicio (ftp, smb, etc.) para hacer más factible engañar al atacante.		
436	6.6.2		La solución debe tener la capacidad de agregar etiquetas personalizables a cada trampa de forma independiente. Esto con el objetivo de simplificar la operación de las trampas desde la interfaz gráfica de la plataforma.		
437	6.6.2		La solución debe integrar de forma nativa en sus Appliances físicos, sin necesidad de realizar configuraciones personalizadas o por medio de servicios profesionales, un sistema operativo Linux completo que contenga y publique el servicio de SSH.		
438	6.6.2		La solución deberá permitir visualizar estadísticas de los eventos o amenazas basado en la naturaleza de esta dentro de la entidad.		

ANEXO 1

PROPUESTA ECONÓMICA

"Suministro, Instalación y Configuración de Soluciones de Seguridad Informática"

FORMATO DE PROPUESTA ECONÓMICA

Se anexa formato propuesto para cotización.

(En papel preferentemente membretado)

ID	Descripción	Solución tecnológica propuesta *	Cantidad de maquinas virtuales requeridas	Costo
1	Servicio de Correlación de Eventos (SIEM)			
2	Servicio de Protección de DNS			
3	Servicio de Detección y Prevención en Correo Electrónico (Antispam)			
4	Servicio de protección antimalware para estaciones de trabajo y servidores (Endpoint)			
5	Servicio de Administración de cuentas privilegiadas			
6	Servicio de puntos de decepción de ataque (Trampas de seguridad)			
			Subtotal	
			I.V.A.	
			Total	

**De la solución tecnológica propuesta integrar nombre, marca, modelo y características.*

Anotar con letra, el subtotal antes de IVA. Anotar con letra el importe total con IVA.

Los precios son en moneda nacional, así como fijos e incondicionados durante la vigencia del contrato. La vigencia de la propuesta deberá ser al menos de 90 días naturales.

Los participantes enviarán su propuesta económica expresando precio unitario y total de la partida única, manifestando que sus precios son fijos e incondicionados durante la vigencia del contrato, en moneda nacional (pesos mexicanos) y deberá presentarse con el I.V.A. desglosado.

Nombre y firma del representante legal.