REQUISITOS DE PARTICIPACIÓN DE LA CONVOCATORIA DE LA LICITACIÓN PÚBLICA DE CARÁCTER NACIONAL ELECTRÓNICA

(LA-006G3A001-E98-2021)

Servicio de Seguridad Perimetral

ÍNDICE

I. DATOS GENERALES O DE INDENTIFICACIÓN DE LA LICITACIÓN PÚBLICA

1.1 NOMBRE DE LA CONVOCANTE, ÁREA CONTRATANTE Y DOMICILIO.

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros **"LA CONDUSEF"**, en cumplimiento a las disposiciones que establece el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos y los artículos 25, 26 fracción I, 26 Bis. fracción II, 28 fracción I, 29, 30, y 32 segundo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y demás disposiciones aplicables en la materia, a través de la Dirección de Recursos Materiales y Servicios Generales, ubicada en Avenida Insurgentes Sur 762, quinto piso, Colonia del Valle, Alcaldía Benito Juárez, Código Postal 03100, Ciudad de México, con teléfono 5448-7000 extensión 7061, convoca a proveedores mexicanos a participar en la Licitación Pública Electrónica Nacional No. LA-006G3A001-E98-2021, relativa al Servicio de Seguridad Perimetral**.**

1.2 MEDIO Y CARÁCTER DE LA LICITACIÓN.

La presente licitación será de carácter **nacional,** el medio de participación será **electrónica,** es decir, los licitantes podrán participar exclusivamente a través del Sistema CompraNet, la o las juntas de aclaraciones, el acto de presentación y apertura de proposiciones, así como el acto de fallo sólo se realizarán a través del Sistema CompraNet y sin la presencia de los licitantes en dichos actos. **No se acepta la participación mediante el uso del servicio postal o de mensajerías.**

1.3 NÚMERO DE IDENTIFICACIÓN DE LA CONVOCATORIA DE LICITACIÓN.

El número de identificación asignado a la convocatoria de esta licitación por el Sistema CompraNet es: LA-006G3A001-E98-2021.

1.4 PERIODO DE LA CONTRATACIÓN.

El periodo de contratación será a partir del día hábil siguiente a la notificación del fallo y hasta el 31 de agosto de 2024. Los servicios que se contraten a través de esta licitación serán prestados conforme a lo establecido en el **ANEXO No. 1, "ANEXO TÉCNICO"**, de la presente convocatoria.

1.5 EJERCICIO FISCAL DE LA CONTRATACIÓN

El presente procedimiento será cubierto con recursos fiscales del ejercicio 2021, en términos del artículo 25 de la Ley.

La contratación de este servicio estará sujeta a la disponibilidad presupuestaria para los ejercicios fiscales 2022, 2023 y 2024, por lo que sus efectos estarán condicionados a la existencia de los recursos presupuestarios respectivos, sin que la no realización de la referida condición suspensiva origine responsabilidad alguna para las partes.

1.6 IDIOMA DE LAS PROPOSICIONES.

La presentación de las propuestas invariablemente deberá ser en **idioma español**, en caso de presentarse alguna información adicional, esta podrá presentarse en otro idioma, pero deberá acompañarse de una traducción simple al español.

1.7 DISPONIBILIDAD PRESUPUESTARIA.

La CONDUSEF cuenta con presupuesto autorizado en la partida presupuestal 31901, con base en la suficiencia presupuestal con número de RC 406-2021, conformidad con el artículo 25 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

La contratación de este servicio estará sujeta a la disponibilidad presupuestaria para los ejercicios fiscales 2022, 2023 y 2024, por lo que sus efectos estarán condicionados a la existencia de los recursos presupuestarios respectivos, sin que la no realización de la referida condición suspensiva origine responsabilidad alguna para las partes.

II. OBJETO Y ALCANCE DE LA LICITACIÓN PÚBLICA

2.1 OBJETO DE LA LICITACIÓN.

"LA CONDUSEF" tiene la necesidad de llevar a cabo la contratación del Servicio de Seguridad Perimetral, de acuerdo con las características y requisitos que se definen en el **ANEXO No. 1, "ANEXO TÉCNICO"** de la presente convocatoria.

2.2 PARTIDAS QUE INTEGRAN LA LICITACIÓN.

Esta contratación está integrada por **1 partida(s),** la(s) cual(es) deberá(n) cotizarse de conformidad con el **ANEXO No. 2 "CÉDULA DE OFERTA ECONÓMICA", y será adjudicada a un solo licitante.**

2.3 NORMAS OFICIALES MEXICANAS, NORMAS MEXICANAS, NORMAS INTERNACIONALES Y/O AUTORIZACIONES.

El prestador de servicios deberá cumplir con aquellas Normas Oficiales Mexicanas, Normas Mexicanas, Normas Internacionales o Normas de referencias o especificaciones, conforme a la Ley Federal sobre Metrología y Normalización, que directa o indirectamente se relacionen con los servicios objeto de la presente contratación.

El prestador de servicios deberá anexar en su propuesta las Certificaciones obligatorias señaladas en el numeral 7.2 CENTRO DE OPERACIONES DE SEGURIDAD (SOC) del ANEXO No. 1 ANEXO TÉCNICO.

2.4 TIPO DE CONTRATACIÓN.

"LA CONDUSEF" Con fundamento en los artículos 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 85 de su Reglamento, "LA CONDUSEF" celebrará un contrato abierto con el licitante que resulte ganador. Con un prespuesto:

PRESUPUESTO	2021	2022	2023	2024
MÁXIMO	$6,840,000.00	$20,520,000.00	$20,520,000.00	$13,680,000.00
MÍNIMO	$2,736,000.00	$8,208,000.00	$8,208,000.00	$5,472,000.00

La presente contratación abarca los ejercicios fiscales 2021, 2022, 2023 y 2024.

2.5 ADJUDICACIÓN E INFORMACIÓN RELATIVA A LA LICITACIÓN.

2.5.1 ADJUDICACIÓN.

Con fundamento en los artículos 29 fracción XII y 36 Bis fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, una vez hecha la evaluación de las proposiciones, la adjudicación será por la totalidad del contrato al licitante cuya propuesta resulte solvente, porque cumple con los requisitos legales, técnicos y económicos establecidos en esta convocatoria, y por lo

tanto garantice satisfactoriamente el cumplimiento de las obligaciones respectivas, y que haya obtenido el mejor resultado en la evaluación combinada de puntos y porcentajes.

Si derivado de los resultados de evaluación, se obtuviera un empate en las proposiciones, de conformidad con lo establecido en el artículo 36 Bis, penúltimo y último párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 54 de su Reglamento, la adjudicación se efectuará en favor de aquel licitante que sea integrante del sector de las micro, pequeñas y medianas empresas nacionales; en el caso de que ambas cumplan este requisito, la adjudicación será al licitante que resulte ganador del sorteo por insaculación que celebre **"LA CONDUSEF"** 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 **en primer lugar el boleto del licitante ganador** y posteriormente los demás boletos empatados, con lo que se determinarán los subsecuentes lugares que ocuparán tales proposiciones.

2.5.2 ACEPTACIÓN DE LOS SERVICIOS OBJETO DE LA LICITACIÓN.

De acuerdo a lo establecido en el Artículo 84 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el Titular de la Dirección de Tecnologías de la Información y Comunicaciones y/o el Servidor Público que lo sustituya, será el responsable de dar por recibido los servicios objeto de la presente licitación. Además, tendrá las facultades de verificar directa o indirectamente el cumplimiento del Contrato que se formalice, de acuerdo a lo contenido en el ANEXO TÉCNICO.

El Jefe de Departamento de Redes y Telecomunicaciones, y/o el Servidor Público que lo sustituya, será responsable de supervisar los servicio(s) objeto del Contrato, de acuerdo a lo establecido en el ANEXO TÉCNICO. Por lo anterior, podrá apoyarse de personal necesario para llevar a cabo la revisión de los servicios e informar y reportar las deficiencias en los mismos.

Se entenderá por aceptado los servicios, cuando el proveedor cumpla en todo momento lo establecido en la presente convocatoria, sus anexos y, en su caso, las modificaciones a la misma; así como lo estipulado en el contrato respectivo. En tanto ello no se cumpla, los servicios se deberán tener por no aceptados.

2.5.3 MONEDA.

Los licitantes participantes deberán presentar su proposición en moneda nacional. De conformidad con el artículo 44 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, los precios ofertados permanecerán firmes durante la vigencia del contrato correspondiente, no aceptándose modificaciones a los mismos.

2.5.4 ANTICIPOS.

No se otorgarán anticipos para esta Licitación.

2.5.5 IMPUESTOS.

Los impuestos que se deriven del cumplimiento de las obligaciones que se establezcan en el contrato a celebrar con el licitante que resulte ganador, serán pagados conforme a los ordenamientos fiscales aplicables vigentes.

2.5.6 CONDICIONES DE PAGO.

El pago será en moneda nacional, dentro de los 20 días naturales siguientes contados a partir de la fecha en que el proveedor presente el Comprobante Fiscal Digital por Internet (CFDI) mismo que deberá cumplir con la legislación fiscal vigente y cuente con la autorización de la Dirección de

Tecnologías de la Información y Comunicaciones, previa verificación de la prestación de los servicios en tiempo y de conformidad con el ANEXO TÉCNICO, que realice el área supervisora, así como de aceptar la factura y con ello validar la prestación de los servicios y con el visto bueno de pago por parte de la Dirección de Planeación y Finanzas. Se realizará mediante transferencia electrónica de fondos a la cuenta de cheques que para ese efecto señale el licitante ganador.

El CFDI referido en este numeral deberá estar acompañado de las copias del o los comprobantes que acrediten que el servicio fue prestado por parte del licitante ganador en tiempo y a satisfacción de la Dirección de Tecnologías de la Información y Comunicaciónes. Se entenderá por aceptado el servicio, cuando el proveedor cumpla en todo momento lo establecido en la presente convocatoria, sus anexos y, en su caso, las modificaciones a la misma; así como lo estipulado en el contrato respectivo. En tanto ello no se cumpla, el servicio se deberá tener por no aceptado.

En el CFDI correspondiente deberá desglosarse el Impuesto al Valor Agregado; cuando se trate de alguna persona física con actividad empresarial, deberá incluir también la retención correspondiente de acuerdo a la legislación fiscal vigente.

En caso de que los CFDI sean devueltos por algún error o deficiencia, **"LA CONDUSEF"** dentro de los tres días hábiles siguientes al de su recepción indicará por escrito al licitante ganador las deficiencias que deba corregir de conformidad con el artículo 90 del Reglamento de Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. 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 artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

De conformidad a las DISPOSICIONES Generales a las que deberán sujetarse las dependencias y entidades de la Administración Pública Federal, así como las empresas productivas del Estado, para su incorporación al Programa de Cadenas Productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo, publicadas en el Diario Oficial de la Federación el 24 de julio de 2020, **"LA CONDUSEF"** incorporará a este programa y dará de alta en el mismo la totalidad de las cuentas por pagar al licitante ganador; para ello, el CFDI aceptado se registrará en dicho Programa dentro de los 15 días naturales posteriores a su recepción, misma que podrá ser consultada en línea en la dirección electrónica **www.nafin.gob.mx**, a efecto de que el licitante ganador pueda ejercer la cesión de derechos de cobro al intermediario financiero seleccionado por el licitante ganador entre los registrados en dicha cadena, en los términos del último párrafo del artículo 46 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

El pago por el costo de la intermediación financiera por las operaciones derivadas del pago a través de este Programa, corresponderá al licitante ganador.

2.5.7 CESIÓN DE DERECHOS DE COBRO.

El licitante ganador no podrá ceder en forma parcial o total a favor de cualquier otra persona, los derechos y obligaciones que se deriven del contrato correspondiente, con excepción de los derechos de cobro, en cuyo caso deberá contar con el consentimiento previo por escrito de **"LA CONDUSEF"**, a través de la Dirección de Tecnologías de la Información y Comunicaciones, de conformidad con el artículo 46 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

2.5.8 GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.

El licitante que resulte ganador deberá garantizar el cumplimiento del contrato que le sea adjudicado, por un equivalente al 10 % del importe máximo del contrato sin incluir el Impuesto al

Valor Agregado, para lo cual el licitante podrá utilizar el **ANEXO No. 14** "FORMATO CON EL TEXTO QUE DEBE CONTENER LA GARANTÍA DE CUMPLIMIENTO".

La presentación de esta garantía deberá ser mediante cualquiera de los siguientes instrumentos:

A) Depósito de dinero constituido a través de certificado o billete de depósito, o
B) Fianza, o
C) Depósito de dinero constituido ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, o
D) Carta de crédito irrevocable, o
E) Cheque certificado o de caja expedido a favor de la Comisión Nacional Para la Protección y Defensa de los Usuarios de Servicios Financieros.

Esta garantía deberá ser entregada **a más tardar dentro de los diez días naturales** siguientes a la firma del contrato de conformidad con los artículos 48, fracción II y último párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 85, fracción III de su Reglamento.

LA FALTA DE PRESENTACIÓN DE ESTA GARANTÍA, EN EL PLAZO ESTIPULADO, DARÁ COMO CONSECUENCIA LA RESCISIÓN ADMINISTRATIVA DEL CONTRATO.

En caso de que **"LA CONDUSEF"** otorgue ampliación al contrato; el licitante ganador deberá gestionar las modificaciones correspondientes que garanticen el cumplimiento de la ampliación.

En caso de que la garantía se constituya a través de una fianza, la póliza de garantía deberá prever, como mínimo, las siguientes declaraciones:

I) Que la fianza se otorga atendiendo a todas las estipulaciones contenidas en el contrato,
II) Que, para liberar la fianza, será requisito indispensable la manifestación expresa y por escrito de **"LA CONDUSEF"**;
III) Que la fianza estará vigente durante la substanciación de todos los recursos legales o juicios que se interpongan y hasta que se dicte resolución definitiva por autoridad competente y;
IV) Que la afianzadora acepta expresamente someterse a los procedimientos de ejecución previstos en la Ley de Instituciones de Seguros y Fianzas para la efectividad de las fianzas, aún para el caso de que procediera el cobro de intereses, con motivo del pago extemporáneo del importe de la póliza de fianza requerida.

Nota: Para la liberación de la fianza será necesaria la solicitud por escrito del interesado.

La garantía que en su caso se constituya para el cumplimiento del contrato, se hará efectiva por **"LA CONDUSEF"**, **cuando se presente de manera enunciativa y no limitativa alguno de los siguientes casos:**

a. Previa rescisión del contrato.
b. Cuando se haya vencido el plazo para la prestación de los servicios y el proveedor por sí mismo o a requerimiento de "LA CONDUSEF", no sustente debidamente las razones del incumplimiento, previo agotamiento de las penas convencionales respectivas.
c. "LA CONDUSEF" podrá hacer efectiva la garantía de cumplimiento del contrato, cuando el proveedor preste el servicio en forma diferente a lo

solicitado en la presente convocatoria o incumpla con cualquiera de las obligaciones establecidas en las mismas, previo procedimiento de rescisión.

d. "LA CONDUSEF" podrá hacer efectiva la garantía de cumplimiento, cuando la suma de las penas convencionales o deducciones alcancen de manera proporcional el monto de la garantía de cumplimiento.

2.5.9 DIVISIBILIDAD O INDIVISIBILIDAD DE LAS OBLIGACIONES A GARANTIZAR:

En concordancia con lo dispuesto por el artículo 81 fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, con relación al artículo 2003 del Código Civil Federal, a las características del servicio, y atendiendo a que los servicios objeto de esta contratación, que se entreguen parcialmente no resultarían útiles, aprovechables o funcionales, se consideran indivisibles las obligaciones contractuales que se deriven a consecuencia del presente procedimiento.

2.5.10 MODELO DEL CONTRATO.

El contrato que se adjunta como **ANEXO No. 13 "MODELO DEL CONTRATO"**, forma parte integral de esta convocatoria, el cual se ajustará a las características específicas de cada bien o servicio a contratar.

III. FORMA Y TÉRMINOS QUE REGIRÁN LOS ACTOS DE LA LICITACIÓN

Esta contratación 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".

3.1. REDUCCIÓN DE PLAZOS

No se aplicará reducción de plazos para esta convocatoria.

Para la presentación y apertura de proposiciones, NO se aplicará reducción de plazos, sujetándose a lo establecido en el artículo 32 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 43 de su Reglamento.

3.2. CONSULTA DE LA CONVOCATORIA

Con fundamento en el artículo 30 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, la publicación de la convocatoria se realiza a través de Internet, en **CompraNet** en la dirección **https://compranet.hacienda.gob.mx/web/login.html** y **su obtención será gratuita**. De forma simultánea se envía para su publicación en el Diario Oficial de la Federación, un resumen de la convocatoria a la licitación.

Asimismo, **"LA CONDUSEF"** pone a disposición de cualquier persona para su consulta, el texto impreso de la convocatoria en la Dirección de Recursos Materiales y Servicios Generales, ubicada en Avenida Insurgentes Sur 762, quinto piso, Colonia del Valle, Alcaldía Benito Juárez, Código Postal 03100, Ciudad de México, a partir de la fecha de su publicación y hasta el , en un horario de 9:00 a 16:00 horas, con Ezequiel Flores Martínez, representante de la Dirección de Recursos Materiales y Servicios Generales por lo que será de la exclusiva responsabilidad de los interesados acudir a enterarse de su contenido.

"LA CONDUSEF" podrá modificar los plazos u otros aspectos establecidos en esta convocatoria a partir de la fecha en que sea publicada en CompraNet y hasta el séptimo día natural previo al acto

de presentación y apertura de proposiciones, debiendo difundir dichas modificaciones en CompraNet, a más tardar el día hábil siguiente a aquel en que se efectúen, en apego a lo establecido en el artículo 33 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

3.3. CALENDARIO DE EVENTOS POR MEDIO DE COMPRANET

"LA CONDUSEF" da a conocer las fechas y horarios de los eventos del presente procedimiento, los cuales se describen a continuación:

Etapas	Fecha	Horario
Junta de Aclaraciones	24 de agosto de 2021	11:00 horas
Acto de presentación y apertura de proposiciones	03 de septiembre de 2021	11:00 horas
Acto de Fallo	09 de septiembre de 2021	13:00 horas

3.4. VISITAS A INSTALACIONES

No habrá visita a las instalaciones.

3.5. LUGAR EN DONDE SE LLEVARÁN A CABO LOS ACTOS PÚBLICOS DE LA LICITACIÓN.

Los actos se realizarán a través de **CompraNet** y sin la presencia de los licitantes en dichos actos, mismos que se llevarán a cabo en la sala del piso 5 ubicada en la ubicada en Avenida Insurgentes Sur 762, quinto piso, Colonia del Valle, Alcaldía Benito Juárez, Código Postal 03100, Ciudad de México. En las fechas antes señaladas en el numeral **3.3** de la presente convocatoria.

3.6. ACTOS DE LA LICITACIÓN

Los actos que forman parte del procedimiento de esta Licitación, 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 el sistema **CompraNet** al concluir dichos actos, en la sección de difusión al público en general, como se establece en el "Acuerdo por el que se establecen las disposiciones que se deberán observar para la utilización del Sistema Electrónico de Información Pública Gubernamental denominado **CompraNet**".

Por tratarse de un procedimiento electrónico, queda bajo la responsabilidad de los licitantes darse de alta en el sistema CompraNet para poder participar.

3.7. LA JUNTA DE ACLARACIONES A LA CONVOCATORIA.

La Junta de Aclaraciones, se desarrollará en los tiempos y conforme lo establecen los Artículos 33, 33 Bis y 37 Bis de "La Ley" así como los Artículos 45 y 46 del "Reglamento".

Los acuerdos y modificaciones que se tomen en esta junta, se asentarán en el acta respectiva, mismas que formarán parte integral de esta Convocatoria y deberán ser consideradas por los licitantes en la elaboración de sus proposiciones.

Las modificaciones que se mencionan en el párrafo anterior en ningún caso podrán consistir en la sustitución de los servicios requeridos y convocados originalmente, adición de otros de distintos rubros o en variación significativa de sus características. Estas modificaciones serán difundidas en

CompraNet, a más tardar el día hábil siguiente a aquel en que fueron efectuadas.

"LA CONDUSEF" podrá celebrar las juntas de aclaraciones que se consideren necesarias, atendiendo a las características de los servicios objeto de esta Licitación, por lo que, de ser el caso, al concluir la primera junta de aclaraciones podrá señalarse la fecha y hora para la celebración de una segunda o ulteriores juntas.

Con la finalidad de agilizar la junta de aclaraciones, los licitantes deberán enviar sus solicitudes de aclaraciones a la convocatoria de esta licitación, a través del sistema de CompraNet, preferentemente en formato PDF y Word, para lo cual los licitantes podrán utilizar el formato adjunto **(ANEXO No. 3 "FORMATO DE ESCRITO PARA FORMULAR PREGUNTAS")** así como el **escrito simple bajo protesta de decir verdad, en el que expresen su interés en participar en la licitación,** por sí o en representación de un tercero, manifestando en todos los casos los datos generales del interesado, conteniendo los siguientes datos: A) Del licitante: Clave del Registro Federal de Contribuyentes; nombre, domicilio, así como, en su caso, de su apoderado o representante legal, descripción del objeto social; datos de las escrituras públicas con las que se acredita la existencia legal de las personas morales y de haberlas, sus reformas y modificaciones, así como nombre de los socios que aparezcan en éstas y B) Del representante: datos de las escrituras públicas en las que le fueron otorgadas las facultades, para lo cual los licitantes podrán utilizar el formato adjunto **(ANEXO No. 4 "FORMATO PARA ACREDITAR LA PERSONALIDAD DEL LICITANTE") a más tardar a las 11:00 horas del día 23 de agosto de 2021.**

IMPORTANTE: Las solicitudes de aclaraciones recibidas con posterioridad al plazo arriba señalado, no serán contestadas por resultar extemporáneas, excepto cuando el servidor público que presida la junta de aclaraciones considere necesario programar una nueva reunión para ello, respetando los plazos previstos en la Ley, de conformidad con el artículo 46 fracción VI del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

El acta de la junta de aclaraciones se pondrá, al finalizar dicho evento y por un término de cinco días hábiles, a disposición de los licitantes y al público en general, fijándose aviso del lugar donde serán proporcionadas las copias, en el pizarrón de "Avisos de Licitaciones" ubicado en el quinto piso del edificio que ocupan las oficinas centrales de **"LA CONDUSEF"**, en el domicilio señalado en el primer párrafo de este punto.

Dicha acta será difundida en CompraNet para efectos de su notificación. Dicho procedimiento sustituirá a la notificación personal con todos sus efectos.

A las juntas de aclaraciones y a los diferentes actos de la Licitación podrá asistir cualquier persona en calidad de observador, bajo la condición de registrar su asistencia y abstenerse de intervenir en cualquier forma en los mismos.

3.8. ACTO DE PRESENTACIÓN Y APERTURA DE PROPOSICIONES.

El acto de presentación y apertura de proposiciones se llevará a través de CompraNet, y sin la presencia de los licitantes, esto de conformidad con lo establecido en el artículo 26 Bis, fracción II, segundo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Las proposiciones únicamente podrán ser enviadas a través de CompraNet, para la firma de éstas se emplearán los medios de identificación electrónica, en términos del artículo 50 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. Los cuales producirán los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio, de acuerdo al último párrafo del artículo 27 de la Ley de

Adquisiciones, Arrendamientos y Servicios del Sector Público. **No se acepta el uso del servicio postal o de mensajerías.**

Al ingresar a CompraNet, los servidores públicos certificados para ello, revisarán que la documentación antes mencionada cumpla con los requerimientos establecidos en la convocatoria de la presente licitación, haciéndose constar la documentación presentada, sin que ello implique la evaluación de su contenido de acuerdo a lo estipulado en el artículo 35, fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Los licitantes deberán presentar sus proposiciones por medios remotos de comunicación electrónica (CompraNet). Los sobres serán generados mediante el uso de tecnologías que resguarden la confidencialidad de la información de tal forma que sean inviolables, deberán ser enviados de conformidad a las disposiciones técnicas que al efecto establezca la Secretaría de la Función Pública. Los licitantes deberán enviar sus proposiciones preferentemente en formato PDF.

En el supuesto de que, durante el acto de presentación y apertura de proposiciones, no sea posible abrir los sobres que contengan las proposiciones enviadas a través de CompraNet, el Servidor Público que presida el acto, o el que éste designe, se comunicará vía telefónica con personal de CompraNet para que éste determine el origen y en su caso, las causas por las que no es posible abrir los sobres correspondientes; lo anterior se hará constar en el acta correspondiente. En caso de que CompraNet determine que es por causas ajenas a la voluntad de la Secretaría de Hacienda y Crédito Público o de **"LA CONDUSEF"**, no sea posible abrir los sobres que contengan las propuestas enviadas por medios remotos de comunicación electrónica, el acto se reanudará a partir de que se restablezcan las condiciones que dieron origen a la interrupción. Salvo que los sobres en los que se incluya dicha información contengan virus informáticos o no puedan abrirse por cualquier causa motivada por problemas técnicos imputables a los programas o equipo de cómputo del licitante, el cual admitirá que se tendrá por no presentada la proposición y la demás documentación requerida por **"LA CONDUSEF"** de conformidad con el 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".

Una vez recibidas las proposiciones, el servidor público que presida el acto comenzará la revisión cuantitativa de las proposiciones recibidas por CompraNet, haciendo constar la documentación recibida, sin que ello implique la evaluación técnica, económica y administrativa de su contenido.

Para la presentación y firma de proposiciones, o en su caso, de inconformidades a través de CompraNet, **los licitantes nacionales, deberán utilizar la firma electrónica avanzada** que emite el Servicio de Administración Tributaria para el cumplimiento de sus obligaciones fiscales, conforme a lo establecido en el artículo 50, primer párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Conforme al **ANEXO No. 11 "DOCUMENTOS QUE DEBERÁN INTEGRAR LA PROPUESTA DEL LICITANTE"**, los licitantes podrán indicar la documentación que fue enviada a través de CompraNet. (La falta de presentación de este documento no será motivo para desechar la proposición)

Una vez realizada la recepción de las proposiciones se procederá al registro de la documentación recibida.

Se instrumentará acta que servirá de constancia de la celebración del acto de presentación y apertura de proposiciones, en la que se harán constar las proposiciones recibidas a través de CompraNet en tiempo y forma; durante este acto, atendiendo al número de proposiciones

presentadas en la que se hará constar, el importe total de cada una de las proposiciones; dicha acta estará disponible en CompraNet el mismo día en que se celebre cada evento, sin menoscabo de que puedan acudir a recoger las actas, en el domicilio señalado en esta Convocatoria.

CompraNet emitirá un aviso de la recepción de las proposiciones; una vez iniciada la presentación y apertura de proposiciones no se aceptará proposición alguna.

Asimismo, se señalará lugar, fecha y hora en que se dará a conocer el fallo de la licitación, esta fecha deberá quedar comprendida dentro de los 20 días naturales siguientes a la establecida para este acto y podrá diferirse, siempre que el nuevo plazo fijado no exceda de 20 días naturales contados a partir del plazo establecido originalmente, conforme a lo establecido en el artículo 35 fracción III de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

No se rubricará la totalidad de los documentos que integran las proposiciones, toda vez que las propuestas se encuentran resguardadas en el servidor del sistema CompraNet, por lo que únicamente se imprimirán las Propuestas Económicas de los licitantes, las cuales serán rubricadas por los servidores públicos participantes, lo cual garantiza la integridad de las proposiciones. Lo anterior, en correlación en lo establecido en el numeral 3.13. de la presente convocatoria.

3.9. VIGENCIA DE PROPOSICIONES

Una vez recibidas las proposiciones en el acto de presentación y apertura, éstas no podrán ser retiradas o dejarse sin efectos, por lo que estarán vigentes dentro del procedimiento de esta licitación hasta su conclusión.

3.10. PROPOSICIÓN ÚNICA.

Los licitantes participantes sólo podrán presentar una proposición para esta licitación, la cual podrá ser de manera individual o conjunta.

3.11. PRESENTACIÓN CONJUNTA DE PROPOSICIONES.

Con fundamento en el artículo 34 párrafo tercero, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y el 44 de su Reglamento, dos o más personas podrán presentar conjuntamente proposiciones sin necesidad de constituir una sociedad o nueva sociedad, en caso de personas morales, cumpliendo con los siguientes aspectos:

A) En la propuesta y en el contrato, se establecerán con precisión y a satisfacción de **"LA CONDUSEF"**, los términos a que cada persona se obligará, así como la manera en que se exigiría el cumplimiento de las obligaciones, para lo cual deberán celebrar entre todas las personas que integran la agrupación, un convenio en los términos de la legislación aplicable, en el que se establecerán con precisión los aspectos siguientes:

I) 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;

II) 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;

III) La 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;

IV) La 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

V) Estipulación expresa de que cada uno de los firmantes quedará obligado junto con los demás integrantes, ya sea en forma solidaria o mancomunada, según se convenga, para efectos del procedimiento de contratación y del contrato, en caso de que se les adjudique el mismo.

B) La propuesta deberá ser firmada por el representante común que para ese acto haya sido designado por el grupo de personas.

C) Únicamente podrán agruparse para presentar una proposición los interesados que no se encuentren en alguno de los supuestos a que se refieren los artículos 50 y 60 penúltimo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

D) Las personas que pretendan presentar una proposición conjunta, deberán cumplir de forma individual con los requisitos establecidos para cada licitante que se consideran en los siguientes numerales de la presente Convocatoria y que a continuación se citan:

- Declaración escrita de los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (Solicitada en el punto 4.1.3. de la presente Convocatoria).
- Declaración de integridad (Solicitada en el punto 4.1.4. de la presente Convocatoria).
- Manifestación de las MIPYMES (Solicitada en el punto 4.1.5. de la presente Convocatoria).
- Acreditación de nacionalidad (Solicitada en el punto 4.1.6. de la presente Convocatoria).

3.12. ACREDITACIÓN DE PERSONALIDAD.

Los licitantes, para acreditar su personalidad en el acto de presentación y apertura de proposiciones, enviarán un escrito en el que el firmante manifieste, bajo protesta de decir verdad, que cuenta con capacidad legal para comprometerse por sí o que cuenta con facultades suficientes para comprometer a su representada, mismo que deberá contener los datos siguientes:

I) **Del licitante:** Clave del Registro Federal de Contribuyentes; nombre, domicilio, así como, en su caso, de su apoderado o representante legal. Tratándose de personas morales, además, descripción del objeto social de la empresa; identificando los datos de las **escrituras públicas con las que se acredita la existencia legal de las personas morales y de haberlas, sus reformas y modificaciones**, así como nombres de los socios que aparezcan en éstas y:

II) **Del representante del licitante:** datos de las escrituras públicas en las que le fueron otorgadas las facultades para suscribir las propuestas.

III) **Dirección de correo electrónico**, en caso de contar con ella.

Asimismo, se aceptará la acreditación de la personalidad de los licitantes que hayan realizado el procedimiento para comprobar su representación y capacidad legal, como personas físicas o morales mediante su inscripción en el Registro Único de Personas Acreditadas (RUPA), para tal efecto deberá enviar copia de la cédula actualizada correspondiente.

Para lo anterior, los licitantes podrán utilizar el formato adjunto **(ANEXO No. 4 "FORMATO PARA ACREDITAR LA PERSONALIDAD DEL LICITANTE")**.

3.13. RÚBRICA DE PROPUESTAS EN EL ACTO DE PRESENTACIÓN Y APERTURA DE PROPOSICIONES.

El servidor público que presida el acto, designará al (los) servidor (es) público (s) quien (es) rubricará (n) el CD (s) o DVD (s) en el (los) que se almacenarán los archivos que contengan las propuestas técnicas y económicas, así como la documentación distinta de éstas, de cada licitante recibidas por CompraNet. Una vez rubricado (s) el (los) medio (s) electrónico (s) de almacenamiento, formarán parte del expediente, junto con impresión rubricada de las siguientes constancias:

- Resumen Técnico y Económico (CompraNet)
- Propuesta Económica: Se rubricará toda la propuesta

Lo anterior de conformidad a los artículos 35 fracción II de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 39 fracción III inciso j) de su Reglamento.

3.14. ACTO DE FALLO.

El Acto de Fallo se dará a conocer a través de CompraNet. A los licitantes se les enviará por correo electrónico un aviso informándoles que el acta de fallo se encuentra a su disposición en CompraNet, conforme lo establecido en el artículo 37 quinto párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Con la notificación del fallo por el que se adjudica el contrato, las obligaciones derivadas de éste serán exigibles, sin perjuicio de las obligaciones de las partes de firmarlo en la fecha y términos señalados en el fallo.

En caso de error aritmético, mecanográfico o de cualquier otra naturaleza, que no afecte la evaluación realizada por **"LA CONDUSEF"**, procederá la corrección en la forma y términos dispuestos por el penúltimo párrafo del artículo 37 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Contra el fallo no procederá recurso alguno; sin embargo, procederá la inconformidad en términos del Título Sexto, Capítulo Primero de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

3.15. FIRMA DEL CONTRATO.

La firma del contrato que se adjudique al licitante ganador, se formalizará dentro de los quince días naturales posteriores a la notificación del fallo a través del módulo de "Formalización de Instrumentos Jurídicos" 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 Diario Oficial de la Federación el 18 de septiembre de 2020. Siendo dicho módulo aquél a través del cual las dependencias y entidades, deberán formalizar de manera electrónica los instrumentos jurídicos que se deriven de los diversos procedimientos de contratación previstos en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y en la Ley de Obras Públicas y Servicios Relacionados con las Mismas, así como generar y/o incorporar la documentación que se les requiera de los mismos.

Por lo cual los servidores públicos, proveedores, contratistas, así como los prestadores de servicios nacionales involucrados en la formalización de un instrumento jurídico, derivado de algún procedimiento de contratación realizado por las dependencias y entidades, utilizarán como medio de identificación electrónica la Firma Electrónica Avanzada (e.firma) que emite el Servicio de Administración Tributaria.

Tratándose de personas físicas o morales extranjeras involucradas en la formalización de un instrumento jurídico derivado de algún procedimiento de contratación, deberán obtener su certificado digital con alguna de las Autoridades Certificadoras de acuerdo a la Ley de Firma Electrónica Avanzada, a efecto de que utilicen el módulo de "Formalización de Instrumentos Jurídicos".

Para lo cual, en la liga electrónica https://www.gob.mx/compranet/documentos/modulo-de-formalizacion-de-instrumentos-juridicos puede consultar el material de apoyo para su registro al módulo de “Formalización de Instrumentos Jurídicos".

El licitante que resulte adjudicado, se presentará a más tardar dentro de los dos días hábiles posteriores a la notificación del fallo en la oficina de la Dirección de Recursos Materiales y Servicios Generales, con Claudia Castillo Campos, que se localiza en Avenida Insurgentes Sur 762, quinto piso, Colonia del Valle, Alcaldía Benito Juárez, Código Postal 03100, Ciudad de México, en un horario de 9:00 a 14:00 horas, debiendo entregar original o copia certificada para su cotejo y en formato electrónico (preferentemente en CD), los siguientes **documentos vigentes con los que se acredite su existencia legal y las facultades de su representante para suscribir el contrato correspondiente:**

1. Registro Federal de Contribuyentes (RFC).
2. Identificación oficial vigente del representante o apoderado legal, quien firmará el contrato.
3. Poder notarial.
4. Tratándose de persona moral, testimonio de la escritura pública en la que conste que fue constituida conforme a las leyes mexicanas y que tiene su domicilio en el territorio nacional,
5. Modificaciones realizadas a la escritura pública.
6. Tratándose de personas físicas, copia certificada del acta de nacimiento o en su caso, carta de naturalización respectiva, expedida por la autoridad competente, así como la documentación que acredite tener su domicilio legal en el territorio nacional.
7. Comprobante de domicilio.
8. Datos de la cuenta bancaria para el depósito correspondiente (Nombre del banco, número CLABE interbancaria y número de cuenta).
9. Respuesta Positiva de la opinión emitida por el SAT, respecto del cumplimiento de sus obligaciones fiscales, de conformidad con lo señalado en el numeral 4.3.2. de la presente convocatoria.
10. Documento en el que conste la opinión positiva emitida por el Instituto Mexicano del Seguro Social (IMSS), sobre el cumplimiento de obligaciones en materia de seguridad social, de conformidad con lo señalado en el numeral 4.3.3. de la presente convocatoria.
11. Constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos vigente expedido por el Instituto del Fondo Nacional de la Vivienda para los

Trabajadores (INFONAVIT), de conformidad con lo señalado en el numeral 4.3.4. de la presente convocatoria.

12. Escrito firmado por sí o por medio de su Representante Legal del licitante en donde manifieste que su representada, reconoce y acepta ser el único patrón de todos y cada uno de los trabajadores que intervengan en el desarrollo y ejecución del servicio durante la vigencia del contrato, por lo que de igual forma será totalmente responsable del pago oportuno a dicho personal, así como de las obligaciones de las cuotas obrero patronales IMSS; de igual forma deberá entregar, en forma bimestral, al Administrador del Contrato, original y copia para cotejo y devolución, las cédulas de determinación y pagos de las cuotas obrero patronales realizadas al Instituto Mexicano del Seguro Social (IMSS) y al Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT).
13. Manifiesto bajo protesta de decir verdad que el licitante, en el caso de personas físicas o sus socios en caso de persona moral, no desempeñan empleo, cargo o comisión en el servicio público o, en su caso, que a pesar de desempeñarlo, en caso de resultar adjudicado con la formalización del contrato correspondiente no se actualiza un Conflicto de Interés
14. Acuse de la presentación del manifiesto en el que afirmen o nieguen los vínculos o relaciones de negocios, laborales, profesionales, personales o de parentesco por consanguinidad o afinidad hasta el cuarto grado que tengan la propia persona, con el o los servidores públicos a que se refiere el Anexo Segundo del PROTOCOLO DE ACTUACIÓN EN MATERIA DE CONTRATACIONES PÚBLICAS, OTORGAMIENTO Y PRÓRROGA DE LICENCIAS, PERMISOS, AUTORIZACIONES Y CONCESIONES. El citado manifiesto lo formularán *a través de la dirección electrónica www.gob.mx/sfp, siendo este medio electrónico de comunicación el único para presentarlo y el acuse de presentación del manifiesto se obtiene a través de la liga* https://manifiesto.funcionpublica.gob.mx/SMP-web/loginPage.jsf.

Enfatizando que el respectivo instrumento jurídico se suscribirá en el Módulo de Formalización de Instrumentos Jurídicos, por lo que deberá estar registrado.

Asimismo, se invita cordialmente al licitante ganador en caso de no estar inscrito en el Registro Único de Proveedores y Contratistas (RUPC) en el Sistema CompraNet, a realizar su inscripción en el mismo.

3.16. MODIFICACIONES AL CONTRATO.

Cualquier modificación al contrato, deberá hacerse dentro de su vigencia, siempre y cuando el monto total de las modificaciones no rebase en conjunto el 20% de los conceptos o volúmenes establecidos originalmente y el precio del servicio sea igual a lo pactado en un principio; en este supuesto no será necesario volver a solicitar la opinión sobre el cumplimiento de sus obligaciones fiscales ante el SAT.

IV. REQUISITOS PARA PARTICIPAR EN ESTA LICITACIÓN

De conformidad a lo dispuesto en el artículo 28, fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, solo podrán participar personas de nacionalidad mexicana.

Los licitantes **deberán adjuntar en el sistema CompraNet**, **en archivo PDF**, mismo que deberá contener los escritos señalados en los numerales 4.1.1. al 4.1.8., 4.2.1 al 4.2.3, 4.3.1. al 4.3.8., los cuales

deberán ser dirigidos a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

De manera enunciativa más no limitativa, se informa que **la falta de presentación de alguno de los documentos señalados** (en lo aplicable) **en los numerales 4.1.1. al 4.1.8, y del 4.2.1 al 4.2.3, será causa de desechamiento de la proposición,** y dará lugar a la descalificación del licitante **en virtud de que su incumplimiento afecta la solvencia de la proposición**.

En caso de que el proveedor se encuentre en el Registro Único de Proveedores y Contratistas (RUPC), deberá enviar copia de la cédula actualizada correspondiente.

4.1. DOCUMENTACIÓN LEGAL Y ADMINISTRATIVA

4.1.1. IDENTIFICACIÓN OFICIAL.

Conforme a lo dispuesto en el artículo 48 fracción X del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, para acreditar la identidad de la persona que firma las proposiciones, tratándose de persona física, copia de una identificación oficial vigente con fotografía (Cartilla del Servicio Militar Nacional, credencial para votar expedida por el Instituto Federal Electoral o Instituto Nacional Electoral, cédula profesional o pasaporte vigentes), o en caso de persona moral, de su representante legal.

4.1.2. ESCRITO DE ACREDITACIÓN DE LA PERSONALIDAD.

Escrito en el que el firmante manifieste, bajo protesta de decir verdad, que cuenta con capacidad legal para comprometerse por sí o que cuenta con facultades suficientes para comprometer a su representada, para lo cual los licitantes podrán utilizar el formato adjunto **(ANEXO No. 4 "FORMATO PARA ACREDITAR LA PERSONALIDAD DEL LICITANTE")**. Lo anterior de conformidad a lo dispuesto por la fracción V del artículo 48 del Reglamento de la Ley. Asimismo, deberá proporcionar una dirección de correo electrónico, en caso de contar con ella.

Nota: Las actividades comerciales o profesionales de los licitantes participantes, deberán estar relacionadas con el objeto del contrato a celebrarse.

En caso de que el proveedor se encuentre inscrito en el Registro Único de Proveedores y Contratistas (RUPC), deberá enviar copia de la cédula actualizada correspondiente.

4.1.3. DECLARACIÓN ESCRITA DE LOS ARTÍCULOS 50 Y 60 DE LA LEY.

Declaración escrita bajo protesta de decir verdad, de no encontrarse en los supuestos de los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, con firma autógrafa, para lo cual los licitantes podrán utilizar el formato adjunto **(ANEXO No. 5 FORMATO DE MANIFESTACIÓN DE NO ENCONTRARSE EN LOS SUPUESTOS DE LOS ARTÍCULOS 50 Y 60 DE LA LEY")**

Nota: En el caso de que dos o más personas presenten conjuntamente una proposición, será necesario que cada una de ellas presente la declaración descrita en el párrafo anterior.

4.1.4. DECLARACIÓN DE INTEGRIDAD.

Declaración escrita bajo protesta de decir verdad, en la que por sí mismos o a través de interpósita persona, se abstendrán de adoptar conductas, para que los servidores públicos de esta Comisión, induzcan o alteren las evaluaciones de las proposiciones, el resultado del procedimiento, u otros aspectos que otorguen condiciones más ventajosas con relación a los demás participantes, para lo

cual los licitantes podrán utilizar el formato adjunto **(ANEXO No. 6 "FORMATO DE DECLARACIÓN DE INTEGRIDAD")**

Nota: En el caso de que dos o más personas presenten conjuntamente una proposición, será necesario que cada una de ellas presente la declaración descrita en el párrafo anterior.

4.1.5. MANIFESTACIÓN DE LAS MIPYMES.

Un escrito bajo protesta de decir verdad (formato libre) mencionando, el tamaño y sector al cual pertenece la empresa a la que representa, debidamente firmado por el representante legal de la misma, de acuerdo a la tabla de estratificación señalada en el **ANEXO No. 8 "FORMATO DE ESTRATIFICACIÓN DE MICRO, PEQUEÑA O MEDIANA EMPRESA (MIPYMES)".**

En el caso de que la empresa a la cual se representa, no se encuentre dentro de la estratificación prevista en el **ANEXO No. 8,** por estar catalogada como empresa grande, bastará con manifestar por escrito que no se encuentran comprendidos en los rangos que establece el **ANEXO No. 8, "FORMATO DE ESTRATIFICACIÓN DE MICRO, PEQUEÑA O MEDIANA EMPRESA (MIPYMES)"** de la Convocatoria de esta licitación.

Nota: En el caso de que dos o más personas presenten conjuntamente una proposición, será necesario que cada una de ellas presente la declaración descrita en el párrafo anterior.

4.1.6. MANIFESTACIÓN DE NACIONALIDAD.

Manifestar por escrito bajo protesta de decir verdad, ser licitantes de nacionalidad mexicana, de conformidad con lo establecido en el artículo 35 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. Para lo anterior, los licitantes podrán utilizar el formato adjunto **(ANEXO No. 9 "FORMATO PARA LA MANIFESTACIÓN DE LA NACIONALIDAD DEL LICITANTE").**

Nota: En el caso de que dos o más personas presenten conjuntamente una proposición, será necesario que cada una de ellas presente la declaración descrita en el párrafo anterior.

4.1.7. COPIA DEL CONVENIO DE PARTICIPACIÓN CONJUNTA.

En caso de que dos o más personas presenten conjuntamente sus proposiciones para esta licitación, sin estar constituidas en una sociedad, o nueva sociedad; deberán enviar copia del convenio al que se hace alusión en el **punto 3.11.** de esta Convocatoria.

4.1.8. ESCRITO DE NO ACEPTACIÓN DE PROPOSICIONES

Los licitantes deberán presentar un escrito libre mediante el cual aceptan que se tendrán como no presentadas sus proposiciones y, en su caso, la documentación requerida por la Convocante, cuando el archivo electrónico en el que se contenga las proposiciones y/o demás información no pueda abrirse por tener algún virus informático o por cualquier otra causa ajena a la Convocante, así como, aquellas proposiciones que no se encuentren firmadas en los términos señalados en el **numeral 3.8.** de la presente convocatoria.

4.2. DOCUMENTACIÓN TÉCNICA-ECONÓMICA

Los licitantes que presenten sus propuestas, deberán dirigirlas a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros "CONDUSEF" de acuerdo a lo siguiente:

4.2.1. PROPUESTA TÉCNICA.

La propuesta técnica de cada Licitante deberá ser enviada en formato PDF a través de CompraNet, preferentemente en papel membretado del licitante, numerando cada hoja en forma consecutiva indicando el número total de hojas (ejemplo: 1 de 10, 2 de 10... etcétera), sin tachaduras ni enmendaduras, en idioma español; la cual deberá estar firmada autógrafamente en su última hoja por la persona que tenga facultades legales para ello. Dicha propuesta técnica deberá contener las especificaciones técnicas del servicio ofertado, indicando descripción y cantidad ofertada, conforme al contenido del **ANEXO No. 1** "**ANEXO TÉCNICO"** así como los documentos requeridos en el citado Anexo de esta Convocatoria. **No se aceptarán descripciones ni aceptaciones genéricas.**

El Licitante integrará en su propuesta para el **SERVICIO DE SERGURIDAD PERIMETRAL** la administración del proyecto, la configuración, el soporte, el mantenimiento, la operación, la gestión, el monitoreo y la transferencia de conocimiento necesarios sobre los servicios requeridos mencionados en el Anexo Técnico.

4.2.2. PROPUESTA ECONÓMICA.

La propuesta económica de cada Licitante deberá ser enviada en formato PDF a través de CompraNet, preferentemente en papel membretado del licitante, numerando cada hoja en forma consecutiva, indicando el número total de hojas (ejemplo: 1 de 10, 2 de 10... etcétera), sin tachaduras ni enmendaduras y con la firma autógrafa en su última hoja de la persona que tenga facultades legales para ello.

Deberá enviar el **ANEXO No. 2 "CÉDULA DE OFERTA ECONÓMICA"** tomando como base el formato que se anexa como parte integrante de esta Convocatoria. El precio deberá ser fijo, preciso y claro e indicarse en moneda nacional, anteponiendo el signo de pesos ($), expresado en número antes de IVA y en número y letra con IVA.

4.2.3. PROPOSICIONES FIRMADAS ELECTRÓNICAMENTE

Deberá enviar a través del Sistema CompraNet proposiciones con el archivo de firma digital válida.

De conformidad a lo establecido en los artículos 113 y 116 de la Ley General de Transparencia y Acceso a la Información Pública, los licitantes participantes deberán manifestar cuales son los documentos e información de su proposición que contienen información confidencial, reservada o comercial reservada, siempre que tengan el derecho de reservarse la información de conformidad con las disposiciones aplicables, explicando los motivos de la clasificación. En caso de resultar aplicable, presentar el escrito firmado por el representante legal del licitante, utilizando el **ANEXO No. 10 "MANIFESTACIÓN DE DOCUMENTOS E INFORMACIÓN DE SU PROPOSICIÓN QUE PODRÍAN CONTENER INFORMACIÓN CONFIDENCIAL".**

4.3. DOCUMENTACIÓN COMPLEMENTARIA QUE NO AFECTA LA SOLVENCIA

La documentación complementaria que no afecte la solvencia de la propuesta enviada por el licitante, o su omisión no será motivo de descalificación, según su elección será la siguiente:

4.3.1. ESCRITO DE CONFORMIDAD.

Manifestar por escrito, que leyó la convocatoria y su conformidad con el contenido de la misma, sus anexos y en su caso, de sus modificaciones, para lo cual los licitantes podrán utilizar el formato adjunto **ANEXO No. 7 "FORMATO DE ESCRITO DE CONFORMIDAD CON LA CONVOCATORIA".**

4.3.2. OPINIÓN POSITIVA DEL SAT.

El licitante deberá presentar el documento en el que conste la opinión positiva por parte de la Autoridad Fiscal competente, respecto del cumplimiento de sus obligaciones fiscales, de conformidad con el artículo 32-D del Código Fiscal de la Federación y con la Regla 2.1.31 de la Resolución Miscelánea Fiscal para 2021, publicada en el Diario Oficial de la Federación el día 29 de diciembre de 2020. Asimismo, deberán hacer público la opinión de cumplimento en términos de la Regla 2.1.27.

4.3.3. OPINIÓN POSITIVA DEL IMSS.

El licitante deberá presentar el documento vigente en el que conste la opinión positiva emitida por el Instituto Mexicano del Seguro Social, sobre el cumplimiento de obligaciones en materia de seguridad social, de conformidad con el artículo 32-D, primero, segundo, tercero y séptimo párrafos del Código Fiscal de la Federación y con la Regla 2.1.31 de la Resolución Miscelánea Fiscal para 2021, publicada en el Diario Oficial de la Federación el día 29 de diciembre de 2020 y con las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social del ACUERDO ACDO.SA1.HCT.101214/281.P.DIR y su Anexo Único, dictado por el H. Consejo Técnico, relativo a las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social.

4.3.4. CONSTANCIA DEL INFONAVIT.

El licitante deberá presentar la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos, documento vigente expedido por el Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT) de conformidad con el 32-D, primero, segundo, tercero y séptimo párrafos del Código Fiscal de la Federación y con la Regla 2.1.31 de la Resolución Miscelánea Fiscal para 2021, publicada en el Diario Oficial de la Federación el día 29 de diciembre de 2020.

4.3.5. MANIFIESTO DE NO DESEMPEÑAR EMPLEO, CARGO O COMISIÓN EN EL SERVICIO PÚBLICO

En este, el particular manifieste bajo protesta de decir verdad que no desempeña 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. En caso de que el proveedor sea persona moral, dichas manifestaciones deberán presentarse respecto a los socios o accionistas que ejerzan control sobre la sociedad, de conformidad con lo establecido en el artículo 49, fracción IX de Ley General de Responsabilidades Administrativas **ANEXO No. 16. "FORMATO NO DESEMPEÑAR EMPLEO, CARGO O COMISIÓN EN EL SERVICIO PÚBLICO".**

4.3.6. 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. Podrá utilizar el formato establecido en el **ANEXO No. 17 MANIFIESTO DE CONOCER EL PROTOCOLO DE ACTUACIÓN EN MATERIA DE CONTRATACIONES PÚBLICAS, OTORGAMIENTO Y PRÓRROGA DE LICENCIAS, PERMISOS, AUTORIZACIONES Y CONCESIONES**

4.3.7. ACUSE DEL MANIFIESTO DE AUSENCIA DE CONFLICTO DE INTERÉS

Acuse de la presentación del manifiesto en el que afirmen o nieguen los vínculos o relaciones de negocios, laborales, profesionales, personales o de parentesco por consanguinidad o afinidad hasta el cuarto grado que tengan la propia persona, con el o los servidores públicos a que se refiere el Anexo Segundo del PROTOCOLO DE ACTUACIÓN EN MATERIA DE CONTRATACIONES PÚBLICAS,

OTORGAMIENTO Y PRÓRROGA DE LICENCIAS, PERMISOS, AUTORIZACIONES Y CONCESIONES. El citado manifiesto lo formularán en a través de la dirección electrónica www.gob.mx/sfp, siendo este medio electrónico de comunicación el único para presentarlo **ANEXO No. 18. "ACUSE DEL MANIFIESTO PARA ACREDITAR LA AUSENCIA DE CONFLICTO DE INTERÉS"**

4.3.8. MANIFIESTO DE CONOCER Y REGISTRARSE EN EL MÓDULO DE FORMALIZACIÓN DE INSTRUMENTOS JURÍDICOS

Declaración escrita en papel membretado que conoce y se estará a lo establecido en los artículos Tercero, Cuarto y demás aplicables 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 Diario Oficial de la Federación el pasado 18 de septiembre de 2020, donde se determina que todo instrumento jurídico que derive de algún procedimiento de contratación realizado por las Dependencias y Entidades, se deberá utilizar la Firma Electrónica Avanzada (e.firma) que emite el Servicio de Administración Tributaria como medio de identificación. En consecuencia, en caso de resultar adjudicado el respectivo instrumento jurídico se suscribirá en el Módulo de Formalización de Instrumentos Jurídicos, por lo que deberá estar registrado. En la liga electrónica https://www.gob.mx/compranet/documentos/modulo-de-formalizacion-de-instrumentos-juridicos puede consultar el material de apoyo para su registro en el citado módulo. **ANEXO No. 19. "MANIFIESTO DE CONOCER Y REGISTRARSE EN EL MÓDULO DE FORMALIZACIÓN DE INSTRUMENTOS JURÍDICOS".**

V. APARTADO CRITERIO DE EVALUACIÓN DE LAS PROPOSICIONES.

5.1. CRITERIO DE EVALUACIÓN

El siguiente criterio se aplicará para la evaluación de las propuestas presentadas por los licitantes y para la adjudicación del pedido de conformidad con el artículo 36, de "La Ley":

5.2. CRITERIO DE EVALUACIÓN PUNTOS Y PORCENTAJES

Solamente serán evaluadas cualitativamente aquellas ofertas que cumplan cuantitativamente con las condiciones y los requerimientos legales, técnicos y económicos, establecidos en la presente convocatoria y sus anexos; así como lo derivado de sus modificaciones.

El área requirente del servicio verificará que las ofertas presentadas correspondan a las características y especificaciones del servicio solicitado, haciendo la valoración que corresponda a cada requisito solicitado, así como en su caso, a la omisión de los mismos, emitiendo el dictamen técnico correspondiente, el resultado de dicha revisión o análisis se dará a conocer en el fallo correspondiente.

El análisis detallado de la documentación administrativa y legal se realizará por conducto de la Dirección de Recursos Materiales y Servicios Generales.

El licitante deberá enviar por CompraNet, un archivo que contenga la documentación de los requerimientos técnicos de cada uno de los rubros que a continuación se describen.

Con fundamento en el artículo 29 fracción XIII y 36 párrafo tercero de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y al "Acuerdo por el que se emiten diversos

Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios y de Obras Públicas y Servicios relacionados con las mismas" publicado en el Diario Oficial de la Federación el 9 de septiembre de 2010, el presente procedimiento se adjudicará bajo el criterio de **puntos o porcentajes**, conforme al artículo Segundo, numeral Décimo Primero, Inciso A, de acuerdo a los siguientes rubros:

CONCEPTOS A EVALUAR	COMPROBANTES		PUNTOS MAXIMOS
I. CAPACIDAD DEL LICITANTE			**22**
a) Capacidad de los Recursos Humanos			**11**
El prestador del servicio cuenta con un Gerente del Centro de Operaciones de Seguridad con experiencia de 5 años en participación de proyectos de seguridad de la información.	El licitante deberá acreditar la siguiente certificación por el Gerente del Centro de Operaciones de Seguridad: • Copia simple de la certificación Certified Information Security Manager (CISM) Deberá presentar la siguiente documentación: • Curriculum vitae debidamente firmado del cual se desprenda el número de años con los que cuenta de experiencia en participación de proyectos de seguridad de la información.	**3**	**3**
El prestador del servicio cuenta con un Gerente del Centro de Operaciones de Seguridad con experiencia de 3 años en participación de proyectos de seguridad de la información.		**2**	
El prestador del servicio cuenta con un Gerente del Centro de Operaciones de Seguridad con experiencia de 1 año en participación de proyectos de seguridad de la información.		**1**	
El prestador del servicio cuenta con un Gerente del Centro de Operaciones de Seguridad que no tiene experiencia en participación de proyectos de seguridad de la información, o la misma es menor a 1 año.		**0**	
El prestador del servicio cuenta con un Coordinador Técnico del Centro de Operaciones de Seguridad con experiencia de 5 años en participación de proyectos de seguridad de la información.	El licitante deberá acreditar la siguiente certificación por el Coordinador Técnico del Centro de Operaciones de Seguridad: • Copia simple de la certificación Certified Information Systems Security Professional (CISSP). Deberá presentar la siguiente documentación: • Curriculum vitae debidamente firmado del cual se desprenda el número de años con los que cuenta de experiencia en participación de proyectos de seguridad de la información.	**3**	**3**
El prestador del servicio cuenta con un Coordinador Técnico del Centro de Operaciones de Seguridad con experiencia de 3 años en participación de proyectos de seguridad de la información.		**2**	
El prestador del servicio cuenta con un Coordinador Técnico del Centro de Operaciones de Seguridad con experiencia de 1 año en participación de proyectos de seguridad de la información.		**1**	
El prestador del servicio cuenta con un Coordinador Técnico del Centro de Operaciones de Seguridad que no tiene experiencia en participación de proyectos de seguridad de la información, o la misma es menor a 1 año.		**0**	
El prestador del servicio cuenta con un Especialista en Incidentes de Seguridad con		**3**	**3**

experiencia de 3 años en participación de proyectos de seguridad de la información.	El licitante debe acreditar una de las siguientes certificaciones para el Especialista en Incidentes de Seguridad: • Copia simple de la certificación EC-Council Certified Incident Handler (ECIH) • Copia simple de la certificación GIAC Certified Incident Handler (GCIH) Deberá presentar la siguiente documentación: • Curriculum vitae debidamente firmado del cual se desprenda el número de años con los que cuenta de experiencia en participación de proyectos de seguridad de la información.		
El prestador del servicio cuenta con un Especialista en Incidentes de Seguridad con experiencia de 2 años en participación de proyectos de seguridad de la información.		**2**	
El prestador del servicio cuenta con un Especialista en Incidentes de Seguridad con experiencia de 1 año en participación de proyectos de seguridad de la información.		**1**	
El prestador del servicio cuenta con un Especialista en Incidentes de Seguridad que no tiene experiencia en participación de proyectos de seguridad de la información, o la misma es menor a 1 año.		**0**	
El prestador del servicio cuenta con un Líder de Proyecto y con un operador de la mesa de servicio del Centro de Operaciones de Seguridad con experiencia de 5 años en participación de proyectos de seguridad de la información.	El licitante deberá acreditar al menos una de las siguientes certificaciones por el Líder de Proyecto: • Copia simple de la certificación EC-Council Project Management in IT Security (PMITS) • Copia simple de la certificación PMI Project Manager Professional (PMP) El licitante deberá acreditar la siguiente certificación por el Operador de la mesa de servicio del Centro de Operaciones de Seguridad: • ITIL v4 Foundation Certification Para ambos perfiles deberá presentar la siguiente documentación: • Curriculum vitae debidamente firmado del cual se desprenda el número de años con los que cuenta de experiencia en participación de proyectos de seguridad de la información.	**2**	**2**
El prestador del servicio cuenta con un Líder de Proyecto y con un operador de la mesa de servicio del Centro de Operaciones de Seguridad con experiencia de 3 años en participación de proyectos de seguridad de la información		**1**	
El prestador del servicio cuenta con un Líder de Proyecto y con un operador de la mesa de servicio del Centro de Operaciones de Seguridad que no tienen experiencia en participación de proyectos de seguridad de la información, o la misma es menor a 3 año.		**0**	
b) Capacidad de los recursos económicos y de equipamiento			**10**
El prestador del servicio acredita que el Centro de Operaciones de Seguridad (SOC) está afiliado al Foro de Respuesta a Incidentes de Seguridad (FIRST)	Para la acreditación de la afiliación a FIRST se debe adjuntar los documentos que lo avalen.	**1**	**1**

El prestador del servicio no acreditar que el Centro de Operaciones de Seguridad (SOC) está afiliado al Foro de Respuesta a Incidentes de Seguridad (FIRST).		**0**	
El licitante cuenta con más de 26 procesos certificados de la Certificación ISO/IEC 27001:2013, para garantizar la confidencialidad e integración de la información de CONDUSEF, a la cual tendrá acceso el licitante ganador	La acreditación de la certificación para cada uno de los procesos del SOC debe estar avalada por una entidad certificadora autorizada, y corresponder con el nombre del participante y encontrarse vigente, debiendo adjuntar el certificado que lo avala y en el que se encuentren listados los procesos certificados.	**4**	**4**
El licitante cuenta de 21 a 25 procesos certificados de la Certificación ISO/IEC 27001:2013, para garantizar la confidencialidad e integración de la información de CONDUSEF, a la cual tendrá acceso el licitante ganador		**3**	
El licitante cuenta de 16 a 20 procesos certificados de la Certificación ISO/IEC 27001:2013, para garantizar la confidencialidad e integración de la información de CONDUSEF, a la cual tendrá acceso el licitante ganador		**2**	
El licitante cuenta de 10 a 15 procesos certificados de la Certificación ISO/IEC 27001:2013, para garantizar la confidencialidad e integración de la información de CONDUSEF, a la cual tendrá acceso el licitante ganador		**1**	
El licitante cuenta de 0 a 9 procesos certificados de la Certificación ISO/IEC 27001:2013, para garantizar la confidencialidad e integración de la información de CONDUSEF, a la cual tendrá acceso el licitante ganador		**0**	
El licitante cuenta con más de 26 procesos certificados en las siguientes Certificaciones, ISO/IEC 20000-1:2018, ISO/IEC 22301:2019 e ISO/IEC 9001:2015.	La acreditación de la certificación para cada uno de los procesos del SOC debe estar avalada por una entidad certificadora autorizada, y corresponder con el nombre del participante y encontrarse vigente, debiendo adjuntar el certificado que lo avala y en el que se encuentren listados los procesos certificados.	**4**	**4**
El licitante cuenta de 21 a 25 procesos certificados en las siguientes Certificaciones, ISO/IEC 20000-1:2018, ISO/IEC 22301:2019 e ISO/IEC 9001:2015.		**3**	
El licitante cuenta de 16 a 20 procesos certificados en las siguientes Certificaciones, ISO/IEC 20000-1:2018, ISO/IEC 22301:2019 e ISO/IEC 9001:2015.		**2**	
El licitante cuenta de 10 a 15 procesos certificados en las siguientes Certificaciones, ISO/IEC 20000-1:2018, ISO/IEC 22301:2019 e ISO/IEC 9001:2015.		**1**	
El licitante cuenta de 0 a 9 procesos certificados en las siguientes Certificaciones, ISO/IEC 20000-1:2018, ISO/IEC 22301:2019 e ISO/IEC 9001:2015.		**0**	

El licitante cuenta con capacidad económica para cumplir con las obligaciones que se deriven del contrato de la presente licitación, acreditando ingresos netos con base a la declaración presentada del último ejercicio anual de al menos el 5% del monto total de su oferta económica	El licitante acreditará este rubro mediante la última declaración fiscal anual y la última declaración fiscal provisional del ISR, en ambos casos que hayan sido presentadas por el licitante ante la SHCP, las cuales deberán contener la cadena digital y/o sello digital de acuse de recibo	**1**	**1**
El licitante no cuenta con capacidad económica para cumplir con las obligaciones que se deriven del contrato de la presente licitación NO acreditando ingresos netos con base a la declaración presentada del último ejercicio anual de al menos el 5% del monto total de su oferta económica		**0**	
c) Participación de Discapacitados o empresas que cuenten con trabajadores con discapacidad.			**0.25**
El licitante acredita que cuenta con trabajadores con discapacidad.	Deberá presentar el aviso de alta de los trabajadores al régimen obligatorio del Instituto Mexicano del Seguro Social y una constancia que acredite que son personas con discapacidad en términos de lo previsto en la Ley General para la Inclusión de las Personas con Discapacidad.	**0.25**	**0.25**
El licitante no acredita que cuenta con trabajadores con discapacidad.		**0**	
d) Políticas y prácticas de equidad de género.			**0.25**
El licitante acredita que aplica políticas y prácticas de igualdad de género.	Deberá presentar certificación emitida por las autoridades y organismos facultados para tal efecto.	**0.25**	**0.25**
El licitante no acredita que aplica políticas y prácticas de igualdad de género.		**0**	
e) Participación de MIPYMES			**0.5**
El licitante acredita ser MIPYMES que produce bienes con innovación tecnológica que se utilizarán en la prestación del servicio	Se otorgará puntaje a la MIPYMES participante que produce bienes con innovación tecnológica conforme a la constancia correspondiente emitida por el Instituto Mexicano de la Propiedad Industrial, la cual no podrá tener una vigencia mayor a cinco años. El licitante deberá presentar copia del documento expedido por autoridad competente que determine su estratificación como micro, pequeña o mediana empresa, o bien, un escrito en el cual manifiesten bajo protesta de decir verdad, en el que determine su estratificación conforme a lo dispuesto en el artículo 34 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público	**.5**	**0.5**
El licitante no acredita ser MIPYMES que produce bienes con innovación tecnológica que se utilizarán en la prestación del servicio		**0**	

II. EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE			**18**
a) Experiencia del Licitante			**9**
El prestador de servicios acredita que cuenta con experiencia de 3 años o más proporcionando servicios similares a los solicitados en cantidad igual o mayor a los establecidos en esta convocatoria	El licitante para acreditar este rubro deberá presentar copia simple de contratos formalizados con empresas, dependencias y/o entidades de la Administración Pública. Los contratos no deberán tener más de 5 años de haber sido firmados y haber concluido a más tardar en junio de 2021 No serán considerados para evaluación aquellos contratos en lo que no se pueda identificar y verificar el objeto y la vigencia, así mismo aquellos cuyo objeto sea distinto a lo solicitado en el presente procedimiento	**9**	**9**
El prestador de servicios acredita que cuenta con experiencia de 2 años proporcionando servicios similares a los solicitados en cantidad igual o mayor a los establecidos en esta convocatoria		**8**	
El prestador de servicios acredita que cuenta con experiencia de 1 año proporcionando servicios similares a los solicitados en cantidad igual o mayor a los establecidos en esta convocatoria		**6**	
El prestador de servicios no acredita que cuenta con experiencia proporcionando servicios similares a los solicitados , o la misma es menor a 1 año.		**0**	
b) Especialidad del Licitante			**9**
El licitante presenta 5 contratos con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.	El licitante para acreditar este rubro deberá presentar copia simple de contratos formalizados con empresas, dependencias y/o entidades de la Administración Pública. Los contratos NO deberán tener más de 5 años de haber sido firmados y haber concluido a más tardar en junio de 2021. No serán considerados para evaluación aquellos contratos en lo que no se pueda identificar y verificar el objeto y la vigencia, así mismo aquellos cuyo objeto sea distinto a lo solicitado en el presente procedimiento	**9**	**9**
El licitante presenta 4 contratos con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.		**8**	
El licitante presenta 3 contratos con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.		**6**	
El licitante presenta 2 contratos con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.		**4**	
El licitante presenta 1 contrato con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.		**2**	
El licitante no presenta contratos con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.		**0**	

III. PROPUESTAS DE TRABAJO			**10**
El licitante presenta la metodología para la prestación del servicio, conforme a las especificaciones técnicas, que deberán estar alineadas a los procesos certificados ISO/IEC 27001:2013	El licitante deberá presentar la metodología para la prestación del servicio, conforme a las especificaciones técnicas alineadas a los procesos certificados ISO/IEC 27001:2013	**6**	**6**
El licitante no presenta la metodología para la prestación del servicio, conforme a las especificaciones técnicas..		**0**	
El licitante presenta el plan de trabajo para la prestación del servicio conforme a las especificaciones técnicas solicitadas.	El licitante deberá presentar un Plan de Trabajo detallado (Calendario de actividades, con las etapas de instalación, pruebas, entrega del servicio a operación y demás actividades relacionadas para poder proporcionar el servicio) El Plan deberá estar firmado por el Líder de Proyecto, debiendo anexar su cédula profesional y certificaciones vigentes.	**3**	**3**
El licitante no presenta el plan de trabajo para la prestación del servicio conforme a las especificaciones técnicas solicitadas.		**0**	
El licitante presenta el esquema estructural de la organización de los recursos humanos necesarios para cumplir con las obligaciones del servicio conforme a las especificaciones técnicas solicitadas.	El licitante deberá presentar el esquema estructural de la organización de los recursos humanos, que prestarán el servicio. Matriz de escalación.	**1**	**1**
El licitante no presenta el esquema estructural de la organización de los recursos humanos necesarios para cumplir con las obligaciones del servicio conforme a las especificaciones técnicas solicitadas.		**0**	
IV. CUMPLIMIENTOS DE LOS CONTRATOS			**10**
El licitante cuenta con 5 contratos satisfactoriamente cumplidos con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.	El licitante deberá presentar el documento en el conste la cancelación de la garantía de cumplimiento respectivo o la manifestación expresa de la contratante sobre el cumplimiento total de las obligaciones contractuales, respecto de los contratos presentados en el rubro de Especialidad.	**10**	**10**
El licitante cuenta con 4 contratos satisfactoriamente cumplidos con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.		**8**	
El licitante cuenta con 3 contratos satisfactoriamente cumplidos con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.		**6**	
El licitante cuenta con 2 contratos satisfactoriamente cumplido con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.		**4**	
El licitante cuenta con 1 contrato satisfactoriamente cumplido con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.		**2**	

El licitante no cuenta con contratos satisfactoriamente cumplidos con las características específicas y en condiciones similares a las establecidas en la presente convocatoria.		**0**	
TOTAL DE LA PROPUESTA TÉCNICA			**60**

El puntaje mínimo para considerar que una propuesta técnica es solvente y por tanto, no ser desechada y ser susceptible de pasar a la evaluación económica será de cuando menos **45 puntos de los 60 puntos** que se pueden obtener en su evaluación.

Será requisito indispensable para la evaluación por puntos que los licitantes presenten la totalidad de los documentos solicitados en la convocatoria cuya presentación es de carácter obligatorio, por lo que, si le falta alguno de ellos, su propuesta será desechada.

Además, será requisito indispensable, para la evaluación de las propuestas que la documentación presentada por los licitantes sea legible, en caso contrario, se tendrá por no presentado dicho documento.

La ponderación técnico-económica **(PTj)** con el que se determinará la proposición solvente que será susceptible de ser adjudicada con el contrato, por haber cumplido con los requisitos exigidos y cuyo resultado sea el de mayor puntuación, se calculará con la fórmula:

PTj = TPT + PPE

EN DONDE:

PTj = Puntuación o unidades porcentuales totales de la proposición
TPT = Total de puntuación o unidades porcentuales asignados a la propuesta técnica
PPE = Total de puntuación o unidades porcentuales asignados a la propuesta económica
J = 1, 2,....,n. Representa todas las demás proposiciones determinadas como solventes como resultado de la evaluación

EVALUACIÓN ECONÓMICA.

PPE = MPemb x 40/MPi
EN DONDE:
PPE = Total de puntuación o unidades porcentuales asignados a la propuesta económica
MPEMB = Monto de la propuesta económica más baja
MPi = Monto de la i-ésima propuesta económica
40 = 40% (PONDERADOR DE LA PROPUESTA ECONÓMICA)

Se considerará que la propuesta del participante cubre con las características de los servicios solicitados, **si los conceptos que integran su propuesta cumplen** con los requisitos solicitados en esta convocatoria y con las especificaciones técnicas establecidas en el **ANEXO No. 1. "ANEXO TÉCNICO".**

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

En caso de que se presente un error de cálculo en las propuestas presentadas, sólo habrá lugar a su rectificación por parte de "LA CONDUSEF", cuando la corrección no implique la modificación de los precios unitarios. **Por lo que en caso de presentarse discrepancia entre las cantidades escritas con letra y con número, prevalecerá la cantidad con letra.**

Si en esta Licitación se presentara igualdad de condiciones entre las propuestas de dos o más licitantes, con fundamento en lo señalado en el Artículo 36, Bis de "La Ley", se dará preferencia a las personas que integren el sector de micro, pequeñas y medianas empresas nacionales.

En caso de que cumplidos los requisitos de la Licitación se tengan precios iguales, la adjudicación se efectuará a favor del licitante que resulte ganador del sorteo manual por insaculación que se desarrollará en el propio acto de fallo, el cual consistirá en la participación de un boleto por cada propuesta que resulte empatada, los que serán depositados en una urna, de la que se extraerá el boleto del licitante ganador, con fundamento en el artículo 54, del "Reglamento".

5.3. REQUISITOS CUYO INCUMPLIMIENTO NO AFECTA LA SOLVENCIA DE LA PROPOSICIÓN.

a) Proponer un plazo de entrega menor al solicitado en esta convocatoria.
b) El omitir aspectos que puedan ser cubiertos con información contenida en la propia propuesta técnica o económica.
c) El no observar los formatos establecidos en esta convocatoria, siempre y cuando la información requerida en ellos sea proporcionada de manera clara y en su totalidad.
d) No presentar su proposición y documentación requerida en papel membretado del licitante.
e) El no presentar acuse de la documentación que entrega el licitante.
f) Entregar la documentación distinta a las proposiciones técnicas y económicas fuera del sobre cerrado que debe contener a estas últimas.

5.4. CAUSALES POR LAS QUE SE DESECHARÁN PROPOSICIONES Y SE DESCALIFICARÁN A LOS LICITANTES.

a) **El enviar a través del Sistema CompraNet proposiciones carezcan de firma electrónica como medio de identificación** bajo los mecanismos establecidos por la SHCP o cuando su **certificado aparezca como NO VÁLIDO** en la plataforma CompraNet, **aún y cuando éstas contengan firma autógrafa** o bien el archivo esté dañado.
b) La **falta** de cualquiera de los documentos solicitados o su incorrecta o diferente redacción que varíe el significado, y/o el **incumplimiento** u **omisión** de cualquiera de los requisitos que **afecten la solvencia de la propuesta** tanto técnica como económica, o información establecida en esta convocatoria.
c) La comprobación de que algún licitante ha acordado con uno u otros elevar el precio del servicio, o cualquier otro acuerdo que tenga como fin obtener ventaja sobre los demás licitantes.
d) En los casos en que las proposiciones presenten información que cause confusión o cree una situación de incertidumbre o inconsistencia, o presente contradicción entre los diversos documentos de la oferta, la proposición será considerada insolvente y será desechada en el Fallo.
e) Cuando los documentos que exhiban los Licitantes no sean legibles imposibilitando el análisis integral de la propuesta, y esto conlleve a un faltante o carencia de información que afecte su solvencia.

f) 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.
g) Por cualquier otra violación a las disposiciones de la ley, "El Reglamento" u otra disposición jurídica aplicable que deba cumplir y que se considere indispensable para evaluar la proposición y que afecte directamente su solvencia.
h) Las establecidas en el cuerpo de la presente convocatoria y sus anexos.

VI. DOCUMENTOS Y DATOS QUE DEBEN DE PRESENTAR LOS LICITANTES.

Las propuestas deberán cumplir con los requisitos señalados en el apartado IV REQUISITOS PARA PARTICIPAR EN ESTA LICITACIÓN solicitados en los presentes requisitos de participación.

De igual forma, al final de la presente Convocatoria se encuentra un formato **(ANEXO No. 11 "DOCUMENTOS QUE DEBERÁN INTEGRAR LA PROPUESTA DEL LICITANTE")** de manera informativa, con la relación de los documentos y/o archivos que deberán presentar los licitantes.

La falta de presentación del formato no será motivo de descalificación y se extenderá un acuse de recibo de la documentación que entregue el licitante en dicho acto.

VII. INCONFORMIDADES.

Los licitantes podrán interponer inconformidad ante la Secretaría de la Función Pública, de conformidad con los artículos 65 y 66 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público en:

- **SECRETARÍA DE LA FUNCIÓN PÚBLICA:** INSURGENTES SUR 1735, COLONIA GUADALUPE INN, ALCALDÍA ÁLVARO OBREGÓN, CÓDIGO POSTAL 01020, CIUDAD DE MÉXICO, TELÉFONO. 2000-3000, o bien en;

- **EL ÓRGANO INTERNO DE CONTROL EN LA CONDUSEF:** INSURGENTES SUR 762, COLONIA DEL VALLE, PISO 9, ALCALDÍA BENITO JÚAREZ, CÓDIGO POSTAL 03100, CIUDAD DE MÉXICO, TELÉFONO 5448-7000, EXTENSIÓN 6175.

Lo establecido en dichos artículos, es sin perjuicio de que las personas interesadas previamente manifiesten a la Secretaría de la Función Pública las irregularidades que a su juicio se hayan cometido en este procedimiento, a fin de que las mismas se corrijan.

La inconformidad será presentada, a elección del licitante, por escrito o a través de medios remotos de CompraNet en contra de los actos que contravengan las disposiciones que rigen las materias objeto de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

7.1. CONTROVERSIAS.

Las controversias que se susciten con motivo de esta licitación, se resolverán de acuerdo al Título Sexto, Capítulo Primero de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En el supuesto de que se suscite alguna controversia relacionada con la información enviada a través de CompraNet, la autoridad competente podrá solicitar a la Secretaría de la Función Pública

exhiba los archivos electrónicos que obren en CompraNet, así como la impresión de éstos debidamente certificados, a efecto de desahogar las pruebas a que haya lugar, conforme a las disposiciones adjetivas que resulten aplicables.

VIII. FORMATOS QUE AGILICEN LA PRESENTACIÓN DE PROPOSICIONES.

Se considerarán como parte integrante de la presente Convocatoria los anexos que a continuación se señalan:

NO. ANEXO	DESCRIPCIÓN DEL ANEXO
ANEXO No. 1	ANEXO TÉCNICO.
ANEXO No. 2	CÉDULA DE OFERTA ECONÓMICA.
ANEXO No. 3	FORMATO DE ESCRITO PARA FORMULAR PREGUNTAS.
ANEXO No. 4	FORMATO PARA ACREDITAR LA PERSONALIDAD DEL LICITANTE.
ANEXO NO. 5	FORMATO DE MANIFESTACIÓN DE NO ENCONTRARSE EN LOS SUPUESTOS DE LOS ARTÍCULOS 50 Y 60 ANTEPENÚLTIMO PÁRRAFO DE LA LEY.
ANEXO No. 6	FORMATO DE DECLARACIÓN DE INTEGRIDAD.
ANEXO No. 7	FORMATO DE ESCRITO DE CONFORMIDAD CON LA CONVOCATORIA.
ANEXO No. 8	FORMATO DE ESTRATIFICACIÓN DE MICRO, PEQUEÑA O MEDIANA EMPRESA (MIPYMES).
ANEXO No. 9	FORMATO PARA LA MANIFESTACIÓN DE LA NACIONALIDAD DEL LICITANTE.
ANEXO No. 10	MANIFESTACIÓN DE DOCUMENTOS E INFORMACIÓN DE SU PROPOSICIÓN QUE PODRÍAN CONTENER INFORMACIÓN CONFIDENCIAL.
ANEXO No. 11	DOCUMENTOS QUE DEBERÁN INTEGRAR LA PROPUESTA DEL LICITANTE.
ANEXO No. 12	ENCUESTA DE TRANSPARENCIA.
ANEXO No. 13	MODELO DE CONTRATO.
ANEXO No. 14	FORMATO CON EL TEXTO QUE DEBE CONTENER LA GARANTÍA DE CUMPLIMIENTO.
ANEXO No. 15	NOTA INFORMATIVA PARA PARTICIPANTES DE PAÍSES MIEMBROS DE LA OCDE.
ANEXO No. 16	MANIFIESTO DE NO DESEMPEÑAR EMPLEO, CARGO O COMISIÓN EN EL SERVICIO PÚBLICO.
ANEXO No. 17	MANIFIESTO DE CONOCER EL PROTOCOLO DE ACTUACIÓN EN MATERIA DE CONTRATACIONES PÚBLICAS, OTORGAMIENTO Y PRÓRROGA DE LICENCIAS, PERMISOS, AUTORIZACIONES Y CONCESIONES
ANEXO No. 18	ACUSE DEL MANIFIESTO PARA ACREDITAR LA AUSENCIA DE CONFLICTO DE INTERÉS.
ANEXO No. 19	MANIFIESTO DE CONOCER Y REGISTRARSE EN EL MÓDULO DE FORMALIZACIÓN DE INSTRUMENTOS JURÍDICOS.

NOTA: Los formatos del **ANEXO No. 12** ENCUESTA DE TRANSPARENCIA, **No. 13** MODELO DE CONTRATO, **No. 15** NOTA INFORMATIVA PARA PARTICIPANTES DE PAÍSES MIEMBROS DE LA OCDE y **No. 17** PROTOCOLO DE ACTUACIÓN EN MATERIA DE CONTRATACIONES PÚBLICAS, OTORGAMIENTO Y PRÓRROGA DE LICENCIAS, PERMISOS, AUTORIZACIONES Y CONCESIONES, son de carácter exclusivamente informativo.

IX. ASPECTOS GENERALES.

9.1. CANCELACIÓN DE LA LICITACIÓN.

Con fundamento en el artículo 38 penúltimo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, "LA CONDUSEF" podrá cancelar la licitación, partidas o conceptos incluidos en esta Convocatoria, cuando:

A) Se presente caso fortuito;
B) Se presente fuerza mayor;
C) Existan circunstancias justificadas que extingan la necesidad para la contratación del servicio, y
D) De continuarse con el procedimiento se pudiera ocasionar un daño o perjuicio a "LA CONDUSEF".

9.2. CAUSALES PARA DECLARAR DESIERTA LA LICITACIÓN.

Con fundamento en el artículo 38 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, se podrá declarar desierta la licitación cuando:

A) No se reciba la propuesta de al menos un licitante en el acto de presentación de proposiciones.
B) Ninguna de las proposiciones presentadas reúna los requisitos de la Convocatoria de la licitación.
C) Derivado de la evaluación de las propuestas se compruebe que estás rebasan el presupuesto autorizado para realizar la contratación correspondiente y no sea factible realizar la reducción de bienes o servicios conforme a lo señalado en el artículo 56 de "El Reglamento".

9.3. PENAS CONVENCIONALES, DEDUCTIVAS Y PENAS CONTRACTUALES.

El Proveedor del Servicio deberá cumplir con la entrega en tiempo y forma de los siguientes requerimientos para garantizar la continua operación de la nueva infraestructura de la CONDUSEF, de lo contrario con fundamento a lo dispuesto en el Artículos 53 y 53-Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, se hará acreedor a las penas convencionales o deducciones correspondientes.

9.3.1. PENAS CONVENCIONALES

Las Penas Convencionales se aplicarán por cada día natural de atraso en los plazos indicados para la entrega de cada requerimiento; los plazos establecidos serán contabilizados como días naturales:

CONCEPTO	PLAZOS ESTABLECIDOS	REQUERIMIENTO	PENALIZACIÓN
Entrada en operación del servicio conforme a lo establecido en este anexo técnico	Al día hábil siguiente a la notificación del fallo	Entrada en operación del servicio	2 al millar por cada día de atraso del monto total de la facturación mensual
Entrega de Plan de Trabajo de Implementación de Servicios	10 días hábiles posteriores al inicio de la vigencia del contrato	Plan de Trabajo de Implementación de Servicios	2 al millar por cada 48 horas de atraso del monto total del contrato
Entrega de la Memoria Técnica inicial	60 días naturales posteriores a la entrada en operación del servicio	Memoria Técnica Inicial	2 al millar por cada día de atraso del monto

			total de la facturación mensual
Entrega de la Memoria Técnica final	60 días naturales antes del término del servicio	Memoria Técnica Final	2 al millar por cada día de atraso del monto total de la facturación mensual
Entrega final del desarrollo del proyecto	15 días naturales después de la implementación del servicio	Entregable final del desarrollo del proyecto	2 al millar por cada día hábil de atraso
Entrega de reportes:	Cada mes durante los primeros 7 días hábiles de cada mes siguiente al mes que concluye	De administración de configuraciones y cambios en la infraestructura.	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios.
Entrega de reportes	Se entregarán dentro de los primeros 7 días hábiles de cada mes siguiente al mes que concluye	Reporte de atención y solución de fallas. Indicando los tipos de fallas, su tiempo de reparación (TTR), si afectan o no la disponibilidad. Informes de Gestión del SOC (Mesa de Ayuda)	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios.
Entrega de reportes	Se entregarán dentro de los primeros 7 días hábiles de cada mes siguiente al mes que concluye	Reportes de las soluciones de seguridad con las que cuenta la convocante ·Métricas de desempeño (%procesador, %memoria, %disco duro, donde apliquen) ·Puertos tcp/udp y protocolos más utilizados ·Top 20 de las aplicaciones utilizadas o pasando a través de la solución ·Top 20 ip's más bloqueadas ·Top 20 de las firmas de ataque más vistas ·Top de los 20 usuarios o cuentas, según tráfico y tiempo de conexión ·Top de las 20 páginas, según número de consultas y tiempo de conexiones ·Consumo de ancho de banda por tipo de protocolo.	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios.
Entrega de reportes	Se entregarán dentro de los primeros 7 días hábiles de cada mes	Reporte de actividades sospechosas e incidentes de seguridad mensuales	2 al millar por cada día de atraso sobre el importe de la

	siguiente al mes que concluye		facturación total mensual de los servicios.
Reporte de Incidente de Seguridad solicitado por la CONDUSEF	Se entregará dentro de los primeros 5 días hábiles posteriores a su solicitud por parte de la CONDUSEF	Reporte de un Incidente de Seguridad	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios.
Entrega de nuevos Servicios de Seguridad	Se entregarán dentro de los primeros 45 días naturales a partir de la solicitud formal	Entrega de nuevos Servicios de Seguridad	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios.

9.3.2. DEDUCTIVAS

En caso de que se presenten fallas en la prestación del servicio derivadas del incumplimiento parcial o prestación deficiente del mismo, se aplicarán las deducciones siguientes:

CONCEPTO	NIVEL DEL SERVICIO	DEDUCTIVA	MÁXIMO PERMITIDO
Monitoreo del SOC	Cuando no se cumplan con los niveles mínimos solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	2 al millar por hora de indisponibilidad sobre el nivel de servicio establecido y con base al importe de la factura total mensual.	Con un máximo de 3 eventos mensuales.
Atención a requerimientos de configuraciones de seguridad	Cuando no se cumpla con el tiempo máximo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada hora natural de atraso del monto total de la facturación mensual de los servicios correspondientes.	Con un máximo de 5 eventos mensuales por servicio.
Tiempo de solución a incidentes de seguridad	Cuando no se cumpla con los tiempos establecidos por prioridad solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada minuto de afectación a los servicios y/o aplicaciones y/o por atraso para la solución del mismo, sobre el monto total de la facturación mensual de los servicios correspondientes.	Con un máximo de 1 eventos mensual por servicio
Licenciamiento y entrega de actualizaciones	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada día hábil de atraso con base al monto total de la facturación mensual de la solución involucrada	Para todos los dispositivos del servicio cuando el fabricante emita una nueva licencia del software
Control de accesos a páginas web, URL's o aplicaciones.	Cuando no se cumpla con el tiempo máximo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar sobre el total de la facturación mensual de la solución involucrada, por cada día de atraso para la categorización, re categorización, bloqueo o acceso a los sitios o categorías web,	Con un máximo de 3 eventos mensuales por servicio

Accesos de usuarios o equipos no autorizados en el mes.	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	5 al millar por cada acceso de usuarios no autorizados con base al monto total de la facturación mensual de la solución involucrada.	• Para la solución de seguridad 5 accesos no autorizados máximo, durante 3 meses consecutivos • Para la solución de seguridad medio y estándar 10 accesos no autorizados máximo, durante 3 meses consecutivos
Control de cambios de las soluciones de seguridad.	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	2 al millar por cada hora natural de atraso con base al monto total de la facturación mensual de la solución involucrada.	Aplica para: Cualquier dispositivo de seguridad. Cuando se solicite un control de cambios en algún componente de las soluciones antes mencionadas.
Control de acceso	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	2 al millar por cada acceso no autorizado con base al monto total de la facturación mensual de la solución involucrada.	Aplica para: Cualquier dispositivo de seguridad Cuando se detecte algún acceso no autorizado por CONDUSEF.
Dictamen de actividades sospechosas	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada hora hábil de atraso con base al monto total de la facturación mensual de la solución involucrada	Aplica para: Cualquier dispositivo de seguridad cuando se detecte alguna actividad sospechosa.
Manejo de incidentes de día cero.	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada día de atraso del monto total de la facturación mensual de los servicios correspondientes al servicio(s) afectado(s)	Aplica para: Cualquier dispositivo de seguridad cuando se detecte algún incidente de día cero.
Personal Certificado para soportar los servicios.	Cuando no se notifique del cambio de los Recursos Humanos solicitados (Gestión del Personal Técnico) solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	2 al millar por cada día de indisponibilidad sobre el monto total de la facturación mensual de los servicios correspondientes al servicio(s) afectado(s)	Aplica para: SOC y personal en sitio

9.3.3. SANCIONES.

En su caso, se aplicarán las sanciones a que se refieren los artículos 59 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

9.3.4. CONDICIONES GENERALES.

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

No podrán participar las personas que se encuentren en los supuestos señalados en los artículos 50 y 60 penúltimo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

LA DIRECTORA DE RECURSOS MATERIALES
Y SERVICIOS GENERALES

GERTRUDIS RODRÍGUEZ GONZÁLEZ

ANEXO No. 1
ANEXO TÉCNICO

1. OBJETIVO

El objetivo del presente documento es establecer los alcances y lineamientos técnicos para la continuidad operativa del **SERVICIO DE SEGURIDAD PERIMETRAL**, con el fin de que se siga proporcionando la conectividad digital segura entre las Oficinas Centrales de la CONDUSEF y sus Unidades de Atención distribuidas en todo el país, garantizando la operación eficaz, segura, oportuna y eficiente de las operaciones de esta Comisión Nacional.

2. SERVICIOS REQUERIDOS

Contar con un proveedor de servicios que proporcione a CONDUSEF el servicio específico de la seguridad perimetral de acuerdo a lo descrito en el presente anexo.

Los Servicios de Seguridad Perimetral requeridos son los siguientes:

1. Servicio de filtrado Web.
2. Servicio de un Sistema de Prevención contra Intrusos (IPS).
3. Servicio de Protección para Aplicaciones Web (WAF).
4. Servicio de Antispam.
5. Servicio de Seguridad en la Resolución de Nombres de Dominio (DNS).
6. Servicio de Seguridad contra amenazas en el dispositivo final.
7. Servicio de Respuesta y Visibilidad Unificada de Incidentes de Seguridad.

3. BENEFICIOS ESPERADOS

El Proveedor del Servicio para garantizar la correcta operación del **SERVICIO DE SEGURIDAD PERIMETRAL** de los servicios requeridos que se mencionan en el Anexo Técnico, debe mantener el cumplimiento de los siguientes puntos:

a) Contar con una arquitectura física de seguridad flexible y escalable que permita el aprovisionamiento de los servicios que se requieren para reaccionar oportunamente a las exigencias que representa el seguimiento y atención de los servicios que demanda CONDUSEF.

b) Mejorar los tiempos de atención y solución de incidentes en caso de falla.

c) Disponer de un contrato de Servicios Administrados que defina niveles de servicio claro y acorde a las necesidades de la Comisión.

d) Contar con la continua administración, operación, soporte y monitoreo de la infraestructura de Seguridad.

e) Contar con niveles de servicio establecidos por CONDUSEF, con planes de mejora continua, y entregables acordados en su forma periodicidad y alcance desde el inicio del contrato.

f) Contar con un monitoreo que permita visualizar el estado del servicio e identificar fallas de forma proactiva y reactiva tanto, a través del envío de alarmas vía correo electrónico y/o mensaje de texto.

4. ALCANCE

El Proveedor del Servicio integrará en su propuesta para el **SERVICIO DE SERGURIDAD PERIMETRAL** la administración del proyecto, la configuración, el soporte, el mantenimiento, la operación, la gestión, el monitoreo y la transferencia de conocimiento necesarios sobre los servicios requeridos mencionados en el Anexo Técnico.
Todos los recursos humanos y materiales necesarios para proporcionar los servicios descritos en este Anexo Técnico serán por cuenta del Proveedor, así como cualquier daño derivado de percances y accidentes en las Oficinas Centrales de la CONDUSEF durante la instalación, puesta a punto y cambio en los servicios a lo largo de la vigencia del contrato.
Todas las características técnicas descritas son enunciativas más no limitativas.
El **SERVICIO DE SERGURIDAD PERIMETRAL**, que en lo sucesivo se denominará como "el Servicio", incluye de manera general:

a) Todos los equipos para la prestación del servicio deberán de ser nuevos.

b) El abastecimiento, soporte técnico y mantenimiento correctivo de los equipos (hardware), partes, accesorios y/o refacciones, necesarios para la prestación del servicio.

c) El abastecimiento, soporte técnico y actualizaciones del software necesario para la prestación del servicio.

d) El abastecimiento, soporte técnico y mantenimiento preventivo y correctivo de los enlaces, necesarios para la prestación del servicio.

e) El suministro y/o sustitución de todos los materiales, elementos, consumibles y refacciones para la prestación del servicio.

f) La correcta instalación, configuración, migración, puesta a punto y/o portabilidad, de todos y cada uno de los elementos de hardware, software necesario para la prestación del servicio.

g) La migración y adecuación de políticas de operación y seguridad.

h) El respaldo de información.

ACTUALIZACIÓN TECNOLÓGICA

Durante la vigencia del contrato, en caso de obsolescencia o cualquier causa que impida brindar la continuidad del Servicio con los niveles de servicio solicitados por esta Comisión Nacional, los equipos o soluciones utilizados por el Proveedor del Servicio, y en general todo el equipamiento, software y licenciamiento que incluya el Proveedor del Servicio en su propuesta, deberá ser sustituido por uno de nueva tecnología, sin costo adicional para esta Comisión Nacional.

5. VIGENCIA DEL SERVICIO

La vigencia del servicio será a partir del día hábil siguiente a la notificación del fallo al 31 de agosto de 2024.
A partir del inicio de la vigencia del contrato, el Proveedor del Servicio iniciará las actividades necesarias para dar el Servicio.
El Servicio será proporcionado en el siguiente domicilio:

Insurgentes sur no. 762
Col. Del valle
Alcaldía Benito Juárez
C.P. 03100

Ciudad de México

Durante la vigencia del contrato se podrá reubicar la localidad para la prestación del Servicio, sin que esto represente ningún tipo de costo adicional para la CONDUSEF.
Cuando se requiera trasladar equipo propiedad del proveedor, este deberá considerar la logística correspondiente y absorber los gastos necesarios, incluyendo sus empaques y embalajes.
El traslado de equipo propiedad de la CONDUSEF, será con recursos propios.

6. SERVICIO DE SEGURIDAD PERIMETRAL

6.1. SERVICIO DE FILTRADO WEB

Se requiere de un servicio de filtrado de contenido y análisis de amenazas en la red que incluya las funciones de protección contra amenazas, anti-malware y filtrado de URL de al menos.
El servicio debe integrar mecanismos de segmentación y filtrado a la arquitectura de red tanto en el perímetro como en los centros de datos para definir políticas de control de seguridad que permitan controlar el tráfico a partir de las políticas de seguridad de la CONDUSEF. Adicionalmente, el servicio deberá brindar la capacidad de visibilidad sobre los eventos de seguridad, indicadores de compromiso (IOCs) y archivos maliciosos identificados en el tráfico.
El servicio debe garantizar mecanismos de alta disponibilidad en el despliegue de los equipos, es decir, redundancia activa-pasiva y activa-activa. Adicionalmente, el fabricante deberá garantizar mecanismos de reemplazo de partes de hardware en un esquema 7x24x4.

Requerimientos generales

a) Operación en hardware de propósito específico y con sistema operativo propietario, ambos desarrollados íntegramente por el mismo fabricante.

b) Incluir todos los accesorios y cables necesarios para la total instalación y puesta en operación.

c) El servicio debe tener la capacidad de integrarse de forma nativa, sin ningún desarrollo adicional al Servicio de Respuesta y Visibilidad Unificada de Incidentes de Seguridad especificado al final de este anexo para poder orquestar y responder a incidentes de seguridad.

Funciones

- Permitir únicamente el tráfico explícitamente autorizado por CONDUSEF hacia Internet.
- Detección de sitios web distribuidos en categorías preconfiguradas, incluidas las siguientes:
  - Banners y publicidad.
  - Narcóticos.
  - Sitios de almacenamiento personal de archivos y datos.
  - Sitios de armas y municiones.
  - Sitios de chateo por Internet.
  - Sitios de compartido de archivos P2P.
  - Sitios de compras y subastas.
  - Sitios de contenido adulto o sexual.
  - Sitios de descarga de audio.
  - Sitios de descarga de software gratis o pago.
  - Sitios de hackers.
  - Sitios de ilegales.
  - Sitios de juegos o apuestas en línea.
  - Sitios de proxies públicos usados para evitar proxies corporativos (Proxy avoidance).
  - Sitios de radio y televisión en línea.
  - Sitios hacia los cuales los spyware, addware y keyloggers envían los datos recolectados de las víctimas.

    - Sitios o páginas de correo electrónico vía Web.
    - Sitios personales y bloggers.
    - Sitios que contienen video o audio (streaming), aunque pertenezcan a otra categoría, tal como noticias, deportes, en base a filtrado por tipo de archivo.
    - Sitios sobre alcohol y tabaco.
    - Sitios sobre violencia y terrorismo.
- Las URL's deberán estar clasificadas según su contenido diario, es decir, en el caso de que el contenido de una URL sea cambiado, máximo en 24 horas naturales deberá estar reclasificada bajo la categoría que refleje su nuevo contenido.
- Mecanismo que permitan al administrador, negar o permitir URL's específicos, que no necesariamente están definidos en una categoría, para poder ser utilizados en la definición de nuevas reglas.
- Acceso a páginas de ciertas categorías, pero bloquear el intento de ciertos tipos de archivo (tales como video, audio, archivos comprimidos, ejecutables, documentos u otros.) desde dichas páginas.
- Técnicas para detectar código malicioso en archivos que se estén descargando y cancelar la descarga, informándolo al usuario.
- Opción de modificar la notificación de bloqueo, y redireccionar al usuario a otra página Bloquear granularmente sitios basados en Web 2.0.
- Identificar y bloquear herramientas de "proxy bypass" sobre protocolos estándar y no estándar (sin la necesidad de instalar un agente en los hosts o licencias adicionales).
- Bloquear Malware sobre sitios Web.
- Método dinámico para la categorización de los sitios Web existentes y nuevos sitios emergentes.
- Inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL. El módulo de Filtrado de URL debe hacer dicha inspección como si fuera texto claro, sin la necesidad de utilizar herramientas de terceros, servidores, licencias adicionales o agentes.
- Integración con AD o LDAP.
- Cifrar las autenticaciones de usuarios con: LDAP y AD.
- Throughput con las funcionalidades de protección contra amenazas, anti-malware y filtrado de URL de al menos 14Gbps con paquetes de 1024 Bytes.
- Integración con sistemas de inteligencia del fabricante y terceros que alimenten al sistema de información actualizada sobre direcciones IP, URLs y nombres de dominio maliciosos, listas negras y listas blancas.

Características técnicas

La solución deberá incluir y operar al menos con las siguientes características:

- 8 puertos SFP
- 8 puertos SFP+
- Al menos un puerto de management
- Al menos 1 puerto de consola
- 1 SSD 400GB
- Última versión de software estable, validada, liberada y recomendada por el fabricante de la solución propuesta.
- Alta Disponibilidad:
    - Capacidad de operar en un esquema de alta disponibilidad Activo/Pasivo
    - Soporte y operación mediante fuentes de poder y ventiladores redundantes.
    - Tanto fuentes de poder como ventiladores redundantes deberán poder ser removidos e insertados en funcionamiento sin afectar la operación del servicio.
- Operativos
    - Montable en rack de 19 pulgadas.
    - Operación con voltaje 100 a 220V

Administración

- El licitante debe ofertar un servidor de propósito específico con las siguientes características donde venga instalado de fábrica el software de administración.

- El software de administración deberá:
  - Soportar al menos 30 millones de eventos
  - Al menos 32GB de RAM
  - 900 GB de almacenamiento para eventos
  - 5,000 flujos por segundo
  - Fuentes redundantes
- Soportar RFC 8600 para integración con terceros para recopilar y distribuir informes de incidentes de seguridad y otra información relevante para la seguridad entre dispositivos conectados a la red, principalmente con el propósito de comunicarse entre los equipos de respuesta a incidentes de seguridad informática.
- La administración del sistema debe ser vía Web (HTTPS), por línea de comando (SSH), SNMPv3 y a través de una consola central de administración.
- Contar y operar al menos con una interfaz Gigabit Ethernet dedicada para administración.
- Contar y operar con al menos un puerto de consola de administración.
- Manejo de un puerto USB 2.0
- Generación logs con, al menos, seis niveles de criticidad.
- Regulaciones
  - UL 60950-1
  - 47CFR parte 15 (CFR 47) clase A
  - CISPR22 clase A
  - EN 60950-1
  - IEC 60950-1
  - EN55022 class A
  - VCCI clase A
  - Marcado CE

6.2. SERVICIO DE SISTEMA DE PREVENCIÓN CONTRA INTRUSOS (IPS)

El servicio debe brindar la capacidad de visibilidad sobre los eventos de seguridad, indicadores de compromiso (IOCs) y archivos maliciosos identificados en el tráfico de red.
El servicio debe descubrir continuamente información sobre su entorno de red, incluidos datos sobre sistemas operativos, dispositivos móviles, archivos, aplicaciones y usuarios. Luego utilizar esta información para crear mapas de red y perfiles de host. Esto debe brindar la información contextual que necesita para tomar mejores decisiones sobre eventos de intrusión. Y esta información debe también ser utilizada como entrada para permitir una mejor automatización de las funciones clave de protección contra amenazas.
El servicio debe garantizar mecanismos de alta disponibilidad en el despliegue de los equipos, es decir, redundancia activa-pasiva y activa-activa. Adicionalmente, el fabricante deberá garantizar mecanismos de reemplazo de partes de hardware en un esquema 7x24x4.

Requerimientos generales

a) Operación en hardware de propósito específico y con sistema operativo propietario, ambos desarrollados íntegramente por el mismo fabricante.

b) Incluir todos los accesorios y cables necesarios para la total instalación y puesta en operación.

c) El servicio debe tener la capacidad de integrarse de forma nativa, sin ningún desarrollo adicional al Servicio de Respuesta y Visibilidad Unificada de Incidentes de Seguridad especificado al final de este anexo para poder orquestar y responder a incidentes de seguridad.

Funciones

- Soporte Multi instancias
- Habilidad de detectar al menos 4,000 aplicaciones
- Capacidad de operar en modo transparente o modo ruteado.

- Operación en IPv4 e IPv6.
- Operación de reglas de firewall de estado completo.
- Segmentación de flujos en zonas de seguridad que permitan habilitar diferentes políticas a cada zona.
- Capacidad de agrupar hasta 16 enlaces físicos en un mismo enlace lógico (802.3ad).
- Manejo de tramas Jumbo de 9000 bytes.
- Manejo de 802.1Q.
- Soporte y operación con al menos 1,000 VLANs.
- Throughput con las funcionalidades de protección contra amenazas, anti-malware y filtrado de URL de al menos 14Gbps con paquetes de 1024 Bytes.
- 10 millones sesiones concurrentes
- 85,000 nuevas sesiones por segundo
- Capacidad de limitar el ancho de banda por interfaz en unidades de Mbps.
- Capacidad de implementar reglas de control de acceso con base en:
    - Direcciones IP fuente y destino
    - Puertos fuente y destino
    - Protocolos
    - Protocolos de encapsulación
    - Puntos de origen y destino de túneles
    - Códigos ICMP
    - Localización geográfica
    - Interfaces fuente y destino
    - Etiqueta de VLAN
    - Etiquetas de identificación
    - URLs individuales o por grupo.
    - Características de las aplicaciones
- Capacidad de caracterizar más de 3,000 aplicaciones por función esencial, tipo, nivel de riesgo y si son recreativas o si están asociadas a la operación de la organización.
- Capacidad de detectar aplicaciones cifradas.
- Capacidad de implementar restricciones de contenido.
- Inspección de los siguientes protocolos: DNS sobre UDP, HTTP, FTP, IMAP, POP, H.323, H.225, SMTP, SSH, ICMP, SSL, SIP, TFTP, SCCP.
- Establecimiento de tiempos de terminación ante inactividad para conexiones TCP, UDP e ICMP, traducciones, conexiones H.323 y SIP.
- Capacidad de agrupar elementos de configuración para facilidad de uso tales como segmentos de red, puertos y VLANs.
- Manejo de ruteo estático, OSPF, BGP y RIP.
- Manejo de PIM, IGMP
- Manejo de IPSEC.
- Manejo de los siguientes algoritmos de cifrado: AES-GMAC (256 bits), AES (256 bits), 3DES
- Manejo de los siguientes algoritmos de hashing: SHA, MD5
- Manejo de los grupos Diffie Hellman 1, 2, 5, 14, 21, 24
- Compatibilidad con NSA Suite B
- Traducción de direcciones IP (NAT) estática, dinámica (entre grupos direcciones IP), dinámica por puertos (PAT) y traducción a sí misma.
- Soporte de NAT para IPv4 e IPv6
- Soporte de NAT de IPv4 a IPv6 y viceversa.
- Capacidad de traducir la dirección fuente y destino
- Soporte de certificados digitales de 2,048 bits
- Prevención de que usuarios maliciosos se hagan pasar por hosts o dispositivos de red autorizados mediante la inspección de ARP.
- Capacidad de no permitir paquetes fragmentados.
- Análisis del tráfico de red para detectar intrusiones, almacenar datos sobre ataques, bloquear y modificar el tráfico malicioso.
- Decodificación de paquetes para prevenir ataques basados en patrones

- Capacidad de crear políticas de intrusiones customizadas.
- Capacidad de detectar datos sensibles tales como números de tarjetas de crédito o información personal en texto ASCII
- Detección de anomalías de tráfico y análisis de impacto por evento para evitar ataques de día cero.
- Realizar capturas de tráfico para el análisis de evidencia en formato soportado por TCPDUMP. El archivo podrá ser usado para hacer playback del ataque.
- Permitir un análisis dinámico y en tiempo real para crear un mapa de la red monitoreada, incluyendo al menos lo siguiente parámetros:
    - Hosts activos
    - Sistema operativo de cada uno de los hosts identificados
    - Servicios activos de cada uno de los hosts identificados
    - Aplicaciones activas de cada uno de los hosts identificados
    - Vulnerabilidades de cada uno de los hosts identificados.
- Permitir la creación de listas negras y listas blancas de direcciones IP
- Capacidad para correlacionar los eventos de intrusión con el descubrimiento de vulnerabilidades internas, mostrando el nivel de impacto correspondiente.
- Deberá de contar con las siguientes reglas de detección:
    - Reglas de detección relacionadas con exploit kits, adware y spyware.
    - Reglas de detección basadas en vulnerabilidades de Apache, Microsoft IIS y Oracle.
    - Reglas de detección sobre comunicación de comando y control (CnC) de botnets.
    - Reglas de detección contra contenido ofuscado.
    - Reglas de detección basadas en vulnerabilidades de los sistemas operativos Windows, Linux, Solaris y otros.
- Capacidad de recopilar la información sobre los flujos de sesión para todos los hosts, incluyendo el tiempo inicio/fin, puertos y cantidad de datos.
- Integración con directorio de usuarios que provea las siguientes características:
    - Permitir la integración con el directorio activo de la red para tener un mapeo de usuario e IP utilizada actualmente.
    - Los eventos de seguridad reportados deberán mostrar el usuario que está generando o recibiendo el ataque y generar una alerta o tomar acciones en base al perfil del usuario en cuestión.
    - Generar un mapa de eventos de seguridad generados/recibidos por usuario.
    - Generar un mapa de tráfico generado/recibido por usuario.
    - Deberá ser capaz de mantener un mapa de los usuarios, IP actual y un historial de las IPs que ese usuario ha usado en el tiempo.
- Soporte del remontaje de paquetes TCP fragmentados y soportar la desfragmentación de paquetes IP fragmentados y coincidentes (empalmados).
- Bloqueo de tráfico por geolocalización
- Capacidad de recopilar información pasivamente sobre hosts de la red y sus actividades, tales como: sistema operativo, puertos abiertos (servicios), aplicaciones y vulnerabilidades, permitiendo la correlación de datos y políticas de cumplimiento.
- Prevención de Intrusos que se adapte en tiempo real en base a un descubrimiento dinámico de la red.
- Proveer la opción de consulta de un histórico de los eventos sucedidos.
- Capacidad de identificar todos los hosts que presenten un atributo o condición especifica de incumplimiento de la política (por ejemplo: identificar los equipos que estén corriendo como servidores de HTTP fuera de la granja de servidores)
- Capacidad de crear reglas basadas en: segmento monitoreado; dirección IP origen y destino; puertos origen y destino.
- Priorización automática de eventos de ataques basado en la relevancia para el ambiente protegido.
- Capacidad de customizar las políticas de intrusión en base a los dispositivos que están en el ambiente protegido.
- Agregación de múltiples eventos en Indicadores de Compromiso ligados a un solo host.
- Capacidad de ver reglas/filtros/firmas (reglas abiertas) del IPS.
- Habilidad de crear reglas customizadas usando nativamente el motor de Snort

- Calificación de impacto automatizado basado en perfilamiento de hosts e información de vulnerabilidades.
- Listas negras categorizadas y mantenidas por el fabricante (Botnet, Phishing, C&C, Spam, etc)
- Inspección de DNS de modo que responda a peticiones de dominios externos específicos, definidos por el administrador, con una IP específica (sinkhole).
- Proveer la opción de consulta, de un histórico de los eventos sucedidos en los equipos ofertados desde la consola principal.
- Protección contra ataques sobre aplicaciones Web como: shell command injections, Server-site injection, cross-site scripting, directory traversal.
- Soporte de búsqueda de firmas por nombre a través de la interfaz gráfica.
- Capacidad de bloquear paquetes de conexiones de TCP que no han terminado la negociación de 3 pasos (three-way handshake)
- Detección de escaneo de puertos TCP, UDP, ICMP y de protocolos IP.
- Detección de barrido de puerto
- Detección de escaneo de puertos con una dirección IP falsa.
- Detección de escaneo de puertos distribuido.
- Prevención de ataques basados en conexiones frecuentes o intentos recurrentes de ataque.
- Capacidad de desplegar una página web cuando el sistema bloqueé una petición web.
- Identificar y bloquear malware avanzado que pase a través del appliance mediante protocolos como web, email u otros vectores.
- Reconocer archivos permitiendo aplicarles políticas de transferencias aún sin ser malware.
- Permitir el rastreo de malware y archivos a través de la red mediante un mapa visual de sus transferencias a lo largo del tiempo mostrando los hosts por los que se ha visto el archivo, así como atributos del archivo.
- Tomar acción con el archivo aun cuando éste haya pasado por la red horas o días atrás en el tiempo, pudiendo tomar acción y mitigar el daño.
- Detectar y bloquear intentos de explotación de vulnerabilidades que pueden derivar en ataques tipo drive by.
- Permitir el bloqueo de comunicaciones del malware.
- Soportar los siguientes tipos de archivos para análisis de malware: ejecutables, DLL, documentos de Office, PDF, Flash, Java,
- Inspeccionar archivos comprimidos y configurar la profundidad de análisis para archivos comprimidos anidados.
- Proveer información de Indicadores de Compromiso (IoC) asociados a detecciones de malware en la Red.
- Contar con un módulo de almacenamiento local para guardar las muestras de malware y archivos marcados como desconocidos.
- Analizar la estructura de los archivos ejecutables para identificar malware.
- Solicitar el análisis dinámico de archivos en función de la política establecida.
- Analizar archivos anexos incluidos en correos electrónicos en los protocolos SMTP, POP3 o IMAP.
- Configuración de listas blancas y negras de archivos definidas por el usuario.
- Contar con una infraestructura que cuente con múltiples fuentes de amenazas incluyendo:
    - 100 TB de datos procesados por día.
    - 1.1 millones de muestras de malware por día.
    - 13 mil millones de solicitudes Web.
    - Inteligencia de amenazas de la solución debe estar respaldada por un grupo de más de 350 investigadores del fabricante con un alcance mundial y que sean responsables de desarrollar nuevas reglas para alertas sobre nuevos ataques. El grupo deberá tener un blog donde publicará nuevas vulnerabilidades encontradas, campañas por actores maliciosos detectadas por ellos mismos y herramientas de código abierto. El grupo debe ofrecer una página de revisión de reputaciones de Dominios, IPs, Email y archivos de forma gratuita proporcionada y alimentada por ellos mismos que permita a los operadores buscar indicadores de compromiso relacionados a nuevos ataques.
- Integración con sistemas de inteligencia del fabricante y terceros que alimenten al sistema de información actualizada sobre direcciones IP, URLs y nombres de dominio maliciosos, listas negras y listas blancas.

- Debe soportar APIs (Application Programming Interfaces, Interfaces de Programación de Aplicaciones) para la integración con una plataforma de software libre y de código abierto para el despliegue de una solución de cloud computing.

Características técnicas

La solución deberá incluir y operar al menos con las siguientes características:

- 8 puertos SFP
- 8 puertos SFP+
- Al menos un puerto de management
- Al menos 1 puerto de consola
- 1 SSD 400GB
- Auto-MDI/MDIX en las interfaces de cobre
- Última versión de software estable, validada, liberada y recomendada por el fabricante de la solución propuesta.
- Alta Disponibilidad:
    - Capacidad de operar en un esquema de alta disponibilidad Activo/Pasivo
    - Soporte y operación mediante fuentes de poder y ventiladores redundantes.
    - Tanto fuentes de poder como ventiladores redundantes deberán poder ser removidos e insertados en funcionamiento sin afectar la operación del servicio.
- Operativos
    - Montable en rack de 19 pulgadas.
    - Operación con voltaje 100 a 220V

Administración

- El sistema de Prevención de Intrusos debe ser administrado por el mismo servidor de propósito específico detallado en la administración del Servicio de Filtrado web contando con las características anteriormente definidas.
- Administración remota vía Web con interfaz gráfica, para el uso en modo de consulta de dispositivos y eventos de seguridad.
- Realizar de manera remota y automática su actualización y configuración de políticas.
- Soportar la creación de múltiples roles, en el cual se permita o niegue el acceso a los diferentes dispositivos, o se otorguen privilegios o no para la administración, visualización de eventos o generación de reportes.
- Los datos que cursen por el dispositivo deben al menos ser almacenados en una base de datos relacional dentro de la misma consola de administración.
- Realizar automáticamente actualizaciones de software vía remota o Web para asegurar una protección en tiempo real.
- Proveer información adicional sobre el evento recibido con una descripción del ataque y una liga de referencia.

6.3. SERVICIO DE PROTECCIÓN PARA APLICACIONES WEB (WAF)

Se requiere de un servicio de seguridad que provea protección a nivel de capa siete, y garantice la seguridad de las aplicaciones Web de la CONDUSEF, a través de la automatización de la seguridad web, con una protección global e integral, inspeccionando peticiones desde Internet e impidiendo que el tráfico malicioso alcance las aplicaciones.
El servicio debe garantizar mecanismos de alta disponibilidad en el despliegue de los equipos, es decir, redundancia activa-pasiva y activa-activa.

Requerimientos generales

a) Operación en hardware de propósito específico y con sistema operativo propietario, ambos desarrollados íntegramente por el mismo fabricante.

b) Incluir todos los accesorios y cables necesarios para la total instalación y puesta en operación.

c) La solución debe de ser del tipo appliance de propósito específico.

d) Debe soportar en Alta Disponibilidad sin la necesidad de licenciamiento adicional.

e) Debe de tener software específico destinado a la finalidad de Firewall de Aplicación Web (WAF – Web Application Firewall), así como las licencias necesarias para su funcionamiento y protección de servidores y aplicaciones Web.

f) La solución propuesta debe de ser formada por software y hardware del mismo fabricante.

g) Debe de contar con certificación de ICSA Labs.

Funciones

- La solución debe de ser capaz de ser implementada en modo Proxy (Transparente y Reverso), Pasivo (Sniffer) y Transparente en línea (Bridge).
- Soportar VLANs del estándar IEEE 802.1q.
- Soportar direccionamiento IPv4 y IPv6 en las interfaces físicas y virtuales (VLANs).
- La solución debe de soportar y brindar clúster de alta disponibilidad entre dos equipos en modo Activo-Pasivo y Activo-Activo, de forma que el tráfico siga siendo procesado en caso de fallo del equipo principal.
- La solución debe soportar en los modos de Proxy Inverso y modo Proxy Transparente Verdadero (True Transparent Proxy) el copiado de tráfico hacia dispositivos terceros como IDS/IPS a través de las interfaces de red para el monitoreo de tráfico.
- Soporte Multi dominios.
- Debe tener la capacidad de recibir tráfico HTTP y HTTPS para inspección a través de WCCP.
- La solución debe de soportar el modelo de seguridad positiva definido por OWASP, por lo menos lo que está en el Top 10
- Deberá tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formularios y lo que se espera de cada campo
- El perfil aprendido de forma automática debe de poder ser ajustado
- La solución debe tener generación de reportes con la información obtenida en auto aprendizaje, con las estadísticas y las políticas de tráfico obtenido, los reportes de ataques, eventos y reportes de chequeo de vulnerabilidades para fines de cumplimiento de regulación
- Tener la capacidad de creación de firmas de ataques personalizables
- Tener la capacidad de protección contra ataques del tipo Adobe Flash binary (AMF) protocol
- Tener la capacidad de protección contra ataques del tipo Botnet
- Tener la capacidad de protección contra ataques del tipo Browser Exploit Against SSL/TLS (BEAST)
- La solución debe tener funcionalidad de protección contra ataques como acceso por fuerza bruta
- Debe soportar detección de ataques de Clickjacking
- Debe soportar detección de ataques de cambios de cookie
- Identificar y proteger contra ataques del tipo Credit Cart Theft
- Identificar y proteger contra ataques del tipo Cross Site Request Forgery (CSRF)
- La solución debe tener funcionalidad de protección contra ataques como cross site scripting (XSS)
- Debe tener protección contra ataques de Denial of Service (DoS).
- Tener la capacidad de protección contra ataques del tipo HTTP header overflow, Local File inclusion (FLI), Man-in-the-middle (MITM), Remote File Inclusion (RFI), tipo Server Information Leakage
- Protección contra envíos de comandos SQL ocultos en las solicitudes enviadas a la base de datos (SQL Injection);
- Tener la capacidad de protección contra ataques del tipo Malformed XML

- Identificar y prevenir ataques del tipo Low-rate DoS
- Prevención contra ataques Slow POST
- Proteger contra ataques Slowloris
- Tener la capacidad de protección contra ataques del tipo SYN flood
- La solución debe tener funcionalidad de protección contra ataques de manipulación de campos ocultos
- Tener la capacidad de protección del tipo Access Control y Rate Limiting
- Identificar y proteger contra Zero Day Attacks
- Tener la capacidad de configurar protección del tipo TCP SYN flood-style para prevención de DoS para cualquier política, a través de Syn Cookie y Half Open Threshold
- Permitir configurar reglas de bloqueo a métodos HTTP no deseados
- Permitir que se configuren reglas de límite de upload por tamaño del archivo
- Debe permitir añadir automática o manualmente, en una lista de bloqueo, las direcciones IP de origen, según la base de datos “IP Reputation”
- Debe se der capaz de hacer aceleración de SSL, donde se instalan los certificados digitales en la solución y las solicitudes HTTP sean enviadas a los servidores sin criptografía
- La solución debe de ser capaz de funcionar como terminador de sesión SSL para aceleración de tráfico
- La solución debe tener la capacidad de almacenar certificados digitales de CA's
- La solución debe de ser capaz de generar CSR para ser firmado por una CA
- La solución debe contener las firmas de robos conocidos como link checkers, indexadores de web, search engines, spiders y web crawlers que puedan ser añadidos a los perfiles de control de acceso, así como resetear dichas conexiones
- La solución debe de tener un sistema de reputación de direcciones IP públicas conocidas como origen de ataques de DDoS, botnets, spammers, etc. Esto sistema debe de ser actualizado automáticamente.
- La solución debe de ser capaz de limitar el total de conexiones permitidas hacia cada servidor real de un pool de servidores
- La solución debe permitir la personalización o reenvío de solicitudes y respuestas HTTP en el HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body y HTTP Location
- La solución debe permitir crear reglas definiendo el orden con que las páginas deben de ser accedidas para prevenir ataques como cross-site request forgery (CSRF).
- La solución debe de tener la capacidad de definir restricción a determinados métodos HTTP
- La solución debe tener la capacidad de proteger contra detección de campos ocultos
- Debe de ser capaz de hacer compresión del contenido HTTP, para reducir la cantidad de información enviada al cliente
- Soportar redirección y reescritura de solicitudes y respuestas HTTP
- Permitir redirección de solicitudes HTTP para HTTPS
- Permitir reescribir la línea URL, HOST, REFERER del encabezado de una solicitud HTTP
- Permitir redirigir solicitudes para otro website
- Permitir enviar respuesta HTTP 403 Forbidden para solicitudes HTTP
- Permitir reescribir el parámetro LOCATION en el encabezado HTTP de una respuesta de redirección HTTP de un servidor web
- Permitir reescribir el cuerpo ("body") de una respuesta HTTP de un servidor web
- Permitir añadir el campo X-Forwarded-For para identificación de la dirección IP real del cliente cuando en modo proxy reverso
- La solución debe de soportar reglas para definir si las solicitudes HTTP serán aceptadas en función de la URL y origen de la petición y, si necesario, aplicar una tasa específica de velocidad (rate limit).
- La solución debe de soportar combinación de control de acceso y autenticación utilizando mecanismos como HTML Form, Basic y soporte a SSO, métodos como LDAP y RADIUS para consultas e integración de los usuarios de la aplicación
- Tener capacidad de caching para aceleración web.

Características técnicas

La solución deberá incluir y operar al menos con las siguientes características:

- Throughput de 2.4 Gbps
- 4 puertos GE RJ45 Bypass
- 4 puertos GE SFP
- 2 puertos 10GE SFP+
- 2 SSD 2 TB
- 2 Fuentes de poder redundantes hot-swap
- Latencia máxima de 5 ms

Administración

- Debe tener incorporado un sistema operacional / firmware que debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS, y también por CLI (interfaz de línea de comando), accediendo localmente por puerto de consola, o remotamente vía SSH.
- Tener auto complementación de comandos en la CLI, así como ayuda contextual.
- Debe de proveer en la interfaz de gestión, la siguiente información del sistema para cada equipo: consumo de CPU y estadísticas de conexión.
- Debe de incluir herramienta dentro de la interfaz gráfica de gestión (dashboard) que permita visualizar los últimos logs de ataques detectados/bloqueados.
- La configuración de administración de la solución debe permitir la utilización de perfiles.
- Debe de ser posible ejecutar y recuperar backup por la interfaz Web (GUI).
- Debe soportar los protocolos de monitoreo SNMP v1, SNMP v2c e SNMP v3.
- Debe ser capaz de realizar notificación de eventos de seguridad a través de e-mail, traps SNMP y Syslog.
- La solución deberá de soportar almacenar logs localmente en disco y en servidor externo vía protocolo SYSLOG.
- La solución debe tener la capacidad de enviar alertas por email de los eventos basado en severidad y/o categorías.
- Debe tener la capacidad de generar reportes detallados basados en tráfico/acceso/actividades del usuario.
- Debe tener base local para almacenamiento y autenticación de los usuarios.
- La solución debe tener la capacidad de autenticar usuarios en bases externas remotas LDAP y RADIUS.
- La solución debe soportar autenticación a través de TACACS+ para usuarios de administración.

6.4. SERVICIO DE PROTECCIÓN DE CORREO ELECTRÓNICO (ANTISPAM)

Se requiere de un servicio de seguridad que permita detectar, controlar y reducir las amenazas de seguridad recibidas a través de correo electrónico, tales como: SPAM, Phishing y malware.
El correo electrónico es uno de los vectores de ataque mayormente utilizados por los atacantes, por tal motivo se requiere proteger esta herramienta de trabajo utilizada por la mayoría de los usuarios dentro de la CONDUSEF.
El servicio debe tener la capacidad de protección dentro y fuera del perímetro de la CONDUSEF.
Se requiere proteger 2000 buzones de correo electrónico.

Requerimientos generales

a) El servicio de Anti-Spam debe integrar la captura eficaz de spam con baja tasa de categorización de mensajes como falsos positivos.

b) Implementado como puerta de enlace de correo electrónico,

c) Debe proteger correos electrónicos y mensajes instantáneos contra malware, spam, phishing, botnets y otros correos no deseados.

d) Debe disponer de recursos flexibles para la administración de spam y actualizaciones de filtros automatizadas.

e) No se aceptarán soluciones que necesiten o sean exclusivamente dependientes de la tecnología de virtualización tipo "sandboxing" para la detección de archivos maliciosos y la presencia de malware en el entorno monitoreado.

f) El servicio deberá de proteger los servidores de correo electrónico dentro de la CONDUSEF, así como en la nube si así fuera necesario, independientemente de si el servicio se despliegue dentro de las instalaciones de la CONDUSEF, en las del proveedor, o en las del fabricante.

g) Incluir todos los accesorios y cables necesarios para la total instalación y puesta en operación.

h) El servicio debe tener la capacidad de integrarse de forma nativa, sin ningún desarrollo adicional al Servicio De Respuesta y Visibilidad Unificada De Incidentes De Seguridad especificado al final de este anexo para poder orquestar y responder a incidentes de seguridad.

Funciones

- Debe poseer sistema de archivo propietario, desarrollado para optimizar las colas de mensajes
- Permitir equilibrio de carga para el mismo dominio
- Poseer un MTA propietario (sin Sendmail, Qmail o Postfix), creado con lenguaje de programación que no utiliza pilas (sin riesgo de vulnerabilidad a ataque del tipo desbordamiento de pila / stack overflow)
- Poseer habilidad para controlar las sesiones SMTP y limitar el tráfico de mensajes, basado en direcciones IP, Rango de IP, Subnet IP, nombre de dominio, nombre parcial de dominio y reputación del emisor
- Capaz de restringir las conexiones basadas en el tamaño máximo de mensajes, el número máximo de destinatarios por mensaje, el número máximo de mensajes por conexión, el número máximo de conexiones simultáneas por IP
- Capaz de limitar el número máximo de conexiones simultáneas
- Posibilitar desactivar la comprobación de DNS inversa para conexiones entrantes
- Posibilitar el bloqueo de malos remitentes y definir políticas individuales por remitente (tanto externo como interno) basado en:
    - IP origen
    - rango de IP
    - dominio
    - reputación del remitente
    - lista de DNS.
- Posibilitar configurar filtro de malware y anti-spam antes de la llegada al ambiente
- Posibilitar tasa de límite controlada por dirección IP, dominio o reputación del remitente:
- Debe ser capaz de definir el flujo de tráfico, basado en períodos de tiempo (en minutos)
- Control granular de políticas capaces de:
    - verificar DNS inverso y asignar políticas
    - permite configurar por política
    - habilitar TLS preferido u obligatorio
    - autenticación SMTP preferida u obligatoria
- Poseer la capacidad de implementar comunicación segura vía TLS (Transport Layer Security)
- Permitir el envío de mensajes a través de TLS por dominio de destino
- Debe proveer prevención a ataques de exploración de directorios (DHAP)
- Integrar con Open LDAP, Active Directory, u otros servidores LDAP que permitan identificación de usuarios no válidos
- Debe ser capaz de sincronizar usuarios y grupos de LDAP para el reconocimiento de los usuarios válidos y las acciones de Malwares, Spam y Filtrado de Contenido diferenciado por grupos LDAP

- Poseer funcionalidad de bloqueo de servidores spammers a través de la metodología conocida por Domain Keys Identified Mail (DKIM), SFP y Sender ID.
- Debe implementar el estándar DMARC.
- Rechazar mensajes a destinatarios no válidos durante el diálogo SMTP (evitar NonDelivery Report Attack)
- Posee detección de spams, mediante la utilización de al menos 4 (cuatro) mecanismos distintos que permitan aumentar la precisión en la detección de mensajes no válidos
- Controlar el número máximo de rechazos por hora, según el número de destinatarios no válidos por IP o rango, dominio o reputación del remitente de los mensajes
- Debe monitorear el tráfico de mensajes en tiempo real, que permita identificar parámetros críticos como el volumen de mensajes, el historial de conexiones, las conexiones aceptadas y rechazadas, la tasa de aceptación y los límites, los filtros de reputación correspondientes, el número de mensajes de spam positivos y sospechosos y el número de amenazas identificadas
- Debe supervisar el flujo de mensajes en tiempo real (detalles del flujo de mensajes por dominio e IP). Los flujos de entrada y salida de mensajes se mostrarán por separado
- Debe tener estadísticas en tiempo real de destinatarios no válidos, bloqueados por reputación, spam y malware encontrados, además de mensajes limpios (por dominio e IP)
- Permitir el chequeo de la red Global (colaborativa) de la reputación de los IP que intentan conectarse al entorno para enviar mensajes. El sistema de reputación debe utilizar datos de una red de supervisión de tráfico web y de correo electrónico para definir la reputación de los remitentes consultando una base de datos global del fabricante.
- Permitir el tratamiento de excepciones al bloqueo por reputación basada en rango de IP o IP
- Debe ser posible realizar una configuración personalizada para cada tipo de ataque (spam, malware, diccionario (DHA) y mensajes de retorno (bounced mails)
- Tener estadísticas en tiempo real de mensajes bloqueados por rate limit, conexiones rechazadas, spam y malware detectados en el último día, la última semana y el último mes, además de los bytes recibidos de acuerdo con el dominio o IP
- Poseer filtro de contenido con búsqueda por palabras clave en el encabezado y cuerpo del mensaje, y en archivos de Microsoft Office o compatibles adjuntos, utilizando operadores lógicos, tales como: AND, OR, OCCUR, NEAR, (,), [,] y así por delante
- Poseer un filtro de reputación
- El sistema de reputación revisará la reputación de los remitentes en redes participantes con cobertura global
- La red de reputación no sólo está basada en la información de flujo de la propia base de Appliances instalada, sino en muchos otros informes procedentes de jaulas de Spam, listas de URL, listas de equipos comprometidos, composición del mensaje, IPs en blacklist, volumen global de tráfico, listas blancas, composición del mensaje y web rastreadores
- Los filtros de reputación basados en URL, deben permitir:
    - Verificación de reputación y categoría de URLs incluidas en los mensajes enviados y recibidos, como criterio adicional en la ayuda de detección de spam y contenido malicioso.
    - Permitir modificar las URL en los mensajes, imposibilitando el clic del usuario, reemplazando por texto o redireccionando a proxy de evaluación de la URL antes de la liberación o bloqueo del acceso, si se considera malicioso o contra la política de acceso.
    - Permitir la creación de filtros de URL por categoría para permitir o bloquear el acceso del usuario de acuerdo con la directiva de acceso.
- Posibilitar el control de tráfico de correo electrónico por reputación asignada por la red de reputación, de cada IP que solicitó una conexión. La red de reputación debe monitorear los parámetros de correo electrónico y de Web
- La información de red de reputación también se utiliza para analizar los mensajes por el filtro Anti-Spam utilizado en el appliance
- Poseer verificación de bounces para combatir ataques de rebote, soportando la sustitución de la dirección del remitente, utilizando una etiqueta de verificación de rebote en la salida de todos los mensajes. Los bounces que llegan sin la etiqueta son removidos y los que llegan con etiqueta, entregados

- Contener el módulo de encriptación de los mensajes. El servicio debe de contar con un dispositivo específico para cifrar los mensajes. En este caso deberá estar explícito la marca y modelo del equipo utilizado para tal fin
- Ser capaz de crear perfiles de encriptación tanto para el uso de servidores externos como servidores internos
- Ser capaz de cifrar mensajes localmente mediante la creación de reglas que especifiquen qué mensajes se deben cifrar. Las reglas deben ser de acuerdo con la necesidad del órgano por lo menos por destinatario, remitente, contenido de anexos (PDF, Word, Excel, etc), asunto o cuerpo del e-mail, caracteres en el Header del mensaje
- Ser capaz de crear perfiles diferentes para cada regla específica de mensajes que se van a cifrar
- El método de criptografía utilizado no debe depender de la instalación de software o plugins en la máquina del remitente y del destinatario
- Debe generar claves por mensaje imposibilitando que la clave de un mensaje pueda abrir otro mensaje, incluso para el mismo destinatario
- Debe tener 2 (dos) niveles de seguridad de acceso en la lectura de los mensajes encriptados:
    - Nivel alto: El receptor del mensaje debe introducir las credenciales de contraseña cada vez que abra el mensaje, aunque la contraseña esté en caché.
    - Nivel bajo: La contraseña no se solicita si está en caché, es decir, si el receptor ha abierto el mensaje una vez, no es necesario volver a escribir al volver a abrir el mensaje mientras la contraseña está en caché.
- Debe utilizar al menos los siguientes algoritmos de criptografía:
    - AES 192 bits
    - RC4 160 bits
- Debe implementar el estándar FIPS.
- Debe permitir que los receptores de los mensajes cifrados puedan responder y / o reenviar al mensaje de forma encriptada para garantizar la seguridad de la información
- Permitir que las plantillas de los mensajes cifrados puedan personalizarse
- Proporcionar los siguientes controles de los mensajes enviados:
    - El remitente puede cancelar la clave del mensaje antes de que el destinatario reciba el mensaje
    - El remitente puede configurar un tiempo de caducidad de la clave. Si el tiempo ha caducado el mensaje no se puede abrir.
    - El sistema debe enviar notificación de lectura del mensaje, tan pronto como el destinatario accede a la clave para abrir el mensaje.
    - Los mensajes no se deben almacenar en el servidor de claves o en el dispositivo de cifrado.
    - El mensaje se debe entregar en un archivo adjunto cifrado y sólo la clave se debe transmitir entre el servidor y el destinatario en un acceso seguro de tipo SSL.
    - Posibilitar el envío de mensajes encriptados sin la necesidad de utilizar Javascripts.
    - Posibilitar crear reglas para expirar un mensaje, basándose en la fecha o por hora después del envío del mensaje.
- Soportar tráfico de entrada y salida, con gestión de políticas separadas
- Posibilitar la personalización del banner SMTP, el hostname y los códigos de respuesta por dirección IP o grupo de remitentes.
- Soporte a múltiples dominios por dirección IP, o múltiples dominios utilizando diferentes IPs.
- Permitir administrar políticas por usuario o grupo de usuarios (basado en la dirección / dominio de remitente / destinatario, o grupo LDAP, por ejemplo, cuando se envía un solo correo electrónico a varios destinatarios, se procesará por la política específica de cada uno receptores)
- Debe poseer visión única de todas las políticas de usuarios, para una administración fácil y objetiva
- Debe tener control de flujo basado en el grupo de remitentes:
    - Blacklists (IP, dominio o reputación)
    - Whitelists (IP, dominio o reputación)
    - Posibilitar la creación de varios grupos (por IP, dominio o reputación)
    - RBLs / ORBLs de terceros
    - Whitelist y blacklist de direcciones de remitentes y destinatarios.
- Permitir crear filtros definidos por el tamaño de mensaje
- Permitir crear reglas distintas para el mensaje que entran y salen del entorno

- Tener recursos que permita posponer la entrega de determinados mensajes para horario específico
- Permitir la dirección del mensaje a un servidor distinto del estándar (siguiente hop) de acuerdo con la necesidad del entorno
- Permitir la elección del lugar donde se colocará la notificación personalizada para el comienzo o fin del mensaje original
- Identificación de archivos adjuntos por el tipo real del archivo, el nombre de archivo, la extensión y el MIME Type
- Posibilidad de poner en cuarentena
- Filtros de contenido que cumplen los siguientes requisitos:
    - El servicio debe tener un primer nivel de filtro de contenido global, que se aplica a los mensajes antes de los chequeos AntiSpam, Antimalware y del segundo nivel de análisis de contenido.
    - Soportar expresiones regulares.
    - El segundo nivel de filtro de contenido debe ser aplicable por usuario o por dominio, analizando los mensajes de entrada y salida.
- Los filtros se deben aplicar basados en el remitente, el destinatario, la dirección IP, el tamaño del mensaje, la reputación, el tipo de datos adjuntos, el nombre de los datos adjuntos, el tamaño del cuerpo del mensaje, las listas públicas de blacklist, los diccionarios, en el asunto o contenido en el cuerpo del mensaje
- Las reglas de filtrado deben posibilitar múltiples acciones, basadas en múltiples condiciones, y chequeadas en secuencia, posibilitando el uso de modelos para análisis de entrada y salida
- Capaz de identificar más de 300 tipos de archivos por los tipos de archivo FileType (Finger Print) y extensiones reales, incluyendo archivos de texto, ejecutables, comprimidos, hojas de cálculo, documentos de MS Office y OpenOffice, archivos de imagen y archivos de imagen base de datos (access, dbase)
- Detectar objetos EXE, DLL, JPEG, GIF, BMP como mínimo dentro de archivos como Excel y Word.
- Permitir convertir mensajes html en texto.
- Debe posibilitar el análisis de imágenes, con al menos los siguientes requisitos:
    - Detección de contenido pornográfico en imágenes de tipo JPEG, BMP, PNG, TIFF, GIF, TGA, ICO y PCX.
    - La detección de contenido pornográfico debe utilizar un algoritmo que utilice el color de la piel y el tamaño y la curvatura del cuerpo para determinar la probabilidad de contenido inapropiado.
    - El filtro debe ser capaz de identificar y extraer las imágenes dentro de otros archivos como Word, Excel y PowerPoint.
- Identificar el contenido en los metadatos de los archivos
- Posibilitar el análisis de contenido en archivos del tipo PDF
- Relay confiable, que cumpla con los siguientes requisitos: a. Permitir la configuración de relé confiable, de forma que el IP original del origen del mensaje se identifique a través del encabezado del mensaje (cuando el dispositivo no es la primera capa de chequeo de mensajes).
- Filtro de spam en múltiples capas que cumpla los siguientes requisitos:
    - Filtro de reputación (IP / dominio del remitente)
    - Filtros reactivos de Anti-Spam
    - Tecnología de detección sensible al contexto
    - Tecnología que engloba reputación de correo electrónico y web
    - Técnica de aprendizaje adaptativo.
- Poseer una regla específica para los archivos adjuntos protegidos por contraseña
- Permitir la verificación contra contenido no autorizado dentro de los archivos adjuntos en los mensajes
- Poseer una función que quita datos adjuntos no deseados y entrega el mensaje original al destinatario
- Permitir bloquear los datos adjuntos por la extensión, el tipo real del archivo, el nombre, el tamaño y el número de datos adjuntos
- Detección de ataques y cambio de políticas en tiempo real, permitiendo cambiar la política de mensajes, también, en tiempo real, para posibles spammers y hackers (por dominio y dirección IP), buscando bloquear / crear obstáculo a esos posibles malos remitentes

- Debe implementar IPv4 e IPv6 simultáneamente.
- Cuarentena, que cumpla los siguientes requisitos:
    - Soportar varias cuarentenas configuradas por separado
    - Presentar acceso individual, con autenticación de usuario y contraseña para cada cuarentena
    - Soportar autenticación LDAP / AD / IMAP / POP para el usuario final
    - Enviar mensajes de notificación al usuario final, cuando hay mensajes de spam o sospechosos en la cuarentena, permitiendo al usuario ver los mensajes en la cuarentena y entregar o borrar los mensajes. La notificación es personalizable y permite la programación del envío para, como mínimo, más de una vez al día
    - Controlar el acceso a la cuarentena
    - Controlar el acceso por cuarentena, posibilitando que, a través de usuario y contraseña, el acceso sea dado sólo a usuarios que tienen acceso liberado (Ejemplo: cuarentena "Confidencial" sólo puede ser accedida por el administrador)
    - Posibilitar almacenar los mensajes en cuarentena en el propio dispositivo virtual o en otro hardware especializado
    - El servicio de Cuarentena externa debe permitir la administración de la cuarentena del usuario final.
    - Posibilitar el bloqueo de mensajes que contienen datos adjuntos dañados.
- Motor de inspección de malware, que cumpla con los siguientes requisitos:
    - Integrada a la misma solución, permitiendo al administrador definir políticas diferenciadas por grupos de usuarios
    - Generar informes y estadísticas específicos para esta funcionalidad.
- Protección día cero, que cumple los siguientes requisitos:
    - Proporcione una capa adicional de protección de día cero para los brotes de nuevos malware. En el caso de brotes, el servicio debe almacenar en cuarentena los mensajes que caracterizan riesgo, durante un período de tiempo configurable, o hasta que las vacunas para los nuevos malware se liberen y se apliquen en el antimalware, reduciendo el tiempo de vulnerabilidad a brotes de nuevos malware.
- Debe permitir la configuración de excepciones de acuerdo con la extensión del archivo
- Capacidad de análisis heurístico, a través de análisis de encabezados, contenido y estructura del mensaje
- Los filtros de protección deben permitir la configuración de acuerdo con el nivel de amenaza
- Todo el proceso de protección día cero es automático, por reglas enviadas al dispositivo virtual de inspección sin la necesidad de la intervención manual del usuario o administrador
- Debe permitir el análisis en retrospectiva contra malware y otras amenazas de día cero
- Debe permitir la verificación del tipo real del archivo, aunque se renombra
- Protección contra “dialers”, sin necesidad de software o agente adicional
- Protección contra herramientas para descubrir contraseñas de aplicaciones, sin necesidad de software o agente adicional
- Debe poseer capacidad para proteger contra ataques dirigidos que utilicen contenido malicioso tipo día-cero aliado a url's de intención maliciosa, aunque no sea conocido por bases de datos de contenido tradicionales, para ello de utilizar recursos específicos y automatizados para evaluación, ejecución y generación de protección bajo demanda dinámicamente, utilizando tecnología dedicada de procesamiento en sitio.
- Debe poseer capacidad para meter en cuarentena mensajes que contengan un archivo adjunto con malware desconocido y automáticamente quitar el mensaje de la cuarentena si no hay detección utilizando las nuevas actualizaciones (incluyendo recursos dinámicos) del mecanismo contra infecciones anteriormente descrito.
- Cuarentena para los brotes de nuevos malware, que cumplen los siguientes requisitos:
    - Cuarentena dinámica, que proporciona liberación automática de los mensajes, que no atiendan a las reglas de filtrado después de las actualizaciones de reglas y vacunas
    - Presentar intervalo entre actualizaciones configurables en lapsos de al menos 5 minutos.
- Debe poseer verificación de:
    - archivos
    - adjuntos

    - archivos comprimidos.
- Debe tener un mecanismo para la identificación de malware en archivos adjuntos de correos electrónicos y URL
- Debe permitir el bloqueo de malware empaquetado de forma heurística
- Debe detectar malware que utilice el mecanismo de Exploit en archivos, como PDF
- Debe poseer la funcionalidad de prevención de malware avanzado nativamente integrada en el appliance.
- Debe permitir la detección y prevención de ataques de día-cero sin depender únicamente de base de firmas.
- Deberá soportar análisis estático de correos electrónicos con verificación de reputación y comportamiento.
- Debe soportar análisis dinámico que sea resistente a técnicas de evasión y cuando observadas tales tentativas debe reportar la ocurrencia en las muestras evaluadas.
- Debe crear un "hash" del malware, éste debe ser rastreado continuamente y debe soportar su búsqueda.
- Debe soportar análisis continuo incluso la detección de causa raíz para auxiliar en la selección de incidentes de seguridad.
- Debe soportar informar métricas e informes de los siguientes criterios:
    - Número de usuarios que recibieron o fueron infectados con más maliciosos
    - Número de amenazas de malware, usuarios asociados e históricos.
    - Información de DNS inverso (hostname e IP)
- El fabricante de la solución del servicio debe poseer una unidad de investigación y desarrollo de seguridad enfocada en la identificación de vulnerabilidades, el mantenimiento de inteligencia de seguridad a escala mundial, el descubrimiento de amenazas explotadas y la creación de mecanismos de contención y respuesta a ataques.
- La lista de archivos soportados para análisis dinámico debe ser entregada, debe incluir y no estar limitada a los siguientes tipos: PDF, ejecutables PE32, documentos de Office (Excel, word, powerpoint)
- Debe soportar la descarga de la muestra de malware para posterior análisis forense o actividades de ingeniería inversa.
- Debe mantener un historial de los resultados de las evaluaciones previas y utilizar esta información para determinar de forma configurable que el archivo se considere malware a partir de cierto límite.
- Implementar red de inteligencia propietaria del fabricante para cubrir ataques originados de cualquier localidad global, con mecanismo opcional de retroalimentación de malware no identificado.
- Implementar el modo de configuración totalmente transparente para el usuario final y los usuarios externos, sin necesidad de configurar proxies, rutas estáticas y cualquier otro mecanismo de redireccionamiento de tráfico
- Debe ofrecer servicios de reputación de contenido web e identificación de amenazas día a cero.
- Debe permitir la identificación y prevención de malware avanzado utilizando reputación de archivos y así permitiendo la realización de bloqueos en tiempo real. Estas capacidades deben estar totalmente integradas al sistema de protección de correo electrónico sin necesidad de re-implementación del equipo, cambios en el flujo de comunicación o introducción de un nuevo punto de fallo en el perímetro de la red monitoreada.
- Debe permitir de forma automática un proceso de análisis continuo de archivos que cruzan el equipo de seguridad utilizando actualizaciones en tiempo real para identificar cambios en el veredicto de archivos analizados previamente o nuevos (para los desconocidos) sean estos maliciosos, no maliciosos.
- Debe mantenerse un historial de los resultados de las evaluaciones previas de los archivos automáticamente enviados al análisis utilizando tecnología de virtualización.
- Debe permitir el uso del resultado del proceso de análisis virtualizado como una actualización dinámica en la infraestructura en sitio, lo que permite ampliar la capacidad de protección en el entorno.
- Debe poseer capacidad de definir acciones para: permitir, detener y / o poner en cuarentena el contenido transferido.

- Todas las funciones y capacidades de detección y prevención de malware avanzado del servicio deben utilizar los mismos mecanismos de configuración, operación e informes del sistema de seguridad de correo electrónico que supervisa el perímetro.
- Debe proporcionar las funciones de inspección de entrada y salida de Malware con el filtro de amenazas avanzadas y el análisis de ejecución en tiempo real.
- Debe poseer capacidad de monitoreo en tiempo real sobre ataques identificados por el módulo de prevención contra malware
- La función de análisis en entorno de virtualización debe permitir un análisis completo del comportamiento del malware o código malintencionado
- Implementar red de inteligencia propietaria del fabricante para cubrir ataques originados de cualquier localidad global, con mecanismo opcional de retroalimentación de archivos no identificados. Esta red debe proveer también información sobre los nuevos orígenes y destinos de comunicaciones y distribución de malware.
- Implementar la actualización de la base de datos de la Red de Inteligencia de forma automática y permitir la programación a intervalos de tiempo
- Implementar a través de interfaz gráfica de administración todas las opciones de análisis y tratamiento de eventos de ataques Malware, detección de tráfico y notificación de eventos en tiempo real, identificando el nombre de archivo, tipo, nivel de amenaza cuando está disponible, sha-256, tipo de evento, cantidad de vistas, día y hora, origen y destino.
- Debe implementar múltiples motores para la comprobación de malware, sin depender únicamente del análisis virtualizado (sandbox) como método de identificación de malware en archivos.
- Debe permitir la visualización integrada de las detecciones y métricas de eventos asociados al análisis, detección y bloqueo de malware avanzado.
- Toda la información asociada a eventos de malware avanzados debe estar disponible en la misma consola de administración de forma nativa y sin establecer otro requisito previo de integración con equipos en la red local para acciones de análisis de archivos, detección y prevención de amenazas de malware avanzadas.
- Debe implementar un proceso de análisis continuo de archivos y transferencias, esto debe ocurrir con un proceso automatizado identificando a través de interfaz gráfica cuando se cambió la disposición del archivo, para así permitir identificar un proceso de remediación automatizado.
- Debe permitir realizar tareas de rastreo e identificación de impacto de uno o más eventos de malware en el entorno protegido, permitiendo las siguientes actividades:
    - Identificar en la consola de gestión del servicio de forma nativa e integrada la actividad maliciosa
    - Identificar el usuario asociado a la conexión
    - Identificar la url accedida
    - Identificar los dominios asociados al tráfico
    - Identificar de forma detallada amenazas de malware como nombres conocidos, comportamientos, índice de riesgo, etc
    - Identificar su (s) origen (s) y destino (s), incluyendo url's
    - Debe permitir identificar otras interacciones de la amenaza en el ambiente buscando asociar así actividades de movimiento lateral
    - Debe permitir ver detalles de la detección como: nombre de archivo, extensión del archivo, hash de integridad sha-256
    - Debe permitir identificar el resultado de los análisis del malware
- Informes y logs, que cumplan con los siguientes requisitos:
    - Monitoreo gráfico del flujo de mensajes de entrada y salida de la última hora, del último día, de la última semana y del último mes
    - Registro del procesamiento de cada mensaje
    - Informe de flujo de mensajes (Ejemplo: enumera los mensajes para un destinatario específico, en un determinado período de tiempo, con detalles de cómo se ha recibido, procesado y procesado, entregado o borrado)
    - Posibilitar estadísticas de mensajes y rendimiento
    - Proporcionar registros de antimalware, Anti-Spam, mensajes, debug, sistema, escaneado, línea de comandos, errores, interfaz de administración y estado
    - Posibilitar exportar datos a CSV y generar archivos PDF para almacenamiento o impresión

    - Proporcionar informes con gráficos, en formato de pizza y barras, que apoyan en la comprobación del ROI
- Los informes deberán permitir:
    - La programación para el envío automático de cada tipo de informe (por día, por semana, por mes), pudiendo distinguir cuál es el informe y para quién será enviado
    - Generación de informes por cantidad de días o meses deseados.
- Poseer herramienta de informe centralizado, que atiende a los siguientes requisitos:
    - Capaz de proporcionar informes de todos los mensajes o, por grupos de dominios
    - De volumen de uso por usuario (mayores remitentes o destinatarios de malware, spam, volumen y tamaño de mensajes)
    - De volumen de uso por dominio (mayores dominios de entrada y salida de mensajes por volumen, spam y malware)
    - Infracción de políticas o filtro de contenido
    - De los principales remitentes o destinatarios de malware
    - De los principales remitentes o destinatarios de spam.
    - Soporte para informes centralizados para múltiples dispositivos en equipos externos.
- Debe proporcionar informes gerenciales que pueden ser "on demand" o programados
- Monitoreo del sistema, que cumpla con los siguientes requisitos:
    - SNMP v1 / v2 / v3
    - MIB-II
    - Syslog.
- Alerta basada en e-mails, pudiendo especificar el tipo de alerta, la criticidad y, para qué e-mail será enviado
- Posibilidad de envío Trampas SNMP.
- Debe permitir administrar más de un dispositivo desde la misma consola
- Debe tener un paso a paso (asistente) de instalación y configuración
- Gestión de las áreas de cuarentena, con investigación, reprocesamiento, entrega o exclusión de mensajes
- Capacidad de cheque por DNS inverso con hasta 4 (cuatro) diferentes niveles de bloqueo
- Soportar tanto los servidores DNS raíz o los servidores locales.
- Soportar múltiples servidores DNS de acuerdo con el (los) dominio (s) de destino. Ejemplo: Servidor DNS A para el dominio A y Servidor DNS B para el dominio B.
- Soportar configuraciones DNS que permiten utilizar dos servidores de caché diferentes.
- Permitir configurar el "saludo" o "greeting" de SMTP en el caso de que haya falta de espacio en el disco, si el servicio no está disponible y si la cola de mensajes llega a un número establecido como máximo por el administrador
- Soporte para conexiones ilimitadas SMTP
- Capacidad de tener varios servidores de rastreo de tráfico SMTP, administrados por consola única
- Debe ofrecer la posibilidad de tener dominio enmascarado
- Definición de timeout de conexión SMTP

Características Técnicas

- Protección mínima de 700 cuentas de correo activas
- 8 puertos SFP
- 8 puertos SFP+
- Al menos un puerto de management
- Al menos 1 puerto de consola de administración
- Almacenamiento mínimo para logs de 1 TB.
- Auto-MDI/MDIX en las interfaces de cobre
- Última versión de software estable, validada, liberada y recomendada por el fabricante de la solución propuesta.
- Alta Disponibilidad:
    - Capacidad de operar en un esquema de alta disponibilidad Activo/Pasivo
    - Soporte y operación mediante fuentes de poder y ventiladores redundantes.

    - Tanto fuentes de poder como ventiladores redundantes deberán poder ser removidos e insertados en funcionamiento sin afectar la operación del servicio.
- Operativos
    - Montable en rack de 19 pulgadas.
    - Operación con voltaje 100 a 220V

Administración

- El licitante debe ofertar un servidor de propósito específico con las siguientes características donde venga instalado de fábrica el software de administración.
- La administración del sistema debe ser vía Web (HTTPS), por línea de comando (SSH), SNMPv3 y a través de una consola central de administración.
- Realizar de manera remota y automática su actualización y configuración de políticas.
- Soportar la creación de múltiples roles, en el cual se permita o niegue el acceso a los diferentes dispositivos, o se otorguen privilegios o no para la administración, visualización de eventos o generación de reportes.
- Los datos que cursen por el dispositivo deben al menos ser almacenados en una base de datos relacional dentro de la misma consola de administración.
- Realizar automáticamente actualizaciones de software vía remota o Web para asegurar una protección en tiempo real. Las actualizaciones aplicadas no deben requerir del reinicio del equipo.
- Proveer información adicional sobre el evento recibido con una descripción del ataque y una liga de referencia.
- Manejo de un puerto USB 2.0
- Generación logs con, al menos, seis niveles de criticidad.
- Regulaciones
    - UL 60950-1
    - 47CFR parte 15 (CFR 47) clase A
    - CISPR22 clase A
    - EN 60950-1
    - IEC 60950-1
    - EN55022 class A
    - VCCI clase A
    - Marcado CE

6.5. SERVICIO DE SEGURIDAD EN LA RESOLUCIÓN DE NOMBRES DE DOMINIO (DNS)

Se requiere de un servicio de seguridad en la resolución de nombres de dominio (DNS) para la comunicación de sus usuarios y servicios hacia Internet, y poseer con la inteligencia sobre los dominios y servicios accedidos al exterior de la organización, por medio del protocolo de resolución de nombres (DNS) y su aseguramiento, para identificar y mitigar amenazas como malware y ransomware, fishing, botnets, servidores de comando y control, DoS, DGA, etc., mediante apuntar la resolución de nombres a un servicio de resolución de dominio (DNS recursivo) en sitio.

Requerimientos generales

a) Debe ofrecerse en sitio para tener la capacidad de protección dentro y fuera del perímetro de la CONDUSEF.

b) Debe de contar con inteligencia forense relacionada con el tráfico global de internet, permitiendo a la CONDUSEF identificar ataques dirigidos a la institución, sus servicios, o su identidad.

c) Se requerirá apuntar la resolución de nombres de dominio (DNS) en Internet hacia este servicio.

d) Deberá de otorgar un 99.99% de disponibilidad en el servicio de resolución y bloqueo de dominios. Para lograrlo no dependerá de la localización geográfica para llevar a cabo las funciones de protección.

e) El servicio debe tener la capacidad de integrarse de forma nativa, sin ningún desarrollo adicional al Servicio De Respuesta y Visibilidad Unificada De Incidentes De Seguridad especificado al final de este anexo para poder orquestar y responder a incidentes de seguridad.

Funciones

- Contar con filtros configurables para la protección contra dominios maliciosos y no permitidos de manera ágil y sin necesidad de instalar equipos en las oficinas locales, solo apuntando los DNS hacia el servicio.
- No depender de apuntar a diferentes DNS en función de la localización geográfica. Todos deberán funcionar con los mismos DNS.
- Contar con una infraestructura global que identifique las relaciones entre dominios, direcciones IP, redes y malware en el Internet. Estos patrones deben permitir identificar infraestructuras de ataques de manera automática para poder prevenir al usuario de ir a destinos maliciosos.
- Contener llamados a infraestructuras de comando y control Web y no Web y no estar limitado a los puertos 80 y 443 de TCP.
- Contar con mecanismos de bloqueos configurables separados para reputaciones de dominios con base en categorías tradicionales y bloqueos específicos para dominios de malware, Botnets, Phishing y otros relacionados con amenazas.
- Contar con un mecanismo de cambio de IP dinámicas para asegurar puntos de salida a Internet remotos.
- Identificar ataques de tipo DNS como Fast Flux, DNS Hijacking o DGA.
- Toda la información relevante a un dominio debe de ser accedida desde un único portal, incluyendo:
    - TTL
    - Geolocalización
    - Información del tipo Whois
    - Información de registro
    - Gráficas de peticiones del dominio a nivel global
    - Gráfica de peticiones del dominio a nivel local y su comparación a nivel global para identificar amenazas dirigidas, campañas de SPAM, botnes y similares.
    - Coocurrencias de dominios.
    - Sistemas Autónomos (AS por sus siglas en inglés).
    - Capacidad para buscar dominios mediante expresiones regulares
- Para mayor visibilidad, deberá poder integrarse con un servicio de Directorio Activo.
- Permitir al administrador poder comparar las solicitudes hacia un dominio específico que provenga de la institución con un estadístico de las solicitudes que se hacen desde el resto del mundo, permitiendo comparar e identificar posibles ataques objetivos hacia la institución.
- Contar con un API de integración con otras herramientas, con integraciones ya hechas y la capacidad de desarrollar las integraciones propias.
- Contar con una herramienta que ayude a generar reportes dentro del mismo portal para identificar los dominios maliciosos más solicitados.
- Contar con un mecanismo de identificación de uso de dominios relacionados con servicios de nube.
- Incluir sin costo adicional el soporte de un grupo de investigación, el cual se dedique a rastrear amenazas proporcionando una compresión integral de las amenazas cibernéticas, causas y alcances de propagación a través de al menos las siguientes tecnologías:
    - Basado en correo electrónico
    - Basado en la navegación (web)
    - Puntos finales (end points)
    - Redes
    - Nube
- Incluir sin costo adicional una herramienta del mismo fabricante que permita correlacionar indicadores de compromiso observados por el servicio para simplificar tareas de investigación y respuesta a incidentes.
- Los data centers del fabricante deben ser certificados ISO27001/SOC2

Características Técnicas

- Contar con un cliente ligero que permita identificar amenazas en los equipos portátiles independientemente de la red en la que se encuentren.
- Contar con la capacidad de montar un servidor local que permita la integración con la red local e identificar los equipos originadores de tráfico malicioso. Dicho servidor no realizará funciones de resolución de dominios para no duplicar funcionalidades en el servicio.
- El servidor local deberá ser replicable de manera virtual para mayor escalabilidad y redundancia, por lo que no se aceptan dispositivos físicos. Podrá ser montado en al menos los siguientes hipervisores:
    - VMWare ESXi
    - Hyper-V.

Administración

- La consola de administración y generación de reportes se encontrará en sitio y deberá tener la capacidad de generar diferentes usuarios y roles con diferentes privilegios (RBAC)
- Soportar la creación de múltiples roles, en el cual se permita o niegue el acceso a los diferentes dispositivos, o se otorguen privilegios o no para la administración, visualización de eventos o generación de reportes.
- Se deberá contar con una API abierta para la integración con orquestadores, generación de reportes. Cualquier desarrollo a través de las APIs será acordado entre la CONDUSEF y el proveedor del servicio.

6.6. SERVICIO DE SEGURIDAD CONTRA AMENAZAS EN EL DISPOSITIVO FINAL

Se requiere de un servicio de protección en el dispositivo final que permita la detección y contención de amenazas. Este elemento deberá de otorgar análisis retrospectivo del ambiente, así como la integración de inteligencia global que permita detectar amenazas dirigidas y de día cero.

Requerimientos generales

a) Debe administrar por lo menos 1500 agentes de protección para endpoints desde un único sistema de administración desplegado en sitio (On-premise) de CONDUSEF. Solo conectándose a internet para descargar los nuevos Indicadores de Compromiso desde la misma consola.

b) Soporte para integrarse con soluciones de terceros como (SIEM, IR management, SOAR, etc.).

c) El servicio debe tener la capacidad de integrarse de forma nativa, sin ningún desarrollo adicional al Servicio De Respuesta y Visibilidad Unificada De Incidentes De Seguridad especificado al final de este anexo para poder orquestar y responder a incidentes de seguridad.

Funciones

- Debe ser capaz de usar, crear y editar ioc's (Indicio de compromiso) para actividades de respuesta a incidentes.
- Debe soportar OpenIoC.
- Debe automáticamente correlacionar eventos de seguridad, actividades sospechosas y condiciones de tráfico para crear y administrar indicativos de comprometimiento en tiempo-real.
- Permitir poner automáticamente en cuarentena amenazas en tiempo-real sin la necesidad de estar integrados con sistemas de monitoreo de redes sean estos del mismo fabricante o terceros.
- Permitir la detección y envío de archivos de forma automática para análisis dinámica (sandbox) o estático con prevalencia baja en el ambiente monitoreado.
- Permitir la detección de software vulnerable presente en el endpoint de esta forma:

    - No depender de un proceso de escaneo o calendarización para identificar software vulnerable.
    - No debe depender de una política de análisis de vulnerabilidades para identificación.
- Debe permitir informar la fecha, hora y listar cuales dispositivos tienen el software vulnerable.
- Informar el CVE (Common Vulnerabilties and Exposures) asociado al software vulnerable detectado.
- Debe permitir la protección de activos cuando no estén en la red interna.
- Debe permite crear automáticamente y mantener un historial o flujo de trabajo forense para:
    - Identificar Causa raíz del malware, por sí mismo aun cuando no sea detectado como malware la causa original.
    - Identificar y seguir en tiempo-real actividades de creación, movimiento, ejecución de archivos y procesos, aun cuando no sean detectados o conocidos como malware.
- Permitir las condiciones anteriores de forma automática y simultánea en todos los activos monitoreados en el ambiente.
- Permitir identificar cambios en la clasificación de seguridad de archivos, aplicaciones y procesos de forma automática y sin necesidad de una acción del administrador como escaneo o ejecución.
- Debe hacer uso de recursos de inteligencia global en tiempo-real sin necesidad de calendarizar e identificar cambios en la postura de amenazas en el ambiente monitoreado.
- Debe integrarse con soluciones de monitoreo y prevención de amenazas avanzadas de red nativamente.
- Tener una API programable, documentada para personalizar e integrar acciones de prevención, respuesta y reporteo.
- Permitir cuarentena y alerta de amenazas no detectadas durante análisis inicial sea esta por escaneo o en tiempo-real.
- Debe usar diversos mecanismos de análisis, determinación y control de amenazas avanzadas en software único en el endpoint que incluye sin costo adicional recursos antivirus tradicionales.
- Debe usar mecanismos de detección y prevención de exploración de vulnerabilidades en aplicaciones y/o procesos en el endpoint.
- Permitir la detección y prevención de amenazas de forma automática al obtener y evaluar en tiempo real metadatos de la estructura de archivos.
- Usar mecanismos de detección basado en machine learning.
- Usar mecanismos de detección basado en reputación global en tiempo real
- Usar mecanismos de detección antivirus
- Usar mecanismos de detección que implementa lógica fuzzy.
- Usar mecanismos de detección de heurística
- Usar mecanismos de detección comportamientos para identificar ataques ransomware
- Usar mecanismos para identificar rootkits
- Debe incluir sin costo adicional la posibilidad de activar de forma centralizada en la solución (a criterio del administrador) el recurso nativo de antivirus tradicional que incluye un mecanismo (motor) de detección y escaneo presente localmente en el endpoint.
- Permitir de forma nativa y opcional la integración con la tecnología de análisis cognitiva en larga escala para automatizar la identificación de amenazas e incidentes en el ambiente con la ayuda de soluciones proxy del mismo fabricante o de terceros.
- Permitir operar en ambientes que usan direcciones IP vía DHCP.
- Permitir rescatar archivos (en cuarentena) de sistemas remotos vía interface grafica.
- Poseer una interfaz para hacer búsquedas de eventos en todo el ambiente monitoreado por condiciones como nombre, extensión, dirección IP, dominios, acciones, resultados sandbox, vulnerabilidades e historial de uso.
- Identificar mutexes, strings, acceso a achivos, cambios del registro, archivos creados, comportamientos que indican maliciosidad.
- Permitir remediación y contención como:
    - Control de aplicaciones
    - Cuarentena de archivos
    - Terminar procesos
    - Bloqueo de trafico de red
- Crear detección personalizada automáticamente.
- Crear detección personalizada en distintos formatos soportados.

- Identificar amenazas personalizadas por uso de hash sha-256, MD5, datos y anomalías de sección de archivos.
- Permitir el uso de operaciones lógicas para datos de detección customizada.
- Permitir identificar, hacer el bloqueo y contención de amenazas en condición de día-cero o personalizadas.
- Debe de operar en modo auditoria o modo bloqueo.
- Implementar comunicación para administración por protocolos de seguridad.
- Permitir su uso en ambientes con proxy.
- Permitir modelo de uso Software as a Service (SaaS).
- Permitir modelo de implementación local en ambiente del cliente (on-premise).
- Permitir whitelists, blacklists para archivos, direcciones IP, CIDR.
- Permite definir exclusiones de forma personalizada por política, por grupo de activos protegidos y tipo de plataforma monitoreada.
- Permitir operación en paralelo con antivirus de terceros en el endpoint
- Permitir protección en tiempo-real por reputación global de amenazas.
- Permitir correlación generadas por recursos de análisis dinámico tipo sandbox de forma integrada y nativa (locales o en nube) con mecanismos globales de reputación y determinación automatizada.
- Debe nativamente implementar de forma automática y constante una reevaluación de postura de detección y debido a cambios de inteligencia de amenazas en escala global, de esta forma se promueve una postura proactiva en la respuesta a amenazas avanzadas y sus variantes, condiciones día-cero y actividades de respuesta a incidentes.
- Permitir definir password de protección para el agente en el endpoint.
- Automatizar la generación de reportes y notificaciones a los administradores.
- Permitir crear exclusiones de detección para: archivos/rutas (path), extensión de archivos, procesos (incluyendo rutas/path, hash y procesos hijos), wildcards y especificando amenazas (nombres).
- Permitir la correlación y consolidación automática de elementos conocidos como causa raíz de infecciones y propagación de malware en tiempo real.
- Realizar el análisis de causa-raíz de forma automática para todo el ambiente monitoreado de la siguiente forma:
    - Debe permitir establecer un intervalo de tiempo deseado para evaluación
    - Debe Informar la cantidad de sistemas afectados
    - Debe informa la cantidad de amenazas detectadas por cada una de las causas raíz identificadas
    - Debe informar el tipo de actividad identificada
    - Debe informar el tipo de amenaza identificada
- Soportar la visualización gráfica de un contexto en tiempo-real, historial de uso y detecciones en endpoints monitoreados, creando un soporte preciso para respuesta a incidentes y actividades de evaluación forense de incidentes de seguridad.
- Contar con protección contra ransomware sin depender de que la firma de amenaza sea detectada por patrón, detectando comportamientos de cifrado o modificación de archivos no autorizados.
- Detectar y proteger los puestos de servicio contra acciones maliciosas que se ejecutan en navegadores Web mediante secuencias de comandos en lenguajes tales como JavaScript, VBScript / ActiveX, etc.
- Detectar y boquear scripts ejecutados por las DLL legítimas de Windows.
- Evitar infecciones provocadas por la ejecución del archivo Autorun.inf contenido en un dispositivo USB al momento de ser conectado en el equipo de cómputo.
- Permitir determinar la realización de análisis dinámico para archivos o artefactos observados en las estaciones monitoreadas en el contexto de la solución, de forma que permite establecer nuevas capacidades de detección, prevención y contención de amenazas en desarrollo en el ambiente.
- Permitir de forma automática la captura y el registro de acciones en la línea de comandos durante el desarrollo de ataques y acciones sospechosas.
- Permitir definir un repositorio de archivos obtenidos a partir de los endpoints monitoreados para análisis dinámica sandbox.
- Debe permitir integración nativa con sistema de análisis machine learning y cognitiva que implemente la correlación de accesos y eventos de sistemas web proxy
- Permitir la creación de snapshots para análisis forense post-mortem

- Permitir la identificación de Indicadores de Compromiso (IOC) en su ambiente alineados a Mitre Attack
- Permitir la creación de acciones automatizadas en las políticas de respuesta a incidentes

Características Técnicas

- Soportar:
  - Microsoft Windows 7, Microsoft Windows 8, 8.1, Windows 10
  - Microsoft Windows Server 2003/2008/2012/2016
  - Mac OS X 10.11, 10.12, 10.13
  - Centos 6.8/6.9/7.3/7.4
  - Redhat Enterprise Linux 6.5/6.6/6.7/6.8/7.2/7.3
  - Y versiones posteriores de los Sistemas Operativos antes mencionados.

Administración

- La solución tecnológica debe administrarse desde una consola, la cual permita la configuración de los agentes de protección instalados en los correspondientes endpoints.
- Generar roles personalizados, asimismo desde la consola se deberá configurar permisos granulares para segregar y delegar operaciones y trabajos específicos a diversos usuarios o grupos de usuarios, así como perfiles de auditoría que solo permitan visualizar datos, pero sin la capacidad de modificar ninguna configuración.
- Debe presentar un log de auditoría de todas las actividades de los usuarios.
- Deberá ser capaz de guardar logs de los eventos de control de los equipos de cómputo.
- Las bitácoras de la solución deberán contener como mínimo la siguiente información:
  - Usuario
  - Hostname de equipo
  - Evento detectado
  - Acción
  - Versión de la aplicación

6.7. SERVICIO DE RESPUESTA Y VISIBILIDAD UNIFICADA DE INCIDENTES DE SEGURIDAD

Se requiere un servicio que permita integrar soluciones de Seguridad y que permita una experiencia de visibilidad unificada, colectando eventos e indicadores de los servicios de seguridad requeridas anteriormente, y permitiendo coordinar acciones de contención y mitigación entre múltiples herramientas.

Requerimientos generales

a) La plataforma de la solución propuesta debe habilitar la automatización y fortalecer la seguridad a través de la red, el punto final, la nube y las aplicaciones.

b) Debe permitir la integración de soluciones de manera simple y que cada fuente de inteligencia global o local sea proporcionada por un módulo y se vincule a través de una clave tipo API

c) Debe contar con un módulo de orquestación para automatizar procesos de seguridad, como la investigación de amenazas y remediación, a fin de reforzar la eficiencia operativa y la precisión.

d) El módulo de orquestación debe permitir trabajar sobre diferentes dominios donde se permita la interacción con sistemas, aplicaciones, bases de datos y redes.

e) La consola de investigación de incidentes de seguridad deberá tener una disponibilidad del 99.99% durante todo el periodo del contrato.

.

Funciones

- Colaborar con flujos de trabajo compartidos
- Contar con la funcionalidad de realizar acciones proactivas y de respuesta de seguridad
- Contar con el acceso a métricas
- Asegurar la operación y reducir el riesgo de error humano
- La plataforma debe poder ser accedida vía SSL o TLS y con soporte a los siguientes navegadores:
    - Google Chrome™
    - Microsoft Edge®
    - Mozilla Firefox®
    - Apple® Safari®
- Dentro de la plataforma deberá incluir las siguientes herramientas:
    - Un tablero de visualización inicial e inteligencia personalizable (Debe ser posible la creación de hasta 5 tableros)
    - Un panel de aplicaciones e integraciones
    - Un panel que presente métricas y datos de los productos integrados
    - Un panel de noticias de industria y blog de seguridad
    - Una barra persistente a través de las soluciones que incluya las capacidades de flujos de trabajo, respuesta a incidentes y búsqueda de amenazas

7. SERVICIO DE OPERACIÓN

Descripción del Servicio

Estos Servicios de Operación son Servicios que deben venir incluidos en el Servicio de Seguridad Perimetral y se requieren para cumplir con la atención, registro, resolución de incidentes, problemas y solicitudes de servicio, que permitan la continuidad operativa, en los niveles de servicio indicados; realizando monitoreo de la operación de los elementos de Seguridad requeridos.

7.1. MESA DE AYUDA

El Proveedor del Servicio deberá implementar una Mesa de Ayuda, La cual será identificada por La Convocante como “Mesa Especializada de Servicios “MES”, con capacidad para atender todos los tickets que se generen y que le lleguen apegándose en todo momento al proceso de Administración y seguimiento de solicitudes, requerimientos, Incidentes y problemas, del MAAGTIC-SI vigente o en su caso el que lo sustituya.

La MES es el centro de atención del Proveedor del Servicio ubicado en sus instalaciones, el cual hará uso de herramientas para monitoreo para el servicio proporcionado, con el propósito de cumplir con los requerimientos de nivel de servicio

El Proveedor del Servicio, alineará todos sus procesos relacionados con la administración del servicio provisto a La Convocante al MAAGTIC-SI vigente o en su caso el que lo sustituya, lo anterior considera a la Mesa Especializada de Servicios y a todos los procesos de entrega y soporte del servicio, a saber:

- Administración de configuraciones.
- Administración de cambios.
- Administración de incidencias.
- Administración de problemas.
- Administración de liberaciones.
- Administración de la capacidad.
- Administración de los niveles de servicio.
- Administración de la disponibilidad.

a) La Mesa Especializada de Servicios del Proveedor del Servicio será responsable en todo momento de la satisfacción de los usuarios en materia de los servicios proporcionados por el Proyecto, asegurando que los incidentes y problemas reportados sean resueltos dentro de los niveles de servicio establecidos, realizando o emprendiendo acciones para eliminar las causas raíz y/o para prevenir fallas potenciales.

b) Se requiere que la solución sea implementada, puesta a punto, en un máximo de 60 días naturales posteriores a la fecha del inicio del contrato derivado de este proceso licitatorio. Así como integrada a la mesa de ayuda de La Convocante.
c) Para seguimiento de reportes, el Proveedor del Servicio deberá implementar durante la vigencia del contrato y sin costo adicional para La Convocante, una herramienta de gestión, que tenga la capacidad de generar y compartir registros históricos, consultas, generación de reportes y seguimiento a los eventos presentados y la solución correspondiente, la cual deberá contar con acceso a la información para La Mesa Especializada de servicios (MES), La Mesa de Ayuda de La Convocante y los Responsables del Proyecto que La Convocante designe. Para gestionar en todo momento los reportes desde su apertura, atención, solución y cierre, el Proveedor del Servicio deberá generar cuentas de lectura para el acceso.
d) Funciones generales de la Mesa Especializada de Servicios:
    - Apegarse a lo establecido en el manual administrativo de aplicación general en las materias de tecnologías de la información y comunicaciones y de seguridad de la información MAAGTIC-SI vigente o en su caso el que lo sustituya.
    - Cumplir con los niveles de servicio definidos por La Convocante para la atención de los reportes, solicitudes de servicio, incidentes y problemas.
    - La solución de software deberá estar basada en el manejo de procesos del MAAGTIC-SI vigente o en su caso el que lo sustituya y administrar como mínimo los módulos de: Recepción de reportes, solicitudes de servicio o de información, incidentes y problemas, manejo de incidentes, manejo de problemas y reportes de estadísticas e indicadores.
    - Proporcionar atención y soporte para mantener la operación de la seguridad perimetral, conforme a los niveles de servicio establecidos.
    - Deberá iniciar operaciones al inicio de los servicios.
    - Deberá operar con un horario de servicio 7x24x365, brindando la atención de acuerdo a los niveles de servicio establecidos.
    - Los responsables del proyecto designados por La Convocante, podrá levantar incidentes y notificar a la MES vía telefónica y/o correo electrónico para la pronta solución de este.
    - Las tareas mínimas que el Proveedor del Servicio deberá realizar con La Convocante son: recibir, registrar, analizar, resolver y canalizar los reportes de incidentes, dar seguimiento, solución y cierre a los incidentes informando a los responsables asignados por La Convocante, para que a su vez se informe al usuario final oportunamente.
    - La atención y soporte deberán realizarse con la interacción y comunicación permanente entre La Convocante y la Mesa Especializada de Servicios.
    - La Mesa Especializada de Servicios deberá tener la capacidad suficiente para almacenar y recuperar todos los reportes que se presenten durante la vigencia del contrato, clasificados por tipo de evento, por mes y por año.
    - Los datos mínimos requeridos en un reporte para el control de eventos e incidentes deberán ser:
        - Identificador del reporte o número de incidente o evento.
        - Identificador del usuario que reporta, (estos son los datos que identifican al usuario que levantó el reporte), al menos nombre, teléfono, correo electrónico y ubicación. La definición final de estos datos se acordará con el Proveedor del Servicio.
        - Hora en que se presenta el evento reportado.
        - Hora en que se reporta el problema por parte del usuario autorizado.
        - Tiempo de solución del incidente y restablecimiento del servicio.
        - Descripción del ticket.
        - Solución del ticket.
e) Cuando se presenten interrupciones, fallas, degradaciones en el desempeño en alguno de los equipos del servicio solicitado, el Proveedor del Servicio informará al personal técnico de La Convocante a través de un correo electrónico, llamada telefónica y mensaje de texto la falla del servicio que requiera atención.
f) Una vez resuelto el problema reportado, el personal asignado por el Proveedor del Servicio informará al personal técnico de La Convocante, la causa del problema y la solución de la misma, con el fin de validar que el servicio fue restablecido y cuente con la información para generar las estadísticas de disponibilidad del servicio de acuerdo a los niveles de servicio requerido.

g) Una vez recuperado el servicio, el Proveedor del Servicio documentará las acciones aplicadas para el cierre del reporte.
h) A solicitud del personal técnico de La Convocante el Proveedor del Servicio entregará un diagnóstico documentado y un plan de solución definitiva a los problemas que generaron interrupción general o parcial del servicio de seguridad perimetral, así como en degradaciones en el desempeño en alguno de los equipos del servicio solicitado.
i) El Proveedor del Servicio, en conjunto con La Convocante, definirá, actualizará y difundirá el catálogo de servicios que proporcionará la Mesa Especializada de Servicios.
j) El Proveedor del Servicio deberá proporcionar a La Convocante al menos una clave de acceso de solo lectura a los equipos de la solución, con el propósito de que se pueda revisar los parámetros de operación del equipo.
k) El Proveedor del Servicio, deberá configurar al menos una comunidad SNMP v3 con derechos de lectura, independiente a la comunidad que el Proveedor del Servicio utilice para el monitoreo de los diferentes equipos de comunicaciones que formen parte de su servicio y se encuentren en instalaciones de La Convocante. Esta comunidad tendrá como objetivo, monitorear todos estos equipos desde un sitio diferente al SOC, con uno o más servidores de La Convocante (o un tercero definido por ésta). En estos servidores se recibirá la notificación automática de incidentes y envío de traps SNMP, según parámetros establecidos por La Convocante, que permitan tener visibilidad sobre variables importantes de desempeño. El número de comunidades será al menos uno.
l) Deberá contar con la opción de extraer e interpretar datos relacionados con el estado y el desempeño de los dispositivos que componen la red de La Convocante.
m) Los registros generados por las herramientas de monitoreo implementadas serán los que se utilizarán para validar los niveles de servicio proporcionados por el Proveedor del Servicio, de acuerdo a los requerimientos de La Convocante y bajo los niveles de servicio definidos en el apartado de Niveles de Servicio.
n) El Proveedor del Servicio deberá proporcionar, previo a la puesta en operación de los servicios, una matriz de escalamiento, la cual contenga al menos la información de los contactos (nombre, puesto, teléfono oficina, teléfono móvil) para su localización en todo momento, así como los tiempos establecidos para pasar al siguiente nivel.

7.2. CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

La Convocante requiere que el proveedor del servicio cuente con un Centro de Operaciones de la Seguridad (SOC) propio y que se encuentre físicamente en sus instalaciones. El objetivo de este centro deberá de ser la gestión de la seguridad y responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad propuestas, además de ejecutar actividades de revisiones de seguridad, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable. El Proveedor del servicio deberá aplicar la proactividad (prevención) necesaria para evitar ataques e incidentes de seguridad y en su caso detectarlos y contenerlos de la red del Instituto. El Centro de Operaciones de la Seguridad (SOC) por ningún motivo podrá ser administrado y operado por un tercero contratado por el Proveedor del Servicio.

A fin de garantizar los niveles de servicio requeridos, el Proveedor del Servicio debe cumplir como mínimo las siguientes especificaciones:

a) El Centro de Operaciones de Seguridad (SOC) deberá ser propiedad del Proveedor del Servicio, y debe de tener la capacidad de servicios solicitada y cumplir con todos los requisitos humanos, técnicos y normas establecidas en el presente anexo.
b) Deberá operar de manera continua las 24 hrs. del día, los 7 días de la semana y durante los 365 días del año (7x24x365), esto último conforme la vigencia del contrato.
c) Deberá proporcionar la atención a las necesidades en cuanto a solicitud de cambios, reportes y atención de incidentes, así como consultas con relación al estado de la seguridad del Instituto.
d) Deberá contar con personal para atención del servicio de forma remota, el cual se debe estar calificado con base en las credenciales requeridas para la administración y monitoreo de los componentes que integran la solución.

e) Deberá contar con infraestructura dedicada para la administración, operación y monitoreo de los componentes de hardware y software que componen los servicios de seguridad.
f) Deberá realizar evaluaciones operativas a los servicios (herramienta de software y activos de infraestructura) que permitan identificar, entre otros: mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software.
g) Deberá realizar acciones correctivas y preventivas para asegurar la confidencialidad, integridad y disponibilidad de la información que se maneja en las diferentes soluciones de seguridad.
h) Deberá realizar la aplicación de las actualizaciones por parte del Licitante para nuevas versiones de sistema operativo, parches, o de cualquier actualización en software recomendada por el fabricante para la correcta operación de los dispositivos; la aplicación no deberá exceder las 48 horas desde que el fabricante informe sobre la necesidad o conveniencia de aplicarla y deberá ser programada con el Instituto en caso de que afecten la disponibilidad del equipo. Si la aplicación es urgente deberá hacerse del conocimiento y aprobación por parte del Instituto, para evitar riesgos a la operación. En ambos casos deberá estar evaluado por el Licitante y con el visto bueno del Instituto.
i) Deberá realizar notificaciones y alertas personalizadas en caso de desviaciones, anormalidades o brechas de seguridad para cada una de las soluciones de seguridad.
j) Deberá llevar a cabo revisiones continuas a la operación del SOC que permitan establecer mejora en los procesos, procedimientos y controles de seguridad.
k) Deberá contar con un Equipo de Atención y Respuesta a Incidentes de Seguridad.
l) Deberá dar soporte y atención a fallas a los componentes de hardware y software que integran la solución, conforme los estipulado en los acuerdos de niveles de servicio.
m) Deberá monitorear la disponibilidad de los componentes de hardware y software que integran la solución ofertada. La solución de monitoreo debe tener la capacidad de generar alertas y notificaciones en caso de fallas, degradación del desempeño de procesamiento de información, intermitencia y/o pérdida de disponibilidad.
n) Realizar mantenimiento correctivo a las soluciones de seguridad habilitadas.
o) Deberá contar con al menos 10 procesos operativos certificados en ISO/IEC 27001:2013, ISO/IEC 20000-1:2018, ISO/IEC 22301:2019 e ISO/IEC 9001:2015.
p) Deberá estar certificado como CERT y/o FIRST.
q) El servicio de requerimientos, cambios, incidentes, entre otros, deberá permitir la generación de eventos (tickets), mediante los mecanismos que se establezcan en las mesas de trabajo correspondiente, que de manera enunciativa más no limitativa, podrán ser:
    - Un número telefónico directo en las instalaciones del SOC.
    - Un número telefónico 800 sin costo.
    - Correo Electrónico
r) El personal del proveedor del servicio que atenderá las operaciones de los servicios de seguridad, deberá contar con experiencia probada en las áreas de tecnología y de seguridad de la información previamente mencionadas, para lo cual, deberá integrarse el Currículum Vitae de todo el personal que participe en el servicio, indicando al menos la experiencia requerida en cada caso en proyectos de Seguridad de la Información
s) El Instituto podrá solicitar la revisión de la infraestructura de seguridad por un tercero en cualquier momento, durante la vigencia del contrato, a fin de dar certeza de la entrega del servicio.
t) Deberá integrar una Base de Datos de la Gestión de la Configuración (CMDB por sus siglas en inglés) que contenga los detalles relevantes de cada elemento de configuración (CI) y de la relación entre ellos, incluyendo el equipo físico, software y la relación entre incidencias, problemas, cambios y otros datos del servicio de seguridad. La CMDB deberá incluir el control, mantenimiento y actualización de inventarios de los equipos de seguridad, incluyendo por lo menos la ubicación, modelo, número de serie, software instalado y versiones tanto en software como de hardware.
u) Deberá generar los reportes de Analítica de Información que permitan tener estadísticas del uso y desempeño de los servicios de seguridad, esto último con el objetivo de coadyuvar a la toma de decisión estratégica y operativa de los servicios, así como para determinar el plan de capacidad de cada tecnología implementada.
v) Deberá proporcionar al Instituto cuentas de acceso a las consolas de administración de los servicios de seguridad, así como herramientas en software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo-

lectura, y cuyos atributos de consulta se definirán en las mesas de trabajo que para este propósito se integren.

w) Las consolas de administración provistas para los servicios de seguridad deberán permitir visualizar al menos:
   - Políticas de Seguridad y de Control de Acceso
   - Configuraciones: Listas de Control de Acceso (Listas Blancas, Listas negras), Líneas base de seguridad.
   - Objetos: Usuarios, Grupos, Direcciones IP
   - Bitácoras.
   - Estadísticas: Desempeño, procesamiento, usuarios conectados, conexiones por segundo.

x) Deberá integrar un plan de continuidad de negocios (BCP, Business Continuity Plan por sus siglas en inglés), que integre aquellos servicios de seguridad del SOC que sean críticos para su operación.

y) El Licitante deberá llevar un proceso de control de cambios que se sujete a la aprobación de un comité conformado por los responsables de cada servicio tanto del Instituto como del Licitante. El control de cambios se apegará al MAAGTIC-SI vigente o en su caso el que lo sustituya.

z) El Licitante deberá considerar los siguientes tipos de control de cambios.

Tipo de Cambio	Definición	Tiempo de Solución
Urgente	Son todos los cambios a un componente de infraestructura de seguridad que se realiza para reparar lo antes posible una falla en algún servicio o que por su naturaleza pueden derivarse de un incidente o de un problema que afecte los niveles de servicio comprometidos y cuya única solución es a través de la aplicación de un cambio.	1 hr después de la solicitud de La Convocante.
Alto	Son todos los cambios a un componente de infraestructura de seguridad, los cuales implican una interrupción sustantiva en el servicio.	Con autorización de la ventana por La Convocante
Estándar	Son todos los cambios a un componente de infraestructura de seguridad, que no representan ningún riesgo de afectación.	4 hrs después de la solicitud de La Convocante

Modelo de Operación SOC

a) El Proveedor del Servicio deberá asegurar al menos 1 ingeniero certificado por el fabricante para cada una de las Tecnologías ofertadas para el SOC, los cuales deberán dar soporte y mantenimiento preventivo a la solución de seguridad de La Convocante, así como al hardware asociado, los sistemas operativos y programas que coadyuven a la operación de las herramientas durante el periodo de vigencia del contrato, con la finalidad de:

- Asegurar el correcto funcionamiento de las soluciones del software de la seguridad perimetral y de infraestructura de las soluciones propuestas.
- Asegurar el correcto funcionamiento del sistema operativo correspondiente para las soluciones del software de seguridad perimetral.
- Brindar asesoría a cada área para el monitoreo de cualquier módulo y del manejo de las soluciones de seguridad perimetral.
- Informar al personal designado por La Convocante sobre la última actualización disponible para las soluciones de seguridad, con el fin de valorar la necesidad de aplicarlas para que, en su caso, el Proveedor del Servicio lleve a cabo dichas actualizaciones.
- Analizar las políticas y reglas de la solución de seguridad de La Convocante, con el fin de llevar a cabo los ajustes y las correcciones en caso de ser necesario. Dichas correcciones serán realizadas por el Proveedor del Servicio bajo la supervisión del área técnica de cada área solicitante.

A continuación, se listan las credenciales y capacidades que deberán cubrir los recursos asignados al proyecto:

PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Gerente del Centro de Operaciones de Seguridad	Acorde a lo solicitado en “Competencias y/o habilidades que debe cumplir el personal propuesto”	5 años de experiencia en participación de proyectos de seguridad de la información.	Responsable de la administración, monitoreo, operación de los servicios proporcionados por el SOC.	Al menos 1 recurso
Coordinador Técnico del Centro de Operaciones de Seguridad	Acorde a lo solicitado en “Competencias y/o habilidades que debe cumplir el personal propuesto”	5 años de experiencia en participación de proyectos de seguridad de la información.	Responsable del soporte, atención a fallas e incidentes de seguridad.	Al menos 1 recurso
Líder de proyecto	Acorde a lo solicitado en “Competencias y/o habilidades que debe cumplir el personal propuesto”	5 años de experiencia en participación de proyectos de seguridad de la información.	Es la persona encargada de administrar y coordinar el proyecto.	Al menos 1 recurso
Operador de la mesa de servicio del Centro de Operaciones de Seguridad	Acorde a lo solicitado en “Competencias y/o habilidades que debe cumplir el personal propuesto”	5 años de experiencia en participación de proyectos de seguridad de la información.	Personal encargado de las operaciones de soporte de primer nivel, el monitoreo de los servicios, así como del registro y seguimiento de solicitudes de ventanas de mantenimiento, reportes de fallas y requerimientos.	Al menos 5 recursos (para garantizar el servicio 7x24x365 durante la vigencia del contrato).
Administración y Operación de soluciones y herramientas de seguridad	Acorde a lo solicitado en “Competencias y/o habilidades que debe cumplir el personal propuesto”	3 años de experiencia en participación de proyectos de seguridad de la información.	Operar administrar y monitorear las soluciones de seguridad propuestas.	Al menos 3 recursos
Analista de Seguridad	Acorde a lo solicitado en “Competencias y/o habilidades que debe cumplir el personal propuesto”	3 años de experiencia en participación de proyectos de seguridad de la información.	Encargado de ejecutar las revisiones de seguridad sobre las aplicaciones y la infraestructura, así como prever, detectar, analizar, contener, erradicar, documentar incidente de seguridad.	Al menos 3

PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Especialista en Incidentes de Seguridad	Acorde a lo solicitado en "Competencias y/o habilidades que debe cumplir el personal propuesto"	3 años de experiencia en participación de proyectos de seguridad de la información.	Encargado de manejar incidentes de seguridad y dar de respuesta, abordándolos con eficacia a fin de reducir el impacto de los incidentes.	Al menos 3
Arquitecto Especializado en Redes	Acorde a lo solicitado en "Competencias y/o habilidades que debe cumplir el personal propuesto"	5 años de experiencia en participación de proyectos de redes y seguridad de la información.	Responsable de la administración, monitoreo, operación de los servicios proporcionados por el SOC, en lo que a servicios de interconexión de red se refiere, así como del soporte, atención a fallas e incidentes que se presenten en la interoperabilidad con otros proveedores y/o fabricantes.	Al menos 2 recursos

b) Competencias y/o habilidades que debe cumplir el personal propuesto.

- Gerente del Centro de Operaciones de Seguridad

Debe acreditar la siguiente certificación:

- Certified Information Security Manager (CISM)

De manera optativa podrá acreditar las siguientes certificaciones:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- GIAC Security Leadership (GSLC)
- EC-Council Certified Chief Information Security Office (CCISO)

Debe tener grado de Licenciatura y/o Ingeniería en área afín a Tecnologías de la Información y/o Electrónica.

Adicionalmente debe acreditar al menos 5 años de experiencia en participación de proyectos de seguridad de la información.

- Coordinador Técnico del Centro de Operaciones de Seguridad

Debe acreditar la siguiente certificación:

- Certified Information Systems Security Professional (CISSP).

De manera optativa podrá acreditar las siguientes certificaciones:

- GIAC Certified Incident Handler (GCIH)
- EC-Council Certified Security Analyst (ECSA)
- GIAC Security Operations Certified (GSOC)

- EC-Council Certified Incident Handler (ECIH)

Debe tener grado de Licenciatura y/o Ingeniería en área afín a Tecnologías de la Información y/o Electrónica.

Adicionalmente debe acreditar al menos 5 años de experiencia en participación de proyectos de seguridad de la información.

- Líder de proyecto

Debe acreditar al menos una de las siguientes certificaciones:

- EC-Council Project Management in IT Security (PMITS)
- PMI Project Manager Professional (PMP)

Debe tener grado de Licenciatura y/o Ingeniería en área afín a Tecnologías de la Información y/o Electrónica.

Adicionalmente debe acreditar al menos 5 años de experiencia en participación de proyectos de seguridad de la información.

- Operador de la mesa de servicio del Centro de Operaciones de Seguridad

El operador de la mesa de servicio debe acreditar la siguiente certificación:

- ITIL v4 Foundation Certification

Debe tener grado de Licenciatura y/o Ingeniería y/o Estudios Profesionales terminados, en cualquier caso, en área afín a Tecnologías de la Información y/o Electrónica.
Debe acreditar al menos 5 años de experiencia en participación de proyectos de seguridad de la información.

- Administración y Operación de soluciones y herramientas de seguridad

Cada persona de dicha plantilla debe tener grado de Licenciatura y/o Ingeniería y/o Estudios Profesionales terminados, en cualquier caso, en área afín a Tecnologías de la Información y/o Electrónica.
La plantilla de personal identificada como Especialista en Incidentes de Seguridad debe estar conformada por al menos 1 recurso humano.
Este personal debe acreditar una de las siguientes certificaciones:

- EC-Council Certified Incident Handler (ECIH)
- GIAC Certified Incident Handler (GCIH)

Debe tener grado de Licenciatura y/o Ingeniería en área afín a Tecnologías de la Información y/o Electrónica.
Debe acreditar al menos 3 años de experiencia en participación de proyectos de seguridad de la información.

- Arquitecto Especializado en Redes

La plantilla de personal identificada como Arquitecto Especializado en Redes debe estar conformada por al menos 1 recurso humano.

Debe acreditar una las siguientes certificaciones:

- CCIE (Cisco Certified Internetwork Expert)
- ITIL v4 Foundation Certification

Debe tener grado de Licenciatura y/o Ingeniería en área afín a Tecnologías de la Información y/o Electrónica.
Adicionalmente cada persona de dicha plantilla debe acreditar al menos 5 años de experiencia en participación de proyectos de seguridad de la información.

- Analista de Seguridad

La plantilla de personal identificada como Analista de Seguridad debe estar conformada por al menos 1 recurso humano.

Debe acreditar una de las siguientes certificaciones:

- EC-Council Certified Security Analyst (ECSA)
- EC-Council Certified Network Defender (CND)

Debe tener grado de Licenciatura y/o Ingeniería en área afín a Tecnologías de la Información y/o Electrónica.
Debe acreditar al menos 3 años de experiencia en participación de proyectos de seguridad de la información.
Los licitantes deberán incluir la documentación que respalde la información requerida, de manera enunciativa más no limitativa, curriculum vitae, comprobante de estudios acorde a lo requerido en cada perfil y certificaciones.
Los recursos humanos que el Licitante presente en la propuesta técnica con las certificaciones solicitadas no deberán tener cambio durante la vigencia del contrato; en caso de realizarlo dará aviso con 15 días naturales de anticipación a la CONDUSEF e indicando el recurso sustituto; el nuevo recurso deberá tener las certificaciones iguales o superiores al de la persona que deja de laborar para el Licitante; el personal presentado en la propuesta técnica será el que brindará la operación a los servicios requeridos por la CONDUSEF. La falta de alguno de los recursos, dará lugar a la aplicación de la deductiva correspondiente. La no presentación de los documentos que avalen la experiencia o capacidad de los Recursos Humanos solicitados afecta la solvencia de la propuesta.

En el monitoreo de los equipos de seguridad se deberá:

a) Centro de monitoreo con las siguientes características, como mínimo:
   - Acceso mediante controles de acceso biométricos o automatizados
   - Consolas de Monitoreo para visualizar los eventos
   - Laboratorio de pruebas y homologaciones.
b) Realizar la detección pro-activa de fallas mediante la generación de alarmas.
c) Notificar automáticamente las alarmas de cada dispositivo de seguridad para la escalación de la falla hacia el sistema de la Mesa de Ayuda.
d) Notificar automáticamente vía correo electrónico y/o vía telefónica a los responsables asignados por La Convocante al detectarse un incidente de seguridad.
e) Herramienta de monitoreo con acceso vía HTTPS para al menos 3 usuarios simultáneos de La Convocante.
f) Monitoreo del desempeño de los equipos de seguridad, incluyendo utilización de CPU, memoria, errores.
g) Capacidad de graficar por día, semana, de manera mensual y anual o incluso de manera personalizada a las necesidades de La Convocante. El monitoreo de los elementos de la solución de seguridad será en Tiempo Real en forma 7x24x365
h) Deberá especificar su centro de atención técnico para el seguimiento de reportes de incidentes, en sus cuatro niveles con un procedimiento de escalamiento que asigne el Proveedor del Servicio, indicando nombre, cargo, correo electrónico y teléfono celular.
i) La Convocante, tendrá derecho a solicitar en cualquier momento al Proveedor del Servicio, el reporte de un incidente de seguridad, así como la información recopilada en periodos específicos, incluyendo el diagnóstico; lo anterior se entregará en un máximo de 24 horas a partir de que La Convocante lo solicite por medio electrónico. Los alcances de este reporte de incidentes de seguridad serán definidos con el Proveedor del Servicio, como parte de las reglas de operación.

Herramientas de Monitoreo

a) Incluir todas las licencias, mantenimientos y actualizaciones necesarias tanto en software y hardware, para mantener su operación continua, con una disponibilidad del 99.9 % mensual de las mismas en el Centro de Operaciones de Seguridad.
b) Monitoreo en línea de las alarmas de seguridad generadas en los equipos de seguridad.
c) Levantamiento automático de un reporte en la herramienta del Centro de Operaciones de Seguridad al detectarse un incidente de seguridad por medio del sistema de monitoreo. Después de esto se deberá notificar inmediatamente al personal asignado por La Convocante sobre el incidente, mediante llamada telefónica, correo electrónico. Para atención de reportes de seguridad el Proveedor del Servicio deberá proporcionar un número único 01800 y una vez establecida la naturaleza, se deberá canalizar

con alguno de los ingenieros especialistas para su atención. En el caso de que falle el 01800, el Proveedor del Servicio deberá proporcionar un número local alternativo, interferir en el desempeño de la red y/o ancho de banda, no mayor al 5% de la capacidad del enlace

d) Una vez que es detectado algún incidente de seguridad se llama proactivamente a La Convocante para iniciar el proceso de soporte, el personal del Centro de Operaciones de Seguridad contará con una hora a partir de que se levantó el reporte, para que en forma remota contenga la incidencia a nivel perimetral, mediante los cambios pertinentes en la configuración de los equipos de seguridad proporcionados, en tanto se determina la corrección que el propio fabricante publique (concepto: día zero).

e) El Proveedor del Servicio deberá contar con una matriz de severidades la cual se definirá con La Convocante para la identificación de incidentes de seguridad usando una plataforma para la correlación de eventos que le permitan identificar un Incidente (evitar falsos positivos) con mínimo los siguientes niveles:

- Crítico**:** Incidente de alto impacto dado el riesgo que representa; puede, potencialmente, ocasionar afectación y/o daño en activos y/o servicios de La Convocante. Afectación total al servicio, pérdida total de algún dispositivo de seguridad o bien mediante la explotación de vulnerabilidades críticas en la infraestructura protegida.
- Medio: Incidente serio en el que hay una degradación, más no una afectación a los servicios e infraestructura que es protegida mediante las soluciones de seguridad. Bloqueo o bajo desempeño al acceder a ciertos servicios de red que requieren el uso de los dispositivos de seguridad, así como la pérdida parcial de alguna funcionalidad. Degradación en el servicio sin llegar a ocasionar caída del mismo.
- Estándar: Incidente menor que no trae consecuencias de impacto a los servicios e infraestructura protegida por las soluciones de seguridad. El incidente se da mediante fallas en visualización de bitácoras o problemas para comunicación de servicios internos del cliente.

a) El Centro de Operaciones de Seguridad deberá detectar y mitigar proactivamente los incidentes de seguridad catalogados como de día cero, contará con una hora a partir de la detección para contener la incidencia a nivel perimetral mediante los cambios pertinentes en la configuración de los equipos de seguridad proporcionados, en tanto se determina la corrección que el propio fabricante publique.

b) Notificación de Incidentes de Seguridad (mecanismos: e-mail, teléfono fijo, teléfono móvil): Son las vías que el Proveedor del Servicio empleará para comunicarse con el cliente ante cualquier incidente de seguridad.

c) Solución a Incidentes Críticos de Seguridad. El Proveedor del Servicio se compromete con La Convocante a:

- Identificar un incidente catalogado como Crítico, con atención inmediata.
- Descartar que se trate de un falso positivo
- Alertar del incidente mediante los mecanismos ya descritos
- Prevenir el ataque
- E implementar solución de remediación (previa notificación a La Convocante). Siempre que no incluya equipo de cómputo de La Convocante.

d) Solución a Incidentes de tipo medio (60 minutos): Es el tiempo en el cual el Proveedor del Servicio se compromete con La Convocante a:

- Identificar un incidente catalogado como medio.
- Descartar que se trate de un falso positivo
- Alertar del incidente mediante los mecanismos ya descritos
- Prevenir el ataque
- E implementar solución de remediación (en caso de que aplique previa aprobación del cliente)

e) Solución a Incidentes de tipo estándar (24 horas naturales): Es el tiempo en el cual el Proveedor del Servicio se compromete con La Convocante:

- Identificar un incidente catalogado como bajo
- Descartar que se trate de un falso positivo
- Alertar del incidente mediante los mecanismos ya descritos
- Prevenir el ataque

- E implementar solución de remediación (en caso de que aplique previa aprobación del cliente)

f) Una vez que la vulnerabilidad ha sido corregida por el Proveedor del Servicio se deberá proceder a realizar recomendaciones y tomar las medidas necesarias en los equipos de seguridad perimetral, para evitar que este tipo de incidencia se repita.

g) El tiempo de resguardo de información se determinará en conjunto con La Convocante, por lo menos 6 meses en línea y posterior el Proveedor del Servicio deberá considerar de forma preventiva, la posibilidad de contar con equipos y espacio necesario para resguardar la información por la vigencia total del contrato, al término del contrato deberá ser entregada a los responsables que La Convocante designe.

h) El Proveedor del Servicio deberá contar con un proceso ya definido de respuesta a incidentes de seguridad, el cual será revisado por personal que La Convocante designe y afinado por el Proveedor del Servicio de acuerdo a la retroalimentación recibida. Para esto, el Proveedor del Servicio deberá contemplar las sesiones de trabajo necesarias para que el proceso quede totalmente adecuado a las necesidades de La Convocante.

i) El Proveedor del Servicio deberá documentar el proceso de atención a La Convocante para requerimientos de cambios, reporte de fallas, solución de dudas.

j) El Proveedor del Servicio deberá presentar sus reportes tipo a generar como resultado de la operación, para que La Convocante los pueda revisar y, de acuerdo a sus necesidades, solicitar los cambios que considere pertinentes.

- Reportes Estándar: Son los reportes predefinidos a los cuales La Convocante tiene acceso para validar el desempeño del servicio contratado
- Reportes Personalizados: Es la capacidad para poder definir y ejecutar reportes a la medida del cliente en formato mínimo PDF.

7.3. ASISTENCIA TÉCNICA EN SITIO Y REMOTA

El Proveedor del Servicio deberá considerar en su proposición los recursos técnicos y humanos necesarios con experiencia de al menos 3 años en proyectos de seguridad de la información, el personal presentado en la proposición técnica será el que brindará la operación a los servicios requeridos por La Convocante para la prestación de asistencia en sitio de acuerdo a los niveles de servicio solicitados durante la vigencia del contrato.

La Convocante definirá y seleccionará las características del personal en sitio, como: horario, días de la semana, perfil entre otros. El Proveedor del Servicio deberá:

a) Integrar como parte de su solución las herramientas de monitoreo, infraestructura de hardware, software y seguridad que considere convenientes, así como el personal necesario para atención de fallas y soporte en sitio, dicha infraestructura y servicio se deberá mantener en la oficina central de La Convocante y será utilizada para atender la operación crítica, en horario de 7:00 a 20:00 hrs., de lunes a viernes.

b) El personal asignado por el Proveedor del Servicio para la administración monitoreo y soporte en sitio de la seguridad perimetral deberá atender sus actividades en las instalaciones de La Convocante de lunes a viernes en un horario de 7:00 a 20 horas. Para los horarios restantes (lunes a viernes de 20:01 a 6:59 horas, sábados y domingos), se deberá atender desde su(s) centro(s) de servicio(s) regional(es).

c) El Proveedor del Servicio deberá supervisar y en su caso corregir en forma proactiva, el estado lógico y físico de los equipos y enlaces de comunicaciones ofertados, utilizando para ello la infraestructura instalada en punto “Servicio de Operación”

d) El Proveedor del Servicio será el responsable en todo momento de mantener la comunicación entre las distintas instancias de asistencia y contará con la información pertinente para el escalamiento de fallas.

e) El Proveedor del Servicio, a través de personal en sitio, deberá garantizar a La Convocante la ejecución de los siguientes procesos:

- Administración y monitoreo continuo de la operación de la red para la prevención de fallas.
- Detección oportuna de fallas inclusive, previo a que sean reportadas por La Convocante.
- Recuperación del servicio conforme a la disponibilidad y niveles de servicio solicitados
- Diagnóstico y corrección de raíz en las fallas presentadas

- Control y gestión oportuna de los reportes de falla que le asigne el área técnica o la Mesa de Ayuda de La Convocante, hasta su cierre y Vo.Bo. de las áreas internas designadas por la misma.
- Notificación en tiempo real a través de una llamada telefónica a la Mesa de Ayuda de La Convocante, en el cual se indique los problemas y las interrupciones así mismo se deberá notificar los restablecimientos correspondientes a cada uno de los enlaces, equipos, interfaces o cualquier componente de la solución de seguridad que impacte el nivel de servicio solicitado. Proporcionar reportes para el cierre de fallas reportadas, documentando causa, diagnóstico y solución.

f) Emisión de la Información para la planeación de capacidad de la infraestructura de conectividad y servicios en la red, en base al monitoreo continuo y reportes estadísticos obtenidos.
g) Emisión de la Información para la planeación de capacidad de la infraestructura, anchos de banda de los canales y servicios en la red, en base al monitoreo continuo y reportes estadísticos obtenidos
h) Ejecución de altas, bajas y cambios, en la infraestructura, considerando:
   - **Altas**, como la nueva configuración o nuevo servicio del sistema de la solución de seguridad
   - **Bajas**, como la eliminación de un servicio integrante del sistema de la solución de seguridad
   - **Cambios**, como cualquier modificación en la configuración de la infraestructura que permita la reubicación de equipos terminales.
i) El Proveedor del Servicio deberá contar cuando menos con un centro nacional de soporte y atención a fallas las 24 horas, los 365 días del año, el cual trabajará en forma complementaria con el esquema de monitoreo y administración descrito en esta sección.
j) La Convocante proporcionará facilidades de espacio, iluminación, conexión a los servicios de voz y datos para la instalación de la infraestructura de administración, monitoreo y recuperación del servicio para el personal técnico que opere dicha infraestructura. Los alcances de estas facilidades por persona a brindar asistencia técnica son enunciativas más no limitativas y se listan a continuación:
   - Espacio Físico
   - 1 línea telefónica digital con aparato para realizar sólo llamadas locales
   - 1 puerto Ethernet para conexión a la red de La Convocante
   - 2 contactos eléctricos soportados a energía no regulada
k) La asistencia técnica y soporte remoto deberá cubrir los requerimientos especificados en la prestación del servicio.

8. ENTREGA DE SERVICIOS

8.1. IMPLEMENTACIÓN DE SERVICIOS AL INICIO DEL PROYECTO

El Proveedor del Servicio cumplirá con las fechas de instalación, de acuerdo al plan de trabajo de transferencia de servicios en el que detalla la entrega de los mismos. Dicho plan será propuesto por el Proveedor del Servicio, a La Convocante dentro de los 10 días hábiles posteriores al inicio de la vigencia del contrato y La Convocante realizará los comentarios pertinentes para su ajuste y aprobación final.

Se deberá realizar una junta de inicio de proyecto con La Convocante, que será realizada con el Administrador del Proyecto y el personal que designe La Convocante. Posteriormente se deberán realizar juntas de seguimiento. La periodicidad de estas juntas será establecida durante la junta de arranque.

Con el fin de garantizar la correcta ejecución del proyecto, durante el desarrollo el Proveedor del Servicio deberá considerar la participación de un Project Manager Professional que deberá estar certificado por el PMI (Project Management Institute) para lo cual deberá entregar copia de la documentación que lo acredite dentro de su proposición. Las funciones que desarrollará son las siguientes, las tareas son enunciativas y no limitativas:

- Plan de Trabajo de la Implementación
- Desarrollo del Plan de Trabajo

- Control del Plan de Trabajo
- Seguimiento a las actividades y ejecución del Plan de Trabajo
- Notificar a la Convocante sobre desviaciones en el Plan de Trabajo.
- Entrega de la memoria técnica final a la Convocante.

El plan de trabajo de la implementación de los servicios solicitados por La Convocante deberá ser detallado por día y durante el desarrollo del proyecto se deberá elaborar un reporte de avance donde se incluyan las desviaciones del proyecto.

El Proveedor del Servicio deberá entregar en la etapa de instalación de cada uno de los servicios solicitados, un inventario de todos y cada uno de los equipos y productos de software que formen parte de la solución propuesta el cual será validado por personal técnico de La Convocante.

El PMP deberá fungir como único punto de contacto entre La Convocante y el Proveedor del Servicio durante la fase de implementación de la red.

El Proveedor del Servicio deberá asignar una Oficina de Proyectos (PMO) para ejecutar la implementación de manera efectiva para La Convocante.

El Proveedor del Servicio y el Proveedor del Servicio de servicios actual, podrán establecer acuerdos de operación y comerciales que apoyen la transferencia de los servicios.

Los horarios de migración de los servicios se establecerán en coordinación con La Convocante.

Se considerará que los servicios son entregados al 100%, cuando el Proveedor del Servicio, cumpla con todos los puntos definidos en el formato de verificación de puesta en operación de los servicios solicitados por La Convocante y firmado de conformidad.
El Proveedor del Servicio deberá considerar para todas las tecnologías, para el diseño de la arquitectura, instalación, configuración, parametrización, pruebas, puesta en operación y ajuste fino de todas las soluciones integradas para el desarrollo del servicio. El diseño deberá estar basado en mejores prácticas y realizado por personal certificado.

- Se deberá considerar la asistencia por parte del fabricante hasta 2 eventos al año en caso de que algún incidente o falla no permita brindar los niveles de servicio solicitados, requerido soporte en sitio y sin costo para la Convocante

8.2. ENTREGA DE SERVICIOS DURANTE LA VIGENCIA DEL CONTRATO

Una vez concluida la entrega de los servicios, los tiempos de entrega máximos que se cumplirán durante la vigencia del contrato son los siguientes:

a) Puesta en servicio de nuevos servicios 45 días naturales a partir de la solicitud formal.
b) Baja de servicios dentro de los 5 días siguientes a la solicitud formal. Transcurrido dicho plazo, la prestación del servicio posterior será bajo responsabilidad del Licitante, sin costo para La CONDUSEF.
c) Estos tiempos comenzarán a contar a partir de que se emita la solicitud de servicios correspondientes por parte de La CONDUSEF.
d) Las notificaciones y/o respuestas serán válidas formalmente por oficio o de forma electrónica.

8.3. ENTREGABLE FINAL PARA LA ACEPTACIÓN FORMAL Y PAGO DE LOS SERVICIOS

Las entregas se darán por concluidas mediante el formato de verificación de puesta en operación de los servicios, el contenido de dicho formato, así como las firmas reconocidas para el mismo y otros aspectos serán definidos con el Proveedor del Servicio y La Convocante, previo a la puesta en operación del servicio.

El siguiente material deberá ser entregado a La Convocante, como entregable final del desarrollo del proyecto, dentro de los 15 días naturales después de la implementación de los servicios requeridos:

a) Documento de implementación del plan de continuidad de la operación de los servicios de seguridad perimetral.
b) Documento de análisis de impacto en la operación de los servicios de seguridad perimetral.
c) Documento de análisis de riesgos en la operación de los servicios de seguridad perimetral.
d) Documento de estrategia de reanudación y continuidad de la operación de los servicios de seguridad perimetral.
e) Metodología del mantenimiento al plan de continuidad de la operación de los servicios de seguridad perimetral.
f) La aceptación formal del inicio del servicio y para propósito del inicio de la facturación del mismo será en el momento en que se concluya con la instalación y puesta a punto de la totalidad de los servicios, la cual deberá ocurrir a más tardar a la fecha de fin de transición de los servicios identificados en el "Anexo1: Servicios de Seguridad Perimetral" como "Entrega inicial mínima", los cuales incluyen en forma enunciativa equipos, sistema de administración y monitoreo, así mismo deberán cumplir con las pruebas que La Convocante y el Proveedor del Servicio definan en la fase de planeación y en forma mínima con las pruebas que a continuación se detallan tanto en la Red Privada Virtual, el Acceso a Internet y solución de seguridad.
g) Validación del cumplimiento de la infraestructura de seguridad propuesta en cuanto a sus capacidades y características mínimas presentadas:
    - Modelo
    - Memoria
    - Interfaces
h) Validación de la aplicación y correcta funcionalidad de las políticas y reglas configuradas en forma mínima necesarias para la operación del servicio.
i) Al cumplimiento total de las pruebas de aceptación de los servicios se firmará el acta de aceptación y a partir de esta fecha empezará a contar la facturación.

8.4. MEMORIA TÉCNICA

Al final de los trabajos de instalación, el Proveedor del Servicio deberá entregar una Memoria Técnica en papel y medio electrónico, reflejando los aspectos técnicos de la infraestructura auxiliar implementada para brindar el servicio, misma que deberá incluir al menos la siguiente información:

a) Índice
b) Diagramas de conexión.
c) Inventario.
d) Configuraciones.

La infraestructura a instalar por parte del Proveedor del Servicio deberá estar debidamente etiquetada en un lugar visible para su identificación.

8.5. REPORTE DEL SERVICIO

Aplica para todos los reportes y será condicionante para el pago de la factura.
Con el objeto de medir el desempeño de los servicios proporcionados por el proveedor, será necesario generar los reportes de comportamiento, desempeño y disponibilidad los servicios solicitados, de acuerdo con los niveles de servicio definidos. Estos reportes serán entregados de forma electrónica.
Los reportes que, de forma enunciativa más no limitativa, serán entregados por el proveedor a la convocante, son los siguientes:

Número de reporte	Nombre y descripción	Frecuencia del reporte
1	• Administración de configuraciones • Cambio en la infraestructura	Cada mes durante los primeros 7 días hábiles

Número de reporte	Nombre y descripción	Frecuencia del reporte
	• Actualización de una memoria técnica integral de los servicios	
2	Reporte de atención y solución de incidentes que contenga lo siguiente: ✓ Tipos de incidentes ✓ Tiempo de solución (ttr) ✓ Si afectan o no la disponibilidad	Cada mes durante los primeros 7 días hábiles
3	Informes de gestión del soc (mesa de ayuda)	Cada mes durante los primeros 7 días hábiles
5	Reportes de las soluciones de seguridad con las que cuenta la convocante • Métricas de desempeño (%procesador, %memoria, %disco duro, donde apliquen) • Puertos tcp/udp y protocolos más utilizados • Top 20 de las aplicaciones utilizadas o pasando a través de la solución • Top 20 ip's más bloqueadas • Top 20 de las firmas de ataque más vistas • Top de los 20 usuarios o cuentas, según tráfico y tiempo de conexión • Top de las 20 páginas, según número de consultas y tiempo de conexiones • Consumo de ancho de banda por tipo de protocolo.	Cada mes durante los primeros 7 días hábiles
6	Reporte de actividades sospechosas e incidentes de seguridad mensuales	Cada mes durante los primeros 7 días hábiles

Todos los reportes se deberán programar y deberán generarse de manera sencilla y deberán permitir la agrupación de dispositivos y la concentración de distintas métricas en un solo reporte.
La interfaz de generación de reportes deberá permitir exportar de forma simple, y mínimo soportará la exportación a los siguientes formatos: pdf y csv.

8.6. REPOSITORIO DE INFORMACIÓN

1. La convocante tendrá únicamente acceso a su repositorio correspondiente, con el fin de realizar consultas, modificaciones o aprobar documentos; a continuación, se menciona parte de la información que al menos deberá estar contenida en el repositorio, ya que durante la vigencia se podrá ampliar:
   - Información sobre la infraestructura de los servicios de seguridad perimetral
   - Direccionamiento ip
   - Calendario de mantenimientos
   - Control de cambios
   - Procesos para el plan de continuidad de los servicios de seguridad perimetral
   - Copias de las configuraciones (versión de sistema operativo, configuración lógica, configuración física) actualizadas de todos los componentes del servicio
   - Memorias técnicas de las soluciones del servicio

- Documentación de los incidentes, requerimientos y soluciones.
- Planes de mejora de los servicios
- Reportes de niveles de servicio

2. El acceso al repositorio de información deberá ser a través del protocolo a través de un canal seguro y cifrado con interfaz web, al menos a 4 usuarios con sesiones simultáneas por la convocante, en caso de requerir más accesos se solicitarán por escrito sin costo alguno para la convocante.

3. Al final del contrato el Proveedor del Servicio deberá entregar en medio electrónico el total de la información generada durante la vigencia del contrato.

8.7. TRANSFERENCIA DE SERVICIOS AL FINAL DEL PROYECTO

El nuevo proveedor en su caso, deberá coordinar la transferencia de servicios con el proveedor actual (el proveedor motivo del proceso de este documento), así como con futuros proveedores de servicios en el caso de un cambio, elaborando conjuntamente la logística de transición, misma que será avalada y autorizada por la Convocante.
El nuevo proveedor y el proveedor de servicios actual, podrán establecer acuerdos de operación y comerciales que apoyen la transferencia de los servicios.
En el plan de transferencia de servicios del proveedor actual al nuevo proveedor, este último deberá detallar la entrega de la infraestructura, instalación, configuración, puesta a punto y operación de los servicios. Este plan, incluirá un apartado de “rollback” o regreso al punto de partida, en caso de no ser posible concluir al 100% la entrega de los servicios de acuerdo al plan de migración presentado en su proposición a la convocante.
En caso que se requiera, el nuevo proveedor, se coordinará con el proveedor actual del servicio, a fin de cumplir con el plan de migración presentado en su proposición a la convocante.

8.8. CONDICIONES TÉCNICAS PARA LA TRANSMISIÓN A UN NUEVO PROVEEDOR POSTERIOR AL TÉRMINO DEL CONTRATO

La obligación del proveedor que preste el servicio durante el periodo de transición a un nuevo contrato de servicios, se deberá realizar bajo las siguientes condiciones:

1. El proveedor, deberá garantizar los niveles de servicios durante el procedimiento de contratación de un nuevo “proyecto”.
   - El proveedor, al término de este proyecto, garantizará los niveles de servicio durante el periodo de transferencia de servicios al nuevo proveedor.
2. En su caso, el proveedor, integrará la infraestructura necesaria para conectarse al nuevo proveedor.
   - El proveedor, durante el periodo de transición que podrá durar máximo 2 meses, mantendrá la infraestructura que proporcione el servicio de la red virtual a la convocante con objeto de que el nuevo proveedor integre su infraestructura total de solución y no afecte sus procesos de operación.
   - Adicionalmente, es importante mencionar que el proveedor, dará todas las facilidades que la convocante considere pertinentes; para garantizar la transparencia en el proceso de transición al nuevo proveedor de servicios.
3. En su caso, el proveedor, se coordinará con el nuevo proveedor para realizar la migración progresiva del proyecto.
   - El proveedor, durante el periodo de transición hacia el nuevo Proveedor del Servicio, integrará un grupo de trabajo para la coordinación en la etapa de migración progresiva del proyecto, estableciendo un plan de trabajo donde se reflejen los límites y participación del proveedor, la convocante y el nuevo proveedor sobre los servicios con objeto de no afectar la operación de la red virtual de la convocante.
   - Es importante señalar que el proveedor, en conjunto con la convocante, apoyará a la integración continua y transparente de los servicios bajo las prioridades y normas que la convocante determine.

8.9. TRANSMISIÓN A TITULO GRATUITO

Al término de la vigencia del contrato, el Prestador del Servicio le transmitirá a la CONDUSEF la propiedad a título gratuito, de toda la infraestructura pasiva e infraestructura activa que elija la CONDUSEF dentro de sus instalaciones, así como el licenciamiento asociado, sin que esto implique un costo para la CONDUSEF.

Para efectos de lo dispuesto en el párrafo anterior, se entenderá como infraestructura pasiva los elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, dentro de las instalaciones de la CONDUSEF, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de procesamiento de datos, de telecomunicaciones y radiodifusión. En el mismo sentido, se entenderá como infraestructura activa a los elementos de las redes de telecomunicaciones o radiodifusión que almacenan, emiten, procesan, reciben o transmiten escritos, imágenes, sonidos, señales, signos o información de cualquier naturaleza.
Al término de la vigencia del contrato, la CONDUSEF podrá solicitar al Prestador del Servicio que retire de forma gratuita, parcial o totalmente la infraestructura pasiva e infraestructura activa dentro de las instalaciones de la CONDUSEF, de manera coordinada con la Dirección de Tecnologías de la Información y Comunicaciones de la CONDUSEF, a efecto de que, en forma simultánea con el retiro de la infraestructura pasiva e infraestructura activa, se realice la instalación de la nueva infraestructura que se instale en las Oficinas Centrales y las Unidades de Atención a Usuarios. La CONDUSEF a través de la Dirección de Tecnologías de la Información y Comunicaciones notificará al Prestador del Servicio a más tardar 90 días naturales antes de la terminación del contrato correspondiente, si requiere que retire parcial o totalmente la infraestructura pasiva e infraestructura activa, así como la forma y fechas en las que deberá hacer dicho retiro.

9. NIVELES DE SERVICIO

Descripción del Servicio

Los niveles de servicio estarán relacionados a los servicios en términos de disponibilidad, desempeño del servicio, entrega de los servicios, tiempo de solución a Incidentes (TTR por sus siglas en inglés), reportes y penalizaciones. En todos los cálculos para la determinación de niveles de servicio serán valores truncados a dos decimales.
El Proveedor del Servicio entregará a La Convocante los reportes del servicio solicitados en este documento. La evaluación se realizará tomando como base los reportes registrados en las Mesas de Ayuda de La Convocante, utilizando sus herramientas de medición; para la evaluación del servicio ofertado y el resultado del nivel de servicio proporcionado en el mes correspondiente.

Características Técnicas del Servicio

9.1. DISPONIBILIDAD CENTRO DE OPERACIÓN DE SEGURIDAD (SOC)

Incluir todas las licencias, mantenimientos y actualizaciones necesarias tanto en software y hardware para mantener la operación continua del servicio.

La disponibilidad se obtendrá a partir de:

1. Disponibilidad de las herramientas de seguridad
   - El Proveedor del Servicio, deberá mantener una disponibilidad de las herramientas de seguridad en una operación 7x24. Cuando algunas de estas no se encuentren disponibles y esto ocasione la pérdida de la información utilizada para la medición de disponibilidad.
   - El Proveedor del Servicio, mantendrá una disponibilidad en las aplicaciones de monitoreo y seguimiento de reportes, a través de un acceso web, en una operación 7x24.

9.2. DISPONIBILIDAD DE LA MESA DE AYUDA

El proveedor, mantendrá la disponibilidad de atención y recepción de llamadas que realice la convocante para la recepción, registro, análisis y solución de los reportes de incidentes bajo un esquema de operación de 7x24.
La mesa de ayuda deberá responder el 95% de los llamados dentro de un período de tiempo de 5 minutos y el máximo número de llamadas abandonadas, después de un tiempo de espera en cola de 20 segundos, no deberá de exceder de 5% mensual.

9.3. NIVELES DE SERVICIO APLICABLES A LOS ELEMENTOS DE SEGURIDAD

El Proveedor del Servicio, garantizará la seguridad mediante el monitoreo en tiempo real al estado de la seguridad relativo a los servicios ofrecidos en su proposición, así como sistemas de detección de intrusiones que pudieran ocurrir, brindando visibilidad, tanto en el flujo de datos y la postura de seguridad en La Convocante. En la siguiente tabla, se presentan los niveles de servicio esperados para las tareas de administración y monitoreo de la infraestructura de seguridad:

SERVICIO	NIVEL COMPROMETIDO
Atención a requerimientos de configuraciones de seguridad	30 minutos después de acordado el cambio entre el Proveedor del Servicio y La Convocante.
Tiempo de solución de incidentes de seguridad	Por prioridad: **Crítico** – Identificación y contención inmediata **Medio**- 60 minutos **Estándar**- 24 hrs Programado
Licenciamiento y entrega de actualizaciones	Licenciamiento y actualización del software proporcionado por el Proveedor del Servicio durante todo el contrato. Entrega de la media máximo 3 días hábiles después de liberada la versión
Administración y control de accesos remotos y túneles VPN	Tiempo máximo de solución: 2 horas después de la solicitud de La Convocante.
Control de cambios	Por tipo **Urgente** - Inmediato, una vez autorizado o solicitado por La Convocante. **Impacto Alto -**24 hrs Programado **Impacto Medio -**48 hrs Programado **Estándar -**24 hrs, una vez autorizado o solicitado por La Convocante.
Control de accesos	Cero accesos de usuarios o equipos no autorizados en la LAN, WAN e Internet.
Dictamen de actividades sospechosas	Tiempo máximo entrega de dictamen: 4 horas
Notificación y atención de actividades sospechosas	Crítico De acuerdo a la disponibilidad de aplicaciones y/o servicios Medio 60 minutos Estándar 24 hrs Programado.
Servicios de remediación de vulnerabilidades	Proceso de control de cambios iniciado en máximo 2 días naturales después de ser publicados por el fabricante.
Atención a Incidentes de día cero	Tiempo máximo de una hora a partir de la detección para contener la incidencia a nivel perimetral mediante los cambios pertinentes en la configuración de los equipos de seguridad.
Recursos Humanos Certificados para soportar los servicios	Disponibilidad de todo el personal solicitado durante la vigencia del contrato.

Control de accesos a páginas web o URL'S no autorizadas

En el caso de existir algún sitio web, al cual se tuvo acceso por primera vez por algún usuario de La Convocante que no se encuentre categorizado en la base de datos del Fabricante, el Proveedor del Servicio deberá considerar por lo menos 24 horas naturales para reclasificar el sitio en la categoría correspondiente; así mismo La Convocante podrán solicitar la reclasificación de URL's, las cuales deberán ser ejecutadas en un máximo de 24 horas naturales.

9.4. MEDICIÓN DE LA DISPONIBILIDAD DEL SERVICIO

La medición de la disponibilidad de los servicios, se realizará en forma diaria recolectando la información generada a través de la herramienta de monitoreo, acumulando esta información hasta el cierre del mes, en donde se realizarán los cálculos finales del comportamiento de la disponibilidad de los servicios durante ese periodo.

La información recolectada en forma diaria, no será compactada ni se realizarán promedios de los promedios al final del mes, la base de cálculo será la información que se obtenga en forma diaria.

El Proveedor del Servicio deberá proporcionar información al menos cada minuto, la cual se almacenará en una base de datos de la misma herramienta y estará disponible en cualquier momento (dentro del plazo de 90 días en línea) para La Convocante por medio de las herramientas de monitoreo mediante su vista WEB. Posteriormente a los 90 días naturales se podrán compactar los datos para la revisión requerida por La Convocante.

En caso de que ocurra algún incidente y no se vea comprometida la disponibilidad en las herramientas de monitoreo, pero si algún servicio o aplicación específica catalogada como critica para La Convocante, se calculará la deductiva con base al tiempo de afectación a dicho servicio o aplicación.

En todos los casos, al reporte mensual que presente el Proveedor del Servicio, se le podrán hacer los ajustes correspondientes a los tiempos de indisponibilidad justificados por La Convocante, en el entendido que estos tiempos justificados serán previamente acordados entre el Proveedor del Servicio y La Convocante, de acuerdo a las necesidades de soporte, mantenimiento, etc.; teniendo el Proveedor del Servicio que recabar la autorización expresa de La Convocante que se vea afectada por estas actividades.

En casos en los que sea necesario acceder al sitio, el personal del Proveedor del Servicio deberá notificar con anticipación de acuerdo con el procedimiento de La Convocante. En caso de que no se permita el acceso al personal, se detendrá el conteo del tiempo de no disponibilidad justo cuando personal del Proveedor del Servicio informe esta eventualidad a la Convocante, y ésta última corrobore la situación. En este caso, el tiempo volverá a contarse a partir de la hora en que esté disponible el acceso al sitio especificado, por La Convocante. Los procedimientos de acceso y los acuerdos operativos para el reinicio del conteo de la no disponibilidad serán definidos con el Proveedor del Servicio. Esto será aplicable en general, para todos los niveles de servicio siempre y cuando el diagnóstico del problema, acordado con La Convocante, identifique que la solución del mismo depende del acceso al sitio en cuestión.

La Convocante requiere de la gestión de niveles de servicio, de acuerdo a las disponibilidades mencionadas anteriormente, con la capacidad de monitorear, medir y dar seguimiento sobre la calidad de los servicios requeridos por La Convocante. La interfaz de generación de niveles de servicio deberá permitir exportar de forma simple y mínimo soportará la exportación a los siguientes formatos: PDF y CSV.

9.5. PENAS CONVENCIONALES Y DEDUCCIONES

El Proveedor del Servicio deberá cumplir con la entrega en tiempo y forma de los siguientes requerimientos para garantizar la continua operación de la nueva infraestructura de la CONDUSEF, de lo contrario con fundamento a lo dispuesto en el Artículos 53 y 53-Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, se hará acreedor a las penas convencionales o deducciones correspondientes.

Las Penas Convencionales se aplicarán por cada día natural de atraso en los plazos indicados para la entrega de cada requerimiento; los plazos establecidos serán contabilizados como días naturales.

CONCEPTO	PLAZOS ESTABLECIDOS	REQUERIMIENTO	PENALIZACIÓN
Entrada en operación del servicio conforme a	Al día hábil siguiente a la notificación del fallo	Entrada en operación del servicio	2 al millar por cada día de atraso del monto

lo establecido en este anexo técnico			total de la facturación mensual
Entrega de Plan de Trabajo de Implementación de Servicios	10 días hábiles posteriores al inicio de la vigencia del contrato	Plan de Trabajo de Implementación de Servicios	2 al millar por cada 48 horas de atraso del monto total del contrato
Entrega de la Memoria Técnica inicial	60 días naturales posteriores a la entrada en operación del servicio	Memoria Técnica Inicial	2 al millar por cada día de atraso del monto total de la facturación mensual
Entrega de la Memoria Técnica final	60 días naturales antes del término del servicio	Memoria Técnica Final	2 al millar por cada día de atraso del monto total de la facturación mensual
Entrega final del desarrollo del proyecto	15 días naturales después de la implementación del servicio	Entregable final del desarrollo del proyecto	2 al millar por cada día hábil de atraso
Entrega de reportes:	Cada mes durante los primeros 7 días hábiles de cada mes siguiente al mes que concluye	De administración de configuraciones y cambios en la infraestructura.	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios.
Entrega de reportes	Se entregarán dentro de los primeros 7 días hábiles de cada mes siguiente al mes que concluye	Reporte de atención y solución de fallas. Indicando los tipos de fallas, su tiempo de reparación (TTR), si afectan o no la disponibilidad. Informes de Gestión del SOC (Mesa de Ayuda)	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios.
Entrega de reportes	Se entregarán dentro de los primeros 7 días hábiles de cada mes siguiente al mes que concluye	Reportes de las soluciones de seguridad con las que cuenta la convocante ·Métricas de desempeño (%procesador, %memoria, %disco duro, donde apliquen) ·Puertos tcp/udp y protocolos más utilizados ·Top 20 de las aplicaciones utilizadas o pasando a través de la solución ·Top 20 ip's más bloqueadas ·Top 20 de las firmas de ataque más vistas ·Top de los 20 usuarios o cuentas, según tráfico y tiempo de conexión	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios.

		·Top de las 20 páginas, según número de consultas y tiempo de conexiones ·Consumo de ancho de banda por tipo de protocolo.	
Entrega de reportes	Se entregarán dentro de los primeros 7 días hábiles de cada mes siguiente al mes que concluye	Reporte de actividades sospechosas e incidentes de seguridad mensuales	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios.
Reporte de Incidente de Seguridad solicitado por la CONDUSEF	Se entregará dentro de los primeros 5 días hábiles posteriores a su solicitud por parte de la CONDUSEF	Reporte de un Incidente de Seguridad	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios.
Entrega de nuevos Servicios de Seguridad	Se entregarán dentro de los primeros 45 días naturales a partir de la solicitud formal	Entrega de nuevos Servicios de Seguridad	2 al millar por cada día de atraso sobre el importe de la facturación total mensual de los servicios.

En caso de que se presenten fallas en la prestación del servicio derivadas del incumplimiento parcial o prestación deficiente del mismo, se aplicarán las deducciones siguientes:

CONCEPTO	NIVEL DEL SERVICIO	DEDUCTIVA	MÁXIMO PERMITIDO
Monitoreo del SOC	Cuando no se cumplan con los niveles mínimos solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	2 al millar por hora de indisponibilidad sobre el nivel de servicio establecido y con base al importe de la factura total mensual.	Con un máximo de 3 eventos mensuales.
Atención a requerimientos de configuraciones de seguridad	Cuando no se cumpla con el tiempo máximo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada hora natural de atraso del monto total de la facturación mensual de los servicios correspondientes.	Con un máximo de 5 eventos mensuales por servicio.
Tiempo de solución a incidentes de seguridad	Cuando no se cumpla con los tiempos establecidos por prioridad solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada minuto de afectación a los servicios y/o aplicaciones y/o por atraso para la solución del mismo, sobre el monto total de la facturación mensual de los servicios correspondientes.	Con un máximo de 1 eventos mensual por servicio
Licenciamiento y entrega de actualizaciones	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada día hábil de atraso con base al monto total de la facturación mensual de la solución involucrada	Para todos los dispositivos del servicio cuando el fabricante emita una nueva licencia del software

Control de accesos a páginas web, URL's o aplicaciones.	Cuando no se cumpla con el tiempo máximo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar sobre el total de la facturación mensual de la solución involucrada, por cada día de atraso para la categorización, re categorización, bloqueo o acceso a los sitios o categorías web,	Con un máximo de 3 eventos mensuales por servicio
Accesos de usuarios o equipos no autorizados en el mes.	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	5 al millar por cada acceso de usuarios no autorizados con base al monto total de la facturación mensual de la solución involucrada.	• Para la solución de seguridad 5 accesos no autorizados máximo, durante 3 meses consecutivos • Para la solución de seguridad medio y estándar 10 accesos no autorizados máximo, durante 3 meses consecutivos
Control de cambios de las soluciones de seguridad.	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	2 al millar por cada hora natural de atraso con base al monto total de la facturación mensual de la solución involucrada.	Aplica para: Cualquier dispositivo de seguridad. Cuando se solicite un control de cambios en algún componente de las soluciones antes mencionadas.
Control de acceso	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	2 al millar por cada acceso no autorizado con base al monto total de la facturación mensual de la solución involucrada.	Aplica para: Cualquier dispositivo de seguridad Cuando se detecte algún acceso no autorizado por CONDUSEF.
Dictamen de actividades sospechosas	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada hora hábil de atraso con base al monto total de la facturación mensual de la solución involucrada	Aplica para: Cualquier dispositivo de seguridad cuando se detecte alguna actividad sospechosa.
Manejo de incidentes de día cero.	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada día de atraso del monto total de la facturación mensual de los servicios correspondientes al servicio(s) afectado(s)	Aplica para: Cualquier dispositivo de seguridad cuando se detecte algún incidente de día cero.
Personal Certificado para soportar los servicios.	Cuando no se notifique del cambio de los Recursos Humanos solicitados (Gestión del Personal Técnico) solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	2 al millar por cada día de indisponibilidad sobre el monto total de la facturación mensual de los servicios correspondientes al servicio(s) afectado(s)	Aplica para: SOC y personal en sitio

10. SERVICIOS COMPLEMENTARIOS

10.1. INFRAESTRUCTURA AUXILIAR

- El Proveedor del Servicio deberá suministrar en cada sitio de acuerdo a los requerimientos de los servicios solicitados los siguientes Racks o Gabinetes, cumpliendo con el estándar EIA310D.
- Rack 7 pies. De aluminio natural de 7 pies de altura x 19" de ancho para la colocación del equipo activo y UPS en los casos necesarios.
- Rack 4 pies. De aluminio natural de 4 pies de altura x 19" de ancho para la colocación del equipo activo y UPS en los casos necesarios.
- Gabinete de 42UR de alto, 0.6m de ancho X 1.0m de profundidad diseñado para el montaje y protección de equipos para toda su red puertas frontal y trasera metálica con ventilación y cerradura de seguridad panel laterales desmontables.
- Gabinete de 20UR de alto, 0.6m de ancho X 1.0m de profundidad diseñado para el montaje y protección de equipos para toda su red puertas frontal y trasera metálica con ventilación y cerradura de seguridad panel laterales desmontables.
- Los racks o gabinetes solicitados deberán ser aterrizados a la barra de tierra que se instalará o que ya se encuentre instalada, dentro del mismo cuarto de telecomunicaciones y deberá contar con los aditamentos necesarios para el montaje de los equipos propuestos.

11. CONFIDENCIALIDAD

Además de las obligaciones que emanan de la naturaleza del acuerdo del que da cuenta el presente Anexo Técnico, el receptor de la información estará obligado a:

- Mantener la información confidencial en estricta reserva y no revelar ningún dato de la información a ninguna otra parte, relacionada o no, sin el consentimiento previo de CONDUSEF.
- Instruir al personal que estará encargado de recibir la información confidencial, debiendo suscribir el correspondiente acuerdo de confidencialidad si fuere necesario, de su obligación de recibir, tratar y usar la información confidencial que reciban como confidencial y destinada únicamente al propósito objeto del acuerdo, en los mismos términos en que se establece en el presente Anexo Técnico.
- Divulgar la información confidencial únicamente a las personas autorizadas para su recepción dentro de la organización.
- Tratar confidencialmente toda la información recibida directa o indirectamente de CONDUSEF, y no utilizar ningún dato de esa información de ninguna manera distinta al propósito del presente Anexo Técnico.

Para cada uno de los recursos, en forma personalizada, el proveedor deberá entregar a CONDUSEF la(s) carta(s) de confidencialidad previamente aprobada(s) por la Institución, firmadas por el recurso y el representante legal.

12. GARANTIA

Garantía de cumplimiento

Para garantizar el cumplimiento del contrato que se le llegase adjudicar al Proveedor, se obliga a entregar dentro de los 10 (diez) días naturales siguientes a la fecha de firma del instrumento contractual, garantía (divisible o indivisible) en moneda nacional (pesos mexicanos) por el equivalente al 10% (diez por ciento) del importe del contrato que suscriba la CONDUSEF, sin considerar el impuesto al valor agregado, la cual deberá emitir a favor de la Tesorería de la Federación o a quien en su caso corresponda y cumplir con los requisitos establecidos en el artículo 103 del reglamento de la LAASSP, aplicable en la materia.
La garantía se deberá de entregar en el domicilio de la CONDUSEF.

13. PROPUESTA ECONÓMICA

El Proveedor del Servicio debe tener en consideración, en todo momento, que:
El Proveedor del Servicio deberá señalar en el Resumen Económico, los precios unitarios expresados en moneda nacional por cada Servicio solicitado en el presente Anexo Técnico.

ANEXO No. 2
"CÉDULA DE OFERTA ECONÓMICA"

El Proveedor del Servicio debe tener en consideración, en todo momento, que:

- El Proveedor del Servicio deberá señalar en el Resumen Económico, los precios unitarios expresados en moneda nacional por cada Servicio solicitado en el presente Anexo Técnico.

SERVICIO DE SEGURIDAD PERIMETRAL

No.	DESCRIPCION DEL SERVICIO	PRECIO UNITARIO MENSUAL
1	SERVICIO DE FILTRADO WEB	$ -
2	SERVICIO DE SISTEMA DE PREVENCIÓN CONTRA INTRUSOS (IPS)	$ -
3	SERVICIO DE PROTECCIÓN PARA APLICACIONES WEB (WAF)	$ -
4	SERVICIO DE PROTECCIÓN DE CORREO ELECTRÓNICO (ANTISPAM)	$ -
5	SERVICIO DE SEGURIDAD EN LA RESOLUCIÓN DE NOMBRES DE DOMINIO (DNS)	$ -
6	SERVICIO DE SEGURIDAD CONTRA AMENAZAS EN EL DISPOSITIVO FINAL	$ -
7	SERVICIO DE RESPUESTA Y VISIBILIDAD UNIFICADA DE INCIDENTES DE SEGURIDAD	$ -
	SUBTOTAL MENSUAL	$ -
	I.V.A.	$ -
	TOTAL	
	TOTAL POR 36 MESES CON I.V.A. INCLUIDO	$ -

Nota: Para el mes de septiembre de 2021, deberá cotizar el mes completo, sin embargo, para efectos de pago, solo se considerarán los días en los que se prestó el servicio.

Los montos deberán ser presentados a dos decimales.

La propuesta deberá presentarse en hoja membretada, por los licitantes incluyendo el lugar y fecha, así como la firma autógrafa del Representante o Apoderado Legal

Los precios de los servicios deberán permanecer fijos durante la vigencia del contrato y calculados antes del IVA.

Dichas cantidades comprenderán los costos directos e indirectos y todos los gastos que se originen como consecuencia de los servicios adquiridos.

MONTO: (LETRA.....)

Esta cotización se fundamenta en la convocatoria de la Licitación Pública Electrónica Nacional LA-006G3A001-XXX-20XX y está ligada a mi propuesta técnica, la cual cumple con los requisitos señalados y el ANEXO TÉCNICO para esta Licitación.

_____
NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL

ANEXO No. 3
"FORMATO DE ESCRITO PARA FORMULAR PREGUNTAS"

Ciudad de México a (día) (mes) (año).

Comisión Nacional Para la Protección y Defensa de los Usuarios de Servicios Financieros
Presente:

Licitación Pública Nacional Electrónica número LA-006G3A001-E***-202X

Nombre del licitante: _____.

El siguiente documento tiene como objetivo agilizar la respuesta a las preguntas sobre la presente Convocatoria de Licitación Pública, por lo que deberá anexar el escrito donde manifieste su interés de participar.

No. DE PREGUNTA	PUNTO DE LA CONVOCATORIA	PÁGINA(S)	PREGUNTA
1			
2			
3			
4			
5			
6			
7			

Instructivo:

En el campo No. de Pregunta, dar un número consecutivo a cada una de las preguntas que se encuentren en el listado. Es importante contemplar una sola pregunta por renglón.
En el campo Punto de la Convocatoria, seleccionar el punto al que se hace referencia la pregunta. Es importante contemplar solo un punto por pregunta, si existen varias preguntas sobre el mismo punto, seleccionar otra fila y el mismo punto. En el campo Página(s) escribir la página o páginas de donde se encuentra el punto de la Convocatoria con referencia a las preguntas.
En el campo Pregunta, redactar la pregunta sobre el punto de la Convocatoria en cuestión, de manera clara y precisa.
El correcto llenado de esta información y dentro del formato establecido, ayudará a agilizar la contestación de las mismas.

Atentamente__
Nombre completo (cuando se trate de persona física) y firma o del
Representante legal (cuando represente a una persona moral) y firma

ANEXO No. 4
"FORMATO PARA ACREDITAR LA PERSONALIDAD DEL LICITANTE"

_____, manifiesto bajo protesta de decir verdad, que los datos aquí asentados, son ciertos y han sido debidamente verificados, así como que cuento con facultades suficientes para suscribir la propuesta en la presente licitación pública, a nombre y representación de:_____

No. de Licitación Pública Electrónica Nacional: _____

Registro Federal de Contribuyentes:_____ Domicilio:_____ Calle y número:_____ Colonia:_____ Alcaldía o Municipio:_____ Código Postal:_____ Entidad Federativa:_____ Teléfonos:_____ Fax:_____ Correo electrónico:_____ No. de la escritura pública en la que consta su acta constitutiva:_____
Nombre, número y lugar del Notario Público ante la cual se dio fe de la misma:_____
Fecha y datos de su inscripción en el registro Público de Comercio _____ Relación de accionistas.-
Apellido Paterno: Apellido Materno: Nombre ____
Descripción del objeto social: **TRANSCRIBIR EN FORMA COMPLETA EL OBJETO SOCIAL TAL COMO APARECE EN SU ACTA CONSTITUTIVA** _____
Reformas al acta constitutiva:_____
Nombre del apoderado o representante:_____
Datos del documento mediante el cual acredita su personalidad y facultades:_____
Escritura pública número:_____ Fecha:_____
Nombre, número y lugar del Notario Público ante el cual se otorgó:_____

(Lugar y fecha)
Protesto lo necesario.
(firma)

Nota: El presente formato deberá ser reproducido por cada participante, debiendo respetar su contenido, en el orden indicado.

ANEXO No. 5
"FORMATO DE MANIFESTACIÓN DE NO ENCONTRARSE EN LOS SUPUESTOS DE LOS ARTÍCULOS 50 Y 60 DE LA LEY"

Ciudad de México a (día) (mes) (año).

Comisión Nacional Para la Protección y
Defensa de los Usuarios de Servicios Financieros
Presente:

Licitación Pública Nacional Electrónica número LA-006G3A001-E***-202X

___(nombre del licitante persona física) ____ bajo protesta de decir verdad manifiesto que el suscrito, no me encuentro en los supuestos de los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, no desempeño empleo, cargo o comisión en el servicio Público, o en su caso a pesar de desempeñarlo con la formalización del instrumento jurídico correspondiente no se actualizará conflicto de interés.

En caso de ser persona moral deberá indicar el nombre del representante legal y manifestar: que por sí o en representación de licitante _____ según se acredita en el Testimonio Notarial o Instrumento Jurídico No. _____ de fecha _____ otorgado ante el Notario Público No. _____ de la ciudad de _____, manifiesto, bajo protesta de decir verdad que ni el suscrito, y ninguno de los socios integrantes del licitante que represento, nos encontramos en los supuestos de los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, no desempeñamos empleo, cargo o comisión en el servicio Público, o en su caso a pesar de desempeñarlo con la formalización del instrumento jurídico correspondiente no se actualizará conflicto de interés.

Para ambos casos indicar que:

En el entendido de que de no manifestarme con veracidad, acepto que ello sea causa de las sanciones correspondientes.

Atentamente__
Nombre completo (cuando se trate de persona física) y firma
Representante legal (cuando represente a una persona moral)

ANEXO No. 6
"FORMATO DE DECLARACIÓN DE INTEGRIDAD"

Ciudad de México a (día) (mes) (año).

Comisión Nacional Para la Protección y Defensa de los Usuarios de Servicios Financieros
Presente:

Licitación Pública Nacional Electrónica número LA-006G3A001-E***-202X

_____, nombre de la persona física o del representante legal del licitante _____, quien participa en el procedimiento de Licitación Pública Nacional Electrónica número LA-006G3A001-E***-202X manifiesto que por mi o por interpósita persona, nos abstendremos de adoptar conductas, en la que los Servidores Públicos de la Comisión Nacional Para la Protección y Defensa de los Usuarios de Servicios Financieros, 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, conforme a lo dispuesto en el artículo 29 fracción IX de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 39, fracción VI inciso f) de su Reglamento.

Atentamente__
Nombre completo (cuando se trate de persona física) y firma o del
Representante legal (cuando represente a una persona moral) y firma.

ANEXO No. 7
"FORMATO DE ESCRITO DE CONFORMIDAD CON LA CONVOCATORIA"

Ciudad de México a (día) (mes) (año).

Comisión Nacional Para la Protección y
Defensa de los Usuarios de Servicios Financieros
Presente:

En relación con la Licitación Pública Nacional Electrónica número LA-006G3A001-E***-202X, declaro que he leído la presente Convocatoria y estoy conforme con los criterios de adjudicación, así como con todos y cada uno de los puntos que en ésta se señalan, asimismo los derivados de la junta de aclaraciones. La presentación de este escrito no me exime de la entrega de cualquier otro documento que sea solicitado por la Convocante.

Asimismo, manifiesta bajo protesta de decir verdad que toda la información y documentación presentada en el acto de apertura y presentación de proposiciones de la presente Convocatoria, es copia fiel de los originales que avalan dicha información, por lo que autorizan a la Convocante para que en cualquier momento verifique la autenticidad de dicha documentación e información, conociendo las consecuencias legales en caso de que la misma resulte apócrifa o se manifiesten hechos falsos.

Atentamente__
Nombre completo (cuando se trate de persona física) y firma o del
Representante legal (cuando represente a una persona moral) y firma

ANEXO No. 8
FORMATO DE LA ESTRATIFICACIÓN DE MICRO, PEQUEÑA O MEDIANA EMPRESA (MIPYMES).

Ciudad de México a (día) (mes) (año).

Comisión Nacional Para la Protección y
Defensa de los Usuarios de Servicios Financieros
Presente:

Me refiero al procedimiento de _____(1)_____ No. LA-006G3A001-E***-202X en el que mi representada, la empresa_____(2)_____, 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 _____(3)_____, y asimismo que considerando los criterios (sector, número total de trabajadores y ventas anuales) establecidos en el Acuerdo por el que se establece la estratificación de las micro, pequeñas y medianas empresas, publicado en el Diario Oficial de la Federación el 30 de junio de 2009, mi representada tiene un Tope Máximo Combinado de _____(4)_____, con base en lo cual se estatifica como una empresa _____(5)_____.

Atentamente__
Nombre completo (cuando se trate de persona física) y firma o del
Representante legal (cuando represente a una persona moral) y firma

INSTRUCTIVO PARA EL LLENADO DEL FORMATO.

NÚMERO	DESCRIPCIÓN
1	Precisar el procedimiento de contratación de que se trate (licitación pública o invitación a cuando menos tres personas)
2	Anotar el nombre, razón social o denominación del licitante
3	Indicar el Registro Federal de Contribuyentes del licitante.
4	Señalar el número que resulte de la aplicación de la expresión: Tope Máximo Combinado = (Trabajadores) x10% + (Ventas anuales en millones de pesos) x 90%. Para tales efectos puede utilizar la calculadora 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.
5	Señalar el tamaño de la empresa (Micro, Pequeña o Mediana), conforme al resultado de la operación señalada en el numeral anterior.

ANEXO NO. 9
"FORMATO PARA LA MANIFESTACIÓN DE LA NACIONALIDAD DEL LICITANTE"

Ciudad de México a [día] [mes] [año]. (1)

COMISIÓN NACIONAL PARA LA PROTECCIÓN Y
DEFENSA DE USUARIOS DE SERVICIOS FINANCIEROS
P R E S E N T E.

Me refiero a la Licitación Pública Electrónica Nacional No. __(2)____ en el que mi representada, la empresa _____(3)_____ participa a través de la propuesta que se contiene en el presente sobre.

Sobre el particular y en los términos de lo previsto en el artículo 35 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; declaramos bajo protesta de decir verdad, ser proveedores de servicio de nacionalidad_____(4)_____.

A T E N T A M E N T E

_____(5)_____

INSTRUCTIVO PARA EL LLENADO DEL FORMATO.

NÚMERO	DESCRIPCIÓN
1	Señalar la fecha de suscripción del documento.
2	Indicar el número respectivo de esta convocatoria de licitación.
3	Citar el nombre o razón social o denominación del licitante.
4	Anotar la nacionalidad del licitante.
5	Anotar el nombre y firma del representante del licitante.

ANEXO No. 10
"MANIFESTACIÓN DE DOCUMENTOS E INFORMACIÓN DE SU PROPOSICIÓN QUE PODRÍAN CONTENER INFORMACIÓN CONFIDENCIAL"

Ciudad de México a (día) (mes) (año).

COMISIÓN NACIONAL PARA LA PROTECCIÓN Y
DEFENSA DE USUARIOS DE SERVICIOS FINANCIEROS
P R E S E N T E.

A nombre de mi representada y en términos de lo establecido en los artículo 116 de la Ley General de Transparencia y Acceso a la información Pública, se describe la documentación legal y administrativa e información de la propuesta técnica y económica, que deberá considerarse como información susceptible de clasificarse como confidencial.

I. Información Legal y Administrativa

Información	Clasificación (Marque con una X)		Motivo
	Confidencial	Secreto Comercial	

II. Información Técnica

Información	Clasificación (Marque con una X)		Motivo
	Confidencial	Secreto Comercial	

III. Información Económica

Información	Clasificación (Marque con una X)		Motivo
	Confidencial	Secreto Comercial	

Atentamente__
Nombre completo (cuando se trate de persona física) y firma
Representante legal (cuando represente a una persona moral)

ANEXO No. 11
DOCUMENTOS QUE DEBERÁN INTEGRAR LA PROPUESTA DEL LICITANTE

De conformidad con lo establecido en el punto "No. 4.- REQUISITOS PARA PARTICIPAR EN ESTA LICITACIÓN", de la presente convocatoria, se citan de manera enunciativa más no limitativa, los documentos que deberán presentar para participar en este procedimiento.

DOCUMENTO	NUMERAL DE LA CONVOCATORIA	PRESENTÓ	
		SI	NO
4.1 DOCUMENTACIÓN LEGAL Y ADMINISTRATIVA			
IDENTIFICACIÓN OFICIAL DEL REPRESENTANTE LEGAL	4.1.1.		
ESCRITO DE ACREDITACIÓN DE LA PERSONALIDAD (ANEXO No. 4 "FORMATO PARA ACREDITAR LA PERSONALIDAD DEL LICITANTE")	4.1.2.		
DECLARACIÓN ESCRITA DE LOS ARTÍCULOS 50 Y 60 DE LA LEY	4.1.3.		
DECLARACIÓN DE INTEGRIDAD	4.1.4.		
MANIFESTACIÓN DE LAS MIPYMES	4.1.5.		
MANIFESTACIÓN DE NACIONALIDAD	4.1.6.		
COPIA DEL CONVENIO DE PARTICIPACIÓN CONJUNTA	4.1.7		
ESCRITO DE NO ACEPTACIÓN DE PROPOSICIONES	4.1.8		
4.2. DOCUMENTACIÓN TÉCNICA-ECONÓMICA			
PROPUESTA TÉCNICA (ANEXO No. 1 "ANEXO TÉCNICO")	4.2.1. ANEXO No. 1		
PROPUESTA ECONÓMICA (ANEXO No. 2 "CÉDULA DE OFERTA ECONÓMICA")	4.2.2. ANEXO No. 2		
PROPOSICIONES FIRMADAS ELECTRÓNICAMENTE	4.2.3.		
4.3 DOCUMENTACIÓN COMPLEMENTARIA QUE NO AFECTA LA SOLVENCIA			
ESCRITO DE CONFORMIDAD	4.3.1.		
OPINIÓN POSITIVA DEL SAT	4.3.2.		
OPINIÓN POSITIVA DEL IMSS	4.3.3.		
CONSTANCIA DEL INFONAVIT	4.3.4.		
MANIFIESTO DE NO DESEMPEÑAR EMPLEO, CARGO O COMISIÓN EN EL SERVICIO PÚBLICO	4.3.5.		
DECLARACIÓN DE CONOCER EL PROTOCOLO DE ACTUACIÓN	4.3.6.		
ACUSE PARA ACREDITAR LA AUSENCIA DE CONFLICTO DE INTERÉS	4.3.7.		
MANIFIESTO DE CONOCER Y REGISTRARSE EN EL MÓDULO DE FORMALIZACIÓN DE INSTRUMENTOS JURÍDICOS	4.3.8		

_____

NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL

ANEXO No. 12
ENCUESTA DE TRANSPARENCIA

FECHA:

NOMBRE O RAZÓN SOCIAL DEL LICITANTE:

TIPO DE PROCEDIMIENTO: (Licitación pública nacional o internacional; o Invitación a cuando menos tres personas nacional o internacional)

NÚMERO DEL PROCEDIMIENTO:

PARA LA CONTRATACIÓN DEL SERVICIO O ADQUISICIÓN DE: (Nombre del procedimiento)

¿DESEA CONTESTAR LA SIGUIENTE ENCUESTA? : ☐ **SI** ☐ **NO**

(Marque con una "X" su elección, si eligió **SI** siga las instrucciones que se detallan a continuación).

INSTRUCCIONES: FAVOR DE CALIFICAR LOS SUPUESTOS PLANTEADOS EN ESTA ENCUESTA CON UNA "X", SEGÚN CONSIDERE.
CALIFICACIÓN

Evento		Totalmente de acuerdo	En general de acuerdo	En general en desacuerdo	Totalmente en desacuerdo
Junta de aclaraciones.					
Supuestos	El contenido de la convocatoria es claro para la adquisición de bienes o contratación de servicios que se pretende realizar.				
	Las preguntas técnicas efectuadas en el evento, se contestaron con claridad.				
Acto de presentación y apertura de proposiciones.					
Supuestos	El evento se desarrolló con oportunidad, en razón de la cantidad de documentación que presentaron los licitantes.				
Dictamen técnico y económico					
Supuestos	El dictamen técnico (análisis cualitativo) fue emitido, conforme a la convocatoria y junta de aclaraciones del procedimiento.				

Evento		Totalmente de acuerdo	En general de acuerdo	En general en desacuerdo	Totalmente en desacuerdo
Fallo					
Supuestos	En el fallo se especificaron los motivos y el fundamento que sustenta la determinación de la adjudicación al proveedor y los que no resultaron adjudicados.				
Generales					
Supuestos	El acceso al inmueble fue expedito.				
	Todos los eventos dieron inicio en el tiempo establecido.				
	El trato que dieron los servidores públicos de la institución durante la licitación, fue respetuosa y amable.				
	Volvería a participar en otra licitación, que emita la institución.				
	El desarrollo del concurso se apegó a la normatividad aplicable.				

¿CONSIDERA USTED QUE EL PROCEDIMIENTO EN QUE PARTICIPÓ FUE TRANSPARENTE?

SI ☐ **NO** ☐

EN CASO DE HABER CONTESTADO QUE NO, POR FAVOR INDICAR BREVEMENTE LAS RAZONES:

SI USTED DESEA AGREGAR ALGÚN COMENTARIO RESPECTO A LA LITACIÓN, FAVOR DE ANOTARLO EN EL SIGUIENTE ESPACIO:

Favor de entregar o enviar la presente encuesta a más tardar dentro de los dos días hábiles siguientes de la emisión del fallo, en alguna de las siguientes opciones:

- En la Dirección de Recursos Materiales y Servicios Generales, ubicada en Av. Insurgentes Sur No. 762, quinto piso, Col. Del Valle, Alcaldía Benito Juárez, C.P. 03100, Ciudad de México, de lunes a viernes en un horario de 9:00 a 14:30 horas y de 16:00 a 18:00 horas.

- En la urna que al final del acto de fallo se encontrará en el lugar donde se celebre el evento.

- Enviarlo al correo electrónico, con la dirección **eflores.martinez@condusef.gob.mx.**

ANEXO No. 13
MODELO DE CONTRATO

CONTRATO ABIERTO PARA LA PRESTACIÓN DEL SERVICIO DE SEGURIDAD PERIMETRAL QUE CELEBRAN, POR UNA PARTE, EL EJECUTIVO FEDERAL POR CONDUCTO DE LA COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS (“CONDUSEF”), REPRESENTADA POR GERTRUDIS RODRÍGUEZ GONZÁLEZ, EN SU CARÁCTER DE DIRECTORA DE RECURSOS MATERIALES Y SERVICIOS GENERALES (DIRECCIÓN DE ÁREA), EN ADELANTE "LA DEPENDENCIA O ENTIDAD" Y, POR LA OTRA, XXXXXXXXXXXX, EN LO SUCESIVO "EL PROVEEDOR", REPRESENTADA POR XXXXXXXXXXXXXXXXXXXXXX, EN SU CARÁCTER DE REPRESENTANTE LEGAL DE LA EMPRESA, A QUIENES DE MANERA CONJUNTA SE LES DENOMINARÁ "LAS PARTES", AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

ANTECEDENTES

Con fundamento en las atribuciones que el Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros confiere a la Dirección de Tecnologías de Información y Comunicaciones en su artículo 46, incisos XII y XXIV.

La Dirección de Tecnologías de Información y Comunicaciones, requiere el servicio de seguridad perimetral.

DECLARACIONES

Cada una de las partes dan a conocer información sobre sí misma, entre otra la siguiente: señalar su naturaleza y personalidad jurídica, objeto social o jurídico, el nombre y cargo de los representantes legales y la forma en que acreditan su personalidad, información adicional esta contendrá todas las declaraciones que, además de las anteriores, deseen hacer las partes, y domicilio legal, en el caso de la dependencia o entidad, la suficiencia presupuestal con la cual pagará las obligaciones contractuales; el nombre del procedimiento de contratación realizado para adjudicar el contrato y su fundamento.

1. "LA DEPENDENCIA O ENTIDAD" declara que:

1.1. Es un Organismo Descentralizado de la Administración Pública Federal con personalidad jurídica y patrimonio propios, en los términos del artículo 4° de la Ley de Protección y Defensa al Usuario de Servicios Financieros.

1.2. Conforme a lo dispuesto por el artículo 45, fracción V, del Estatuto Orgánico de la CONDUSEF la C. GERTRUDIS RODRÍGUEZ GONZÁLEZ, DIRECTORA DE RECURSOS MATERIALES Y SERVICIOS GENERALES (DIRECCIÓN DE ÁREA), con R.F.C ROGG740306ST3, DIRECTORA DE RECURSOS MATERIALES Y SERVICIOS GENERALES es el servidor público que tiene conferidas las facultades legales para celebrar el presente contrato, quien podrá ser sustituido en cualquier momento en su cargo o funciones, sin que ello implique la necesidad de elaborar convenio modificatorio.

1.3. Que el C. RICARDO BECERRIL HERRERA, con R.F.C XXXXXXXXX, facultado para administrar el cumplimiento de las obligaciones que deriven del objeto del presente contrato, quien podrá ser sustituido en cualquier momento en su cargo o funciones, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, dirigido al representante de “EL PROVEEDOR” para los efectos del presente contrato, encargados del cumplimiento de las obligaciones contraídas en el presente instrumento jurídico.

1.4. Que el C. ISRAEL SÁNCHEZ ESPINOSA, Jefe de Departamento de Redes y Telecomunicaciones, R.F.C XXXXXXXXXXX, tendrá en todo tiempo la facultad de verificar directa, indirecta o a través de un tercero, si el proveedor está desarrollando correctamente el objeto de este pedido, de acuerdo a las especificaciones técnicas del presente instrumento jurídico y comunicará por escrito las observaciones que estime pertinentes en relación con su ejecución en la forma convenida.

1.5. La adjudicación del presente contrato se realizó mediante el procedimiento de LICITACIÓN PÚBLICA, ELECTRÓNICA de carácter NACIONAL, realizado al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos y en los artículos 25, 26 FRACCIÓN I, 26 BIS FRACCIÓN II y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, "LAASSP", y los correlativos de su Reglamento.

Cuando la proposición ganadora haya sido presentada en forma conjunta por varias personas, se estará a lo dispuesto por el artículo 44 del Reglamento de la "LAASSP"

1.6. "LA DEPENDENCIA O ENTIDAD" cuenta con recursos suficientes y con autorización para ejercerlos en el cumplimiento de sus obligaciones derivadas del presente contrato, como se desprende del reporte general de suficiencia presupuestaria número
406 con folio de autorización 1837, de fecha 08 de julio de 2021, emitido por la Dirección de Planeación y Finanzas.

1.7. Para efectos fiscales las Autoridades Hacendarias le han asignado el Registro Federal de Contribuyentes N° CNP990419B40

1.8. Tiene establecido su domicilio en el inmueble sito en Avenida Insurgentes Sur No. 762, Colonia del Valle, Alcaldía Benito
Juárez, C.P. 03100, en la Ciudad de México, mismo que señala para los fines y efectos legales del presente instrumento jurídico.

2. "EL PROVEEDOR" declara que:

2.1. Es una persona XXXXXXX legalmente constituida de conformidad con la legislación mexicana, según consta en la escritura pública No. XXXXX de fecha XX de XXXXXX de XXXXXX, otorgada ante la fe del titular de la Notaría Pública No. XXXX, en XXXXXXXX, el Lic. XXXXXXXXXXXXXX, e inscrito el día XX de XXXXX de XXXX, en el Registro Público de Comercio de XXXXXXX, Bajo el folio mercantil No. XXXXX, denominada XXXXXXXXXXXX, cuyo objeto social es, entre otros, XXXXXXXXXXXXXXXX.

2.2. El C. XXXXXXXXXXX, representante legal está facultada para suscribir el presente contrato, según consta en la escritura pública No. XXXXXXX de fecha XX de XXXXX de XXXX, otorgada ante la fe del titular de la Notaría Pública No. XXX, en XXXXXXX, el Lic. XXXXXXXXXXXXX, e inscrito el día XX de XXXXXX de XXXX, en el Registro Público de Comercio de XXXXXXXX, Bajo el folio mercantil No. XXXXXX; manifestando que a la fecha de la firma del presente instrumento jurídico, sus facultades no le han sido modificadas, revocadas o limitadas.

2.3. Ha considerado todos y cada uno de los factores que intervienen en el presente contrato, manifestando reunir las condiciones técnicas, jurídicas y económicas, así como la organización y elementos necesarios para su cumplimiento.

2.4. Bajo protesta de decir verdad, manifiesta que ni él ni ninguno de los socios o accionistas desempeñan un empleo, cargo o comisión en el servicio público, ni se encuentran inhabilitados para ello, o en su caso que, a pesar de desempeñarlo, con la formalización del presente contrato no se actualiza un conflicto de interés, en términos del artículo 49, fracción IX de la Ley General de Responsabilidades Administrativas lo cual se constató por el Órgano Interno de Control en "LA DEPENDENCIA O ENTIDAD", en concordancia con los artículos 50, fracción II de la "LAASSP" y 88, fracción I de su Reglamento; así como que "EL PROVEEDOR" no se encuentra en alguno de los supuestos del artículo 50 y penúltimo y antepenúltimo párrafos del artículo
60 de la "LAASSP".

2.5. Bajo protesta de decir verdad, declara que conoce y se obliga a cumplir con el Convenio 138 de la Organización Internacional del Trabajo en materia de erradicación del Trabajo Infantil, del artículo 123 Constitucional, apartado A) en todas sus fracciones y

de la Ley Federal del Trabajo en su artículo 22, manifestando que ni en sus registros, ni en su nómina tiene empleados menores de quince años y que en caso de llegar a tener a menores de dieciocho años que se encuentren dentro de los supuestos de edad permitida para laborar le serán respetados todos los derechos que se establecen en el marco normativo transcrito.

2.6. Cuenta con su Registro Federal de Contribuyentes XXXXXXXXXX

2.7. Bajo protesta de decir verdad, manifiesta estar al corriente en los pagos que se derivan de sus obligaciones fiscales, en específico de las previstas en el artículo 32-D del Código Fiscal Federal vigente, así como de sus obligaciones fiscales en materia de seguridad social, ante el Instituto del Fondo Nacional de la Vivienda para los Trabajadores y el Instituto Mexicano del Seguro Social; lo que acredita con las Opiniones de Cumplimiento de Obligaciones Fiscales y en materia de Seguridad Social en sentido positivo, emitidas por el SAT e IMSS respectivamente, así como con la Constancia de Situación Fiscal en materia de Aportaciones Patronales y Entero de Descuentos, sin adeudo emitida por el INFONAVIT, las cuales se encuentran vigentes y obran en el expediente respectivo.

2.8. Señala como su domicilio para todos los efectos legales el ubicado en XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

3. De "LAS PARTES":

3.1. Que es su voluntad celebrar el presente contrato y sujetarse a sus términos y condiciones, para lo cual se reconocen ampliamente las facultades y capacidades necesarias, mismas que no les han sido revocadas o limitadas en forma alguna, por lo que de común acuerdo se obligan de conformidad con las siguientes:

CLÁUSULAS

Establecen el objeto del contrato, así como los derechos y obligaciones que tendrán cada una de las partes como consecuencia de la suscripción del mismo, esta parte contiene una a una y debidamente numeradas, las distintas obligaciones y derechos de las partes y en las que se detalla, entre otros aspectos lo siguiente:

PRIMERA. OBJETO DEL CONTRATO.

"EL PROVEEDOR" acepta y se obliga a proporcionar a "LA DEPENDENCIA O ENTIDAD" la adquisición de o la prestación del servicio de seguridad perimetral, al amparo del procedimiento de contratación señalado en el punto I.5. de las declaraciones de este instrumento jurídico.

SEGUNDA. DE LOS MONTOS Y PRECIOS
El(los) precio(s) unitario(s) del presente contrato, expresado(s) en moneda nacional es (son):

Clave control interno	Clave CUCoP	Descripción	Unidad de medida	Cantidad	Precio unitario	Precio total antes de imp.	Precio con impuestos
						SUBTOTAL	$XXXXXX
						IMPUESTOS	$XXXXXX
						TOTAL	$XXXXXX

El monto total del mismo es por la cantidad de $XXXXXXX (XXXXXXXXXXXXXXXXXXXXXX PESOS XX/100 M.N.) en moneda nacional antes de impuestos y $XXXXXXX (XXXXXXXXXXXXXXXXXXX PESOS XX/100M.N.) en moneda nacional después de impuestos.

El precio unitario es considerado fijo y en moneda nacional (pesos mexicanos) hasta que concluya la relación contractual que se formaliza, incluyendo "EL PROVEEDOR" todos los conceptos y costos involucrados en la adquisición del (o prestación del servicio de) seguridad perimetral, por lo que "EL PROVEEDOR" no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

Con un presupuesto mínimo de $24'624,000.00 (veinticuatro millones setecientos veinticuatro mil pesos 00/100 M.N.) y un máximo de $61'560,000.00 (sesenta y un millones quinientos sesenta mil pesos 00/100 M.N.), incluido el Impuesto al Valor Agregado.

TERCERA. FORMA Y LUGAR DE PAGO

"LA DEPENDENCIA O ENTIDAD" se obliga a pagar a "EL PROVEEDOR" la cantidad señalada en la cláusula segunda de este instrumento jurídico, en moneda nacional, en un plazo máximo de 20 días naturales siguientes, a partir de la fecha en que sea entregado y aceptado el Comprobante Fiscal Digital por Internet (CFDI) o factura electrónica por "LA DEPENDENCIA O ENTIDAD", con la aprobación (firma) del Administrador del presente contrato mencionado en la Declaración I.3; a través del Sistema Integral de Administración Financiera Federal (SIAFF).

El cómputo del plazo para realizar el pago se contabilizará a partir del día hábil siguiente de la recepción de los bienes y del CFDI o factura electrónica, esto considerando que no existan aclaraciones al importe o a los bienes facturados, para lo cual es necesario que el CFDI o factura electrónica que se presente reúna los requisitos fiscales que establece la legislación en la materia, el

desglose de los bienes entregados y los precios unitarios; asimismo, deberá acompañarse con la documentación completa y debidamente requisitada.

De conformidad con el artículo 90 del Reglamento de la "LAASSP", en caso de que el CFDI o factura electrónica entregado presenten errores, el Administrador del presente contrato mencionado en la Declaración I.3, dentro de los 3 (tres) días hábiles siguientes de su recepción, indicará a "EL PROVEEDOR" las deficiencias que deberá corregir; por lo que, el procedimiento de pago reiniciará en el momento en que "EL PROVEEDOR" presente el CFDI o factura electrónica corregido.

El tiempo que "EL PROVEEDOR" utilice para la corrección de la documentación entregada, no se computará para efectos de pago, de acuerdo con lo establecido en el artículo 51 de la "LAASSP".

El CFDI o factura electrónica deberá ser presentada por Internet debidamente cumplimentado conforme a la legislación fiscal vigente, incluyendo los montos de las retenciones correspondientes al impuesto al valor agregado y al impuesto sobre la renta, y cuente con la autorización del Director de Tecnologías de la Información y Comunicaciones y con el visto bueno de pago por parte de la Dirección de Planeación y Finanzas de la CONDUSEF, siempre y cuando el proveedor haya quedado registrado como proveedor de la CONDUSEF.

En caso de que el CFDI entregado por el proveedor para su pago presente errores o deficiencias, el administrador del contrato específico, dentro de los tres días hábiles siguientes al de su recepción, indicará por escrito al proveedor las deficiencias que deberá corregir. 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 artículo 51 de la ley.

El CFDI o factura electrónica se deberá presentar desglosando el IVA cuando aplique.

"EL PROVEEDOR" manifiesta su conformidad de que hasta en tanto no se cumpla con la verificación, supervisión y aceptación de los bienes o prestación de los servicios, no se tendrán como recibidos o aceptados por el Administrador del presente contrato mencionado en la Declaración I.3,

Para efectos de trámite de pago, conforme a lo establecido en el SIAFF, "EL PROVEEDOR" deberá ser titular de una cuenta de cheques vigente y para tal efecto proporciona la CLABE XXXXXXXXXXXXXXX, del banco XXXXXXXXXXXXX a nombre de XXXXXXXXXXXXXX, en la que se efectuará la transferencia electrónica de pago, debiendo anexar:

1. Constancia de la institución financiera sobre la existencia de la cuenta de cheques abierta a nombre del beneficiario que incluya:

1.1. Nombre del beneficiario (conforme al timbre fiscal);

1.2. Registro Federal de Contribuyentes;

1.3. Domicilio fiscal: calle, N° exterior, N° interior, colonia, código postal, alcaldía y entidad federativa;

1.4. Nombre(s) del(los) banco(s); y

1.5. Número de la cuenta con once dígitos, así como la Clave Bancaria Estandarizada (CLABE) con 18 dígitos, que permita realizar transferencias electrónicas de fondo, a través del Sistema de Pago.

2. Copia de estado de cuenta reciente, con no más de dos meses de antigüedad.

El pago de los servicios, objeto de este instrumento jurídico, quedará condicionado proporcionalmente, al pago que el proveedor deba efectuar por concepto de penas convencionales, en el entendido de que, si es rescindido el contrato, no se procederá al cobro de dichas penalizaciones ni a la contabilización de las mismas, para hacer efectiva la garantía.

En caso de pago en moneda extranjera, indicar la fuente oficial que se tomará para llevar a cabo la conversión y la tasa de cambio o la fecha a considerar para hacerlo.

El pago será efectuado mediante transferencia bancaria a la cuenta que "EL PROVEEDOR" proporcione.

Para el caso de que se presenten pagos en exceso, se estará a lo dispuesto por el artículo 51 párrafo tercero, de la "LAASSP". No se otorgará ningún anticipo.
CUARTA. VIGENCIA

El contrato comprenderá una vigencia considerada a partir de XXXXXXXXXXXX y hasta el 31/08/2024 sin perjuicio de su posible terminación anticipada, en los términos establecidos en su clausulado.

QUINTA. MODIFICACIONES DEL CONTRATO.

"LAS PARTES" están de acuerdo en que por necesidades de "LA DEPENDENCIA O ENTIDAD" podrá ampliarse el suministro de los bienes, prestación del servicio o arrendamiento objeto del presente contrato, de conformidad con el artículo 52 de la "LAASSP", siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) del monto o cantidad de los conceptos y volúmenes establecidos originalmente. Lo anterior, se formalizará mediante la celebración de un Convenio Modificatorio del Contrato Principal. Asimismo, con fundamento en el artículo 91 del Reglamento de la "LAASSP", "EL PROVEEDOR" deberá entregar las modificaciones respectivas de las garantías, señaladas en la CLÁUSULA SÉPTIMA de este contrato.

Por caso fortuito o de fuerza mayor, o por causas atribuibles a "LA DEPENDENCIA O ENTIDAD", se podrá modificar el presente instrumento jurídico, la fecha o el plazo para la entrega de los bienes o prestación de los servicios o arrendamiento. En dicho supuesto, se deberá formalizar el convenio modificatorio respectivo, no procediendo la aplicación de penas convencionales por atraso. Tratándose de causas imputables a "LA DEPENDENCIA O ENTIDAD", no se requerirá de la solicitud de "EL PROVEEDOR".

SEXTA. GARANTÍAS DE LOS BIENES O PRESTACIÓN DE LOS SERVICIOS O ARRENDAMIENTO Y ANTICIPOS "EL PROVEEDOR" se obliga a otorgar a "LA DEPENDENCIA O ENTIDAD", las siguientes garantías:
El otorgamiento de anticipos, deberá garantizarse en los términos del artículo 48 de la "LAASSP" y primer párrafo del artículo 81 de su Reglamento. Si las disposiciones jurídicas aplicables lo permitan, la entrega de la garantía de anticipos se realice de manera electrónica.

La póliza de garantía de anticipo será devuelta a "EL PROVEEDOR" una vez que el "LA DEPENDENCIA O ENTIDAD" entregue a "EL PROVEEDOR", autorización por escrito de que demuestre haber cumplido con la totalidad de las obligaciones adquiridas en el presente contrato, para lo cual "EL PROVEEDOR", deberá solicitar por escrito a "LA DEPENDENCIA O ENTIDAD" una vez concluida la verificación de cumplimiento o terminación del contrato la liberación de la fianza a

efecto de que "EL PROVEEDOR" pueda solicitar a la afianzadora la cancelación o liberación de la fianza.

En caso de que "LA DEPENDENCIA O ENTIDAD" requiera hacer efectivo un importe parcial de la póliza de garantía de fianza de anticipo, "EL PROVEEDOR" se obliga a presentar a "LA DEPENDENCIA O ENTIDAD" otra póliza nueva de fianza o un endoso a la misma, amparando el importe restante de la obligación total requerida.

SÉPTIMA. GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.

Conforme a los artículos 48 fracción II, y 49 fracción I, de la "LAASSP", 85 fracción III, y 103 de su Reglamento; 166 de la Ley de Instituciones de Seguros y de Fianzas, 48 fracción II, de la Ley de COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS 70 de su Reglamento, las Disposiciones Generales a que se sujetarán las garantías otorgadas a favor del Gobierno Federal para el cumplimiento de obligaciones distintas de las fiscales que constituyan las Dependencias y Entidades en los actos y contratos que celebren, publicadas en el DOF el 08 de septiembre de 2015, "EL PROVEEDOR" se obliga a constituir una garantía indivisible por el cumplimiento fiel y exacto de todas y cada una de las obligaciones derivadas de este contrato, mediante fianza expedida por compañía afianzadora mexicana autorizada por la Comisión Nacional de Seguros y de Fianzas, a favor de la COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS , por un importe equivalente al 10.0% (DIEZ POR CIENTO) del monto total del contrato, sin incluir el IVA. Dicha fianza deberá ser entregada a "LA DEPENDENCIA O ENTIDAD", a más tardar dentro de los 10 días naturales posteriores a la firma del contrato.

Si las disposiciones jurídicas aplicables lo permitan, la entrega de la garantía de cumplimiento se realice de manera electrónica.

En caso de que la garantía a que se refiere esta cláusula sea una fianza, ésta deberá ser expedida por una compañía autorizada en términos de la Ley de Instituciones de Seguros y de Fianzas, a favor de la CONDUSEF, debiéndose asentar, como mínimo, lo siguiente:

1. Expedirse a favor de la COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS y señalar su domicilio;
2. La indicación del importe total garantizado con número y letra;
3. La referencia de que la fianza se otorga atendiendo a todas las estipulaciones contenidas en el contrato y anexos respectivo), así como la cotización y el requerimiento asociado a ésta;
4. La información correspondiente al número de contrato, su fecha de firma, así como la especificación de las obligaciones garantizadas;
5. El señalamiento de la denominación o nombre de "EL PROVEEDOR" y de la institución afianzadora, así como sus domicilios correspondientes;
6. La condición de que la vigencia de la fianza deberá quedar abierta para permitir que cumpla con su objetivo, y continuará vigente durante la sustanciación de todos los recursos legales o juicios que se interpongan hasta que se dicte resolución definitiva por la autoridad competente, 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 previstas en el contrato y actos administrativos garantizados;
7. La indicación de que la fianza se hará efectiva conforme al procedimiento dispuesto en el artículo 282 de la Ley de Instituciones de Seguros y de Fianzas, el cual será aplicable también para el cobro de los intereses que en su caso se generen en los términos previstos en el artículo 283 del propio ordenamiento;

8. La indicación de que la cancelación de la póliza de fianza procederá una vez que "LA DEPENDENCIA O ENTIDAD" otorgue el documento en el que se señale la extinción de derechos y obligaciones, previo otorgamiento del finiquito correspondiente, o en caso de existir saldos a cargo de "EL PROVEEDOR", la liquidación debida;
9. Para efectos de la garantía señalada en esta cláusula, se deberá considerar la indivisibilidad de ésta, por lo que en caso de incumplimiento del contrato se hará efectiva por el monto total de la garantía de cumplimiento;
10. Para acreditar a la institución afianzadora el incumplimiento de la obligación garantizada, tendrá que cumplirse con los requisitos establecidos en las Disposiciones Generales a que se sujetarán las garantías otorgadas a favor del Gobierno Federal para el cumplimiento de obligaciones distintas de las fiscales que constituyan las dependencias y entidades en los actos y contratos que celebren, publicadas en el Diario Oficial de la Federación el 08 de septiembre de 2015; y
11. El momento de inicio de la fianza y, en su caso, su vigencia.

Considerando los requisitos anteriores, dentro de la fianza, se deberán incluir las declaraciones siguientes en forma expresa:

1. "Esta garantía estará vigente durante la sustanciación de todos los recursos legales o juicios que se interpongan hasta que se pronuncie resolución definitiva por autoridad competente, de forma tal que su vigencia no podrá acotarse en razón del plazo de ejecución del contrato.
2. "La institución de fianzas acepta expresamente someterse al procedimiento de ejecución establecido en el artículo 282 de la Ley de Instituciones de Seguros y de Fianzas, para la efectividad de la presente garantía, procedimiento al que también se sujetará para el caso del cobro de intereses que prevé el artículo 283 del mismo ordenamiento legal, por pago extemporáneo del importe de la póliza de fianza requerida.";
3. "La cancelación de la fianza no procederá sino en virtud de manifestación previa de manera expresa y por escrito de "LA DEPENDENCIA O ENTIDAD"; y
4. "La afianzadora acepta expresamente tener garantizado el contrato a que esta póliza se refiere, aún en el caso de que se otorgue prórroga o espera al deudor principal o fiado por parte de "LA DEPENDENCIA O ENTIDAD" para el cumplimiento total de las obligaciones que se garantizaran, por lo que la afianzadora renuncia expresamente al derecho que le otorga el artículo 179 de la Ley de Instituciones de Seguros y de Fianzas."

De no cumplir con dicha entrega, "LA DEPENDENCIA O ENTIDAD" podrá rescindir el contrato y remitir el asunto al Órgano Interno de Control para que determine si se aplican las sanciones estipuladas en el artículo 60 fracción III de la "LAASSP".

La garantía de cumplimiento de ninguna manera será considerada como una limitación de la responsabilidad de "EL PROVEEDOR", derivada de sus obligaciones y garantías estipuladas en el presente instrumento jurídico, y de ninguna manera impedirá que "LA DEPENDENCIA O ENTIDAD" reclame la indemnización o el reembolso por cualquier incumplimiento que pueda exceder el valor de la garantía de cumplimiento.

En caso de incremento al monto del presente instrumento jurídico o modificación al plazo, "EL PROVEEDOR" se obliga a entregar a "LA DEPENDENCIA O ENTIDAD" dentro de los diez días naturales siguientes a la formalización del mismo, de conformidad con el último párrafo del artículo 91 del Reglamento de la "LAASSP", los documentos modificatorios o endosos correspondientes, debiendo contener en el documento la estipulación de que se otorga de manera conjunta, solidaria e inseparable de la garantía otorgada inicialmente.

"EL PROVEEDOR" acepta expresamente que la garantía expedida para garantizar el cumplimiento se hará efectiva independientemente de que se interponga cualquier otro tipo de recurso ante instancias del orden administrativo o judicial, así como que permanecerá vigente durante la substanciación de los juicios o recursos legales que se interponga con relación a dicho contrato, hasta que sea pronunciada resolución definitiva que cause ejecutoria por la autoridad competente.

El trámite de liberación de garantía, se realizará inmediato a que se extienda la constancia de cumplimiento de obligaciones contractuales por parte de "LA DEPENDENCIA O ENTIDAD", de conformidad con lo dispuesto por el artículo 81, fracción VIII del Reglamento de la "LAASSP".

Considerando que la entrega de los bienes o prestación de los servicios o arrendamiento, cuando aplique se haya previsto un plazo menor a diez días naturales, se exceptúa el cumplimiento de la garantía, de conformidad con lo establecido en el artículo 48 último párrafo de la "LAASSP", en concordancia con lo señalado en el tercer párrafo del artículo 86 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público

Para este caso, el monto máximo de las penas convencionales por atraso que se puede aplicar, será del veinte por ciento del monto de los bienes entregados fuera de la fecha convenida, de conformidad con lo establecido en el tercer párrafo del artículo 96 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

OCTAVA. OBLIGACIONES DE “EL PROVEEDOR”

1. Prestar los servicios en las fechas o plazos y lugares específicos conforme a lo requerido en el presente instrumento jurídico y anexos respectivos.
2. Correrá bajo su cargo los costos de flete, transporte, seguro y de cualquier otro derecho que se genere, hasta el lugar de entrega.
3. Cumplir con las especificaciones técnicas y de calidad y demás condiciones establecidas en el contrato respectivos anexos, así como la cotización y el requerimiento asociado a ésta;
4. En bienes de procedencia extranjera, asumirá la responsabilidad de efectuar los trámites de importación y pagar los impuestos y derechos que se generen.
5. Asumir su responsabilidad ante cualquier situación que pudiera generarse con motivo del presente contrato.
6. No difundir a terceros sin autorización expresa de "LA DEPENDENCIA O ENTIDAD" la información que le sea proporcionada, inclusive después de la rescisión o terminación del presente instrumento, sin perjuicio de las sanciones administrativas, civiles y penales a que haya lugar.
7. Proporcionar la información que le sea requerida por parte de la Secretaría de la Función Pública y el Órgano Interno de Control, de conformidad con el artículo 107 del Reglamento de la "LAASSP".

NOVENA. OBLIGACIONES DE "LA DEPENDENCIA O ENTIDAD”

1. Otorgar todas las facilidades necesarias, a efecto de que "EL PROVEEDOR" lleve a cabo en los términos convenidos.
2. Sufragar el pago correspondiente en tiempo y forma, por el suministro de los bienes o prestación de los servicios o arrendamiento.
3. Extender a "EL PROVEEDOR", en caso de que lo requiera, por conducto del Administrador del Contrato, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa de dicho servidor público para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.

DÉCIMA. LUGAR, PLAZOS Y CONDICIONES DE ENTREGA DE LOS BIENES PRESTACIÓN DE LOS SERVICIOS O ARRENDAMIENTO

La entrega del servicio, será conforme a los plazos, condiciones y entregables establecidos por "CONDUSEF" en las Especificaciones Técnicas y Alcances del Servicio.

No se otorgarán prórrogas para el cumplimiento de las obligaciones contractuales y los requisitos que deberán observarse en el presente instrumento jurídico.

DÉCIMA PRIMERA. LICENCIAS, AUTORIZACIONES Y PERMISOS

El señalamiento de las licencias, autorizaciones y permisos que conforme a otras disposiciones sea necesario contar para la adquisición o arrendamiento de bienes y prestación de los servicios correspondientes, cuando sean del conocimiento de la "LA DEPENDENCIA O ENTIDAD".

DÉCIMA SEGUNDA. SEGUROS

Los seguros que, en su caso, deben otorgarse, indicando los bienes que ampararían y la cobertura de la póliza correspondiente.

DÉCIMA TERCERA. CALIDAD

"EL PROVEEDOR" deberá contar con la infraestructura necesaria, personal técnico especializado en el ramo, herramientas, técnicas y equipos adecuados para proporcionar los bienes o la prestación de los servicios o arrendamiento requeridos, a fin de garantizar que el objeto de este contrato sea proporcionado con la calidad, oportunidad y eficiencia requerida para tal efecto, comprometiéndose a realizarlo a satisfacción de "LA DEPENDENCIA O ENTIDAD" y con estricto apego a lo establecido en las cláusulas del presente instrumento jurídico y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta.

"LA DEPENDENCIA O ENTIDAD" no estará obligada a recibir los bienes o aceptación de los servicios o arrendamiento cuando éstos no cumplan con los requisitos establecidos en el párrafo anterior.

DÉCIMA CUARTA. DEFECTOS Y VICIOS OCULTOS

"EL PROVEEDOR" queda obligado ante "LA DEPENDENCIA O ENTIDAD" a responder de los defectos y vicios ocultos derivados de las obligaciones del presente contrato, así como de cualquier otra responsabilidad en que hubiere incurrido, en los términos señalados en este instrumento jurídico y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta, y/o en la legislación aplicable en la materia.

Para los efectos de la presente cláusula, se entiende por vicios ocultos los defectos que existan en los bienes o prestación de los servicios o arrendamiento, que los hagan impropios para los usos a que se le destine o que disminuyan de tal modo este uso, que de haberlo conocido "LA DEPENDENCIA O ENTIDAD" no lo hubiere adquirido o los hubiere adquirido a un precio menor.

DÉCIMA QUINTA. RESPONSABILIDAD

"EL PROVEEDOR" se obliga a responder por su cuenta y riesgo de los daños y/o perjuicios que por inobservancia o negligencia de su parte lleguen a causar a "LA DEPENDENCIA O ENTIDAD", con

motivo de las obligaciones pactadas, o bien por los defectos o vicios ocultos en los bienes entregados o prestación de los servicios, de conformidad con lo establecido en el artículo 53 de la "LAASSP".

DÉCIMA SEXTA. IMPUESTOS Y DERECHOS

Los impuestos, derechos y gastos que procedan con motivo de la adquisición de los bienes o prestación de los servicios o arrendamiento, objeto del presente contrato, serán pagados por "EL PROVEEDOR", mismos que no serán repercutidos a "LA DEPENDENCIA O ENTIDAD".

"LA DEPENDENCIA O ENTIDAD" sólo cubrirá, cuando aplique, lo correspondiente al IVA, en los términos de la normatividad aplicable y de conformidad con las disposiciones fiscales vigentes.

DÉCIMA SÉPTIMA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES

"EL PROVEEDOR" no podrá ceder total o parcialmente los derechos y obligaciones derivados del presente contrato, a favor de cualquier otra persona física o moral, con excepción de los derechos de cobro, en cuyo caso se deberá contar con la conformidad previa y por escrito de "LA DEPENDENCIA O ENTIDAD" deslindando a ésta de toda responsabilidad.

DÉCIMA OCTAVA. DERECHOS DE AUTOR, PATENTES Y/O MARCAS

"EL PROVEEDOR" asume la responsabilidad total en caso de que, al suministrar los bienes o prestación de los servicios o arrendamiento, objeto del presente contrato, infrinja patentes, marcas o viole otros registros de derechos de propiedad industrial a nivel nacional e internacional, por lo que, se obliga a responder personal e ilimitadamente de los daños y perjuicios que pudiera causar a "LA DEPENDENCIA O ENTIDAD" o a terceros.

En tal virtud, "EL PROVEEDOR" manifiesta en este acto bajo protesta de decir verdad, no encontrarse en ninguno de los supuestos de infracción administrativa y/o delito establecidos en la Ley Federal del Derecho de Autor ni en la Ley de la Propiedad Industrial.

En caso de que sobreviniera alguna reclamación en contra de "LA DEPENDENCIA O ENTIDAD", por cualquiera de las causas antes mencionadas, la única obligación de ésta será la de dar aviso en el domicilio previsto en el apartado de Declaraciones de este instrumento a "EL PROVEEDOR", para que éste, utilizando los medios correspondientes al caso, garantice salvaguardar a "LA DEPENDENCIA O ENTIDAD" de cualquier controversia, liberándole de toda responsabilidad de carácter civil, penal, mercantil, fiscal o de cualquier otra índole.

En caso de que "LA DEPENDENCIA O ENTIDAD" tuviese que erogar recursos por cualquiera de estos conceptos, "EL PROVEEDOR" se obliga a reembolsar de manera inmediata los recursos erogados por aquella.

DÉCIMA NOVENA. CONFIDENCIALIDAD

"LAS PARTES" están conformes en que la información que se derive de la celebración del presente instrumento jurídico, así como toda aquella información que "LA DEPENDENCIA O ENTIDAD" entregue a "EL PROVEEDOR" tendrá el carácter de confidencial, por lo que este se compromete, de forma directa o a través de interpósita persona, a no proporcionarla o divulgarla por escrito, verbalmente o por cualquier otro medio a terceros, inclusive después de la terminación de este contrato.

La información contenida en el presente contrato es pública, de conformidad con lo dispuesto en los artículos 70 fracción XXVIII de la Ley General de Transparencia y Acceso a la Información Pública y 68 de la Ley Federal de Transparencia y Acceso a la Información Pública; sin embargo la información que proporcione “LA "LA DEPENDENCIA O ENTIDAD" a "EL PROVEEDOR" para el cumplimiento del objeto materia del mismo, será considerada como confidencial en términos de los artículos 116 y 113, respectivamente, de los citados ordenamientos jurídicos, por lo que "EL PROVEEDOR" se compromete a recibir, proteger y guardar la información confidencial proporcionada por "LA DEPENDENCIA O ENTIDAD" 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 de este instrumento.

"EL PROVEEDOR" se compromete a que la información considerada como confidencial no será utilizada para fines diversos a los autorizados con el presente contrato especifico; 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 publicar informes, datos y resultados obtenidos objeto del presente instrumento, toda vez que son propiedad de "LA DEPENDENCIA O ENTIDAD".

Cuando de las causas descritas en las cláusulas de RESCISIÓN y TERMINACIÓN ANTICIPADA, del presente contrato, concluya la vigencia del mismo, subsistirá la obligación de confidencialidad sobre los bienes establecidos en este instrumento legal.

En caso de incumplimiento a lo establecido en esta cláusula, "EL PROVEEDOR" tiene conocimiento en que "LA DEPENDENCIA O ENTIDAD" podrá ejecutar o tramitar las sanciones establecidas en la "LAASSP" y su Reglamento, así como presentar las denuncias correspondientes de conformidad con lo dispuesto por el Libro Segundo, Título Noveno, Capítulos I y II del Código Penal Federal y demás normatividad aplicable.

De igual forma, "EL PROVEEDOR" se compromete a no alterar la información confidencial, a llevar un control de su personal y hacer de su conocimiento las sanciones que se aplicarán en caso de incumplir con lo dispuesto en esta cláusula, por lo que, en su caso, se obliga a notificar a "LA DEPENDENCIA O ENTIDAD" cuando se realicen actos que se consideren como ilícitos, debiendo dar inicio a las acciones legales correspondientes y sacar en paz y a salvo a "LA DEPENDENCIA O ENTIDAD" de cualquier proceso legal.

"EL PROVEEDOR" se obliga a poner en conocimiento de "LA DEPENDENCIA O ENTIDAD" cualquier hecho o circunstancia que en razón de los bienes prestados sea de su conocimiento y que pueda beneficiar o evitar un perjuicio a la misma.

Asimismo, "EL PROVEEDOR" no podrá, con motivo del suministro de los bienes o prestación de los servicios o arrendamiento que realice a "LA DEPENDENCIA O ENTIDAD", utilizar la información a que tenga acceso, para asesorar, patrocinar o constituirse en consultor de cualquier persona que tenga relaciones directas o indirectas con el objeto de las actividades que lleve a cabo.

VIGÉSIMA. ADMINISTRACIÓN, VERIFICACIÓN, SUPERVISIÓN Y ACEPTACIÓN DE LOS BIENES O SERVICIOS O ARRENDAMIENTO

"LA DEPENDENCIA O ENTIDAD" designa como responsable de administrar y vigilar el cumplimiento del presente contrato al C. RICARDO BECERRIL HERRERA, DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, con el objeto de verificar el óptimo cumplimiento del mismo,

por lo que indicará a “EL PROVEEDOR” las observaciones que se estimen pertinentes, quedando éste obligado a corregir las anomalías que le sean indicadas, así como deficiencias en la entrega de los bienes o prestación de los servicios o de su personal.

Asimismo, "LA DEPENDENCIA O ENTIDAD" sólo aceptará los bienes o prestación de los servicios o arrendamiento materia del presente contrato y autorizará el pago de los mismos previa verificación de las especificaciones requeridas, de conformidad con lo especificado en el presente contrato y sus correspondientes anexos, así como la cotización y el requerimiento asociado a ésta.

Los bienes o prestación de los servicios o arrendamiento serán recibidos previa revisión del administrador del contrato; la inspección de los bienes consistirá en la verificación del cumplimiento de las especificaciones técnicas establecidas en el contrato y en su caso en los anexos respectivos, así como la cotización y el requerimiento asociado a ésta.

En tal virtud, "EL PROVEEDOR" manifiesta expresamente su conformidad de que hasta en tanto no se cumpla de conformidad con lo establecido en el párrafo anterior, los bienes o prestación de los servicios o arrendamiento, no se tendrán por aceptados por parte de "LA DEPENDENCIA O ENTIDAD".

VIGÉSIMA PRIMERA. DEDUCCIONES

En términos del artículo 53 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento, por motivo de incumplimientos parciales o deficientes en la prestación de los servicios, se aplicarán deducciones al pago, conforme a lo siguiente:

CONCEPTO	NIVEL DEL SERVICIO	DEDUCTIVA	MÁXIMO PERMITIDO
Monitoreo del SOC	Cuando no se cumplan con los niveles mínimos solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	2 al millar por hora de indisponibilidad sobre el nivel de servicio establecido y con base al importe de la factura total mensual.	Con un máximo de 3 eventos mensuales.
Atención a requerimientos de configuraciones de seguridad	Cuando no se cumpla con el tiempo máximo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada hora natural de atraso del monto total de la facturación mensual de los servicios correspondientes.	Con un máximo de 5 eventos mensuales por servicio.
Tiempo de solución a incidentes de seguridad	Cuando no se cumpla con los tiempos establecidos por prioridad solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada minuto de afectación a los servicios y/o aplicaciones y/o por atraso para la solución del mismo, sobre el monto total de la facturación mensual de los servicios correspondientes.	Con un máximo de 1 eventos mensual por servicio
Licenciamiento y entrega de actualizaciones	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el	6 al millar por cada día hábil de atraso con base al monto total de la facturación mensual de la solución involucrada	Para todos los dispositivos del servicio cuando el fabricante emita una nueva licencia del software

	numeral 7.2 del ANEXO 1 ANEXO TÉCNICO		
Control de accesos a páginas web, URL's o aplicaciones.	Cuando no se cumpla con el tiempo máximo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar sobre el total de la facturación mensual de la solución involucrada, por cada día de atraso para la categorización, re categorización, bloqueo o acceso a los sitios o categorías web,	Con un máximo de 3 eventos mensuales por servicio
Accesos de usuarios o equipos no autorizados en el mes.	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	5 al millar por cada acceso de usuarios no autorizados con base al monto total de la facturación mensual de la solución involucrada.	• Para la solución de seguridad 5 accesos no autorizados máximo, durante 3 meses consecutivos • Para la solución de seguridad medio y estándar 10 accesos no autorizados máximo, durante 3 meses consecutivos
Control de cambios de las soluciones de seguridad.	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	2 al millar por cada hora natural de atraso con base al monto total de la facturación mensual de la solución involucrada.	Aplica para: Cualquier dispositivo de seguridad. Cuando se solicite un control de cambios en algún componente de las soluciones antes mencionadas.
Control de acceso	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	2 al millar por cada acceso no autorizado con base al monto total de la facturación mensual de la solución involucrada.	Aplica para: Cualquier dispositivo de seguridad Cuando se detecte algún acceso no autorizado por CONDUSEF.
Dictamen de actividades sospechosas	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada hora hábil de atraso con base al monto total de la facturación mensual de la solución involucrada	Aplica para: Cualquier dispositivo de seguridad cuando se detecte alguna actividad sospechosa.
Manejo de incidentes de día cero.	Cuando no se cumpla con lo establecido en los niveles de servicio solicitados en el numeral 7.2 del ANEXO 1 ANEXO TÉCNICO	6 al millar por cada día de atraso del monto total de la facturación mensual de los servicios correspondientes al servicio(s) afectado(s)	Aplica para: Cualquier dispositivo de seguridad cuando se detecte algún incidente de día cero.
Personal Certificado para soportar los servicios.	Cuando no se notifique del cambio de los Recursos Humanos solicitados (Gestión del Personal Técnico) solicitados en el	2 al millar por cada día de indisponibilidad sobre el monto total de la facturación mensual de los servicios correspondientes al servicio(s) afectado(s)	Aplica para: SOC y personal en sitio

	numeral 7.2 del ANEXO 1 ANEXO TÉCNICO		

En caso de no existir pagos pendientes, la deducción se aplicará sobre la garantía de cumplimiento del contrato siempre y cuando "EL PROVEEDOR" no realice el pago de la misma y para el caso de que la garantía no sea suficiente para cubrir la deducción correspondiente, "EL PROVEEDOR" realizará el pago de la deductiva a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA´s), a favor de la Tesorería de la Federación.

Lo anterior, en el entendido de que se cumpla con el objeto de este contrato de forma inmediata, conforme a lo acordado. En caso contrario, "LA DEPENDENCIA O ENTIDAD" podrá iniciar en cualquier momento posterior al incumplimiento, el procedimiento de rescisión del contrato, considerando la gravedad del incumplimiento y los daños y perjuicios que el mismo pudiera ocasionar a los intereses del Estado, representados por "LA DEPENDENCIA O ENTIDAD".

Las deducciones económicas se aplicarán sobre la cantidad indicada sin incluir el IVA.

La notificación y cálculo de las deducciones correspondientes las realizará el administrador del contrato de "LA DEPENDENCIA O ENTIDAD".

Cuando el monto total de aplicación de deducciones alcance el 20% (veinte por ciento) del monto total del contrato, se iniciará el procedimiento de rescisión.

VIGÉSIMA SEGUNDA. PENAS CONVENCIONALES

Con fundamento en lo dispuesto en el artículo 53 de Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, "LA DEPENDENCIA O ENTIDAD" aplicará penas convencionales al proveedor en la prestación de los servicios objeto de la contratación de la siguiente manera:

Se aplicará una pena de 2 al millar por cada día hábil de atraso sobre los servicios no prestados en tiempo, sin incluir importe al valor agregado, conforme a la tabla establecida en el numera 9.5 PENAS CONVENCIONALES Y DEDUCTIVAS del Anexo Técnico, la cual no podrá rebasar el 10% (diez por ciento) del monto total del contrato antes del impuesto al valor agregado.

Por lo anterior, el pago de la adquisición o prestación de los servicios o arrendamiento quedará condicionado, proporcionalmente, al pago que "EL PROVEEDOR" deba efectuar por concepto de penas convencionales por atraso, en el entendido de que, si el contrato es rescindido en términos de lo previsto en la CLÁUSULA DE RESCISIÓN, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento del contrato.

El pago de la pena deberá efectuarse a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA´s), a favor de la Tesorería de la Federación, sin que la acumulación de esta pena exceda el equivalente al monto total de la garantía de cumplimiento del contrato y se aplicará sobre el monto proporcional sin incluir el IVA.

Cuando la suma de las penas convencionales exceda el monto total de la garantía de cumplimiento del presente contrato, se iniciará el procedimiento de rescisión del mismo, en los términos del artículo 54 de la "LAASSP".

Independientemente de la aplicación de la pena convencional a que hace referencia el párrafo que antecede, se aplicarán además cualquiera otra que la "LAASSP" establezca.

Esta pena convencional no descarta que "LA DEPENDENCIA O ENTIDAD" en cualquier momento posterior al incumplimiento determine procedente la rescisión del contrato, considerando la gravedad de los daños y perjuicios que el mismo pudiera ocasionar a los intereses de "LA DEPENDENCIA O ENTIDAD".

En caso que sea necesario llevar a cabo la rescisión administrativa del contrato, la aplicación de la garantía de cumplimiento será por el monto total de las obligaciones garantizadas.

La penalización tendrá como objeto resarcir los daños y perjuicios ocasionados a "LA DEPENDENCIA O ENTIDAD" por el atraso en el cumplimiento de las obligaciones estipuladas en el presente contrato.

La notificación y cálculo de la pena convencional, corresponde al administrador o el supervisor del contrato de "LA DEPENDENCIA O ENTIDAD".

VIGÉSIMA TERCERA. SANCIONES ADMINISTRATIVAS

Cuando "EL PROVEEDOR" incumpla con sus obligaciones contractuales por causas imputables a éste, y como consecuencia, cause daños y/o perjuicios graves a "LA DEPENDENCIA O ENTIDAD", o bien, proporcione información falsa, actúe con dolo o mala fe en la celebración del presente contrato o durante la vigencia del mismo, por determinación de la Secretaría de la Función Pública, se podrá hacer acreedor a las sanciones establecidas en la "LAASSP", en los términos de los artículos 59, 60 y 61 de dicho ordenamiento legal y 109 al 115 de su Reglamento.

VIGÉSIMA CUARTA. SANCIONES APLICABLES Y TERMINACIÓN DE LA RELACIÓN CONTRACTUAL

"LA DEPENDENCIA O ENTIDAD", de conformidad con lo establecido en los artículos 53, 53 Bis, 54 y 54 Bis de la "LAASSP", y 86 segundo párrafo, 95 al 100 y 102 de su Reglamento, aplicará sanciones, o en su caso, llevará a cabo la cancelación de partidas total o parcialmente o la rescisión administrativa del contrato.

VIGÉSIMA QUINTA. RELACIÓN LABORAL

"EL PROVEEDOR" reconoce y acepta ser el único patrón del personal que ocupe con motivo del suministro objeto de este contrato, así como el responsable de las obligaciones derivadas de las disposiciones legales y demás ordenamientos en materia de trabajo y seguridad social. Asimismo, "EL PROVEEDOR" conviene en responder de todas las reclamaciones que sus trabajadores presenten en su contra o en contra de "LA DEPENDENCIA O ENTIDAD", en relación con el suministro materia de este contrato.

VIGÉSIMA SEXTA. EXCLUSIÓN LABORAL

"LAS PARTES" convienen en que "LA DEPENDENCIA O ENTIDAD" no adquiere ninguna obligación de carácter laboral con "EL PROVEEDOR" ni con los elementos que éste utilice para el suministro de los bienes o prestación de los servicios o arrendamiento objeto del presente contrato, por lo cual no se le podrá considerar como patrón ni como un sustituto. En particular el personal se entenderá relacionado exclusivamente con la o las personas que lo emplearon y por ende cada una de ellas asumirá su responsabilidad por dicho concepto.

Igualmente, y para este efecto y cualquiera no previsto, "EL PROVEEDOR" exime expresamente a "LA DEPENDENCIA O ENTIDAD" de cualquier responsabilidad laboral, civil, penal, de seguridad social o de otra especie que, en su caso, pudiera llegar a generarse; sin embargo, si "LA DEPENDENCIA O ENTIDAD" tuviera que realizar alguna erogación por alguno de los conceptos que anteceden, "EL PROVEEDOR" se obliga a realizar el reembolso e indemnización correspondiente.

Por lo anterior, "LAS PARTES" reconocen expresamente en este acto que "LA DEPENDENCIA O ENTIDAD" no tiene nexo laboral alguno con "EL PROVEEDOR", por lo que éste último libera a "LA DEPENDENCIA O ENTIDAD" de toda responsabilidad relativa a cualquier accidente o enfermedad que pudiera sufrir o contraer cualquiera de sus trabajadores durante el desarrollo de sus labores o como consecuencia de ellos, así como de cualquier responsabilidad que resulte de la aplicación de la Ley Federal del Trabajo, de la Ley del Seguro Social, de la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores y/o cualquier otra aplicable, derivada de la entrega de los bienes o prestación de los servicios materia de este contrato.

VIGÉSIMA SÉPTIMA. SUSPENSIÓN DEL SUMINISTRO DE LOS BIENES O PRESTACIÓN DE LOS SERVICIOS O ARRENDAMIENTO.

Cuando en la entrega de los bienes o prestación de los servicios o arrendamiento, se presente caso fortuito o de fuerza mayor, "LA DEPENDENCIA O ENTIDAD" bajo su responsabilidad, podrá de resultar aplicable conforme a la normatividad en la materia, suspender el suministro de los bienes o la prestación de los servicios, en cuyo caso únicamente se pagarán aquellos que hubiesen sido efectivamente recibidos por "LA DEPENDENCIA O ENTIDAD".

Cuando la suspensión obedezca a causas imputables a "LA DEPENDENCIA O ENTIDAD", a solicitud escrita de "EL PROVEEDOR", cubrirá los gastos no recuperables, durante el tiempo que dure esta suspensión, para lo cual "EL PROVEEDOR" deberá presentar dentro de los 30 (treinta) días naturales siguientes de la notificación del término de la suspensión, la factura y documentación de los gastos no recuperables en que haya incurrido, siempre que estos sean razonables, estén debidamente comprobados y se relacionen directamente con el contrato.

"LA DEPENDENCIA O ENTIDAD" pagará los gastos no recuperables, en moneda nacional (pesos mexicanos), dentro de los 45 (cuarenta y cinco) días naturales posteriores a la presentación de la solicitud debidamente fundada y documentada de "EL PROVEEDOR", así como del CFDI o factura electrónica respectiva y documentación soporte.

En caso de que "EL PROVEEDOR" no presente en tiempo y forma la documentación requerida para el trámite de pago, la fecha de pago se recorrerá el mismo número de días que dure el retraso.

El plazo de suspensión será fijado por "LA DEPENDENCIA O ENTIDAD", a cuyo término en su caso, podrá iniciarse la terminación anticipada del presente contrato, o bien, podrá continuar produciendo todos los efectos legales, una vez que hayan desaparecido las causas que motivaron dicha suspensión.

VIGÉSIMA OCTAVA. RESCISIÓN

"LA DEPENDENCIA O ENTIDAD" podrá en cualquier momento rescindir administrativamente el presente contrato y hacer efectiva la fianza de cumplimiento, cuando "EL PROVEEDOR" incurra en incumplimiento de sus obligaciones contractuales, sin necesidad de acudir a los tribunales competentes en la materia, por lo que, de manera enunciativa, más no limitativa, se entenderá por incumplimiento:

1.Si incurre en responsabilidad por errores u omisiones en su actuación;
2. Si incurre en negligencia en el suministro de los bienes o prestación de los servicios o arrendamiento objeto del presente contrato, sin justificación para "LA DEPENDENCIA O ENTIDAD";
3. Si transfiere en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual;
4. Si cede los derechos de cobro derivados del contrato, sin contar con la conformidad previa y por escrito de "LA DEPENDENCIA O ENTIDAD";
5. Si suspende total o parcialmente y sin causa justificada la entrega de los bienes o prestación de los servicios o arrendamiento. del presente contrato o no les otorga la debida atención conforme a las instrucciones de "LA DEPENDENCIA O ENTIDAD";
6. Si no suministra los bienes o prestación de los servicios o arrendamiento en tiempo y forma conforme a lo establecido en el presente contrato y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta;
7. Si no proporciona a "LA DEPENDENCIA O ENTIDAD" o a las dependencias que tengan facultades, los datos necesarios para la inspección, vigilancia y supervisión del suministro de los bienes objeto o prestación de los servicios o arrendamiento del presente contrato;
8. Si cambia de nacionalidad e invoca la protección de su gobierno contra reclamaciones y órdenes de "LA DEPENDENCIA O ENTIDAD";
9. Si es declarado en concurso mercantil por autoridad competente o por cualquier otra causa distinta o análoga que afecte su patrimonio;
10. Si no acepta pagar penalizaciones o no repara los daños o pérdidas, por argumentar que no le son directamente imputables, sino a uno de sus asociados o filiales o a cualquier otra causa que no sea de fuerza mayor o caso fortuito;
11. Si no entrega dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato, la garantía de cumplimiento del mismo;
12. Si la suma de las penas convencionales excede el monto total de la garantía de cumplimiento del contrato y/o de las deducciones alcanzan el 20% (veinte por ciento) del monto total de este instrumento jurídico;
13. Si "EL PROVEEDOR" no suministra los bienes o prestación de los servicios o arrendamiento objeto de este contrato de acuerdo con las normas, la calidad, eficiencia y especificaciones requeridas por "LA DEPENDENCIA O ENTIDAD" conforme a las cláusulas del presente contrato y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta;
14. Si divulga, transfiere o utiliza la información que conozca en el desarrollo del cumplimiento del objeto del presente contrato, sin contar con la autorización de "LA DEPENDENCIA O ENTIDAD" en los términos de lo dispuesto en la cláusula DÉCIMA NOVENA del presente instrumento jurídico;
15. Si se comprueba la falsedad de alguna manifestación contenida en el apartado de sus declaraciones del presente contrato;
16. Cuando "EL PROVEEDOR" y/o su personal, impidan el desempeño normal de labores de "LA DEPENDENCIA O ENTIDAD", durante el suministro de los bienes, por causas distintas a la naturaleza del objeto del mismo;
17. Cuando exista conocimiento y se corrobore mediante resolución definitiva de autoridad competente que "EL PROVEEDOR" incurrió en violaciones en materia penal, civil, fiscal, mercantil o administrativa que redunde en perjuicio de los intereses de "LA DEPENDENCIA O ENTIDAD" en cuanto al cumplimiento oportuno y eficaz en la entrega de los bienes objeto o prestación de los servicios del presente contrato; y
18. En general, incurra en incumplimiento total o parcial de las obligaciones que se estipulen en el presente contrato o de las disposiciones de la "LAASSP" y su Reglamento.

Para el caso de optar por la rescisión del contrato, "LA DEPENDENCIA O ENTIDAD" comunicará por escrito a "EL PROVEEDOR" el incumplimiento en que haya incurrido, para que en un término de 5

(cinco) días hábiles contados a partir de la notificación, exponga lo que a su derecho convenga y aporte en su caso las pruebas que estime pertinentes.

Transcurrido dicho término "LA DEPENDENCIA O ENTIDAD", en un plazo de 15 (quince) días hábiles siguientes, tomando en consideración los argumentos y pruebas que hubiere hecho "EL PROVEEDOR", determinará de manera fundada y motivada dar o no por rescindido el contrato, y comunicará a "EL PROVEEDOR" dicha determinación dentro del citado plazo.

Cuando se rescinda el contrato, se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar "LA DEPENDENCIA O ENTIDAD" por concepto del contrato hasta el momento de rescisión.

Iniciado un procedimiento de conciliación "LA DEPENDENCIA O ENTIDAD" podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido el contrato se entregaran los bienes o prestación de los servicios, el procedimiento iniciado quedará sin efecto, previa aceptación y verificación de "LA DEPENDENCIA O ENTIDAD" de que continúa vigente la necesidad de los bienes o prestación de los servicios o arrendamiento, aplicando, en su caso, las penas convencionales correspondientes.

"LA DEPENDENCIA O ENTIDAD" podrá determinar no dar por rescindido el contrato, cuando durante el procedimiento advierta que la rescisión del mismo pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, "LA DEPENDENCIA O ENTIDAD" elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

Al no dar por rescindido el contrato, "LA DEPENDENCIA O ENTIDAD" establecerá con "EL PROVEEDOR" otro plazo, que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento. El convenio modificatorio que al efecto se celebre deberá atender a las condiciones previstas por los dos últimos párrafos del artículo 52 de la "LAASSP".

Cuando se presente cualquiera de los casos mencionados, "LA DEPENDENCIA O ENTIDAD" quedará expresamente facultada para optar por exigir el cumplimiento del contrato, aplicando las penas convencionales y/o rescindirlo, siendo esta situación una facultad potestativa.

Si se llevara a cabo la rescisión del contrato, y en el caso de que a "EL PROVEEDOR" se le hubieran entregado pagos progresivos, éste deberá de reintegrarlos más los intereses correspondientes, conforme a lo indicado en el artículo 51 párrafo cuarto, de la "LAASSP".

Los intereses se calcularán sobre el monto de los pagos progresivos efectuados y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de "LA DEPENDENCIA O ENTIDAD".

"EL PROVEEDOR" será responsable por los daños y perjuicios que le cause a "LA DEPENDENCIA O ENTIDAD".

VIGÉSIMA NOVENA. TERMINACIÓN ANTICIPADA

"LA DEPENDENCIA O ENTIDAD" podrá dar por terminado anticipadamente el presente contrato, cuando concurran razones de interés general o bien cuando por causas justificadas se extinga la

necesidad de requerir los bienes o prestación de los servicios o arrendamiento originalmente contratados, y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas, se ocasionaría algún daño o perjuicio a "LA DEPENDENCIA O ENTIDAD", o se determine la nulidad total o parcial de los actos que dieron origen al contrato con motivo de una resolución de una inconformidad o intervención de oficio emitida por la Secretaría de la Función Pública, lo que bastará sea comunicado a "EL PROVEEDOR" con 30 (treinta) días naturales anteriores al hecho. En este caso, "LA DEPENDENCIA O ENTIDAD" a solicitud escrita de "EL PROVEEDOR" cubrirá los gastos no recuperables, siempre que estos sean razonables estén debidamente comprobados y relacionados directamente con el contrato.

TRIGÉSIMA. DISCREPANCIAS

"LAS PARTES" convienen que, en caso de discrepancia entre la solicitud de cotización, la propuesta económica de "EL PROVEEDOR" y el presente contrato, prevalecerá lo establecido en la solicitud de cotización respectiva, de conformidad con lo dispuesto por el artículo 81 fracción IV, del Reglamento de la "LAASSP".

TRIGÉSIMA PRIMERA. CONCILIACIÓN.

"LAS PARTES" acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente contrato se someterán al procedimiento de conciliación establecido en los artículos 77, 78, 79 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 126 al 136 de su Reglamento y al Decreto por el que se establecen las acciones administrativas que deberá implementar la Administración Pública Federal para llevar a cabo la conciliación o la celebración de convenios o acuerdos previstos en las leyes respectivas como medios alternativos de solución de controversias, publicado en el Diario Oficial de la Federación el 29 de abril de 2016.

La solicitud de conciliación se presentará mediante escrito, el cual contendrá los requisitos contenidos en el artículo 15 de la Ley Federal de Procedimiento Administrativo, además, hará referencia al número de contrato, al servidor público encargado de su administración, objeto, vigencia y monto del contrato, señalando, en su caso, sobre la existencia de convenios modificatorios, debiendo adjuntar copia de los instrumentos consensuales debidamente suscritos.

TRIGÉSIMA SEGUNDA. DOMICILIOS

"LAS PARTES" señalan como sus domicilios legales para todos los efectos a que haya lugar y que se relacionan en el presente contrato, los que se indican en el apartado de Declaraciones, por lo que cualquier notificación judicial o extrajudicial, emplazamiento, requerimiento o diligencia que en dichos domicilios se practique, será enteramente válida, al tenor de lo dispuesto en el Título Tercero del Código Civil Federal y sus correlativos en los Estados de la República Mexicana.

TRIGÉSIMA TERCERA. LEGISLACIÓN APLICABLE

"LAS PARTES" se obligan a sujetarse estrictamente para el suministro de bienes o prestación de los servicios o arrendamiento objeto del presente contrato a todas y cada una de las cláusulas que lo integran, así como la cotización y el requerimiento asociado a ésta, a la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento; al Código Civil Federal; la Ley Federal de Procedimiento Administrativo; al Código Federal de Procedimientos Civiles; a la Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento, el Acuerdo por el que se expide el

protocolo de actuación en materia de contrataciones públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones y a las demás disposiciones jurídicas aplicables.

TRIGÉSIMA CUARTA. JURISDICCIÓN

"LAS PARTES" convienen que, para la interpretación y cumplimiento de este contrato, así como para lo no previsto en el mismo, se someterán a la jurisdicción y competencia de los Tribunales Federales en la Ciudad de México, renunciando expresamente al fuero que pudiera corresponderles en razón de su domicilio actual o futuro.

FIRMANTES O SUSCRIPCIÓN.

En esta parte se formaliza el documento suscribiéndolo, señalando en forma clara el lugar y la fecha en que se suscribe, el nombre, cargo y firma de las partes y representantes, tiene relación con lo establecido en el proemio, en las declaraciones en los puntos I.2 y II.2.

Las facultades de los servidores públicos comúnmente se enuncian o describen en la normatividad interna de cada dependencia o entidad como puede ser, estatuto orgánico, reglamento interno, manual de organización, manual de procedimientos, POBALINES, entre otros.

Por lo anteriormente expuesto, tanto "LA DEPENDENCIA O ENTIDAD" como "EL PROVEEDOR", declaran estar conformes y bien enterados de las consecuencias, valor y alcance legal de todas y cada una de las estipulaciones que el presente instrumento jurídico contiene, por lo que lo ratifican y firman electrónicamente en las fechas especificadas en cada firma electrónica.

POR:

"LA DEPENDENCIA O ENTIDAD"

NOMBRE	CARGO	R.F.C
GERTRUDIS RODRÍGUEZ GONZÁLEZ	DIRECCIÓN DE ÁREA	XXXXXXXXXXXXX
RICARDO BECERRIL HERRERA	DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	XXXXXXXXXXXXX
ISRAEL SÁNCHEZ ESPINOSA	JEFE DE DEPARTAMENTO DE REDES Y TELECOMUNICACIONES	XXXXXXXXXXXXX

POR:

"EL PROVEEDOR"

NOMBRE	R.F.C
XXXXXXXXXXXXX	XXXXXXXXXX

ANEXO No. 14
FORMATO CON EL TEXTO QUE DEBE CONTENER LA GARANTÍA DE CUMPLIMIENTO

El importe de esta fianza será el equivalente al **10%** (diez por ciento) del monto máximo total del ejercicio fiscal, sin incluir el Impuesto al Valor Agregado (I.V.A.).

Dicha fianza deberá sujetarse a las disposiciones que rigen esta materia y en su redacción se transcribirá el siguiente texto:

MONTO DE LA FIANZA
$

FIANZAS.....NOMBRE DE LA AFIANZADORA, S.A. DE C.V. en ejercicio de la autorización que le otorgó el Gobierno Federal por conducto de la Secretaría de Hacienda y Crédito Público se constituye fiadora hasta el monto de:

$0,000 .00 M.N. (CANTIDAD EN LETRA)

A FAVOR DE LA COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS. (Conforme a lo dispuesto en el artículo 49 fracción II de la LAASSP)

Para garantizar por (NOMBRE DE LA EMPRESA), con R.F.C. _____, con domicilio en (DOMICILIO FISCAL DEL PROVEEDOR) ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, el fiel y exacto cumplimiento de las obligaciones derivadas del Contrato N° _____, de fecha_____, con vigencia del _____, relativo a los servicios de _____, con un importe de $_____00 M.N. mas I.V.A.

"La Institución Afianzadora se somete expresamente al procedimiento de ejecución previsto en el Artículo 282 de la Ley de Instituciones de Seguros y Fianzas, el cual también será aplicable para el cobro de indemnización por mora que en su caso se genere en los términos previstos en el artículo 283 del mismo ordenamiento, así como a lo dispuesto por el Reglamento del Artículo 95 de la Ley Federal de Instituciones de Fianzas, para el cobro de fianzas otorgadas a favor de la Tesorería de la Federación, asimismo, se obliga a observar lo dispuesto por el Artículo 178 de la Ley antes citada, en el sentido de que la fianza no tendrá fecha de vencimiento."

Esta garantía estará vigente durante el cumplimiento de la obligación que garantiza (se encontrará vigente hasta la total amortización o devolución del anticipo) y continuará vigente en caso de que se otorgue prorroga al cumplimiento del contrato, así como durante la sustanciación de todos los recursos legales o juicios que se interpongan hasta que se pronuncie resolución definitiva por autoridad competente, 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.

En caso de hacerse efectiva la presente garantía, la institución de fianzas acepta expresamente someterse al procedimiento de ejecución establecido en el artículo 282 de la Ley de Instituciones de Seguros y Fianzas, procedimiento al que también se sujetará para el caso del cobro de la indemnización de mora que prevé el artículo 283 del mismo ordenamiento legal, por pago extemporáneo del importe de la póliza de fianza requerida.

Que para liberar la fianza será requisito indispensable la manifestación expresa y por escrito de la CONDUSEF u órgano desconcentrado, según corresponda.

Por lo que la cancelación de la póliza de fianza procederá una vez que la CONDUSEF otorgue el acta administrativa o documento equivalente en el que se señale la extinción de derechos y obligaciones, previo otorgamiento del finiquito correspondiente, o en caso de existir saldos a cargo del proveedor, la liquidación debida.

En caso de prórroga o espera, la vigencia de esta fianza quedará automáticamente prorrogada en concordancia con dicha prórroga o espera y al efecto (**denominación o razón social de la compañía emisora de la fianza**) pagará en términos de Ley hasta la cantidad del **10%** del monto *máximo total* del Contrato.

Con independencia de lo anterior el "Proveedor" quedará obligado a recabar el endoso modificatorio a la póliza de fianza por cualquier modificación que se realice al Contrato, garantizando los extremos de la misma.

La falta de presentación de la fianza de cumplimiento en el plazo estipulado, dará como consecuencia el inicio del proceso de rescisión por incumplimiento a lo aquí establecido.

En caso de rescisión del Contrato, la aplicación de la garantía de cumplimiento será proporcional al monto de las obligaciones no cumplidas."

En el caso de que la "CONDUSEF" hiciera efectiva la fianza, ésta lo comunicará por escrito al "Proveedor" y a la Afianzadora, obligándose el primero a que la fianza permanezca vigente hasta que se subsanen las causas que motivaron el incumplimiento de las obligaciones a su cargo y que afecten el interés principal de esta contratación. La aplicación de la garantía será divisible.

Una vez que las obligaciones señaladas en el presente contrato sean cumplidas por el "Proveedor" y a entera satisfacción de la CONDUSEF previo pronunciamiento del servidor público responsable de administrar y vigilar el cumplimiento del contrato, la CONDUSEF realizará la cancelación de la garantía de cumplimiento del contrato y la de anticipo, en su caso.

ANEXO No. 15
NOTA INFORMATIVA PARA PARTICIPANTES DE PAÍSES MIEMBROS DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y 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 (OCDE) 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, iniciará en **noviembre de 2003** una segunda fase de **evaluación** –la primera ya fue aprobada– en donde un grupo de expertos verificará, 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 **impactará** 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.

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 valuable, se impondrán de tres meses a dos años de prisión, de treinta a trescientos días multa 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 a catorce años de prisión, de trescientos a mil días multa y destitución e inhabilitación de dos 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 o a un tercero que éste determine, para que dicho servidor público 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, o a un tercero que éste determine, para que dicho servidor público lleve a cabo la tramitación o resolución de cualquier asunto que se encuentre fuera del ámbito de las funciones inherentes a su empleo, cargo o comisión, o

III. A cualquier persona para que acuda ante un servidor público extranjero y le requiera o le proponga llevar a cabo la tramitación o resolución de cualquier asunto relacionado con las funciones inherentes al empleo, cargo o comisión de este último.

Para los efectos de este artículo se entiende por servidor público extranjero, toda persona que desempeñe un empleo, cargo o comisión en el poder legislativo, ejecutivo o judicial o en un órgano público autónomo en cualquier orden o nivel de gobierno de un Estado extranjero, sea designado o electo; cualquier persona en ejercicio de una función para una autoridad, organismo o empresa pública o de participación estatal de un país extranjero; y cualquier funcionario o agente de un organismo u organización pública internacional.

Cuando alguno de los delitos comprendidos en este artículo se cometa en los supuestos a que se refiere el artículo 11 de este Código, el juez impondrá a la persona moral hasta mil días multa y podrá decretar su suspensión o disolución, tomando en consideración el grado de conocimiento de los órganos de administración respecto del cohecho en la transacción internacional y el daño causado o el beneficio obtenido por la persona moral.”

ANEXO No. 16
"MANIFIESTO DE NO DESEMPEÑAR EMPLEO, CARGO O COMISIÓN EN EL SERVICIO PÚBLICO"

Ciudad de México a (día) (mes) (año).

Comisión Nacional Para la Protección y
Defensa de los Usuarios de Servicios Financieros
Presente:

PROCEDIMIENTO No. _____

PARA PERSONAS MORALES:

_____, en mi carácter de _____, de la ___ (Persona Moral) ___, manifiesto bajo protesta de decir verdad que los socios o accionistas cuyos nombres aparecen al final de este documento, no desempeñan empleos, cargos o comisiones en el servicio público o, en su caso, que a pesar de desempeñarlo, en caso de resultar adjudicado con la formalización del contrato correspondiente no se actualiza un Conflicto de Interés. En el entendido de que dicha manifestación se deberá hacer del conocimiento del Órgano Interno de Control, previo a la celebración del contrato, tal como se prevé en el artículo 49, fracción IX de la Ley General de Responsabilidades Administrativas

1.
2.
3.

_____
(Nombre y firma del licitante o representante legal de la persona moral

PARA PERSONA FÍSICAS:

Manifiesto bajo protesta de decir verdad que no desempeño empleo, cargo o comisión en el servicio público o, en su caso, que a pesar de desempeñarlo, en caso de resultar adjudicado con la formalización del contrato correspondiente no se actualiza un Conflicto de Interés. En el entendido de que dicha manifestación se deberá hacer del conocimiento del Órgano Interno de Control, previo a la celebración del contrato, tal como se prevé en el artículo 49, fracción IX de la Ley General de Responsabilidades Administrativas.

_____
(Nombre y firma del licitante o representante legal de la persona moral

ANEXO No. 17
"MANIFIESTO DE CONOCER EL PROTOCOLO DE ACTUACIÓN EN MATERIA DE CONTRATACIONES PÚBLICAS, OTORGAMIENTO Y PRÓRROGA DE LICENCIAS, PERMISOS, AUTORIZACIONES Y CONCESIONES"

Ciudad de México a (día) (mes) (año).

Comisión Nacional Para la Protección y Defensa de los Usuarios de Servicios Financieros
Presente:

Me refiero al procedimiento de _____(1)_____ No. LA-006G3A001-E***-202X en el que mi representada, la empresa_____(2)_____, participa a través de la presente proposición.

(NOMBRE DE LA PERSONA FACULTADA LEGALMENTE), y en mi carácter de representante legal de la empresa_____ y que cuento con las facultades suficientes declaro bajo protesta de decir verdad que conozco el contenido del "ACUERDO POR EL QUE SE EXPIDE EL PROTOCOLO DE ACTUACIÓN EN MATERIA DE CONTRATACIONES PÚBLICAS, OTORGAMIENTO Y PRÓRROGA DE LICENCIAS, PERMISOS Y AUTORIZACIONES Y CONCESIONES".

Atentamente

_____
Nombre completo (cuando se trate de persona física) y firma
Representante legal (cuando represente a una persona moral)

ANEXO No. 18
"ACUSE DEL MANIFIESTO PARA ACREDITAR LA AUSENCIA DE CONFLICTO DE INTERÉS"

ACUSE DEL MANIFIESTO EN EL QUE 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

De conformidad al Acuerdo por el que se expide el Protocolo de Actuación en Materia de Contrataciones Públicas, Otorgamiento y Prórroga de Licencias, Permisos, Autorizaciones y Concesiones. Publicado en el Diario Oficial de la Federación el pasado 20 de agosto del 2015, así como a sus diversos que lo modifican publicados en el mismo medio de difusión oficial los días 19 de febrero de 2016 y 28 de febrero de 2017.

Los interesados deberán presentar el **Acuse del manifiesto** en el que 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, mismo que puede 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.

De conformidad con 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, que a la letra dice:

(...)

3. *Los particulares personas morales que se encuentren en los supuestos previstos en el numeral 4 de este Anexo, podrán formular por medio de sus representantes legales un manifiesto en el que afirmen o nieguen los vínculos o relaciones de negocios, laborales, profesionales, personales o de parentesco por consanguinidad o afinidad hasta el cuarto grado que tengan las personas que a continuación se señalan, con el o los servidores públicos a que se refiere el número 5 del presente Anexo:*

   a) *Integrantes del consejo de administración o administradores;*
   b) *Director general, gerente general, o equivalentes;*
   c) *Representantes legales, y*

d) *Personas físicas que posean directa o indirectamente cuando menos el diez por ciento de los títulos representativos del capital social de la persona moral.*

4. *A fin de fomentar las mejores prácticas en la prevención de conflictos de interés, los particulares formularán el manifiesto **por única vez** cuando tengan la intención de participar en los siguientes procedimientos:*

   I. *Contrataciones públicas;*
   II. *Otorgamiento y prórroga de concesiones, y*
   III. *Otorgamiento y prórroga de licencias, permisos y autorizaciones. Fracción reformada por Acuerdo DOF 28/02/2017.*

5. *El manifiesto incluirá los vínculos o relaciones entre el particular y los servidores públicos que a continuación se indican:*

   I. *Presidente de la República;*
   II. *Secretarios de Estado;*
   III. *Jefe de la Oficina de la Presidencia de la República;*
   IV. *Consejero Jurídico del Ejecutivo Federal;*
   V. *Procurador General de la República;*
   VI. *Titulares de entidades;*
   VII. *Titulares de órganos reguladores coordinados;*
   VIII. *Subprocuradores o titulares de fiscalías especializadas;*
   IX. *Comisionados adscritos a órganos reguladores coordinados;*
   X. *Subsecretarios, oficiales mayores, consejeros adjuntos, titulares de órganos administrativos desconcentrados, titulares de unidad y directores generales en las dependencias;*
   XI. *Directores generales, gerentes, subgerentes, directores o integrantes de los órganos de gobierno o de los comités técnicos de las entidades, y*
   XII. *Personal que interviene en contrataciones públicas, en el otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones, incluidos en el Registro que lleva la Secretaría de la Función Pública.*

6. *Los particulares formularán el manifiesto a través de la dirección electrónica www.gob.mx/sfp, siendo este medio electrónico de comunicación el único para presentarlo. El Sistema generará un acuse de presentación del manifiesto. A través de dicho medio electrónico los particulares podrán también denunciar presuntos conflictos de interés de los que tengan conocimiento, enunciando las pruebas con las que en su caso cuenten.*

***** El acuse de presentación del manifiesto se obtiene a través de la liga:

https://manifiesto.funcionpublica.gob.mx/SMP-web/loginPage.jsf

***** Consulta el Protocolo de Actuación en Materia de Contrataciones Públicas, Otorgamiento y Prórroga de Licencias, Permisos, Autorizaciones y Concesiones a través de la liga:

https://www.gob.mx/cms/uploads/attachment/file/196367/Protocolo_versi_n_integrada_28-feb-17_v2.pdf

ó en el siguiente archivo:

ANEXO No. 19
"MANIFIESTO DE CONOCER Y REGISTRARSE EN EL MÓDULO DE FORMALIZACIÓN DE INSTRUMENTOS JURÍDICOS"

Ciudad de México a (día) (mes) (año).

Comisión Nacional Para la Protección y
Defensa de los Usuarios de Servicios Financieros
Presente:

PROCEDIMIENTO No. _____

PARA PERSONAS MORALES:

_____, en mi carácter de _____, de la ___(Persona Moral)___, manifiesto bajo protesta de decir verdad que conozco y estaré a lo establecido en los artículos Tercero, Cuarto y demás aplicables 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 Diario Oficial de la Federación el pasado 18 de septiembre de 2020, donde se determina que todo instrumento jurídico que derive de algún procedimiento de contratación realizado por las Dependencias y Entidades, se deberá utilizar la Firma Electrónica Avanzada (e.firma) que emite el Servicio de Administración Tributaria como medio de identificación.

En consecuencia, en caso de resultar adjudicado, me comprometo a formalizar el instrumento jurídico en el Módulo de Formalización de Instrumentos Jurídicos del sistema CompraNet; para lo cual deberé estar registrado en el citado módulo.

Asimismo, manifiesto conocer que se puede consultar el material de apoyo para el registro en el citado módulo, en la liga electrónica https://www.gob.mx/compranet/documentos/modulo-de-formalizacion-de-instrumentos-juridicos.

_____

(Nombre y firma del licitante o representante legal de la persona moral

PARA PERSONA FÍSICAS:

Manifiesto bajo protesta de decir verdad que conozco y estaré a lo establecido en los artículos Tercero, Cuarto y demás aplicables 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 Diario Oficial de la Federación el pasado 18 de septiembre de 2020, donde se determina que todo instrumento jurídico que derive de algún procedimiento de contratación realizado por las Dependencias y

Entidades, se deberá utilizar la Firma Electrónica Avanzada (e.firma) que emite el Servicio de Administración Tributaria como medio de identificación.

En consecuencia, en caso de resultar adjudicado, me comprometo a formalizar el instrumento jurídico en el Módulo de Formalización de Instrumentos Jurídicos del sistema CompraNet; para lo cual deberé estar registrado en el citado módulo.

Asimismo, manifiesto conocer que se puede consultar el material de apoyo para el registro en el citado módulo, en la liga electrónica https://www.gob.mx/compranet/documentos/modulo-de-formalizacion-de-instrumentos-juridicos.

_____

(Nombre y firma del licitante)