Instituto Mexicano del Seguro Social

Dirección de Administración
Unidad de Adquisiciones e Infraestructura
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística.

Calle Durango número 291, Piso 5, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc,
Código Postal 06700, Ciudad de México, México.

Convocatoria
Licitación Pública Nacional Electrónica
Núm. LA-050GYR019-E22-2021

“SERVICIOS ADMINISTRADOS DE SEGURIDAD INTEGRAL 2021” (SASI)

Índice

Convocatoria

En observancia al artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, y de conformidad con los artículos, 26 fracción I, 26 Bis fracción II, 28 fracción I, y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, los relativos de su Reglamento y demás disposiciones aplicables en la materia, se convoca a las personas físicas o morales de nacionalidad mexicana al presente procedimiento cuya actividad comercial esté relacionada con los servicios a contratar descritos en el **Anexo 1.- Anexo Técnico**.

1.- Identificación de la licitación pública nacional.

1.1.- Datos de identificación.

Entidad contratante: Instituto Mexicano del Seguro Social.
Dirección de Administración.
Unidad de Adquisiciones e Infraestructura.
Coordinación de Adquisición de Bienes y Contratación de Servicios.
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos.

Área contratante: División de Contratación de Activos y Logística.

Domicilio: Calle Durango número 291, Piso 5, Colonia Roma Norte, Código Postal 06700, Demarcación Territorial Cuauhtémoc, Ciudad de México, México.

Área requirente/técnica: Coordinación de Mantenimiento y Operación de Servicios de Cómputo / División de Seguridad Informática Integral.

1.2.- Medio y carácter del procedimiento.

La presente licitación pública nacional, conforme al medio utilizado es electrónica, por lo cual los licitantes deberán participar únicamente a través de CompraNet de conformidad con lo dispuesto en los artículos 26 Bis fracción II de la LAASSP, y en el ***"Acuerdo por el que se establecen las disposiciones que deberán observar para la utilización del Sistema Electrónico de Información Pública Gubernamental, denominado CompraNet"***, publicado en DOF el 28 de junio de 2011.

El carácter del presente procedimiento de contratación es nacional.

1.3.- Número de identificación de la licitación pública nacional asignado por CompraNet.

LA-050GYR019- E22-2021

1.4.- Indicación de los ejercicios fiscales para la contratación.

La presente contratación implicará solo para el ejercicio fiscal 2021.

1.5.- Idioma en que se deberán presentar las propuestas, los anexos legales, administrativos y técnicos, así como en su caso los folletos que se acompañen.

Las proposiciones deberán presentarse en idioma español.

1.6.- Disponibilidad presupuestaria.

Se cuenta con el recurso presupuestal para el ejercicio 2021 conforme al dictamen de disponibilidad presupuestal previo con folio: 000016273-2021.

2.- Objeto y alcance de la licitación pública nacional.

2.1.- Objeto de la contratación.

Se requiere contar con los Servicios Administrados de Seguridad Integral para los activos de Información donde se alojan los aplicativos, sistemas de información y bases de datos sensibles del Instituto, en las ubicaciones en donde los requiera el Instituto, así como con los niveles de servicio establecidos en el apéndice del presente documento y conforme a las características técnicas solicitadas en el Anexo Técnico.

La descripción amplia y detallada del servicio a contratar se encuentra especificada en los **Anexos 1 y 2,** "**Anexo Técnico", "Términos y Condiciones"** respectivamente de esta convocatoria.

2.2.- Agrupación de Partidas.

La adjudicación del presente procedimiento de contratación se llevará mediante partida única.

2.3.- Normas Oficiales Mexicanas, Normas Mexicanas, Internacionales, Referencia o Especificaciones.

NOM-002-STPS-2010
NOM-024-SSA3-2012.

2.4.- Cantidades a contratar.

Se contratará UN SERVICIO: Servicios Administrados de Seguridad Integral 2021.

CONCEPTO	CANTIDAD MINIMA	CANTIDAD MAXIMA
I. Servicios de Seguridad - Continuidad Operativa		
1. Arquitectura de Firewall.	**2**	**4**
2. Prevención de Intrusiones (IPS)	**2**	**4**
3. Anti-denegación de servicios DDoS	**2**	**4**
4. Redes Privadas Virtuales	**2**	**4**
5. Filtrado de contenido web	**2**	**4**
6. Antispam	**2**	**4**
7. Firewall Especializado en Servicios Web	**2**	**4**
8. Firewall de Base de Datos	**2**	**4**
9. Gestión Unificada de Amenazas (UTM)	**2**	**4**
II.- Servicios de Seguridad – Verificación / Calidad		
1. Análisis de Vulnerabilidades	**40**	**100**
2. Pruebas de Penetración	**40**	**100**
3. Borrado Seguro de Información	**25**	**50**
4. Gestión de Dominios	**1**	**1**
5. Certificados Digitales SSL	**4**	**6**
6. Análisis Forense	**1**	**2**
7. Sistema de Gestión de Seguridad de la Información (SGSI)	**1**	**1**
III.- Servicios del Centro de Operaciones de Seguridad (SOC)		
1. Servicios del Centro de Operaciones de Seguridad (SOC)	**1**	**1**

2.5 Forma de adjudicación.

Se requiere una sola fuente de abasto por partida.

2.6.- Modelo de contrato.

Se adjunta como **Anexo 14** el modelo de contrato específico que será empleado para formalizar los derechos y obligaciones que se deriven de la presente licitación pública nacional, a los cuales estará obligado el licitante que resulte adjudicado.

En caso de discrepancia entre el contenido del modelo de contrato y el de la presente convocatoria, prevalecerá lo estipulado en ésta última.

3.- Forma y términos que regirán los diversos actos de la licitación pública nacional.

3.1.- Fecha, hora y lugar para los actos de la licitación pública nacional.

Acto	Fecha	Hora	Lugar
Junta de Aclaraciones	12 de febrero de 2021	11:00 Horas.	CompraNet Remitir las solicitudes de aclaración, interés en participar y propuestas técnico-económicas por los medios remotos de comunicación electrónica. "CompraNet".
Presentación y Apertura de Proposiciones	22 de febrero de 2021	11:00 Horas.	
Notificación de Fallo	26 de febrero de 2021	14:00 Horas.	

3.2.- Junta de aclaraciones.

La junta de aclaraciones se llevará a cabo en términos de los artículos 33 Bis de la LAASSP, 45 y 46 del RLAASSP, por lo que los licitantes que manifiesten su interés en participar en la licitación pública nacional electrónica deberán presentar un escrito, por si o en representación de un tercero, de acuerdo con el **Anexo 13** que se adjunta para tal efecto, con el cual serán considerados licitantes y tendrán derecho a formular solicitudes de aclaración utilizando para tal caso el **Anexo 13 y 13.1** de la presente convocatoria.

Con el objeto de agilizar la junta de aclaraciones se solicita a los licitantes remitir el **Anexo 13 y 13.1** en formato Word.

Es importante mencionar que los licitantes deberán enviar las solicitudes de aclaración, a través de CompraNet, en la sección "Mensajes Unidad Compradora/Licitantes" del "Procedimiento de Contratación", en formato Word a más tardar veinticuatro horas antes de la fecha y hora programada que se realice la junta de aclaraciones**.**

3.2.1. Los licitantes que deseen enviar solicitudes de aclaración **Anexo 13.1**, las cuales deberán plantearse de manera concisa y estar directamente vinculadas con los puntos contenidos en la convocatoria, indicando el numeral o punto específico con el cual se relaciona.

3.2.2. El plazo para enviar dichas solicitudes será a partir de la publicación de esta convocatoria y hasta las **11:00 horas del 11 de febrero de 2021.**

3.2.3. La convocante procederá a enviar, a través de CompraNet, las contestaciones a las solicitudes de aclaración recibidas.

3.3.- Recepción de proposiciones.

La presentación y apertura de proposiciones se llevará a cabo en términos de los artículos 34 primer párrafo y 35 de la LAASSP, 47, 48, 49 segundo párrafo y 50 del RLAASSP, para lo cual podrán hacer uso de los formatos previstos en el numeral 8 de la presente convocatoria.

Solo serán consideradas las proposiciones que se reciban por medio de CompraNet en respuesta al requerimiento técnico y económico. **El licitante deberá firmar electrónicamente la proposición**; para que se considere que la proposición se envió firmada, deberán descargarse los archivos PDF generados por CompraNet

y que contienen los datos capturados en la propuesta, sólo esos archivos deberán firmarse utilizando el módulo de Firma Electrónica de documentos y cargarse en el área correspondiente.

Una vez alcanzada la fecha y hora de inicio del evento de apertura de proposiciones, el licitante no podrá enviar su proposición o modificación de la misma.

Una vez recibidas las proposiciones en la fecha, hora y lugar establecidos, éstas no podrán retirarse o dejarse sin efecto, por lo que deberán considerarse vigentes dentro del procedimiento de contratación hasta su conclusión.

Cada uno de los documentos que integren la proposición y aquéllos distintos a ésta, deberán estar foliados en todas y cada una de las hojas que los integren. Al efecto, se deberán numerar de manera individual las propuestas técnica y económica, así como el resto de los documentos que entregue el licitante.

3.3.1.- Proposiciones conjuntas.

Conforme al artículo 34 de la LAASSP, los interesados podrán presentar propuestas conjuntas, siempre y cuando éstas cumplan con lo establecido en los artículos 44 y 48, fracción VIII, segundo párrafo del Reglamento de la LAASSP.

Las personas interesadas podrán agruparse para presentar una propuesta, para tal efecto deberán cubrir los siguientes requisitos.

I) Uno de los integrantes podrá presentar el escrito mediante el cual se manifieste el interés en participar en la junta de aclaraciones y en el procedimiento de contratación.

II) Los integrantes deberán celebrar en términos de la legislación aplicable un convenio, en el cual se establezcan con precisión los siguientes aspectos, de conformidad con el **Anexo 15,** de la presente convocatoria:

- Nombre, Domicilio y RFC 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,
- 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,
- Designación de un representante común, otorgándole poder amplio y suficiente, para atender todo lo relacionado con la propuesta y con el procedimiento de licitación pública nacional electrónica.
- 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
- Estipulación expresa de que cada uno de los firmantes quedará obligado junto con los demás integrantes, en forma solidaria, según se convenga, para efectos del procedimiento de contratación y del contrato, en caso de que se les adjudique el mismo.

III) Deberán presentar en forma individual los escritos siguientes: **Escrito de no impedimento, Declaración de integridad, Escrito de nacionalidad mexicana, Escrito de estratificación y Escrito de facultades**, conforme a los Anexos señalados en el numeral **4.1.3 Documentación** Legal de la presente convocatoria

En el acto de presentación y apertura de proposiciones el representante común de la agrupación deberá señalar que la propuesta se presenta en forma conjunta. El convenio a que hace referencia el inciso II), se presentará con la propuesta y, en caso de que a los licitantes que la hubieren presentado se les adjudique el contrato, dicho convenio, formará parte integrante del mismo como uno de sus anexos.

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

3.3.2.- Proposición única.

Los licitantes sólo podrán presentar una proposición para la partida del presente procedimiento de contratación.

3.3.3.- Documentación distinta a las propuestas.

El licitante podrá presentar documentación distinta a la que conforma las propuestas técnica y económica, misma que forma parte de su proposición.

3.3.4.- Acreditamiento de existencia legal.

El licitante deberá acreditar su existencia legal y, en su caso, la personalidad jurídica de su representante, en el acto de presentación y apertura de proposiciones, para lo cual podrá hacer uso del **Anexo 3** de la convocatoria.

3.4.- Acto de fallo y firma de contrato.

El fallo se emitirá de conformidad con el artículo 37 de la LAASSP y su contenido se difundirá a través de CompraNet el mismo día en que se emita, en el entendido de que este procedimiento sustituye a la notificación personal. Así también el fallo podrá ser consultado en el portal de compras del IMSS en el apartado “Transparencia” (http.//compras.imss.gob.mx/), o bien en el mural de comunicación ubicado en el piso 5 del inmueble en la Calle Durango número 291, Colonia Roma Norte, Código Postal 06700, Demarcación Territorial Cuauhtémoc, Ciudad de México, México en donde se fijará copia de un ejemplar del acta por un término no menor de cinco días hábiles.

El licitante adjudicado deberá firmar el contrato que se señala en el **Anexo 14** de la presente convocatoria, el **9 de marzo de 2021,** en la División de Contratos, ubicada en la Calle Durango número 291, Piso 10, Colonia Roma Norte, Código Postal 06700, Demarcación Territorial Cuauhtémoc, en la Ciudad de México, México.

En caso de que la fecha prevista originalmente esté rebasada o no se encuentre vigente, o bien no se mencione en el fallo, *el término para la firma del contrato quedará comprendido dentro de los quince días naturales posteriores a la notificación del fallo* mediante notificación personal en el domicilio o a través de correo electrónico que para tales efectos haya señalado el licitante.

Previo a la firma del contrato deberá presentar los siguientes documentos:

3.4.1.- Persona moral.

a. Acta constitutiva y, en su caso, sus respectivas modificaciones. **(*Presentar en su proposición* *en caso de no presentarla no será causa de desechamiento*).**

b. Poder notarial del representante legal que firmará el contrato.

3.4.2.- Persona física:

a. Acta de nacimiento o carta de naturalización. **(*Presentar en su proposición* *en caso de no presentarla no será causa de desechamiento*).**

3.4.3.- Ambos:

a) Identificación oficial vigente y con fotografía del representante legal.

b) Cédula de Registro Federal de Contribuyentes.

c) Comprobante de domicilio con vigencia no mayor a 3 meses.

d) En su caso, escrito de estratificación de empresa en términos del artículo 3 de la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa.

e) Escrito en términos del artículo 50 y 60 de la LAASSP.

f) Opinión positiva de cumplimiento de obligaciones fiscales emitida por el SAT vigente a la firma del contrato, en términos del artículo 32-D del Código Fiscal de la Federación. (*Presentar en su proposición* *en caso de no presentarla no será causa de desechamiento*).

g) Opinión positiva de cumplimiento de obligaciones en materia de seguridad social vigente a la firma del contrato emitida por el IMSS, en términos del artículo 32-D del Código Fiscal de la Federación y del Acuerdo ACDO.SA1.HCT.101214/281.P.DIR publicado en el DOF el 27 de febrero de 2015 y su modificación mediante el Acuerdo ACDO.AS1.HCT.260220/64.P.DIR publicado en el DOF el 30 de marzo de 2020. (*Presentar en su proposición* *en caso de no presentarla no será causa de desechamiento*).

En caso de que el licitante:

a) No se encuentre registrado ante este instituto o;

b) Cuente con Registro Patronal pero se encuentre dado de baja o;

No tenga personal que sea sujeto de aseguramiento obligatorio, de conformidad con lo dispuesto por el artículo 12 de la LSS.

No podrá obtener la citada Opinión, por lo cual dicho licitante podrá dar cumplimiento a tal requerimiento presentando lo siguiente:

I. Documento emitido por este Instituto (resultado de la consulta en el sistema para obtener la Opinión), en el que se haga constar que no se puede emitir la Opinión de cumplimiento, de conformidad con la Regla Quinta del Anexo único del ACDO.AS1.HCT.260220/64.P.DIR;

II. Escrito libre, bajo protesta de decir verdad, que no le es posible obtener la multicitada Opinión, justificando el motivo y anexando el documento en el que conste que no se puede emitir la misma y;

III. En el caso de que el licitante manifieste que presta sus servicios a través de trabajadores subcontratados con un tercero, deberá de presentar en tal caso, junto con la documentación citada en los dos párrafos anteriores , la Opinión de cumplimiento de obligaciones del subcontratante, desde luego, vigente y positiva (lo anterior en términos del artículo 15-A de la LSS).

En caso de que el licitante forme parte de un grupo comercial y uno de los entes que forma parte del grupo se encarga de administrar la plantilla laboral de todas las empresas que lo conforman, será necesario que exhiba el documento que acredite la subcontratación para situarse en el supuesto del párrafo anterior.

En caso de que el licitante no cuente con trabajadores debido a que celebró contrato de prestación de servicios con otra empresa que es la que tiene contratados a los trabajadores (outsourcing), deberá presentar dicho contrato, así como escrito libre en el que manifieste que no se encuentra obligado debido a tal situación y opinión positiva vigente de cumplimiento de obligaciones en materia de seguridad social de la empresa subcontratada emitida por el IMSS.

En caso de que el licitante no cuente con trabajadores, deberá presentar escrito libre en el que manifieste que no se encuentra obligado a inscribirse ante el IMSS, por lo que no puede obtener la opinión de cumplimiento de obligaciones en materia de seguridad social.

Para los casos de contratos que se formalicen con personas físicas que presten sus servicios por sí mismos y por lo tanto no cuentan con un Registro Patronal ni tengan trabajadores registrados en el Instituto, el particular **deberá de manifestar mediante escrito libre, bajo protesta de decir verdad, que no le es posible obtener la multicitada Opinión, justificando el motivo y anexando el documento (resultado de la solicitud de Opinión que le da el Sistema institucional) en el que conste que no se puede emitir la misma**.

En el caso de aquellos patrones (proveedores o contratistas y sus subcontratados) que tengan más de un Registro Patronal ante el Instituto y alguno o más de uno de estos Registros no se encuentre al corriente en el cumplimiento de las multicitadas obligaciones, **no se podrá considerar que se encuentra al corriente en el cumplimiento de dichas obligaciones, aun cuando el registro patronal que haya utilizado para el contrato que se trate si se encuentre al corriente en sus pagos, por lo que deberá regularizar todos sus Registros a efecto de poder obtener la Opinión positiva.**

En caso de que el participante cuente con trabajadores contratados bajo el régimen de honorarios asimilados a salarios, deberá presentar el(los) contrato(s) con los que acredite el régimen de contratación, así como escrito libre en el que manifieste que no se encuentra obligado a inscribirse ante el IMSS debido a tal situación, por lo que no puede obtener la opinión de cumplimiento de obligaciones en materia de seguridad social.

h) Escrito 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. (Artículo 49 fracción IX de la Ley General de Responsabilidades Administrativas DOF 18-07-2016). (Anexo 12), (*Presentar en su proposición* en caso de no presentarla no será causa de desechamiento*).*

i) Constancia vigente de situación fiscal emitida por el Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT) en los términos establecidos por las "Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de amortizaciones" publicadas en el Diario Oficial de la Federación (DOF) el 28 de junio del 2017. (*Presentar en su proposición* en caso de no presentarla no será causa de desechamiento*).*

j) En su caso, convenio de participación conjunta.

En caso de que el licitante acredite estar inscrito en el Registro Único de Proveedores y Contratistas de CompraNet, deberá remitir únicamente la documentación referida en los incisos: **f), g), h), i).**y en su caso **j)**

4. Requisitos que los licitantes deben cumplir.

4.1 Con fundamento en los artículos 26 Bis fracción II y 34 de la LAASSP, el licitante deberá remitir a través del sistema CompraNet, la siguiente documentación:

4.1.1 Propuesta técnica.

Deberá incluir la descripción amplia y detallada del servicio, para lo cual el licitante deberá cumplir con las especificaciones contenidas en el **Anexo 1 y Anexo 2** de la presente convocatoria, así como anexar a su propuesta los documentos solicitados en dichos anexos.

Los licitantes, para la presentación de su propuesta técnica, deberán ajustarse estrictamente a los requisitos y especificaciones previstos en el **Anexo 1.-** "**Anexo Técnico"** describiendo en forma amplia y detallada el servicio que esté ofertando, así como lo señalado por el **Anexo 2.- "Términos y Condiciones",** lo anterior para que sus proposiciones se declaren solventes técnicamente, cabe señalar que el incumplimiento a cualquiera de los contenidos será causal de desechar la proposición.

4.1.2 Propuesta económica.

El licitante deberá presentar su propuesta económica, para lo cual podrá hacer uso del **Anexo 9** de la presente convocatoria.

Los licitantes, para la presentación de su propuesta económica, deberán ajustarse estrictamente a los requisitos y especificaciones previstos en el **Anexo 1.-** "**Anexo Técnico** así como lo señalado por el **Anexo 9.- "Propuesta Económica",** lo anterior para estar en posibilidades de realizar la evaluación económica, cabe señalar que no presentar la proposición económica será causal de desechar la proposición.

4.1.3 Documentación legal

Los licitantes, para la presentación de su proposición, deberán presentar los escritos señalados en este numeral, cabe señalar que la falta de presentación de los escritos o manifestaciones bajo protesta de decir verdad, previstos en la LAASSP o su Reglamento será motivo de desechamiento.

El licitante deberá presentar los siguientes documentos, para lo cual podrá hacer uso de los anexos indicados a continuación:

4.1.3.1 Escrito de facultades.

Escrito bajo protesta de decir verdad que cuenta con facultades suficientes para comprometerse por sí o por su representada, de acuerdo con el **Anexo 3** de la presente convocatoria que se adjunta para tal efecto. Acompañándose de copia simple por ambos lados de su identificación oficial vigente con fotografía, (cartilla del servicio militar nacional, pasaporte, credencial para votar ó cédula profesional), tratándose de personas físicas, y en el caso de personas morales, de la persona que firme la propuesta.

4.1.3.2 Escrito de nacionalidad mexicana.

Escrito bajo protesta de decir verdad, que el licitante es de nacionalidad mexicana, de acuerdo con el **Anexo 4** de la presente convocatoria que se adjunta para tal efecto.

4.1.3.3 Escrito de normas.

Escrito en el que manifieste que en caso de resultar adjudicado, los servicios propuestos cumplirán con las normas solicitadas en la presente convocatoria, de acuerdo con el **Anexo 5** que se adjunta para tal efecto**.**

4.1.3.4 Escrito de no impedimento.

Escrito bajo protesta de decir verdad, que no se ubica en los supuestos establecidos en los artículos 50 y 60 de la LAASSP, de acuerdo con el **Anexo 6** de la presente convocatoria que se adjunta para tal efecto.

4.1.3.5 Declaración de integridad.

Escrito en el que el licitante manifieste, bajo protesta de decir verdad que se abstendrán de adoptar conductas, por si o a través de interpósita persona, para que los servidores públicos del IMSS 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, de acuerdo con el **Anexo 7** de la presente convocatoria que se adjunta para tal efecto.

4.1.3.6 Escrito de estratificación.

En su caso, escrito bajo protesta de decir verdad que el licitante cuenta con estratificación como micro, pequeña o mediana empresa, de acuerdo con el **Anexo 8** de la presente convocatoria que se adjunta para tal efecto.

4.1.3.7 Escrito relativo a las proposiciones vía CompraNet.

Escrito libre en el que manifieste su aceptación de que se tendrán como no presentadas sus proposiciones y, en su caso, la documentación requerida, cuando el archivo electrónico en el que se contengan las proposiciones y/o demás información no pueda abrirse por tener algún virus informático o por cualquier otra causa ajena al IMSS, en términos de lo dispuesto por el numeral 29 del ***"Acuerdo por el que se establecen las disposiciones que deberán observar para la utilización del sistema electrónico de información pública gubernamental, denominado CompraNet".***

4.2 Causales expresas de desechamiento.

De conformidad con el artículo 29 fracción XV de la LAASSP, será causa de desechamiento:

4.2.1 El incumplimiento de alguno de los requisitos establecidos en la convocatoria a la licitación pública nacional contenidos en los numerales **4.1.1. y 4.1.2. y 4.1.3.**, que con motivo de dicho incumplimiento se afecte la solvencia de la proposición.

4.2.2 Si se comprueba que algún licitante ha acordado con otro u otros elevar el costo de los servicios objeto de la presente convocatoria, o cualquier otro acuerdo que tenga como fin obtener una ventaja sobre los demás licitantes.

4.2.3 La falta de presentación de los escritos o **manifestaciones bajo protesta de decir verdad**, previstos en la LAASSP o su Reglamento que se soliciten como requisito de participación en la presente convocatoria será motivo de desechamiento, por incumplir las disposiciones jurídicas que los establecen, conforme al artículo 39 penúltimo párrafo de la LAASSP.

4.2.4 Cuando no cotice la totalidad del servicio requerido conforme a las condiciones y características solicitadas en la presente Convocatoria.

4.2.5 **Cuando la propuesta técnica o económica no cuente con la firma electrónica** en el sistema CompraNet, establecida por la Secretaría de la Función Pública como medio de identificación electrónica, es decir, la firma electrónica avanzada que emite el SAT para el cumplimiento de obligaciones fiscales. Se tendrá como no firmada la proposición cuendo en alguno de los campos de CompraNet denominados "Anexo Requerimiento Técnico Firmado Digitalmente" y "Anexo Requerimiento Económico Firmado Digitalmente" se aprecie el mensaje: *"sin archivo adjunto".*

4.2.6 Cuando la firma electrónica de la proposición técnica o económica no sea válida. Se considerará como no valida la firma cuando en el resultado de la verificación de firma electrónica en CompraNet se aprecie la leyenda "Archivo con Firma Digital No Valido".

4.2.7 No cumplir con las especificaciones técnicas del "**Anexo Técnico"** y **"Términos y Condiciones" Anexo 1** y **Anexo 2**.

4.2.8 Cuando los licitantes se encuentren dentro de algunos los supuestos del Art. 50 y 60 de la Ley.

4.2.9 Cuando los documentos que envíen los licitantes a través de la plataforma CompraNet no sean legibles, imposibilitando el análisis integral de la proposición, y esto conlleve a un faltante o carencia de información que afecte la solvencia de la proposición, ésta se considerará insolvente.

4.2.10 Que la propuesta técnica no alcance el mínimo de 45 puntos de los 60 puntos disponibles en la evaluación técnica.

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

4.2.12 Cuando se opte por participación conjunta esta deberá cumplir cabalmente con lo señalado en el numeral 3.3.1. de la convocatoria, caso contrario se desechara la proposición.

4.2.13 En el caso de proposiciones conjuntas, no presentar el convenio correspondiente debidamente firmado por todos los integrantes de la misma, conforme a lo establecido en el artículo 34 de la LAASSP y 44 de su Reglamento.

4.2.14 En el caso de proposiciones conjuntas, que en el mismo, no se establezcan con precisión las partes a que cada persona se obligará, así como la manera en que se exigiría el cumplimiento de las obligaciones.

4.2.15 Cuando el licitante presente más de una proposición técnica o económica para la misma partida.

4.2.16 Falta de folio en la proposición conforme al artículo 50 segundo párrafo del RLAASSP

4.2.17 Cuando el licitante incurra en cualquier violación a las disposiciones de la LAASSP, a su Reglamento o a cualquier ordenamiento legal o normativo vinculado a este procedimiento.

4.2.18 Si el licitante envía su proposición por medio distinto a CompraNet

4.2.19 Cuando no cumplan con alguno de los requisitos y anexos de la Convocatoria, así como los que se deriven del Acto de la Junta de Aclaraciones, y que con motivo de dicho incumplimiento se afecte directamente la solvencia de la propuesta, conforme a lo previsto en el último párrafo del Artículo 36 de la LAASSP.

5. Criterios específicos conforme a los cuales se evaluarán las proposiciones.

5.1 Evaluación de la propuesta técnica.

Con fundamento en lo dispuesto por el artículo 36 y 36 Bis fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP) y 52 de su Reglamento, el criterio que se utilizará será el de puntos, de acuerdo al Anexo **Matriz de Puntos y Porcentajes "Servicios Administrados de Seguridad Integral 2021;** conforme a la metodología que se señala a continuación:

Número	Rubros	Puntos Máximos Posibles
I	Capacidad del Licitante	20.0
II	Experiencia y especialidad del Licitante	18.0
III	Propuesta de Trabajo	10.0
IV	Cumplimiento de Contratos	12.0
	TOTAL:	**60.00**

La documentación que deberá presentar el licitante para acreditar los rubros a evaluar, se encuentra detallada en el Anexo **Matriz de Puntos y Porcentajes "Servicios Administrados de Seguridad Integral 2021**.

La propuesta técnica deberá contemplar los requisitos, condiciones y especificaciones técnicas establecidas en el **Anexo 1.**

La propuesta técnica que obtenga al menos 45 puntos de los 60 máximos, será considerada solvente. Las proposiciones técnicas que no obtengan al menos 45 puntos, serán desechadas y no serán tomadas en cuenta para su evaluación económica ni legal.

Se establece que el puntaje máximo que podrán obtener el o los licitantes en el presente requerimiento será de 100 puntos, de los cuales la propuesta técnica del licitante tendrá una ponderación máxima de 60 puntos.

La convocante realizará en primer término la evaluación de las propuestas técnicas y posteriormente la evaluación de las propuestas económicas.

La **proposición técnica deberá contar con la Firma electrónica,** de acuerdo con los medios de identificación electrónica establecidos por la Secretaría de la Función Pública

5.2 Evaluación de la propuesta económica.

Solo las propuestas técnicas que resulten solventes por haber obtenido una puntuación igual o superior a **45 puntos**, serán consideradas para realizar la evaluación de las proposiciones económicas.

La propuesta económica, deberá contener la cotización del servicio ofertado, indicando Precio Unitario de Referencia Ofertado. Para la elaboración de la propuesta económica se adjunta el **Anexo 9** el cual forma parte de la presente convocatoria.

En caso de que se detecte un error de cálculo en alguna propuesta, se podrá llevar a cabo su rectificación cuando la corrección no implique la modificación del precio unitario.

En caso de discrepancia entre las cantidades escritas con letra y número, prevalecerá la primera, asimismo, de presentarse errores en las cantidades o volúmenes solicitados, estos podrán corregirse, en apego al artículo 55 del Reglamento de la LAASSP.

El servicio objeto de este procedimiento deberá cotizarse en pesos mexicanos sin incluir el IVA a 2 (dos) decimales, sin fórmulas y truncado, es decir sin redondear.

Se establece que el puntaje máximo que podrán obtener el o los licitantes en el presente requerimiento será de 100 puntos, de los cuales la propuesta económica del licitante tendrá una ponderación máxima de **40** puntos.

Para determinar la puntuación que corresponda a la propuesta económica de cada licitante, se aplicará la siguiente formula:

PPE = MPemb x 40 / MPi.

Dónde:
PPE = Puntuación que corresponde a la Propuesta Económica;
MPemb = Monto de la Propuesta económica más baja, y
MPi = Monto de la i-ésima Propuesta económica;

La proposición económica deberá contar con la Firma Electrónica, de acuerdo con los medios de identificación electrónica establecidos por la Secretaría de la Función Pública

5.3 Adjudicación de contrato.

La proposición solvente más conveniente para el Estado, será aquélla que cumplió los requisitos legales, su propuesta técnica obtuvo igual o más puntuación a la mínima exigida y la suma de ésta con la puntuación de la propuesta económica dé como resultado la mayor puntuación de las proposiciones recibidas.

Para calcular el resultado final de la puntuación que obtuvo cada proposición, la convocante aplicará la siguiente fórmula:

PTj = TPT + PPE Para toda j = 1, 2,…..,n

Dónde:
PTj = Puntuación Total de la proposición;
TPT = Total de Puntuación asignados a la propuesta Técnica;
PPE = Puntuación asignados a la Propuesta Económica.

El subíndice **"j"** representa a las demás proposiciones determinadas como solventes como resultado de la evaluación.

En caso de existir empate en dos o más proposiciones, se dará preferencia en primer término a las micro empresas, a continuación se considerará a las pequeñas empresas y en caso de no contarse con alguna de las anteriores empresas, la adjudicación se efectuará a favor del licitante que tenga el carácter de mediana empresa.

De no actualizarse el supuesto anterior se realizará la adjudicación del contrato a favor del licitante que resulte ganador del sorteo por insaculación que realice la convocante, de ser posible en presencia del OIC, conforme al artículo 54 del RLAASSP.

En caso de que la propuesta supere el presupuesto autorizado no será adjudicada.

6. Relación de documentos que debe presentar el licitante.

En el Anexo **10** de la presente convocatoria se relacionan los documentos que debe presentar cada licitante.

7. Inconformidades.

De acuerdo con lo dispuesto en artículo 66 de la LAASSP, los licitantes podrán interponer inconformidad en las oficinas de la SFP ubicadas en Avenida de los Insurgentes Sur número 1735, Colonia Guadalupe Inn, Código Postal 01020, Demarcación Territorial Álvaro Obregón, en la Ciudad de México, México o ante el OIC en el IMSS ubicado en. Avenida Revolución número 1586, Colonia San Ángel, Demarcación Territorial Álvaro Obregón, Código Postal 01000, en la Ciudad de México, México.

Asimismo, se señala que tales inconformidades podrán presentarse mediante el sistema CompraNet en la dirección electrónica https://compranet.hacienda.gob.mx Lo anterior, contra actos del procedimiento de contratación que contravengan las disposiciones que rigen las materias objeto del mencionado ordenamiento.

7.1 Operación de CompraNet.

Para aclarar dudas en relación a la operación de CompraNet (consulta de actas y documentos publicados por la Unidad Compradora, presentación de solicitudes de aclaración, envío y firma electrónica de proposiciones, etc.), los licitantes podrán dirigirse al correo **rupc@hacienda.gob.mx** o al **Centro de Atención Telefónico (CAT): (0155) 3688 1977** de lunes a viernes de 9:00 AM a 6:00 PM (Ciudad de México).

También puede consultar la Guía “Envío de proposiciones electrónicas en CompraNet” en la liga siguiente:

https://compranetinfo.hacienda.gob.mx/descargas/Gu%C3%ADa_Env%C3%ADo_de_proposiciones_en_CompraNet.pdf

AVISO DE COMPRANET: Se comunica que, si algún licitante tiene problemas para firmar electrónicamente las propuestas técnicas/legales y/o económicas, el área de operaciones de CompraNet ha generado una infografía que puede ayudarles a solventar el problema, para ello, se comparte el siguiente enlace:

https://www.gob.mx/compranet/prensa/avisos-importantes

8. Formatos que facilitarán y agilizarán la presentación y recepción de las proposiciones.

Número	Descripción
Anexo 1	Anexo Técnico
Anexo 2	Términos y Condiciones.
Anexo 3	Escrito de acreditación legal y personalidad jurídica del licitante para comprometerse y suscribir propuestas.
Anexo 4	Escrito de nacionalidad mexicana.
Anexo 5	Escrito de cumplimiento de Normas.
Anexo 6	Escrito de no encontrarse en los supuestos de los artículos 50 y 60 de la LAASSP.
Anexo 7	Declaración de integridad.
Anexo 8	Escrito de estratificación de MIPYME.
Anexo 8 Bis.	Instructivo de llenado Estratificación de micro, pequeña o mediana empresa (MIPYMES).
Anexo 9	Propuesta Económica
Anexo 10	Relación de documentos a presentar.
Anexo 11	Formato información reservada y confidencial.

8.1. Anexos adicionales.

Número	Descripción
Anexo 12	Escrito de manifestación que no desempeña empleo, cargo o comisión en el servicio público.
Anexo 13	Escrito de interés.
Anexo 13.1	Formato de solicitud de aclaraciones.
Anexo 14	Modelo de Contrato.
Anexo 15	Modelo de convenio de proposición conjunta.
Anexo 16	Glosario.

9. Información reservada y confidencial.

Se hace del conocimiento del licitante, que en términos de lo dispuesto por los artículos 97, 98, 110 fracción XIII, 111 y 113 de la Ley Federal de Transparencia y Acceso a la Información Pública, deberá indicar si en los documentos que proporcionan al IMSS se contiene información de carácter confidencial o comercial reservada, señalando los documentos o las secciones de éstos que la contengan, así como el fundamento por el cual considera que tengan ese carácter, para lo cual se anexa el formato **Anexo 11**.

Anexo 1.- "Anexo Técnico".

1. Objetivo del Documento

Elaborar el Anexo Técnico que contenga las especificaciones, requerimientos técnicos y funcionalidades de las soluciones requeridas para los **Servicios Administrados de Seguridad Integral 2021.**

2. Objetivo

El Instituto Mexicano del Seguro Social (IMSS), a través de la Dirección de Innovación y Desarrollo Tecnológico (DIDT) requiere contar con servicios que permitan robustecer y complementar la Seguridad de la Información para salvaguardar la integridad y confidencialidad de los activos que resguardan los aplicativos, sistemas de información y bases de datos sensibles propiedad de "EL INSTITUTO".

Es importante señalar que "EL INSTITUTO" necesita contar con los Servicios Administrados de Seguridad Integral que tenga la capacidad y flexibilidad de incorporar soluciones robustas de seguridad bajo un esquema por demanda conforme "EL INSTITUTO" lo vaya necesitando y requiriendo, dichos servicios deben de brindarse con los mayores estándares de calidad, de seguridad y cumpliendo con los niveles de servicio establecidos por "EL INSTITUTO" en el presente documento, de manera integrada y unificada, con los servicios administrados que garanticen la continuidad operativa, de negocios y de seguridad de la información del Instituto Mexicano del Seguro Social (Instituto) mediante: (1) la toma en operación y transición de la infraestructura y base instalada de los servicios administrados de seguridad de la información, (2) servicios de infraestructura que operen, den soporte y mantenimiento a la infraestructura existente, y que, implementen y gestionen infraestructura para los Centros de Datos institucionales, (3) servicios que brinden protección mediante una solución integral, (4) servicios de seguridad de la información, en materias específicas relacionadas con las Tecnologías de la Información, Comunicaciones y seguridad de la Información, incluyendo servicios especializados y, por último (5) servicios desagregados, cuyo objetivo es posibilitar los anteriores servicios.

3. Alcance

"EL INSTITUTO" requiere de los **Servicios Administrados de Seguridad Integral,** para robustecer y complementar la Seguridad de la Información en los Centros de Datos del Instituto (propios o contratados) así como en donde "EL INSTITUTO" lo requiera.

Un esquema de servicios de seguridad que complementen el esquema de protección, mediante servicios orientados a: seguridad para bases de datos, aplicaciones, servicios normativos, control de acceso para claves privilegiadas, administración y correlación de bitácoras, evaluación y administración de vulnerabilidades, servicios de investigación forense,

de evaluación de cumplimiento, servicios de gestión de procesos de seguridad y servicios especializados en materia de seguridad de la información, de este modo, se tiene un esquema de seguridad completo.

4. Requerimientos

Los Servicios requeridos son los siguientes:

- **Servicios de Seguridad - Continuidad Operativa**
  Son los servicios necesarios de seguridad perimetral (Firewalls, IPS, AntiDDoS, Filtrado Web, Firewall de Aplicaciones WEB, Firewall de base de datos, cifrado de información, Control de Accesos, etc.), que se requiere su implementación, puesta a punto y operación para que inmediatamente en donde lo requiera el Instituto se pueda continuar con la operación. Estos servicios serán bajo de manda conforme lo solicite el Instituto, los tiempos de entrega serán conforme al sitio y dependiendo del tipo de tecnología de acuerdo al Apéndice 1 "Tabla de Catálogo de Servicios". En donde se contemplan los tiempos de entrega y los tipos de modalidades como alta disponibilidad (HA), así como los Niveles de Servicio requeridos tanto para la implementación como la operación, incluyendo los temas de soporte y resolución de problemas e incidentes.

- **Servicios de Seguridad – Verificación / Calidad**
  Son los elementos necesarios para que los servicios de calidad de la Seguridad de la Información se implementen, las pruebas estáticas y dinámicas de seguridad (revisiones de vulnerabilidades a los aplicativos y sistemas de información), temas de cumplimientos normativo (MAAGTICSI) y elementos como la Ciberseguridad y herramientas de seguridad, así como los Niveles de Servicio requeridos tanto para la implementación como la operación, incluyendo los temas de soporte y resolución de problemas e incidentes.

- **Servicios del Centro de Operaciones de Seguridad (SOC)**
  El Instituto requiere que el proveedor del servicio cuente con un Centro de Operaciones de la Seguridad (SOC), que se encuentre físicamente en las instalaciones del proveedor. 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, que ejecute actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, análisis forense, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable. la gestión del centro de operaciones de seguridad (SOC) por sus siglas en inglés (análisis de bloqueos de seguridad, parches y actualizaciones de las firmas de las soluciones de seguridad funcionamiento 7x24x365, etc.),

5. Especificaciones técnicas

a. SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA

i. Servicios de Firewall

Descripción del servicio:
El instituto requiere de la seguridad y protección de control de acceso, bloqueo contra ataques dirigidos a las aplicaciones e inspección sobre los paquetes a nivel de aplicación para identificar patrones de tráfico anómalo. La infraestructura propuesta deberá ser nueva, de última generación y dedicada exclusivamente para las necesidades del Instituto, a través de equipos de propósito específico (appliances) con capacidades de expansión , y el Proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas:

Detalles del Servicio:

El proveedor deberá brindar el presente servicio conforme lo siguiente:

- Proporcionar activos de infraestructura nuevos, de última generación y dedicados exclusivamente para las necesidades del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades de expansión , pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice de Seguridad.
- Definir en conjunto con el Instituto la estrategia de habilitación de los activos de infraestructura en la arquitectura de seguridad y comunicaciones.
- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centros de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún

  momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.
- Integrar cada activo de infraestructura hacia su respectiva consola de administración, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Asegurar que los activos de infraestructura propuestos cuente con la última versión liberada, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente.

- Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.
- Proporcionar el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZs), realizando la gestión de acuerdo al esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicios, cumpliendo al menos:
    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
    - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.
- Integrar todo el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- 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. Dichas evaluaciones deberán ejecutarse cada 2 meses, desde el inicio de operaciones de los servicios y antes del término de los mismos.
- Realizar todas aquellas integraciones de conectividad que permitan habilitar el servicio antes descrito, incluyendo al menos los siguientes rubros: comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, 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 cuyo atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de

los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice de Seguridad.

ii. Servicios de Prevención de Intrusos (IPS)

Descripción del servicio:
El Instituto requiere del servicio de protección perimetral basado en firmas y que identifique vulnerabilidades, para contener los intentos de obtener acceso a los recursos o servicios publicados en Internet o Intranet que pudieran afectar la operación de la organización, detectar accesos no autorizados y prevenir fugas de información.

Detalles del Servicio:

- Proporcionar activos de infraestructura nuevos, de última generación y dedicados exclusivamente para las necesidades del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades de expansión , pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice de Seguridad.
- Definir en conjunto con el Instituto la estrategia de habilitación de los activos de infraestructura de prevención de intrusos (IPS por sus siglas en ingles) en la arquitectura de seguridad y comunicaciones.
- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.
- Integrar cada activo de infraestructura hacia su respectiva consola de administración, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Asegurar que los activos de infraestructura propuestos cuente con la última versión liberada, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente.

- Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicios, cumpliendo al menos:
    - **Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.**
    - **Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.**
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.
- Integrar todo el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- 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. Dichas evaluaciones deberán ejecutarse cada 2 meses, desde el inicio de operaciones de los servicios y antes del término de los mismos.
- Realizar todas aquellas integraciones de conectividad que permitan habilitar el servicio antes descrito, incluyendo al menos los siguientes rubros: comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, 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 cuyo atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice de Seguridad.

iii. Servicios de Protección contra Denegación (DDoS)

Descripción del servicio:

El Instituto requiere de un servicio de protección contra ataques de Denegación de Servicio Distribuido que se encuentren basados en firmas y volúmenes de conexión altos.

Detalles del Servicio:

- Proporcionar activos de infraestructura nuevos, de última generación y dedicados exclusivamente para las necesidades del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades de expansión , pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice de Seguridad.
- Definir en conjunto con el Instituto la estrategia de habilitación de los activos de infraestructura de Anti-denegación de Servicios (DDoS por sus siglas en ingles) en la arquitectura de seguridad y comunicaciones.
- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, cualquier otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.
- Integrar cada activo de infraestructura hacia su respectiva consola de administración, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Asegurar que los activos de infraestructura propuestos cuente con la última versión liberada, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente.
- Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicios, cumpliendo al menos:
  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.
- Integrar todo el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- 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. Dichas evaluaciones deberán ejecutarse cada 2 meses, desde el inicio de operaciones de los servicios y antes del término de los mismos.
- Realizar todas aquellas integraciones de conectividad que permitan habilitar el servicio antes descrito, incluyendo al menos los siguientes rubros: comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, 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 cuyo atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice de Seguridad.

iv. Servicios de Redes Privadas Virtuales (VPN)

Descripción del servicio:
El Instituto requiere del Servicio de interconexión a través de Internet que permitan establecer comunicación desde localidades remotas para la transferencia de información a través de un canal cifrado.

Detalles del Servicio:

- Proporcionar activos de infraestructura nuevos, de última generación y dedicados exclusivamente para las necesidades del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).

- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades de expansión, pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice de Seguridad.
- Definir en conjunto con el Instituto la estrategia de habilitación de los activos de infraestructura para Redes Privadas Virtuales (VPN por sus siglas en ingles) en la arquitectura de seguridad y comunicaciones.
- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún
  momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.
- Integrar cada activo de infraestructura hacia su respectiva consola de administración, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Asegurar que los activos de infraestructura propuestos cuente con la última versión liberada, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente.
- Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicios, cumpliendo al menos:
  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.
- Integrar todo el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- 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. Dichas evaluaciones deberán ejecutarse cada 2 meses, desde el inicio de operaciones de los servicios y antes del término de los mismos.

- Realizar todas aquellas integraciones de conectividad que permitan habilitar el servicio antes descrito, incluyendo al menos los siguientes rubros: comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, 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 cuyo atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice de Seguridad.

v. Servicios de Filtrado de Contenido Web

Descripción del servicio:

El Instituto requiere del servicio de filtrado de contenido Web mediante políticas de acceso que permita controlar y filtrar la utilización del servicios de acceso a Internet, en función de roles y perfiles.

Detalles del Servicio:

- Proporcionar activos de infraestructura nuevos, de última generación y dedicados exclusivamente para las necesidades del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades de expansión , pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice de Seguridad.
- Definir en conjunto con el Instituto la estrategia de habilitación de los activos de infraestructura para Filtrado de Contenido Web en la arquitectura de seguridad y comunicaciones.
- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y

en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.

- Integrar cada activo de infraestructura hacia su respectiva consola de administración, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Asegurar que los activos de infraestructura propuestos cuente con la última versión liberada, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente.
- Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.
- Integrar todo el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- 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. Dichas evaluaciones deberán ejecutarse cada 2 meses, desde el inicio de operaciones de los servicios y antes del término de los mismos.
- Realizar todas aquellas integraciones de conectividad que permitan habilitar el servicio antes descrito, incluyendo al menos los siguientes rubros: comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, 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 cuyo atributos de consulta se definirán en las mesas que para este propósito se integren.

- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre

  los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice de Seguridad.

vi. Servicios de Filtrado de Contenido de Correo (Antispam)

Descripción del servicio:

El Instituto requiere de un servicio para analizar correos electrónicos de entrada y salida con el objetivo de bloquear aquellos que sean clasificados como spam, malware, phishing, entre otros.

Detalles del Servicio:

- Proporcionar activos de infraestructura nuevos, de última generación y dedicados exclusivamente para las necesidades del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades de expansión , pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice de Seguridad.
- Definir en conjunto con el Instituto la estrategia de habilitación de los activos de infraestructura para Filtrado de Contenido de Correo Electrónico (Antispam) en la arquitectura de seguridad y comunicaciones.
- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.
- Integrar cada activo de infraestructura hacia su respectiva consola de administración, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Asegurar que los activos de infraestructura propuestos cuente con la última versión liberada, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente.

- Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.

- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
  - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
  - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.
- Integrar todo el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- 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. Dichas evaluaciones deberán ejecutarse cada 2 meses, desde el inicio de operaciones de los servicios y antes del término de los mismos.
- Realizar todas aquellas integraciones de conectividad que permitan habilitar el servicio antes descrito, incluyendo al menos los siguientes rubros: comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, 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 que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice de Seguridad.

vii. Servicios de Firewall Especializado en Servicios Web (WAF)

Descripción del servicio:

El Instituto requiere del servicio de protección, prevención y control de ataques para aplicativos web expuestos en Internet/Intranet.

Detalles del Servicio:

- Proporcionar activos de infraestructura nuevos, de última generación y dedicados exclusivamente para las necesidades del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).

- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades de expansión , pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice de Seguridad.
- Definir en conjunto con el Instituto la estrategia de habilitación de los activos de infraestructura para Firewall Especializado en Servicios Web (WAF por sus siglas en ingles) en la arquitectura de seguridad y comunicaciones.
- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.
- Integrar cada activo de infraestructura hacia su respectiva consola de administración, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Asegurar que los activos de infraestructura propuestos cuente con la última versión liberada, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente.
- Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
    - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.
- Integrar todo el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- 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. Dichas evaluaciones deberán ejecutarse cada 2 meses, desde el inicio de operaciones de los servicios y antes del término de los mismos.

- Realizar todas aquellas integraciones de conectividad que permitan habilitar el servicio antes descrito, incluyendo al menos los siguientes rubros: comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, 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 cuyo atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio. Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice de Seguridad.

viii. Servicios de Firewall de Base de Datos (DBF)

Descripción del servicio:

El Instituto requiere de un servicio de protección a las instancias de bases de datos en tiempo real, así como el monitoreo del tráfico de base de datos con la finalidad de realizar la detección de ataques avanzados.

Detalles del Servicio:

- Proporcionar activos de infraestructura nuevos, de última generación y dedicados exclusivamente para las necesidades del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades de expansión bajo demanda, pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice de Seguridad.
- Definir en conjunto con el Instituto la estrategia de habilitación de los nuevos activos de infraestructura para Firewall Especializado en Base de Datos (DBF por sus siglas en ingles) en la arquitectura de seguridad y comunicaciones.
- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otro localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.
- Integrar cada activo de infraestructura hacia su respectiva consola de administración, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Asegurar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente.
- Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
- Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.

- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.
- Integrar todo el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- 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. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.

- Realizar todas aquellas integraciones de conectividad que permitan habilitar el servicio antes descrito, incluyendo al menos los siguientes rubros: comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, 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 que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice de Seguridad.

ix. Servicios de Gestión Unificada de Amenazas (UTM)

Descripción del servicio:

El Instituto requiere de un servicio de protección perimetral especializada en control de acceso, prevención de intrusos, filtrado de contenido Web y VPN, para control de tráfico y detección de actividad anómala.

Detalles del Servicio:

- Proporcionar activos de infraestructura nuevos, de última generación y dedicados exclusivamente para las necesidades del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en ingles).
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidades de expansión , pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice de Seguridad.
- Definir en conjunto con el Instituto la estrategia de habilitación de los activos de infraestructura para Gestión Unificada de Amenazas (UTM por sus siglas en ingles) en la arquitectura de seguridad y comunicaciones.

- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.
- Integrar cada activo de infraestructura hacia su respectiva consola de administración, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Asegurar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente.
- Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

    - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
    - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.
- Integrar todo el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- 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. Dichas evaluaciones deberán ejecutarse cada 2 meses, desde el inicio de operaciones de los servicios y antes del término de los mismos.
- Realizar todas aquellas integraciones de conectividad que permitan habilitar el servicio antes descrito, incluyendo al menos los siguientes rubros: comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, 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 cuyo atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes,

licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice de Seguridad.

b. SERVICIOS DE SEGURIDAD – VERIFICACIÓN/CALIDAD

El Instituto requiere integrar servicios que permitan robustecer las confidencialidad, integridad y disponibilidad de la información, atendiendo a las necesidades operativas del Instituto.

i. Servicios de Análisis de Vulnerabilidades

Descripción del servicio:
El Instituto requiere de un servicio que permita ejecutar análisis técnicos especializados sobre los activos de infraestructura de procesamiento y redes que permitan identificar vulnerabilidades nuevas o conocidas.

Detalles del Servicio:

- Integrar todas las tareas necesarias para la ejecución de los Análisis de Vulnerabilidades en los Centro de Datos correspondiente, o en su caso, en aquellas otras localidades donde le sea solicitado por el Instituto.
- Integrar al menos dos herramientas que permitan complementar los análisis de vulnerabilidad ejecutados.

- Integrar todo el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- Asegurar que las herramientas de Análisis de Vulnerabilidades propuestas cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios con el que cuente el servicio correspondiente.
- Capacidad para identificar los servicios a analizar, incluyendo el número de equipos involucrados y la versión de las plataformas de los sistemas.
- Identificación de vulnerabilidades documentadas en organismos internacionales como el CVE (Common Vulnerability Exposures).
- Identificación de configuraciones por omisión.
- Capacidad para determinar el grado de vulnerabilidad ante técnicas de ataque como:
    - SQL injection
    - Cross Site Scripting
    - Cross Site Request Forgery
    - Sensitive Data Exposure
    - Security Misconfiguration
    - Broken Authentication and Session Management
- Elaborar un reporte ejecutivo y técnico, por cada requerimiento atendido, donde se describa los detalles de los riesgo asociado a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP llamada “OWASP risk rating Methodology”, detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.

- Integrar un proceso y/o procedimiento para la implementación de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.
- Integrar al personal operativo necesario para llevar a cabo el proceso de remediación conforme las vulnerabilidades reportadas, contemplando personal especializado para las plataformas operativas y herramientas en software descubiertas.

ii. Servicios de Pruebas de Penetración

Descripción del servicio:

El Instituto requiere de un servicio que permita realizar una serie de pruebas de penetración sobre la infraestructura del Instituto con el fin de buscar huecos o fallas en la seguridad establecida.

Detalles del Servicio:

- Integrar todas las tareas necesarias para la ejecución de las Pruebas de Penetración en los Centro de Datos correspondiente, o en su caso, en aquellas otras localidades donde le sea solicitado por el Instituto.
- Capacidad para integrar los servicios o activos de información que sea analizaran, incluyendo el número de equipos involucrados, y la versión de las plataformas de los sistemas analizados.
- Identificación de vulnerabilidades y malas configuraciones.

- Explotación de acceso a los sistemas mediante el aprovechamiento de los huecos de seguridad detectados y/o vulnerabilidades detectadas.
- Evaluación de vulnerabilidades de al menos los siguientes rubros:
    - Autenticación y Autorización
        - Intentos ilimitados de inicio de sesión
        - Insuficiente autenticación
        - Insuficiente autorización
    - Gestión de sesión
        - Predicción de sesión
        - Secuestro de sesión
        - Reproducir sesión
        - Expiración de sesión insuficiente
    - Inyección de código
        - Inyección comando de Sistema Operativo
        - Inyección SQL
        - Cross-site Scripting
        - Inyección LDAP
        - Inyección HTML
        - Parameters Tampering
        - Cookie Poisoning
        - Hidden Field Manipulation
    - Criptografía
        - Fortaleza del algoritmo
        - Gestión de llaves
    - Ataques Lógicos

        - Abuso de funcionalidades
        - Input Field Validation Checking
    - Protección de Datos
        - Transporte
        - Almacenamiento
    - Divulgación de Información
        - Indexado de directorio
        - Path Traversal
        - Manejo inseguro de errores
        - Comentarios HTML
- Elaborar un reporte ejecutivo y técnico, por cada requerimiento atendido, donde se describa los detalles de los riesgo asociado a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP llamada "OWASP risk rating Methodology", detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.
- Integrar un proceso y/o procedimiento para la implementación de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.
- Integrar al personal operativo necesario para llevar a cabo el proceso de remediación conforme las vulnerabilidades reportadas, contemplando personal especializado para las plataformas operativas y herramientas en software descubiertas.

iii. Servicios de Borrado Seguro de Información

Descripción del servicio:

Realizar el borrado seguro de información en activos de infraestructura, discos duros externos y otras unidades de almacenamiento, que el Instituto solicite mediante una solución de borrado seguro, a fin de que se imposibilite, ante cualquier intento o medio, la recuperación de la información borrada, que permita la generación de un certificado que respalde la ejecución de borrado y que sea totalmente automatizada y gestionada centralmente.

Detalles del Servicio:

El servicio se describe en las etapas que a continuación se indican:

- Integrar todo el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- Asegurar que las herramientas de Borrado Seguro propuestas cuente con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios con el que cuente el servicio correspondiente.
- Debe permitir realizar borrados completos en medios de almacenamiento dispuestos en activos de infraestructura como: equipos de cómputo (de escritorio y portátil), equipos de propósito específico (appliance), servidores físicos o virtuales, derivado de la sustitución, migraciones o retiro por finalización del contrato.

- Debe asegurar que los datos no puedan ser recuperados, basándose en al menos los siguientes estándares internacionales
  - HMG Infosec Standard 5 (baseline and enhanced)
  - Opnavinst 5239.1A
  - Extended NIST 800-88
  - DoD 5220.22-M
- Borrado de Discos duros IDE/ATA, SCSI, SAS, USB, SATA, Fiber Channel y FireWire de cualquier tamaño.
- Debe brindar la destrucción local y/o remota en múltiples dispositivos de almacenamiento.
- Debe posibilitar el desmontaje RAID (SCSI).
- Debe permitir el borrado y detección de zonas bloqueadas / ocultas (DCO, HPA).
- Deberá generar certificados de borrado infalsificables que ofrezcan protección ante cualquier instancia legal, en donde se incluya el resultado del proceso de borrado, fecha, hora, los datos del equipo, el detalle del dispositivos de almacenamiento borrado.
- Deberá emitir una firma electrónica para la autenticación de la integridad del reporte de Sanitización emitido por el software de borrado.
- La solución debe poder ejecutarse sin importar de que sistema operativo se trate.

- El reporte que generé la solución deberá poder ser exportado a un medio de almacenamiento como USB o disco duro.
- El servicio de Borrado Seguro será provisto mediante un proceso o flujo operativo, el cual contemplará, entre otros, los siguientes puntos:
  - Solicitud de borrado.
  - Identificación del medio de borrado.
  - Definición de fecha de borrado.
  - Flujos operativos para la autorización de borrado o destrucción.

iv. Servicios de gestión de Dominios

Descripción del servicio:

Contar con un servicio que permita al Instituto poder registrar ante las instancias certificadas por el NIC, los dominios que requiera el Instituto y su correcta gestión.

Detalles del Servicio:

- Registro – Llevar a cabo los tramite correspondientes ante las instancias certificadoras
  - Proponer el nombre de domino acordado con el personal designado por el Instituto
  - Revisar que no se encuentre duplicado o usado ningún tercero

- Alojamiento – Llevar a cabo para realizar el alojamiento de dicho dominio
  - Generación de directivas de seguridad.
  - Realizar el mantenimiento requerido

- Cambio de proveedor – Llevar a cabo los tramites necesarios para realizar el cambio de proveedor en caso de que el proveedor actual del alojamiento incumpla con lo siguiente:
    - No cumple con la/s característica/s deseadas
    - Asistencia deficiente o de mala calidad
    - Pocas garantías de seguridad
    - Lentitud del servidor
    - Fallos frecuentes en el servidor

El Instituto deberá contar con las cuentas de gestión. El proveedor deberá hacerse cargo de la gestión en cuanto a pagos de derecho y cualquier cargo derivado de las necesidades de registro, cambio de dominio o de proveedor sin que exista un costo adicional para el Instituto.

v. Servicio de certificados Digitales SSL

Descripción del Servicio

Se requiere contar con un servicio que permita al Instituto contar con certificados SSL los que requiera para la protección de las páginas web del Instituto por hasta 2 años.

Detalles del Servicio

- Validación de dominios
- Encripción SSL de hasta 256 bits
- No debe de ser auto firmado, sino emitido por instancia certificadora valida.
- El tiempo de emisión debe de ser menor a 24 Horas y hacerlo llegar al personal del Instituto.
- El proveedor deberá hacerse cargo de la gestión en cuanto a pagos de derecho y cualquier cargo derivado de contar con el certificado o wildcards necesarias.

vi. Servicios de Análisis Forense

Descripción del servicio:

El Instituto requiere de un servicio de análisis de incidentes de seguridad para determinar y documentar en que consistió a través de la integración de registros o bitácoras que permitan obtener indicios de eventos y su relación en el tiempo y que permitan identificar cuando ocurrió, que infraestructura, servicios tecnológicos o sistema de información fueron comprometidos, como fue realizado y quien estuvo relacionado con el incidente y el impacto del evento.

Detalles del Servicio:

- Integrar todas las tareas necesarias para la ejecución de los Análisis Forenses en los Centro de Datos correspondiente, o en su caso, en aquellas otras localidades donde le sea solicitado por el Instituto.
- Apoyar en la definición del objetivo parámetros y cuestionario que resulten de interés para la investigación solicitada.
- Dar continuidad y seguimiento a los casos solicitados, así como, el registro de los indicadores correspondientes.
- Preservar la integridad de la información recibida durante la ejecución del proceso de análisis forense (cadena de custodia).
- Participar en entrevistas con los principales involucrados con la finalidad de obtener el contexto necesario en las investigaciones digitales que deban realizarse.
- Obtener información de fuentes públicas en la red en caso de que estas pudieran llegar a ser relevantes para la investigación realizada.
- Realizar la evaluación de información en los equipos de cómputo, servidores físicos, servidores virtuales, dispositivos móviles, equipo de comunicaciones, entre otros, para la identificación de indicios de compromiso y su evidencia correspondiente.
- Realizar un proceso de recuperación de información que haya sido borrada previamente.
- Proporcionar una herramienta colaborativa que facilite la visualización de hallazgos a los usuarios finales, así como generar reporte de hallazgos en caso de ser requerido.
- Elaborar un dictamen técnico, por cada requerimiento atendido, con la información identificada en el o los procesos de análisis forense, considerando la generación y firma de los documentos que expresen los resultados de la investigación en forma clara y concisa, de

  manera que puedan ser comprendidos por aquellos que no conocen o dominen el lenguaje técnico.

vii. Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)

Descripción del servicio:

Apoyar al Instituto en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en el estándar ISO 27001, que permita emitir directivas en materia de seguridad de la información a las áreas de TI y a los terceros que soportan la operación de TI.

Detalles del Servicio:

El proveedor del servicio deberá cumplir con al menos las siguientes funcionalidades operativas:

Planear

- Apoyo en inducción Interna – Curso interno “Inducción a la norma 27001:2013. Curso introductorio que permite al participante:
  - Conocer la estructura de la norma ISO/IEC27001:2013
  - Interpretar los requisitos solicitados para el cumplimiento de la norma
  - Conocer las etapas para la implementación de un SGSI

- Generación de directivas de seguridad. Manual de políticas de seguridad de la información:
    - Basadas en los dominios que establece la norma ISO 27001.
    - Alineadas a los procesos de seguridad ASI y OPEC del MAAGTIC SI.
    - Enfocadas a las áreas de TI y a los terceros que proveen servicios de TI al Instituto, considerando como alcance el catálogo de infraestructuras críticas del Instituto.
- Identificación y valuación de activos (relacionado al catálogo de infraestructuras críticas) del proceso involucrado en el Sistema de Gestión de Seguridad de la Información. La metodología contempla los siguientes puntos:
    - Identificación de los activos del proceso.
    - Valoración de los activos del proceso.
    - Identificación de requerimientos de seguridad.
    - Identificación de los controles de seguridad existentes.
- Generación de la Declaración de Aplicabilidad. (SoA: Statement of Applicability). La metodología contempla los siguientes puntos:
    - Identificación y aplicabilidad de los requerimientos internos y externos:
    - Selección de los objetivos de control y controles para el tratamiento de los riesgos
    - Verificación de requerimientos contractuales y legales
    - Identificación de los requerimientos internos y externos
    - Validación de aplicabilidad de los requerimientos
    - Formato para la Autorización para implantar y operar el Sistema de Gestión de Seguridad de la Información
    - Preparación de la Declaración de Aplicabilidad
    - Documentar los objetivos de control y los controles elegidos y la justificación de su elección
    - Documentar los controles actualmente implementados
    - Documentar la exclusión de controles y la justificación de su exclusión

Implementar y Operar el Sistema de Gestión de Seguridad de la Información

- Análisis de Riesgos de Seguridad de la Información
- Realización del análisis de riesgo con base en lo definido en el servicio de gestión de riesgos de seguridad.
- Generación del plan de tratamiento de riesgos. La metodología contempla los siguientes puntos:
    - Identificación de las acciones a realizar por parte de la organización y su administración
    - Identificación de los recursos necesarios y prioridades
    - Identificación de las responsabilidades para administrar los riesgos de seguridad de la información
- Aplicación del plan de tratamiento de riesgos. La metodología contempla los siguientes puntos:
    - Asignación de los roles y responsabilidades en la implantación de los controles relativos a personas, procesos y tecnología involucrados en la mitigación de los riesgos.
    - Actualización de documentación. Alineada a los requisitos establecidos en el proceso ASI y OPEC de MAAGTICSI.

- Afinación de políticas y procedimientos de seguridad existentes
- Definición del proceso de reporte y atención de incidentes de seguridad (ERISC)
- Propuestas de implementación de los controles seleccionados: La metodología contempla los siguientes puntos:
    - Control de accesos
    - Monitoreo de cuentas
    - Definición del proceso de Continuidad del negocio
    - Implantación de los Roles y responsabilidades definidas para el Sistema de Gestión de Seguridad de la Información
    - Controles de seguridad en la infraestructura tecnológica de acuerdo a lo definido en el alcance.
- Administración del cambio cultural. La metodología contempla los siguientes puntos:
    - Desarrollo de un Programa de concientización con usuarios y operadores del Sistema de Gestión de Seguridad de la Información
    - Determinación de las necesidades de capacitación para el personal que administra el Sistema de Gestión de Seguridad de la Información
    - Apoyo en la inducción relativa a temas de seguridad de la información.
    - Manual de Gestión de Seguridad de la Información. Se documentará un manual que contiene las referencias de la documentación generada en esta fase para dar trazabilidad al de las cláusulas de la norma.

Monitorear y Revisar el Sistema de Gestión de Seguridad de la Información

- Revisiones gerenciales. La metodología contempla los siguientes puntos:
    - Los dueños del proceso deberán hacer una revisión al Sistema de Gestión de Seguridad de la Información a fin de verificar que los objetivos del Sistema de Gestión de Seguridad de la Información están alineados a los objetivos de negocio en materia de seguridad de la información y que garantizan el adecuado manejo de los riesgos existentes.
    - El proveedor generará el procedimiento de revisiones gerenciales.
    - El proveedor propondrá los formatos requeridos para llevar a cabo las revisiones
- Auditorías internas. La metodología contempla lo siguiente:
    - Apoyo en la generación del plan de auditorías internas a las áreas de TI y a los terceros que proveen servicios de TI al Instituto.
    - Definición de los formatos requeridos para llevar a cabo las auditorías
    - Aplicación de una auditoría interna al Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2013 y a los procesos de seguridad ASI y OPEC del MAAGTICSI

Mantener y Mejorar el Sistema de Gestión de Seguridad de la Información

- Implementación de mejoras. Contempla los siguientes puntos:
    - Priorización de las acciones correctivas y no conformidades identificadas en las revisiones gerenciales, revisiones independientes, auditorías internas y revisiones técnicas
    - Identificación de los responsables de llevar a cabo las mejoras por parte de la organización.

  - El Instituto definirá las fechas compromiso para la terminación de las mejoras, únicamente para seguimiento interno.
- Tomar acciones correctivas y en las no conformidades. Contempla los siguientes puntos:
  - Apoyo en la definición del procedimiento para realizar acciones correctivas y no conformidades derivadas de las auditorias.
  - Definición del formato para llenado de acciones correctivas y no conformidades.
  - Coordinación de la ejecución de las acciones correctivas ya definidas y en su caso las no conformidades que se identifiquen.

Comunicar los resultados de las acciones tomadas. Contempla el siguiente punto:

- Apoyo en la programación de reuniones de seguimiento al Sistema de Gestión de Seguridad de la Información para dar a conocer el alcance de las acciones correctivas y no conformidades realizadas y verificar su apego a los requerimientos de los dueños de la información y a los involucrados en los procesos del Instituto

c. SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

El Instituto requiere que el proveedor del servicio cuente con un Centro de Operaciones de la Seguridad (SOC), que se encuentre físicamente en las instalaciones del proveedor. 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, que ejecute actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, análisis forense, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable.

Detalles del Servicio:

- Ubicarse dentro de territorio mexicano (a fin de que se encuentre dentro de jurisdicción de las leyes mexicanas)
- Operación 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.
- Contar con personal para atención del servicio en sitio y de forma remota, el cual se encuentre calificado con base en las credenciales requeridas para la administración y monitoreo de los componentes que integran la solución.
- Operación en un centro de datos alterno ubicado dentro de territorio nacional.
- Mantenimiento de las suscripciones a sitios y listas de empresas, fabricantes y medios especializados en seguridad de la información, que permitan alertar sobre nuevas vulnerabilidades.
- Infraestructura dedicada para la administración, operación y monitoreo de los componentes hardware y software que componen los servicios de seguridad.
- 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. Dichas evaluaciones deberán ejecutarse cada 2 meses, desde el inicio de operaciones de los servicios y antes del término de los mismos.
- Realizar acciones correctivas y preventivas para asegurar la confidencialidad, integridad y disponibilidad de la información que se maneja en las diferentes soluciones se seguridad.
- Notificaciones y alertas personalizadas, en caso de desviaciones, anormalidades o brechas de seguridad, para cada una de las soluciones de seguridad.
- Revisiones continuas a la operación del SOC, que permitan establecer mejora en los procesos, procedimientos y controles de seguridad.
- Analizar los eventos de seguridad y administración de bitácoras que se integran en los servicios de correlación de información, a fin de establecer acciones preventivas a través de modificaciones a las configuraciones de las soluciones de seguridad.
- Integrar un Equipo de Atención y Respuesta a Incidentes de Seguridad.
- Cumplir con la ISO 20000:2018
- Soporte y Atención a fallas a los componentes hardware y software que integran la solución, conforme los estipulado en los acuerdos de niveles de servicio.

- Monitorear la disponibilidad de los componentes 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.
- Realizar mantenimiento preventivo y correctivo a las soluciones de seguridad habilitadas, así como a los activos de infraestructura que soportan cada servicio.
- Ejecutar procesos operativos para al menos los siguientes rubros:
    - Administración de Dispositivos.
    - Administración de Requerimientos.
    - Administración de Cambios.
    - Administración de Configuraciones.
    - Administración de Vulnerabilidades.
    - Administración de Incidentes.
    - Administración de Problemas.
    - Investigación de Incidentes.
- Integrar una Mesa de servicio apegada a ITIL v4, la cual podrá integrarse con la Mesa de Servicios Tecnológicos del Instituto, considerando todas las actividades de puesta a punto, desarrollo de piezas de software, configuraciones, entre otros, que permitan establecer la comunicación para la generación de requerimientos, cambios, incidentes, y otros procesos que determine el Instituto.
- 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 01800 sin costo.
    - Correo Electrónico
    - Portal Web
- 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:
    - Experiencia profesional: bajo este rubro, se considerarán todos los cargos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los cargos que ha ejercido y el tipo de funciones bajo su responsabilidad, y deberá contar con experiencia comprobable de cuando menos 10 años.
    - Experiencia en proyectos de su especialidad en Seguridad de la Información: bajo este rubro se citarán y describirán todos los proyectos que el integrante ha participado, y deberá contar con experiencia comprobable de cuando menos 10 años.
    - Estudios: bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo “vendor-neutral”.
    - Incluir la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias.

- 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.
- Integrar una Base de Datos de la Gestión de la Configuración (CMDB por sus siglas en ingles) 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.
- Generar los reportes de Inteligencia de Negocio y 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. Dichos reportes podrán considerar, de manera enunciativa más no limitativa, la siguiente información:
    - Estadísticas de uso de procesamiento por tecnología
    - Estadísticas de desempeño por tecnología (throughput)
    - Estadísticas de ataques informáticos bloqueados.
    - Estadísticas de comportamientos tipo esperado de uso por tecnología (líneas base)
    - Estadísticas de usuarios concurrentes por servicio.
    - Estadísticas de crecimiento diario, mensual y anual por cada servicio.
- 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 cuyo atributos de consulta se definirán en las mesas que para este propósito se integren.
- Las consolas de administración provistas para los servicios de seguridad deberán permitir visualizar al menos:
    - Políticas: Control de Acceso
    - Configuraciones: Listas de Control de Acceso (Listas Blancas, Listas negras), Líneas base de seguridad.
    - Objetos: Usuarios, Grupos, Direcciones IP
    - Bitácoras.
    - Estadísticas en tiempo real: Desempeño, procesamiento, usuarios conectados, conexiones por segundo, ancho de banda utilizado.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para cada solución o servicio, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso de los servicio de seguridad.
- Integrar un portal único de administración de los servicios de seguridad que contenga información estratégicas sobre el uso de los servicios, y que permita al Instituto tener el contexto general sobre el desempeño de las soluciones, su estado de salud, incidentes registrados, reportes de actividades sospechosas relevantes a nivel mundial, u otra información relevante que permita tomar decisiones sobre las condiciones de operación de los servicios.

- Integrar un plan de recuperación en caso de desastre (DRP por sus sigla en inglés), que integre aquellos servicios de seguridad que resulten críticos para el Instituto, mismo que se

definirán en las mesas de trabajo correspondientes, y que tenga el objetivo de trasladar la operación de los presentes servicios a otros centros de datos, pudiendo ser estos del tipo nube privada o nube pública, conforme el alcance del presenta anexo técnico.

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
Administrador del Centro de Operaciones de Seguridad	CISM (Certified Information Security Manager) o CISSP (Certified Information Systems Security Professional)	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, así como del soporte, atención a fallas e incidentes de seguridad.	Al menos 1 recurso
Administración y Operación de soluciones y herramientas tecnológicas	Consultor especializado en cada una de las soluciones de seguridad integradas. Se aceptan como documentos comprobables el certificado vigente que haya tomado directamente del fabricante.	5 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	CEH (Certified Ethical Hacker)	5 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 2

PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Líder de proyecto	PMP (Project Manager Professional) Certificado por PMI o ITIL v4 (Expert o Master)	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
Operador de la mesa de servicio SOC	ITIL v4 Foundation Certification	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.	Los necesarios para garantizar el servicio 7x24x365 durante la vigencia del contrato
Consultor de Penetración	GPEN (GIAC Certified Penetration Tester) o CEH (Certified Ethical Hacker) Examiner) o CICP (Core Impact Certified Profesional)	5 años de experiencia en participación de proyectos de seguridad de la información.	Realizar simulacros de ataque a la red de la infraestructura o las aplicaciones para determinar lo que los atacantes pueden acceder y qué problemas pueden causar. Evaluar la seguridad de la infraestructura de red y aplicaciones utilizando herramientas y técnicas que un atacante podría utilizar.	Al menos 1 recurso

PERFIL	CERTIFICACIONES A DEMOSTRAR	EXPERIENCIA A DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Consultor Forense de Cómputo	EnCE (EnCase Certified Examiner) o CHFI (Certified Hacker Forensics Investigator)	5 años de experiencia en participación de proyectos de seguridad de la información.	Analizar, en el supuesto de un ataque y penetración exitoso a la infraestructura, la metodología de ataque para determinar cómo se logró, cuál fue el alcance del daño, logrando así determinar las medidas preventivas a implementar. Debe tener la capacidad de ejecutar investigaciones forenses en caso de ser necesario.	Al menos 1 recurso
Arquitecto Especializado en Redes y Seguridad	CCNP (Cisco Certified Network Professional) o CCSP (Cisco Certified Security Professional)	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 1 recurso

6. ENTREGABLES

Durante la habilitación, transición y operación de los servicios de seguridad, el Instituto requiere recibir distintos tipos de documentos, reportes, artefactos, dictámenes o esquemas que favorezcan el desempeño y la continuidad del servicio, y que den certidumbre a las actividades diarias que el proveedor efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

a. Entregables Generales

Durante la habilitación, transición y operación de los servicios de seguridad, el Instituto requiere recibir distintos tipos de documentos, reportes, artefactos, dictámenes o esquemas

que favorezcan el desempeño y la continuidad del servicio, y que den certidumbre a las actividades diarias que el proveedor efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posterior a la emisión del fallo
	Documento Compromiso de suscripción de OLAs	Única Vez	15 días naturales posterior a la emisión del fallo
	Matriz de Escalación	Única Vez	15 días naturales posterior a la emisión del fallo
	Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	Única Vez	15 días naturales posterior a la emisión del fallo
Servicios de Seguridad – Continuidad Operativa	Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Memorias Técnicas Iniciales de las Soluciones de	Única Vez	10 días hábiles posteriores al término de la

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Seguridad Implementadas		habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad	Única Vez	20 días hábiles previo al termino del contrato para aquellos servicios que se encuentren habilitados
Servicios de Seguridad – Verificación/Calidad	Documento con el diseño de Alto Nivel de los servicios de Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integran activos de infraestructura para su habilitación	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integran activos de infraestructura para su habilitación	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
			y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integran activos de infraestructura para su habilitación	Única Vez	20 días hábiles previo al termino del contrato para aquellos servicios que se encuentren habilitados
Servicios de Análisis de Vulnerabilidades	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Pruebas de Penetración	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Análisis Forense	Procedimientos de Operación del servicios	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Borrado Seguro de Información	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)	Metodología de implementación de los servicios	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios del Centro de Operaciones de Seguridad (SOC)	Procesos de operación implementados: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posterior a la emisión del fallo
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posterior a la emisión del fallo
	Procedimiento de operación de la Mesa de Servicios: • Requerimientos • Cambios	Única Vez	15 días naturales posterior a la emisión del fallo

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	• Configuraciones • Incidentes • Problemas • Monitoreo		
	Plan de Recuperación en caso de desastre (DRP)	Única Vez	60 días naturales posterior a la integración de las mesas de trabajo
	Expedientes Curriculares del personal del SOC	Única Vez	15 días naturales posterior a la emisión del fallo

b. Entregables Verificación/Calidad

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis	Evento	7 días hábiles posterior a la solicitud generada por parte del Instituto
Servicios de Prueba de Penetración	Reporte Técnico y Ejecutivo en formato electrónico (MS Word,	Evento	10 días hábiles posterior a la solicitud generada

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis		por parte del Instituto
Servicios de Borrado Seguro de Información	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
Servicios de Análisis	Reporte Técnico y	Evento	15 días hábiles

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Forense	Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados		posterior a la solicitud generada por parte del Instituto
Servicios de Sistema de Gestión de Seguridad de la Información	Plan de Trabajo de implementación y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posterior a la solicitud generada por parte del Instituto
Servicios del Centro de Operaciones de Seguridad (SOC)	Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad	Evento	5 días hábiles posterior al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto
	Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad	Evento	5 días hábiles posterior al término de la implementación de cualquier solución de seguridad o conforme cada solicitud generada por el Instituto
	Actualización de la matriz de escalación	Evento	5 días hábiles posterior a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad	Evento	5 días hábiles posterior a la ejecución de la ventana mantenimiento
	Reporte con Estadísticas de uso y	Evento	5 días hábiles posterior a la

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	desempeño (información analítica) de la soluciones de seguridad		solicitud generada por parte del Instituto
	Reporte Técnico de las configuraciones de las soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de los incidentes presentados en las soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de los requerimientos registrados en la mesa de servicios	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y su diagrama de interrelación conforme fueron registrados en la CMDB	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Diagramas de Arquitectura de las soluciones de seguridad	Evento	2 días hábiles posterior a la solicitud generada por parte del Instituto

c. Entregables Periódicos

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de los activos de infraestructura que contemplen: • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
Servicios de Seguridad – Verificación/Calidad	Reportes Técnicos de los activos de infraestructura que contemplen: • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
Servicios del Centro de Operaciones de Seguridad (SOC)	Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de	Mensual	5 días hábiles

	los incidentes presentados en los servicios de seguridad implementados		posterior al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posterior al cumplimiento de cada trimestre calendario
	Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados	Trimestral	5 días hábiles posterior al cumplimiento de cada trimestre calendario

Los entregables proporcionados durante las etapas de implementación, transición y operación de los servicios de seguridad, deberán ser entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados por el Instituto.

De igual manera, el proveedor deberá establecer un repositorio digital, que de manera alterna, servirá para depositar los entregables antes señalados, mismo que estarán disponibles para su consulta durante la vigencia del contrato, teniendo en cuenta que el Instituto definirá en las mesas de trabajo los permisos de acceso correspondientes para el administrador del contrato, cuerpo de gobierno que se conforme para este propósito u otros funcionaros que sean designados por el primero mencionado.

7. NIVELES DE SERVICIOS

Los Niveles de Servicio, así como las deductivas y penas convencionales, se aplicaran conforme a lo estipulado en el documento de “Términos y Condiciones”.

8. CONVENIO DE CONFIDENCIALIDAD Y RESGUARDO DE LA INFORMACIÓN

El Proveedor de los servicios de seguridad deberá suscribir el Convenio de Confidencialidad y Resguardo de Información correspondiente. Así mismo, deberá considerar al menos los siguientes mecanismos de control de acceso a la información del Instituto:

- Se deberán establecer controles de acceso y privilegios restringidos al personal del Proveedor del SASI, a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del Instituto.
- Se deberá implantar y aceptar en todo momento el uso de controles que permitan registrar “Pistas de Auditoria” para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.
- La seguridad lógica deberá estar protegida mediante el uso de dispositivos de control de acceso (Firewalls), mecanismos de encriptación y seguridad física entre las redes del Proveedor del SASI y las del Instituto.
- Los empleados del Proveedor de SASI y sus sub-contratados, con acceso a la información sensible del Instituto, deberán firmar acuerdos de confidencialidad con este último.
- El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por el proveedor de los servicios SASI, observando los requisitos de seguridad y resguardo de la información.
- El Proveedor del SASI deberá permitir el acceso a información relacionada con el servicio prestado al Instituto para la realización de auditorías.
- El Proveedor SASI no deberá hacer uso indebido de la documentación, información, ni activos de TIC a los que tengan acceso o que se generen con motivo de la prestación del servicio.

9. NORMATIVIDAD APLICABLE

El Proveedor del SASI deberá sujetarse a las políticas internas vigentes del Instituto y a cualquier modificación o inclusión de nuevas políticas que se realice durante la vigencia del contrato. Las políticas aplicables se le darán a conocer durante las mesas de trabajo, sin embargo, se deberán considerar las que se enlistan a continuación, de manera enunciativa más no limitativa:

- MAAGTICSI, como un marco normativo de aplicación general y obligatoria en la administración pública federal, así como en el alcance de algunos de los Servicios de Gestión de Procesos de Seguridad.
- NOM-002-STPS-2010

- NOM-024-SSA3-2012
- ISO 270001:2013
- Lineamientos, manuales, guías técnicas, procedimientos, del Instituto.
- Políticas de seguridad con base en el Sistema de Gestión de Seguridad de la Información (SGSI) del Instituto.
- Procedimientos para terceros.
- Reglas y políticas de administración y operación en los inmuebles.
- Reglamentos internos de conducta

a. Cumplimiento de Políticas

El Proveedor del SASI deberá respetar todas las políticas de seguridad vigentes en el Instituto y bajo ninguna circunstancia deberá permitir que se viole ninguno de los lineamientos vigentes. Si alguno de los lineamientos de Seguridad implantados en el Instituto llegase a cambiar en el transcurso del contrato establecido con el Proveedor, éste deberá asegurarse de modificar su infraestructura y procesos de tal forma que cumpla con los nuevos requerimientos.

Todos los equipos de cómputo personal propiedad del Proveedor de SASI que estén involucrados en la prestación de los servicios, deberán estar protegidos con sistemas de detección de intrusos, control de infecciones virales, detección y eliminación de programas tipo “back door” o “Troyanos”. Esta regla aplica tanto para los equipos de cómputo móviles (laptops, handheld, smartphones, tablet PC, etc.) como para los equipos de escritorio (desktop, deskside, etc.) usados por los recursos designados para las diversas tareas de administración y gestión.

Si dichos equipos requirieran de la instalación de sistemas operativos, aplicaciones, sistemas antivirus, sistemas de seguridad y demás herramientas que el proveedor decida necesario para la correcta operación de su personal, así como de la adquisición, instalación, mantenimiento y licenciamiento de los mismos, el costo será absorbido por el Proveedor de SASI.

b. Consideraciones en la finalización del Contrato

En el caso de terminación anticipada o a la finalización de la vigencia del contrato, el Proveedor será responsable de iniciar el proceso de respaldo de la información, el proceso de baja, de realizar los movimientos de resguardo, traslado y empaquetado de todo el equipo ubicado en

las instalaciones del Instituto que forma parte de los servicios y que no constituya parte de las modificaciones, adecuaciones y/o activos que hayan sido realizados como permanentes.

El retiro será realizado en coordinación con la entrega del nuevo contrato o de la solución que dará continuidad a la operación del Instituto referente a los servicios de SASI, observando los acuerdos operativos de migración de un contrato a otro, que consideren aspectos como la migración de la información de usuario en la plataforma de cómputo actual hacia la nueva.

El Proveedor deberá entregar al Instituto, a más tardar 1 mes antes de la finalización del Contrato, un plan de trabajo detallado para lograr una transición efectiva, en el que se incluyan todos los hitos y plazos necesarios para efectuarlo. Dicho plan deberá permitir una completa y correcta transición de los servicios, incluyendo la conformación y actualización de la documentación necesaria del proyecto.

La documentación deberá incluir información que se generó durante la vigencia del contrato, documentación de los procesos internos de aprovisionamiento, configuración y tareas de operación, soporte y mantenimiento debidamente actualizadas, tomando en consideración los eventos de administración de cambios y configuración, incidentes y problemas, además de un inventario actualizado a la fecha de entrega de todos los componentes habilitadores e infraestructura auxiliar que el Instituto solicite se mantengan para la transición de un nuevo contrato de servicios, procurando afectar de forma mínima la operación.

El Proveedor deberá garantizar los Niveles de Servicio durante la Licitación de un “nuevo proyecto”. Asimismo, al término del contrato, garantizará los Niveles de Servicio durante el período de transferencia de servicios al nuevo proveedor.

Dicho período de transición estará sujeto al Plan de Trabajo que el Proveedor haya presentado previamente, y que el Instituto hubiera aprobado. No obstante, durante dicho periodo, el Proveedor deberá proporcionar la orientación tecnológica adecuada al personal del Instituto para garantizar la

continuidad de los servicios requeridos, poniendo a disposición de un tercero la transferencia o quien el Instituto designe para dicho propósito.

c. Condiciones posteriores al término del Contrato

A la finalización de la vigencia del contrato, por las diferentes causas previstas, el Proveedor de SASI será el responsable de iniciar el proceso de baja, realizar los movimientos de desmontaje, empaquetado, resguardo y traslado de todo el equipo ubicado en las instalaciones del Instituto que forma parte de los servicios de seguridad, y que no constituya parte de las modificaciones, adecuaciones y/o activos considerados como permanentes como son el cableado eléctrico, el cableado de datos y cualquier otro definido en las Mesas de Trabajo.

Del mismo modo, los cambios o mejoras en la infraestructura realizados por el Proveedor del SASI serán permanentes a favor del Instituto, a la fecha de expiración de la vigencia del contrato. Lo

anterior no incluye ninguna infraestructura de hardware y/o software ubicada en las instalaciones del Proveedor.

Una vez terminado el periodo de transición de SASI hacia el nuevo servicio, el proveedor entregará a Título gratuito para el Instituto toda la Infraestructura considerada en el presente anexo, por lo que deberá realizar todas las gestiones para las sesiones correspondientes.

El Proveedor del SASI deberá considerar que si en algún momento antes de terminado el periodo del contrato, se llegará a reemplazar uno o varios equipos o componentes, todos los equipos o componentes con los que prestó los servicios y que serán retirados de las instalaciones del Instituto, deberán de someterse a un borrado seguro de información y configuración, el cual será responsabilidad de este último, con la supervisión del Instituto, y deberá de considerar las herramientas necesarias y todo lo que se requiera para garantizar la sanitización de los dispositivos a retirar, certificando el borrado seguro de la información y configuración. Esta tarea deberá de realizarse en las instalaciones del Instituto previo a su retiro y no deberá representar costo alguno.

10. PERFIL DEL PROVEEDOR

El proveedor deberá contar con la capacidad, flexibilidad, solvencia económica y competencia técnica certificada que permita implementar y operar las soluciones de seguridad y sus mecanismos con todo lo necesario para su correcto funcionamiento, en los sitios en donde “EL INSTITUTO” lo requiera conforme a las características y especificaciones mencionadas en el presente Anexo Técnico.

11. CLAVE CUCoP

31900004

12. REQUERIMIENTOS DE ARQUITECTURA TECNOLÓGICA

No Aplica

13. RESTRICCIONES E INTERFACES CON OTROS ELEMENTOS

No Aplica

APÉNDICE DEL ANEXO TÉCNICO
"Servicios Administrados de Seguridad Integral"

.1. Servicio de Firewall

Especificaciones Técnicas:

- Cumplir con el desempeño y capacidades considerando al menos las siguientes especificaciones:

	Tipo 1	Tipo 2	Tipo 3	Tipo 4
Desempeño	5 Gbps	10 Gbps	20 Gbps	240 Gbps
Conexiones simultaneas por seg.	1,000,000	2,000,000	4,000,000	32,000,000
Conexiones nuevas por seg.	50,000	125,000	200,000	1,000,000
Paquetes por seg.	1,000,000	3,000,000	5,000,000	30,000,000
Interfaces 10GbE	8	8	12	12

Se requiere 2 equipos tipo 4 para el Centro de Datos Principal en HA
Se requiere 2 Equipos tipo 3 para el filtrado web en HA
Se requiere 2 equipos tipo 2 para los Cenati México y Monterrey
Se requiere 1 equipo Tipo 1 para el ambiente de Pruebas

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
- Certificado por organismos de la industria como Common Criteria o ICSA Labs.
- Incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Integrar listas de control de acceso basadas en dirección origen, dirección destino, protocolos, interfaces de red, puertos, URL destino, identidad, rangos de tiempo o periodo.
- Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
- Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
- Capacidad de implementar mecanismos de calidad de servicio tales como la asignación de ancho de banda a cada tipo de flujo, encolamiento prioritario y moldeado de tráfico (traffic shaping).
- Capacidad de inspeccionar tráfico FTP, HTTP, HTTPS, DNS, ICMP, RADIUS, SMTP y SNMP, H.323, SIP, RSTP, SNMP, entre otros.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.

- Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (firewalls virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
- Capacidad de crear hasta 100 instancias de dispositivos virtuales (firewalls virtuales).
- Debe soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Soportar y operar bajo protocolos de ruteo BGP y OSPF.
- Soportar y operar mediante rutas estáticas.
- Realizar inspección en capa 3 y 4.
- Soporte y operación con al menos 1,000 VLANs
- Integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Contar y operar al menos con una interface Gigabit Ethernet dedicada para administración.
- Generación de bitácoras de eventos (logs) con múltiples niveles de criticidad.
- Incluir una consola centralizada de gestión con las siguientes características:
    - Configuración, de manera centralizada, de políticas en todos los firewalls de la infraestructura.
    - Identificación de qué reglas corresponden a fuentes, destinos y tipos de tráfico.
    - Ejecución de operaciones para grupos o bloques de dispositivos de frontera de seguridad.
    - Capacidad de ofrecer diferentes vistas durante el monitoreo de dispositivos, topologías o políticas.
    - Agrupación de parámetros de configuración para su posterior implementación.
- Durante una actualización de configuración, debe ser capaz de regresar a la configuración anterior, si es necesario o requerido.
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.

2. Servicio de Prevención de Intrusos (IPS)

Especificaciones Técnicas:

- Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

	Tipo 1	Tipo 2	Tipo 3	Tipo 4
Desempeño	10 Gbps	15 Gbps	20 Gbps	24 Gbps
Conexiones simultaneas por seg.	9,000,000	15,000,000	25,000,000	30,000,000
Conexiones nuevas por seg.	70,000	120,000	160,000	200,000
Interfaces 10GbE	4	4	8	8

Se requiere 2 Equipos tipo 4 para el centro de datos Principal en HA
Se requiere 2 Equipos tipo 3 para el centro de datos Principal en HA
Se requiere 1 Equipo tipo 2 para Cenati Monterrey
Se requiere 1 equipo Tipo 1 para Cenati México

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Latencia máxima de 0.5 milisegundos.
- Las Interfaces de Inspección deberán operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- Capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado.
- Capacidad de detección en línea sin bloquear tráfico (Modo transparente o supervisión). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de configuración del modo transparente o supervisión para todo el tráfico o sólo para los paquetes especificados por dirección IP, protocolo, VLAN ID, entre otros.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
- La solución de IPS deberá contemplar que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
- Soporte de funcionalidades de alta disponibilidad y configuraciones del tipo activo/activo y activo/failover. Esto debe ser soportado sin degradar el desempeño del IPS y manteniendo las tasas de transmisión requerida.
- Soporte de actualizaciones automáticas de seguridad del archivo de firmas de cuando menos una veces por mes.
- Soporte de análisis de tráfico de voz sobre IP.
- Soporte de monitoreo de VLANs, incluyendo tramas 802.1q
- Soporte de monitoreo de IPv6.

- Soporte de monitoreo con inspección profunda de paquete y monitoreo de paquete en escenarios de alta disponibilidad y con handshake TCP incompleto.
- Reconocimiento de Tuneleo de Protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de escaneo de puertos.
- Detección de re-ensamblaje de paquetes fragmentados.
- Captura de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y de manera opcional en formato .ENC (estándar para el software de análisis de protocolos), dicho archivo podrá ser usado para hacer reconstrucción o análisis forense del ataque.
- Integración de Listas Blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.
- Integración de firmas definidas por el Instituto mediante el uso de expresiones regulares.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos host de la red y crear una alarma cuando cierto umbral sea rebasado.
- Capacidad de integración con el directorio de usuarios (Active Directory y/o LDAP).
- Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Administración de seguridad centralizada que incluya las políticas, actualización, respuestas (bloquear, notificar, ignorar, etc.) y opciones de auditoria.
- Consola centralizada que administre los IPS y la integración de usuarios que realice las configuraciones necesarias para remediación de incidentes de seguridad.
- Consola remota con interfaz gráfica o Web cifrada (HTTPS) para el uso en modo de consulta, con diferente perfiles de usuarios.
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
- Debe soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (IPS virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
- Capacidad de crear hasta 100 instancias de dispositivos virtuales (IPS virtuales).
- Para los equipos en el centro de datos principal se requiere una consola de Administración.

3. Servicios de Protección contra Denegación (DDoS)

	Tipo 1	Tipo 2
Desempeño	20 Gbps	120 Gbps
Conexiones simultaneas por seg.	25,000,000	120,000,000
Conexiones nuevas por seg.	160,000	600,000
Interfaces 10GbE	8	8

Se requiere 2 equipos tipo 2 para el Centro de Datos Principal en HA
Se requiere 2 Equipos tipo 1 para el centro de Datos Alterno en HA
Para esta solución también se podrá proponer un servicio de Nube o una combinación.

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Deberá garantizar el paso transaccional de datos legítimos, privilegiando la eliminación de trafico anómalo dentro de los canales de comunicación del Instituto (Clean Pipes).
- Detección del tráfico basado en el lenguaje TCPDUMP (con información definida en las capas 3 y 4)
- Deberá tener la capacidad de advertir anticipadamente algún posible ataque, analizando tendencias de tráfico malicioso en tiempo real.
- Deberá de tener capacidad de monitoreo en tiempo real de los circuitos dedicados que entregan la conectividad a Internet/Intranet para detectar el comportamiento anormal del tráfico que pueda estar dirigido a atacar las interfaces de los enrutadores implicados en los enlaces.
- Deberá de tener la capacidad de monitoreo en tiempo real las subredes pública que conectan los enlaces, para que permita la detección de tráfico anormal que pueda significar un ataque dirigida a ella.
- Detección de ataques basado en la línea de base contra los recursos definidos, con opciones configurables por recursos que permitan filtrar la sensibilidad de la anomalía y disparar un evento de tipo alerta, en paquetes por segundo y bytes por segundo.
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
- Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
- Deberá monitorear, de manera enunciativa más no limitativa, las siguientes variables en tiempo real:
    - Para el protocolo IP:
        - ICMP
        - Paquetes IP fragmentados
        - Paquetes IP NULL
        - Paquetes IP con direcciones privadas
    - Para el protocolo TCP:
        - Segmentos TCP NULL

  - Segmentos TCP RST
  - Segmentos SYN
  - Tráfico total
- Deberá como mínimo detectar los siguientes tipos de ataques DoS/DDoS sobre las interfaces, subredes y activos de infraestructura:
  - ACK Flood
  - SYN Flood
  - Hogging CPU
  - Chargen (Character generator)
  - FIN Flood
  - ToS Flood
  - DNS Malformed
  - HTTP Flood
  - ICMP Flood
  - UDP Flood
  - Non- UDP/TCP/ICMP Protocol Flood
  - PPS Flood Attack
  - Zombie attack
  - Land Attack
- Deberá de permitir la personalización de los niveles de alarma o umbrales que sirvan para la detección de ataques, a una granularidad por objeto monitoreado.
- Deberá monitorear actividad sospechosa que pueda significar algún ataque de gusanos, virus, entre otros.
- Deberá monitorear actividad “Dark IP”.
- Detección de anomalías DDoS y amenazas de día cero antes de que impacten en los servicios.
- Detección de zombis (con selecciones de umbrales en bytes por segundos y paquetes por segundos) para clasificar una IP como zombis y con la opción de conocer una lista de zombis activos detectados.
- Protección contra amenazas conocidas
  - Ping de la muerte
  - Ataque por inundación SYN
  - Fragmentacion de paquetes y reensamblaje
  - Broadcast de correo electrónico
  - Saturadores de CPU
  - Scripts generadores de trafico
  - Generadores de caracteres
  - Ataques fuera de banda (WinNuke)
  - Ataque Smurf (generador de gran cantidad de paquetes ICMP)
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

4. Redes Privadas Virtuales – VPN (C2S – S2S)

Se requiere un equipo para el Centro de Datos principal.

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Deberá incluir al menos 4 interfaces 10/100/1000 Gb, expandibles a interfaces 10Gb de ser necesario.
- Deberá tener un desempeño de al menos 2Gbps y 1,000,000 conexiones concurrentes
- Capacidad de permitir 50,000 nuevas conexiones por segundo.
- Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Deberá permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Deberá soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Deberá integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Deberá permitir la creación de grupos de usuarios.
- Deberá permitir delimitar la cantidad de conexiones por usuarios.
- Deberá permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un servicio de autenticación externo.
- Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Deberá soportar DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKEv2.
- Deberá soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Deberá soportar integridad de datos con md5, sha1 y sha2.
- Deberá soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Deberá establecer VPNs con gateways con direcciones IP dinámicas públicas.
- Deberá crear una única asociación de seguridad (SA) por par de redes o subredes.
- Deberá realizar VPNs SSL.
- Deberá soportar la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto. Dicho cliente debe soportar al menos las siguientes plataformas operativas: MAC OS X desde v10.4.10, iOS desde v4, Android desde v4.2, Windows desde v7.

5. Filtrado de Contenido Web

Se requiere una solución en HA para el Centro de Datos Principal

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Soportar de forma mínima 120,000 usuarios de forma simultánea.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Permitir operar en modo de proxy explicito y/o proxy transparente.
- Mecanismos de autenticación tales como: archivos locales de contraseña NTLM, LDAP, RADIUS, Active Directory y certificados.
- Control de autenticaciones simultáneas con una misma cuenta de usuario.
- Cifrado de datos (usuario/contraseña) en el proceso de autenticación.
- Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL), FTP, CIFS, MAPI, DNS, P2P, SOCKS (v4/v5), IM (AOL, MSN, Yahoo Messengers), TCP-Tunnel, MMS, RTSP.
- Catalogar las páginas por Dominio (o subdominio), URL o IP.
- Bloqueo de las amenazas emergentes más comunes como: pop-ups, banners, spyware, adware, compartición de archivos punto a punto (P2P file sharing).
- Clasificación en tiempo real de sitios en internet (on-the-fly) que aún no han sido asignados a alguna categoría (servicio automático de validación en línea del sitio para determinar si es malicioso en caso de no tenerlo asignado en alguna categoría).
- Monitoreo y bloqueo de aplicaciones P2P tales como: BitTorrent, eDonkey, Gnutella, Fasttrack.
- Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
- Permitir la clasificación de URL (dominio o subdominio) o IP en una sola categoría.
- Permitir el uso de expresiones regulares.
- Permitir la creación de categorías de filtrado personalizadas así como la creación de listas blancas y negras de filtrado URL.
- Capacidad de evitar la ejecución de códigos maliciosos.
- Bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
- Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).
- Permitir la recopilación (caching) de páginas web en disco duro y memoria RAM, con el fin de hacer más eficiente el uso de los recursos del equipo.
- Proporcionar capacidades de administración y reporteo centralizado incluyendo control de acceso discrecional, control de versiones, auditoria de usuario, sistema y utilerías de restauración de configuración.
- Deberá proporcionar soporte de administración multisesión (múltiples administradores utilizando el servicio de administración centralizado), a través de una interfaz gráfica vía Web cifrada (HTTPS).
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas,

configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.

6. Servicios de Filtrado de Contenido de Correo (Antispam)

Se requiere una solución en HA para el Centro de Datos Principal

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Capacidad de hasta 1.5M de correos por hora
- Con una capacidad de por lo menos 120,000 usuarios
- 12 TB por equipo, en HA por lo menos 24 TB.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Capacidad de revisar tanto el correo entrante como el saliente.
- Deberá escanear y analizar el asunto, encabezados y el cuerpo de los correos recibidos y enviados.
- Contar con un filtro de contenido para buscar palabras clave en el cuerpo del mensaje, en los encabezados From, To, CC, Subject y en X-Headers. Así mismo, deberá poder detectar estas palabras en archivos adjuntos.
- Capacidad para poder configurar el tamaño máximo del mensaje y el número de destinatarios del correo tanto a nivel de conexión SMTP, como en políticas cuando el correo ya ha sido recibido.
- Contar con mecanismos para clasificar los remitentes por su origen y tomar decisiones de flujo y volumen en consecuencia. Además se debe contar con la facilidad de designar ciertas fuentes de correo en grupos como listas negras, listas blancas o cualquier otro grupo al que deba aplicársele una política específica.
- Capacidad para ofrecer el análisis de archivos comprimidos en los formatos más populares, incluyendo aquellos con 7 capas de compresión.
- Capacidad de detectar el verdadero formato de un archivo y permitir aplicar políticas basadas en este rubro.
- Capacidad para detectar enlaces maliciosos dentro de los correos recibidos en base a la reputación de la URL, utilizando la tecnología de reputación del fabricante, permitiendo la configuración de umbrales para esta detección.
- Contar con un módulo de bloqueo de correo electrónico no deseado con base en la reputación de cuentas de correo, dominios y direcciones IP.
- Capacidad para soportar la revisión de firmas DKIM en los encabezados de correos entrantes.
- Contar con actualizaciones para sus patrones y motores de detección de spam (heurística), phising y código malicioso.
- Capacidades de colaboración con los centros de investigación de amenazas del fabricante, con la finalidad de reportar de manera automática cualquier comportamiento sospechoso relacionado con el tráfico de correo electrónico.
- Capaz de recibir tráfico con conexiones seguras (TLS) y poder hacer conexiones con otros servidores bajo el mismo protocolo.
- Contar con mecanismos que permitan evitar la recepción de correos de notificaciones dirigidas a cuentas de usuarios no válidos o que no existen en el dominio destino (correos de rebote o Bounced Mails).

- Bloqueo automático de IP debido a alta cantidad de envío de spam, ataque tipo DHA (Directory Harvest Attack), Bounced Mails o código malicioso, totalmente parametrizable al número de mensajes recibidos en un intervalo de tiempo determinado a discreción.
- Capacidad para Integrar excepciones, tanto en hosts remitentes como en destinatarios, así como para cuentas de usuarios o dominios específicos.
- Permitir la creación de cuarentenas o carpetas de auditoría de correo, la cuarentena debe poder ser almacenada por la solución como mínimo 30 días.
- Cuando se encuentre contenido malicioso en cuerpo del correo y archivos adjuntos, podrá realizar cualquiera de las siguientes acciones:
    - Reemplazar texto del mensaje afectado.
    - Poner en cuarentena el mensaje completo.
    - Eliminar el mensaje completo.
    - Hacer copia de seguridad (copia del mensaje), para reportarlo con los centros de investigación de amenazas del fabricante.
- Detectar correos masivos con virus y removerlos además de los archivos adjuntos, incluyendo la característica de archivos adjuntos Zero-byte.
- Proporcionar la facilidad de enviar notificaciones a los usuarios (cuentas de correo electrónico) cuando algún evento sospechoso sea detectado.
- Capacidad de integrar agentes que realicen la función de escaneo y detección de spam en activos de infraestructura o servicios de correo electrónico bajo plataformas operativas Linux y/o Windows.
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

7. Firewall Especializado en Servicios Web (WAF)

Se requiere 2 equipos para el Centro de Datos Principal en HA

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Inspección y análisis de perfiles de comportamiento normal de usuarios para detectar y mitigar el uso anormal de aplicativos Web.
- Soportar un throughput de 5 Gbps en capa 7.
- Soportar 100,000 Transacciones por Segundo (TPS).
- Servicio de reputación para identificar y bloquear ataques automatizados y/o usuarios maliciosos.
- Detección de ataques por clientes automatizados y robots.
- Detección de URL rewriting u ofuscación del URL.
- Manejo de errores y reescritura de errores para aplicativos Web.
- Capacidad para soportar inspección del protocolo XML.
- Certificado por organismos de la industria como ICSA Labs o PCI.
- Actualización automática de firmas de prevención contra código malicioso.
- Parcheo sobre aplicativos Web contra vulnerabilidades nuevas o conocidas (parcheo virtual).
- Protección contra ataques/vulnerabilidades conocidas (OWASP), de manera enunciativa más no limitativa:
    - SQL injection
    - Cross Site Scripting
    - Cross Site Request Forgery
    - Sensitive Data Exposure
    - Security Misconfiguration
    - Broken Authentication and Session Management
    - Otras nuevas identificadas por OWASP
- Soportar formatos de mensaje:
    - Web 2.0
    - HTML
    - XHML
    - HTML5
    - XML
    - JSON
    - AJAX
    - FLASH
    - JavaScript.
- Soportar Protocolos: TCP, HTTP, HTTPS, SSL/TLS.
- Soportar mitigación de amenazas:
    - HTML Content Aware
    - Intrusion Detection and Prevention (URI patterns)
    - URI rate-based heuristics

  - Vendor Vulnerabilities
  - URL cloaking / rewrite
  - Parameter Inspection
  - Learning mode
- Integridad de transacciones:
  - Session Tracking Cookies, Source/Destination IPs
  - HTTP RFC conformance
  - HTML Form parameter checking
  - Cross-Site Scripting
  - Cookie Signing
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Debe soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).

08. Servicios de Gestión Unificada de Amenazas (UTM)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

	Tipo 1	Tipo 2	Tipo 3	Tipo 4
Desempeño	1 Gbps	2 Gbps	5 Gbps	10 Gbps
Conexiones simultaneas por seg.	10,000	20,000	50,000	100,000
Conexiones nuevas por seg.	150,000	500,000	1,000,000	2,000,000
Interfaces 10/100/1000 Mbps.	4	4	8	8

Se requiere 1 Equipo tipo 4 para el centro de datos móvil en Jalisco
Se requiere 1 equipo tipo 3 para el centro de convenciones en Oaxtepec
Se requiere 1 equipo tipo 2 para el centro vacacional Metepec
Se requiere 1 equipo tipo 1 para el centro vacacional Atlixco

Generales

- Deberá incluir un sistema operativo endurecido propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.

Funcionalidad Firewall

- Deberá estar basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
- Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Deberá permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Deberá soportar y operar bajo protocolos de ruteo BGP y OSPF.
- Deberá soporte y operar mediante rutas estáticas.
- Deberá realizar inspección en capa 3 y 4.

Funcionalidad IPS

- Soporte de al menos: 1,000,000 conexiones simultáneas por cada Gigabit de inspección.
- Latencia máxima de 0.5 milisegundos.
- Las Interfaces de Inspección deberán operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- El equipo deberá ser capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado
- Capacidad de detección en línea sin bloquear tráfico (Modo transparente). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.

- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
- La solución de IPS deberá contemplar que el flujo de información esté asegurado ante una falla en el IPS, pudiendo conmutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
- Reconocimiento de Tuneleo de Protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de re-ensamblaje de paquetes fragmentados.
- Integración de Listas Blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.
- Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos host de la red y crear una alarma cuando cierto umbral sea rebasado.

Filtrado de Contenido Web

- Deberá permitir operar en modo de proxy explicito y/o proxy transparente.
- Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL).
- Catalogar las páginas por Dominio (o subdominio), URL o IP.
- Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
- Permitir la creación de categorías de filtrado personalizadas así como la creación de listas blancas y negras de filtrado URL.
- Capacidad de evitar la ejecución de códigos maliciosos.
- Permitir el bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
- Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).

Funcionalidad VPN

- Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Deberá permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Deberá soportar DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKE v2.
- Deberá soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Deberá soportar integridad de datos con md5, sha1 y sha2.
- Deberá soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Deberá establecer VPNs con gateways con direcciones IP dinámicas públicas.
- Deberá crear una única asociación de seguridad (SA) por par de redes o subredes.
- Deberá soportar Secure Sockets Layer (SSL) versión 3, con al menos los siguientes algoritmos de cifrado simétrico y longitud de llaves: RC4 (128 bits) y 3DES (192bits).

GENERALES PARA TODAS LAS SOLUCIONES

- Todas las soluciones deben de cumplir como mínimo con estas especificaciones y capacidades, lo cual son enunciativas más no limitativas.
- Las propuestas deberán considerar todos los componentes necesarios para su correcta operación (Equipo activo de Telecomunicaciones, cableado, módulos, etc.)
- Las propuestas Técnicas, deberán ser acompañadas de las hojas de especificaciones, trípticos y demás información que permita verificar el cumplimiento de las mismas.
- Los proveedores podrán realizar propuestas de mejora de cada una de las soluciones y/o diseño de la red con forme a sus propuestas. (Ver el diagrama 01 propuesta mínima esperada de las soluciones).
- De las propuestas de solución, podrán proponer arreglos tipo cluster.

9. Firewall Especializado en Servicios Web (WAF)

Se requiere 2 equipos para el Centro de Datos Principal en HA

Especificaciones Técnicas:

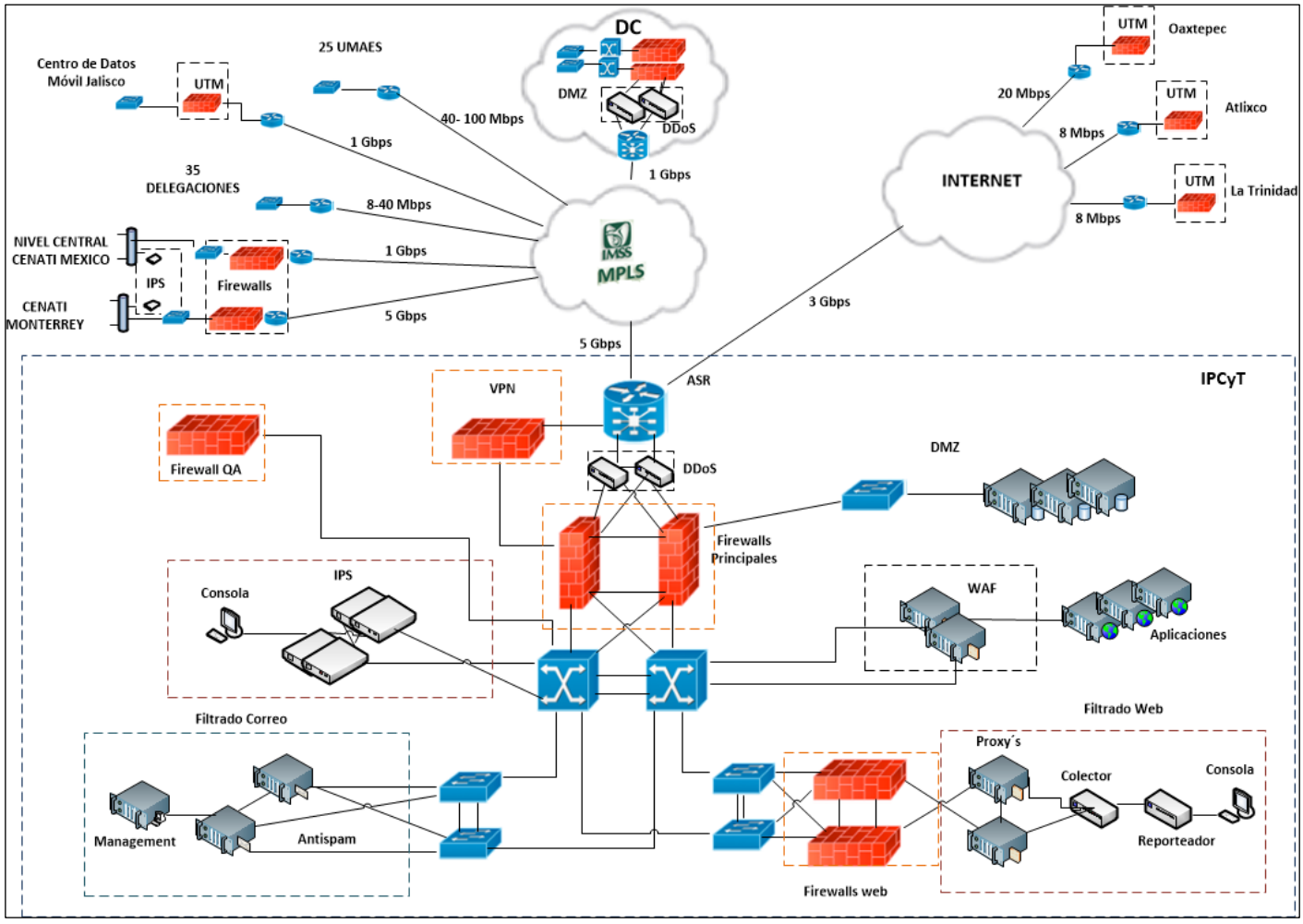
Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Inspección y análisis de perfiles de comportamiento normal de usuarios para detectar y mitigar el uso anormal de aplicativos Web.
- Soportar un throughput de 5 Gbps en capa 7.
- Soportar 100,000 Transacciones por Segundo (TPS).
- Servicio de reputación para identificar y bloquear ataques automatizados y/o usuarios maliciosos.
- Detección de ataques por clientes automatizados y robots.
- Detección de URL rewriting u ofuscación del URL.
- Manejo de errores y reescritura de errores para aplicativos Web.
- Capacidad para soportar inspección del protocolo XML.
- Certificado por organismos de la industria como ICSA Labs o PCI.
- Actualización automática de firmas de prevención contra código malicioso.
- Parcheo sobre aplicativos Web contra vulnerabilidades nuevas o conocidas (parcheo virtual).
- Protección contra ataques/vulnerabilidades conocidas (OWASP), de manera enunciativa más no limitativa:
    - SQL injection
    - Cross Site Scripting
    - Cross Site Request Forgery
    - Sensitive Data Exposure
    - Security Misconfiguration
    - Broken Authentication and Session Management
    - Otras nuevas identificadas por OWASP
- Soportar formatos de mensaje:
    - Web 2.0
    - HTML
    - XHML
    - HTML5
    - XML
    - JSON
    - AJAX
    - FLASH
    - JavaScript.
- Soportar Protocolos: TCP, HTTP, HTTPS, SSL/TLS.
- Soportar mitigación de amenazas:
    - HTML Content Aware
    - Intrusion Detection and Prevention (URI patterns)
    - URI rate-based heuristics

  - Vendor Vulnerabilities
  - URL cloaking / rewrite
  - Parameter Inspection
  - Learning mode
- Integridad de transacciones:
  - Session Tracking Cookies, Source/Destination IPs
  - HTTP RFC conformance
  - HTML Form parameter checking
  - Cross-Site Scripting
  - Cookie Signing
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).

Debe soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en ingles) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).

DIAGRAMA 01 PROPUESTA MÍNIMA ESPERADA DE LAS SOLUCIONES



Anexo 2.- "Términos y Condiciones".

1. OBJETIVO DEL DOCUMENTO

Establecer las necesidades y condiciones de entrega los Servicios Administrados de Seguridad Integral.

2. PREMISA

Las bases de datos, aplicaciones y cualquier otro tipo de información utilizadas en el suministro de los servicios o a la que se tenga acceso derivado de la naturaleza de los mismos, que sean propiedad exclusiva del Instituto Mexicano del Seguro Social ("EL INSTITUTO") continuarán siendo propiedad exclusiva del mismo. En ese sentido, el proveedor se obliga a utilizarlas exclusivamente para cubrir los servicios requeridos.

El proveedor deberá presentar como parte de su propuesta técnica escrito firmado por su representante legal respecto de las obligaciones de confidencialidad, las cuales estarán sujetas a lo dispuesto por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental o por la Ley correlativa aplicable a "EL INSTITUTO".

3. NOMBRE DEL PROYECTO

Servicios Administrados de Seguridad Integral 2021

4. OBJETIVO DEL PROYECTO

Contar con los **Servicios Administrados de Seguridad Integral** para los activos de Información donde se alojan los aplicativos, sistemas de información y bases de datos sensibles del Instituto, en las ubicaciones en donde los requiera el Instituto, así como con los niveles de servicio establecidos en el apéndice del presente documento y conforme a las características técnicas solicitadas en el Anexo Técnico.

5. SOLICITUD DE APEGO A NORMAS OFICIALES O CERTIFICACIONES

Se Indica específicamente en el punto 9 del documento del Anexo Técnico del presente proyecto.

6. VISITAS A INSTALACIONES

No se requiere.

7. TIPO DE ABASTECIMIENTO REQUERIDO

El Instituto requiere recibir los servicios objeto del Anexo Técnico con las funcionalidades descritas y en apego a los tiempos definidos.

8. GARANTÍAS

El Proveedor, se obliga a constituir en la forma y términos previstos por los artículos 48 y 49 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 103 de su Reglamento y

numeral 4.18.5 de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Prestación de Servicios de "EL INSTITUTO" y demás disposiciones legales aplicables en la materia, las garantías a que haya lugar con motivo del presente Contrato.

En cualquier momento, "EL INSTITUTO" podrá hacer válida la Póliza de Garantía del contrato en caso de que el proveedor no cumpla con los tiempos y plazos de entrega establecidos en los presentes Términos y Condiciones.

Las modificaciones a las fianzas deberán formalizarse con la participación que corresponda a la afianzadora, en términos de las disposiciones aplicables.

La garantía permanecerá vigente a partir de la fecha de adjudicación del contrato respectivo, y hasta que se cumplan plenamente todas y cada una de las obligaciones del contrato, así como durante la substanciación de todos los recursos legales o juicios que, en su caso, sean interpuestos por cualquiera de las partes y hasta que se dicte la resolución definitiva por autoridad competente.

Para garantizar el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato Adjudicado, el proveedor se compromete a entregar, dentro de los 10 (diez) días naturales a partir del día siguiente al de la notificación de la adjudicación del inicio de los servicios la garantía, de conformidad con el artículo 103 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, expedida por institución debidamente autorizada, por el 10% del monto máximo por el que se adjudica el contrato, a favor de "EL INSTITUTO", el cual será un contrato cerrado y la garantía será divisible.

a) Devolución de garantías

La liberación de garantías relativas al cumplimiento del Contrato podrán realizarse una vez que haya transcurrido el plazo de garantía indicado, a solicitud expresa por el proveedor por escrito en papel membretado de su empresa, dicha solicitud debe dirigirse a la Coordinación de Adquisición de Bienes y Contratación de Servicios, quien autorizará la devolución o cancelación de la póliza de garantía (fianza) correspondiente, dicha autorización se entregará al proveedor, siempre que demuestre haber cumplido con la totalidad de las obligaciones adquiridas por virtud del presente Contrato.

La garantía de cumplimiento a las obligaciones del contrato, únicamente podrá ser liberada mediante autorización expresa y por escrito otorgado por la División de Seguridad Informática Integral (DSII).

b) Ejecución de la garantía

- Se hará efectiva la garantía relativa al cumplimiento del contrato cuando:
- El proveedor incumpla con cualquiera de las obligaciones establecidas en el contrato que se celebre.
- Se rescinda administrativamente el contrato.
- La ejecución de la garantía será con independencia de la aplicación de las Penas Convencionales que procedan y de la rescisión administrativa del contrato.
- La ejecución de la garantía de cumplimiento del contrato, será proporcional al monto de las obligaciones incumplidas.
- Además de las sanciones anteriormente mencionadas, serán aplicables las que estipulen las disposiciones legales vigentes en la materia.

9. ACUERDOS DE NIVEL DE SERVICIO

El objetivo de los Niveles de Servicio consiste en proporcionar al Instituto un mecanismo que permita:

- Medir de forma efectiva el desempeño de los servicios proporcionados por EL Proveedor.
- Procurar que los servicios de sean proporcionados con la calidad prevista.

Con fundamento en lo dispuesto por el Artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios de la Administración Pública Federal, el Instituto aplicará penas convencionales por el atraso en la prestación del servicio basado en el importe del servicio prestado con atraso conforme al plan de trabajo y los plazos previstos, en el entendido de que esta penalización no excederá al importe de la garantía de cumplimiento de contrato.

9.1. Penas Convencionales

Se aplicarán penas convencionales por incumplimiento en el plazo de prestación de los servicios por parte del proveedor adjudicado, del 0.2% por cada día natural de atraso en el inicio en la prestación del servicio, respecto del valor máximo total del contrato.

9.2. Servicios de Habilitación, Operación y Transición

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	DEDUCTIVA MENSUAL	CÓMPUTO DE LA DEDUCTIVA
Plan de Trabajo detallado de los servicios del proyecto	15 días naturales posterior a la emisión del fallo	1% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Documento Compromiso de suscripción de OLAs	15 días naturales posterior a la emisión del fallo	1% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Matriz de	15 días naturales	1% por cada día	Valor unitario de la

Escalación	posterior a la emisión del fallo	natural de atraso	facturación mensual del servicio relacionado con el incumplimiento
Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	15 días naturales posterior a la emisión del fallo	1% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.3. Servicios de Seguridad – Continuidad Operativa

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	DEDUCTIVA MENSUAL	CÓMPUTO DE LA DEDUCTIVA
Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Memorias Técnicas Actualizadas de las Servicios de Seguridad	20 días hábiles previo al termino del contrato para aquellos servicios que se encuentren habilitados	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.4. Servicios de Seguridad – Verificación/Calidad

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	DEDUCTIVA MENSUAL	CÓMPUTO DE LA DEDUCTIVA
Documento con el diseño de Alto Nivel de los servicios de	5 días hábiles posteriores a la integración de las	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del

Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integran activos de infraestructura para su habilitación	mesas de trabajo por cada servicio que se pretenda habilitar		servicio relacionado con el incumplimiento
Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integran activos de infraestructura para su habilitación	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integran activos de infraestructura para su habilitación	20 días hábiles previo al termino del contrato para aquellos servicios que se encuentren habilitados	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Procedimientos de Operación del servicios • Servicio de Análisis de Vulnerabilidades • Servicios de Pruebas de	10 días hábiles posterior a la integración de las mesas de trabajo	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Penetración • Servicios de Análisis Forense • Servicios de Borrado Seguro de Información •			
Metodología de implementación de los servicios • Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)	10 días hábiles posterior a la integración de las mesas de trabajo	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.5. Servicios del Centro de Operaciones de Seguridad (SOC)

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	DEDUCTIVA MENSUAL	CÓMPUTO DE LA DEDUCTIVA
Procesos de operación implementados: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	15 días naturales posterior a la emisión del fallo	2% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Matriz de Escalación Técnica y Organizacional	15 días naturales posterior a la emisión del fallo	2% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Procedimiento de operación de la Mesa de Servicios: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	15 días naturales posterior a la emisión del fallo	2% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Plan de Recuperación en	60 días naturales posterior a la	2% por cada día natural de atraso	Valor unitario de la facturación

caso de desastre (DRP)	integración de las mesas de trabajo		mensual del servicio relacionado con el incumplimiento
Expedientes Curriculares del personal del SOC	15 días naturales posterior a la emisión del fallo	2% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.6. Deducciones

Durante la vida del contrato, al presentarte una falla, incidente, atención de requerimientos, ventana de mantenimiento, entre otras, cuya causa raíz haya sido derivada por un tercero, la deductiva correspondiente al servicio asociado no será aplicada al proveedor de SASI, siempre y cuando demuestre con evidencias fehacientes que el servicio correspondiente se presentó bajo las especificaciones del anexo técnico y sus apéndices.

Con base en lo anterior, y cuando las fallas, incidentes, atención de requerimientos, ventanas de mantenimiento, entre otras, sean atribuibles a la entrega de los servicios de seguridad por parte del Proveedor, se aplicarán deductivas conforme lo siguiente rubros:

9.7. Disponibilidad

La disponibilidad se define como la medida del porcentaje de tiempo, en que el sistema que brinda el servicio de seguridad de SASI (o un componente del sistema) realiza la función que le es propia. Es decir; disponibilidad es la proporción de tiempo en que el sistema cumple con la función para la cual está dispuesto, en relación con el tiempo en que debería haber estado disponible.

Las mediciones de disponibilidad deberán ser realizadas por el Proveedor de SASI usando su correspondiente herramienta de monitoreo del servicio y herramienta de gestión de incidentes, con el afán de obtener mediciones precisas con respecto a los tiempos operacionales y los no operacionales y sus atribuibles.

Deberán realizarse mediciones de disponibilidad desde el inicio del período operacional de los servicios de infraestructura SASI, para todos los módulos o posiciones de servicio contratados.

El Proveedor de SASI comprometerá la disponibilidad en base a los siguientes factores:

- Incluye todos los componentes WAN, LAN, dispositivos de seguridad, y demás dispositivos que soportan al servicio de seguridad, así como su equivalente de configuración lógica.
- El origen de medición será por una correlación de los poleos y/o muestras recolectadas cada 5 minutos por el sistema de monitoreo y los períodos de indisponibilidad extraídos de los incidentes abiertos en el sistema de administrador de incidencias del Proveedor de SASI, restándosele aquellos períodos de indisponibilidad cuya responsabilidad no sea atribuible al Proveedor de SASI. La forma de medición en específico se describirá de la siguiente manera.
    - Calculada en base a 30 días por mes
    - Calculada a partir del inicio de la falla
    - Se considera indisponible cuando el protocolo de la interfaz se encuentra caído (Down) o por caída de tráfico imputable a infraestructura del proveedor.
    - Solo es calculada en base a fallas imputables al Proveedor de SASI.
    - Disponibilidad por sitio y por Posición de Servicio

Las caídas originadas por falla de energía responsabilidad del Instituto no serán tomadas en cuenta para la disponibilidad.

$$\text{Disponibilidad\_del\_Servicio} = \left[\frac{\text{Tiempo\_Total} - (\text{Tiempo\_Indisponible} - \text{Tiempo\_Instituto})}{\text{Tiempo\_Total}} \right] X\,100$$

Dónde:

Tiempo Total: Tiempo total de disponibilidad para el mes de medición.
Tiempo Indisponible: Tiempo indisponible según plataforma de monitoreo.
Tiempo Instituto: Tiempos atribuibles al Instituto extraídos del sistema de administración de incidentes.

Objetivos por métrica:

Disponibilidad Servicio	% Disponibilidad
Servicios de Seguridad – Continuidad Operativa	99.99%
Servicios de Seguridad – Verificación/Calidad	99.97%
SOC	99.99%

Deductiva por incumplimiento:

DESCRIPCIÓN DEL NIVEL DE SERVICIO	MÉTRICA	DEDUCTIVA	CÓMPUTO DE LA DEDUCTIVA
Cuando no se cumplan con los objetivos de servicio, para los diferentes niveles de disponibilidad, conforme al esquema de medición propuesto	% Disponibilidad conforme la tabla de objetivos	0.5% por cada minuto de indisponibilidad	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.8. Tiempo de Detección y Solución de Fallas

La métrica de tiempo de solución a fallas es independiente de la métrica de disponibilidad, dado que se refiere al tiempo en el cual será devuelta a la normalidad (restitución de la operación estable) uno o varios servicios al presentarse una falla. Las mediciones de Tiempo de Solución de Fallas deberán ser realizadas por el Proveedor de SASI usando su correspondiente herramienta de gestión y monitoreo del servicio. El Proveedor deberá realizar esta medición en un periodo mensual considerando el promedio del tiempo de solución para cada tipo de severidad. La metodología que se realice, las herramientas y los responsables sobre las mediciones, quedarán definidos en las mesas de trabajo.

El Tiempo de Solución a Fallas se divide en tres casos, en función de la severidad, causa e impacto de los mismos:

Severidad Critica: Representa un incidente de alto impacto dado el riesgo que representa. Este tipo de incidente puede, potencialmente, ocasionar afectación y daño en activos y servicios del cliente. Eventos de afectación total al servicio, pérdida total del sistema de comunicaciones y/o seguridad, degradación de los recursos del Instituto o bien mediante el descubrimiento de vulnerabilidad en la infraestructura protegida. La alarma relativa en el sistema de gestión se mantiene por más de 10 minutos.

Severidad Alta: Representa un incidente serio en el que hay una degradación más no una afectación de negocio a los servicios e infraestructura que es protegida mediante los dispositivos de alta disponibilidad o de seguridad. El incidente se manifiesta mediante el bloqueo o bajo desempeño al acceder a ciertos servicios de red que requieren el uso de los dispositivos de comunicaciones y/o seguridad así como la pérdida parcial de alguna funcionalidad en el equipo de comunicaciones y/o seguridad. Eventos de afectación que ocasionan degradación en el servicio sin llegar a ocasionar caída del mismo.

Severidad Media: Representa un incidente menor que no trae consecuencias de impacto de negocio a los servicios e infraestructura protegida por los dispositivos de seguridad. El incidente se da mediante fallas en visualización de bitácoras o problemas para comunicación de servicios internos del Instituto y hacia un grupo reducido de usuarios. Eventos de afectación al servicio por períodos de tiempo menores a 10 minutos ocasionando intermitencia en la disponibilidad del servicio.

Severidad Baja: Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad. Estos casos de severidad deben ser atendidos por ingenieros del proveedor de servicios en sitio con la colaboración del fabricante vía un centro de asistencia técnica personalizada. El tiempo de resolución de este tipo de falla será definido por el Instituto y el Proveedor de SASI al momento de presentar el caso.

La severidad de un incidente es determinada por la convocante. Conforme la operación y criticidad de un servicio, se define la severidad, así como su nivel de escalación, con base en lo siguiente:
Objetivos de la métrica:

SEVERIDAD	AFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Critica	Representa una falla de alto impacto que impide la operación total de un servicio, mismo que soporta una función de negocio del Instituto a nivel nacional.	10 minutos posterior a la detección de la falla	2 horas posterior al registro y notificación de la falla
Alta	Representa una falla en la que hay una degradación que impide la operación de un servicio, mismo que soporta una función de	20 minutos posterior a la detección de la falla	4 horas posterior al registro y notificación de la falla

	negocio del Instituto pero que no tiene un impacto a nivel nacional.		
Media	Representa una falla menor que impide la operación de un servicio, mismo que afecta a un grupo de usuarios reducido del Instituto.	120 minutos posterior a la detección de la falla	48 horas posterior al registro y notificación de la falla
Baja	Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad, tienen un bajo impacto en la operación del negocio y su atención y/o solución puede ser calendarizada.	5 días hábiles posterior a la detección de la falla	Se define entre el Instituto y el Proveedor de SASI conforme las mesas de trabajo que se establezcan para este propósito.

Deductiva por incumplimiento:

DESCRIPCIÓN DEL NIVEL DE SERVICIO	MÉTRICA	DEDUCTIVA	CÓMPUTO DE LA DEDUCTIVA
Tiempo máximo de registro y notificación conforme al nivel de severidad critica	10 minutos posterior al registro y notificación de la falla	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad critica	2 horas posterior al registro y notificación de la falla	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posterior al registro y notificación de la falla	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad alta	4 horas posterior a la registro y notificación de la falla	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Tiempo máximo de registro y notificación conforme al nivel de severidad media	120 minutos posterior al registro y notificación de la falla	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad media	48 horas posterior al registro y notificación de la falla	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad baja	5 días hábiles posterior al registro y notificación de la falla	0.1% por cada día hábil de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad baja	Se define entre el Instituto y el Proveedor de SASI conforme las mesas de trabajo que se establezcan para este propósito.	0.5% por cada día de atraso en la solución de la falla conforme la fecha establecida en las mesas de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.9. Tiempo de Detección y Mitigación de Incidentes

Una actividad sospechosa son acciones que pudieran estar encaminadas a comprometer la seguridad de la red y de los activos de información, es la etapa previa a la materialización de un incidente de seguridad. Un incidente de seguridad es el registro de una violación a las políticas de seguridad informática o al uso aceptable de políticas o de prácticas de seguridad estandarizado; es la evidencia inequívoca de que la confidencialidad, integridad y disponibilidad de la información ha sido vulnerada.

Las métricas de tiempo para la actividad sospechosa se refieren al tiempo de notificación y envió de dictamen que el proveedor SASI deberá realizar ante el Instituto al momento de detectar una actividad sospechosa. Ante una actividad sospechosa, el proveedor del SASI deberá registrar y notificar al personal del Instituto en máximo 30 minutos. Posterior a su detección y registro, se deberá emitir un dictamen de actividad sospechosa con recomendaciones para erradicarla, este dictamen será enviado al personal del Instituto en máximo 90 minutos.

La métricas para el tiempo de registro y notificación se refiere al tiempo en que proveedor SASI avisa al Instituto cuando ha confirmado un incidente de seguridad, ésta métrica deberá realizarse en los tiempos definidos según la prioridad a partir de que se apertura algún registro relacionado con un incidente de seguridad. La métrica de tiempo de contención se refiere a que, tras la detección del incidente, el Proveedor de SASI deberá detener y aislar el mismo según los tiempos definidos para cada prioridad.

Las mediciones deberán ser realizadas por el proveedor de SASI usando su correspondiente herramienta de gestión y monitoreo del servicio. El proveedor deberá realizar esta medición en un periodo mensual según el nivel de servicio para cada tipo de métrica y/o prioridad.

Objetivos de la métrica:

SEVERIDAD	AFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Critica	Representa un incidente de alto impacto que impide la operación total de un servicio, mismo que soporta una función de negocio del Instituto a nivel nacional.	10 minutos posterior a la detección del incidente	1 hora posterior al registro y notificación del incidente
Alta	Representa un incidente en el que hay una degradación que impide la operación de un servicio, mismo que soporta una función de negocio del Instituto pero que no tiene un impacto a nivel nacional.	20 minutos posterior a la detección del incidente	4 horas posterior al registro y notificación del incidente
Media	Representa un incidente menor que impide la operación de un servicio, mismo que afecta a un grupo de usuarios reducido del Instituto.	30 minutos posterior a la detección del incidente	24 horas posterior al registro y notificación del incidente
Baja	Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad, tienen un	60 minutos posterior a la detección del incidente	48 horas posterior al registro y notificación del incidente

	bajo impacto en la operación del negocio y su atención y/o solución puede ser calendarizada.		

Deductiva por incumplimiento:

DESCRIPCIÓN DEL NIVEL DE SERVICIO	MÉTRICA	DEDUCTIVA	CÓMPUTO DE LA DEDUCTIVA
Registro y notificación de Actividad Sospechosa	30 minutos posterior a la detección actividad sospechosa	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Envío de Dictamen de Actividad Sospechosa	90 minutos posterior al registro y notificación de actividad sospechosa	1% por cada minuto de atraso en la elaboración del dictamen	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

DESCRIPCIÓN DEL NIVEL DE SERVICIO	MÉTRICA	DEDUCTIVA	CÓMPUTO DE LA DEDUCTIVA
Tiempo máximo de registro y notificación conforme al nivel de severidad critica	10 minutos posterior al registro y notificación del incidente	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad critica	1 hora posterior al registro y notificación del incidente	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posterior al registro y notificación del incidente	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad alta	4 horas posterior al registro y notificación del incidente	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de	30 minutos	0.5% por cada	Valor unitario de la

registro y notificación conforme al nivel de severidad media	posterior al registro y notificación del incidente	minuto de atraso en el registro y notificación	facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad media	24 horas posterior al registro y notificación del incidente	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad baja	60 minutos posterior al registro y notificación del incidente	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad baja	48 horas posterior al registro y notificación del incidente	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.10. Solicitudes de Requerimientos y Cambios

Es el tiempo que tarda el Proveedor de SASI en realizar una alta, cambio o baja sobre la infraestructura del servicio en seguridad, basada en el menú de configuraciones comunes preestablecidas durante las mesas de trabajo correspondientes. Estas configuraciones deberán ser acorde a las necesidades de conectividad y flujos de información de las aplicaciones del Instituto, entendiendo que la complicación para su atención es menor dado que se tiene la experiencia y el conocimiento de las mismas configuraciones de los módulos de los servicio de seguridad en operación.

Objetivos de la métrica:

<u>Requerimientos</u>

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
Alta	Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación emergentes.	10 minutos posterior a la solicitud formal por parte del Instituto	1 hora posterior al registro realizado por el Instituto
Media	Requerimiento generado por parte	30 minutos posterior a la	8 horas posterior al registro realizado

	del Instituto a fin de atender a necesidades de operación comunes.	solicitud formal por parte del Instituto	por el Instituto
Baja	Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación programadas.	60 minutos posterior a la solicitud formal por parte del Instituto	24 horas posterior al registro realizado por el Instituto

Cambios

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
Emergente	Cambios requeridos como resultado de una pérdida repentina del servicio, falla en un activo de infraestructura o a petición del Instituto.	1 hora posterior a la solicitud formal por parte del Instituto	Conforme al plan de trabajo definido entre el Instituto y el Proveedor
Normal	Cambios solicitados para mejorar o restaurar un servicio o ampliar un activo de infraestructura, que no están considerados en el catálogo de cambios estándar, mismos que deben ser analizados y aprobados por el Instituto.	1 hora posterior a la solicitud formal por parte del Instituto	Conforme al plan de trabajo definido entre el Instituto y el Proveedor
Estándar	Cambios en los servicio y/o activos de infraestructura que se realiza en línea y sigue una trayectoria establecida, mismos que representan una	1 hora posterior a la solicitud formal por parte del Instituto	24 horas posterior al registro realizado por el Instituto

	solución aceptada a un requerimiento o conjunto de requerimientos específicos.		

Cualquier cambio ejecutado por el Proveedor, mismo que no se encuentre autorizado por el Instituto, derive o no en alguna falla de los servicios de seguridad, será catalogado como un incidente de seguridad, mismo que será clasificado con base en las afectaciones o riesgos que pudieron generar.

Deductiva por incumplimiento:

Requerimientos

DESCRIPCIÓN DEL NIVEL DE SERVICIO	MÉTRICA	DEDUCTIVA	CÓMPUTO DE LA DEDUCTIVA
Tiempo máximo de registro y notificación conforme al nivel de prioridad Alta	10 minutos posterior al registro y notificación del requerimiento	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de ejecución conforme al nivel de prioridad Alta	1 hora posterior al registro y notificación del requerimiento	0.5% por cada minuto de atraso en la ejecución del requerimiento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Media	30 minutos posterior al registro y notificación del requerimiento	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Media	8 horas posterior al registro y notificación del requerimiento	0.5% por cada hora o fracción de atraso en la ejecución del requerimiento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Baja	60 minutos posterior al registro y notificación del requerimiento	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad	24 horas posterior al registro y notificación del	0.5% por cada hora o fracción de atraso en la ejecución del	Valor unitario de la facturación mensual del

Baja	requerimiento	requerimiento	servicio relacionado con el incumplimiento

Cambios

DESCRIPCIÓN DEL NIVEL DE SERVICIO	MÉTRICA	DEDUCTIVA	CÓMPUTO DE LA DEDUCTIVA
Tiempo máximo de registro y notificación conforme al nivel de prioridad Emergente	1 hora posterior al registro y notificación del cambio	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de ejecución conforme al nivel de prioridad Emergente	Conforme al plan de trabajo definido entre el Instituto y el Proveedor	5% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Normal	1 hora posterior al registro y notificación del cambio	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Normal	Conforme al plan de trabajo definido entre el Instituto y el Proveedor	5% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Estándar	1 hora posterior al registro y notificación del cambio	0.1% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Estándar	24 horas posterior al registro y notificación del cambio	5% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.11. Servicios de Seguridad – Continuidad Operativa

DESCRIPCIÓN DEL NIVEL DE SERVICIO	MÉTRICA	DEDUCTIVA	CÓMPUTO DE LA DEDUCTIVA
Reportes Técnicos de los activos de infraestructura que contemplen: • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	5 días hábiles posterior al cumplimiento del mes vencido	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.12.Servicios de Seguridad – Verificación/Calidad

DESCRIPCIÓN DEL NIVEL DE SERVICIO	MÉTRICA	DEDUCTIVA	CÓMPUTO DE LA DEDUCTIVA
Reportes Técnicos de los activos de infraestructura que contemplen: • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	5 días hábiles posterior al cumplimiento del mes vencido	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Análisis de Vulnerabilidades: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades	7 días hábiles posterior a la solicitud generada por parte del Instituto	2% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis			
Servicios de Prueba de Penetración: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación	10 días hábiles posterior a la solicitud generada por parte del Instituto	2% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis			
Servicios de Análisis Forense: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados	15 días hábiles posterior a la solicitud generada por parte del Instituto	2% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Borrado Seguro de Información: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.	5 días hábiles posterior a la solicitud generada por parte del Instituto	2% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Servicios de Sistema de Gestión de Seguridad de la Información: Plan de Trabajo de implementación y operación de los servicios conforme al alcance definido en las mesas de trabajo	10 días hábiles posterior a la solicitud generada por parte del Instituto	2% por cada día hábil de atraso en la entrega del plan de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Sistema de Gestión de Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora del Sistemas De Gestión de Seguridad de la Información (SGSI)	Conforme a la fecha estipulada en el plan de trabajo acordado entre el Instituto y el Proveedor	2% por cada día hábil de atraso en la entrega de los reporte de actividades, por periodo, por evento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

9.13.Servicios del Centro de Operaciones de Seguridad (SOC)

DESCRIPCIÓN DEL NIVEL DE SERVICIO	MÉTRICA	DEDUCTIVA	CÓMPUTO DE LA DEDUCTIVA
Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	5 días hábiles posterior al cumplimiento del mes vencido	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	5 días hábiles posterior al cumplimiento del mes vencido	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los incidentes presentados en los servicios de	5 días hábiles posterior al cumplimiento del mes vencido	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado

seguridad implementados			con el incumplimiento
Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	5 días hábiles posterior al cumplimiento del mes vencido	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo	5 días hábiles posterior al cumplimiento del mes vencido	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte de las evaluaciones operativas a los servicios de seguridad implementados	5 días hábiles posterior al cumplimiento de cada trimestre vencido	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados	5 días hábiles posterior al cumplimiento de cada trimestre vencido	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Creación de cuentas de acceso en las consolas de administración de las servicios de seguridad	5 días hábiles posterior al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto	1% por cada día hábil de atraso en la entrega de las cuentas de acceso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad	5 días hábiles posterior al término de la implementación de cualquier solución de seguridad o	1% por cada día hábil de atraso en la entrega de las cuentas de acceso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

	conforme a cada solicitud generada por el Instituto		
Actualización de la matriz de escalación	5 días hábiles posterior a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad	1% por cada día hábil de atraso en la entrega de la matriz de escalación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad	5 días hábiles posterior a la ejecución de la ventana mantenimiento	2% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte con Estadísticas de uso y desempeño (información analítica) de la soluciones de seguridad	5 días hábiles posterior a la solicitud generada por parte del Instituto	2% por cada día hábil de atraso en la entrega del reporte	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de las configuraciones de las soluciones de seguridad	5 días hábiles posterior a la solicitud generada por parte del Instituto	2% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los incidentes presentados en las soluciones de seguridad	5 días hábiles posterior a la solicitud generada por parte del Instituto	2% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los requerimientos registrados en la mesa de servicios	5 días hábiles posterior a la solicitud generada por parte del Instituto	2% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y su diagrama de	5 días hábiles posterior a la solicitud generada por parte del Instituto	2% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

interrelación conforme fueron registrados en la CMDB			
Diagramas de Arquitectura de las soluciones de seguridad	2 días hábiles posterior a la solicitud generada por parte del Instituto	2% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Cualquier cambio ejecutado por el SOC, mismo que no se encuentre autorizado por el Instituto, derive o no en alguna falla de los servicios de seguridad, será catalogado como un incidente de seguridad, mismo que será clasificado con base en las afectaciones o riesgos que pudieron generar.

10. CONDICIONES DE PAGO

Como se establece en el numeral 25 Administrador del Contrato del presente documento, el administrador de contrato, será el servidor público responsable de supervisar que se cumplan en tiempo y forma los compromisos contenidos en el contrato que para tal efecto se celebre.

Los pagos se realizarán previa validación y aceptación de los servicios por parte del Administrador del Contrato**,** es decir, el Titular de la División de Seguridad Informática Integral, que reciba cada uno de “Los Servicios” y que será responsable de realizar los trámites de pago en estricto apego al procedimiento administrativo vigente en “EL INSTITUTO”.

Para proceder a la liberación de pago, el Titular de la Seguridad Informática Integral o el Servidor Público que para tal efecto haya designado el Titular de la Coordinación de Mantenimiento y Operación de Servicios de Cómputo, será responsable de la supervisión y administración de todas las obligaciones a cargo del proveedor.

Así como de la ejecución, validación, técnica y administrativamente de todos y cada uno de los documentos que acreditan que los servicios proporcionados por el proveedor se cumplieron en tiempo, forma y cantidad con las características, especificaciones y condiciones contractualmente pactadas para el proyecto, procederá de conformidad con lo establecido en el artículo 51 de la LAASSP, la forma de pago al proveedor será la estipulada en los contratos y quedará sujeta a las condiciones que establezcan las mismas; sin embargo, no podrá exceder de veinte días naturales contados a partir de la entrega de la factura respectiva, previa entrega de certificado de licencia o de la prestación de los servicios en los términos del contrato.

El proveedor deberá entregar en la División de Trámite de Erogaciones, situada en la calle de Tiburcio Montiel No. 15, PB, Col. San Miguel Chapultepec, Código Postal 11850, Delegación Miguel Hidalgo, México, D.F., en días y horas hábiles, los siguientes documentos:

- Original y copia de la factura que expida el Proveedor, a nombre del Instituto

Mexicano del Seguro Social, con dirección en Av. Paseo de la Reforma N° 476, Col. Juárez, Delegación Cuauhtémoc, C.P. 06600, México, D.F., y R.F.C. IMS-421231-I45; que reúna los requisitos fiscales, en la que se indiquen los servicios proporcionados y el número de contrato que ampara dichos servicios,

- Original y Copia de la documentación que avale la entrega de los servicios a satisfacción de "EL INSTITUTO" (Acta Entrega-Recepción de los Servicios).
- Carta firmada por el representante legal, en la cual haga del conocimiento de "EL INSTITUTO" la cuenta bancaria a la que se efectuará la transferencia electrónica bancaria correspondiente.
- Nota de crédito (en caso de que aplique) a favor del Instituto Mexicano del Seguro Social por el importe de la sanción en caso de entrega extemporánea de los servicios contratados.
- Presentará Orden de Ingreso (Nota de Crédito) (en caso de que aplique para Soporte Técnico dentro de los primeros 10 días hábiles después de la fecha del Acta Entrega-Recepción de los Servicios del trimestre firmada, a favor del Instituto Mexicano del Seguro Social por el importe de la sanción en caso de entrega extemporánea de los servicios contratados, en caso de no entregar la Orden de ingreso (Nota de Crédito) correspondiente al plazo citado en este punto, se aplicara la ejecución de garantía.

En caso de que el proveedor presente sus facturas con errores o deficiencias, estos se le harán saber por parte de "EL INSTITUTO" dentro del término estipulado para ello, y el plazo de pago se ajustará, debiendo presentar nuevamente toda la documentación mencionada anteriormente (en original y/o copia, según corresponda).

El Pago se realizará en pesos mexicanos y constara de 3 pagos conforme a las entregas programadas, las cuales serán al termino de cada mes del servicio.

11. ENTREGABLES

El proveedor deberá entregar al Titular de la División de Seguridad Informática Integral dependiente de la Coordinación Técnica de Seguridad de Tecnologías de la Información y Comunicaciones, dependiente a su vez de la Coordinación de Mantenimiento y Operación de Servicios de Cómputo:

11.1. Entregables Generales

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posterior a la emisión del fallo
	Documento Compromiso de suscripción de OLAs	Única Vez	15 días naturales posterior a la emisión del fallo
	Matriz de Escalación	Única Vez	15 días naturales posterior a la emisión del fallo
	Escrito por parte del proveedor,	Única Vez	15 días naturales posterior a la

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios		emisión del fallo
Servicios de Seguridad – Continuidad Operativa	Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad	Única Vez	20 días hábiles previo al termino del contrato para aquellos servicios que se encuentren habilitados
Servicios de Seguridad – Verificación/Calidad	Documento con el diseño de Alto Nivel de los servicios de	Única Vez	5 días hábiles posteriores a la integración de las

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integran activos de infraestructura para su habilitación		mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integran activos de infraestructura para su habilitación	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integran activos de infraestructura para su habilitación	Única Vez	20 días hábiles previo al termino del contrato para aquellos servicios que se encuentren habilitados
Servicios de Análisis de Vulnerabilidades	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Pruebas de Penetración	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Análisis	Procedimientos de	Única Vez	10 días hábiles

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Forense	Operación del servicios		posterior a la integración de las mesas de trabajo
Servicios de Borrado Seguro de Información	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)	Metodología de implementación de los servicios	Única Vez	10 días hábiles posterior a la integración de las mesas de trabajo
Servicios del Centro de Operaciones de Seguridad (SOC)	Procesos de operación implementados: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posterior a la emisión del fallo
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posterior a la emisión del fallo
	Procedimiento de operación de la Mesa de Servicios: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posterior a la emisión del fallo
	Plan de Recuperación en caso de desastre (DRP)	Única Vez	60 días naturales posterior a la integración de las mesas de trabajo
	Expedientes Curriculares del personal del SOC	Única Vez	15 días naturales posterior a la emisión del fallo

11.2. Entregables Verificación Calidad

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades	Evento	7 días hábiles posterior a la solicitud generada por parte del Instituto

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis		
Servicios de Prueba de Penetración	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos	Evento	10 días hábiles posterior a la solicitud generada por parte del Instituto

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis		
Servicios de Análisis Forense	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados	Evento	15 días hábiles posterior a la solicitud generada por parte del Instituto
Servicios de Borrado Seguro de Información	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
Servicios de Sistema de Gestión de Seguridad de la Información	Plan de Trabajo de implementación y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posterior a la solicitud generada por parte del Instituto
Servicios de Gestión del Cambio en Seguridad de la	Plan de Trabajo de implementación y operación de los	Evento	10 días hábiles posterior a la solicitud generada

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Información	servicios conforme al alcance definido en las mesas de trabajo		por parte del Instituto
Servicios del Centro de Operaciones de Seguridad (SOC)	Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad	Evento	5 días hábiles posterior al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto
	Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad	Evento	5 días hábiles posterior al término de la implementación de cualquier solución de seguridad o conforme cada solicitud generada por el Instituto
	Actualización de la matriz de escalación	Evento	5 días hábiles posterior a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad	Evento	5 días hábiles posterior a la ejecución de la ventana mantenimiento
	Reporte con Estadísticas de uso y desempeño (información analítica) de la soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de las configuraciones de las soluciones de seguridad	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de los incidentes	Evento	5 días hábiles posterior a la

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	presentados en las soluciones de seguridad		solicitud generada por parte del Instituto
	Reporte Técnico de los requerimientos registrados en la mesa de servicios	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y su diagrama de interrelación conforme fueron registrados en la CMDB	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Diagramas de Arquitectura de las soluciones de seguridad	Evento	2 días hábiles posterior a la solicitud generada por parte del Instituto

11.3. Entregables Periódicos

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de los activos de infraestructura que contemplen: • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
Servicios de Seguridad –	Reportes Técnicos de los activos de	Mensual	5 días hábiles posterior al

Verificación/Calidad	infraestructura que contemplen: • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)		cumplimiento del mes vencido
Servicios del Centro de Operaciones de Seguridad (SOC)	Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posterior al cumplimiento del mes vencido
	Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de	Mensual	5 días hábiles posterior al cumplimiento del mes vencido

	seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo		
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posterior al cumplimiento de cada trimestre calendario
	Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados	Trimestral	5 días hábiles posterior al cumplimiento de cada trimestre calendario

El Proveedor deberá cumplir con los formatos provistos por el Instituto y en apego al MAAGTICSI.

12. CONDICIONES DE ACEPTACIÓN

Se deberán formalizar los entregables descritos en el numeral anterior a efecto de dar por recibido los servicios requeridos.

Todos los documentos deben ser entregados en papel membretado de la empresa de manera impresa y en electrónico.

Se entregará a la División de Seguridad Informática Integral (DSII) perteneciente a la Coordinación Técnica de Seguridad de Tecnologías de la Información y Comunicaciones, dependiente a su vez de la Coordinación de Mantenimiento y Operación de Servicios de Cómputo.

13. LUGAR Y HORARIO PARA LA ENTREGA

- La entrega se realizará en las instalaciones de “EL INSTITUTO” ubicadas en la calle de Toledo número 21 piso 6, Colonia Juárez, Delegación Cuauhtémoc, Ciudad de México, C.P. 06600.
- El horario para la entrega será de las 9:00 horas a las 17:00 horas
- En caso de contingencia podrá solicitarse la entrega de las cartas requeridas en el presente documento en cualquiera de los inmuebles que formen parte de las Oficinas Centrales de “EL INSTITUTO”, ubicadas en la Colonia Juárez, Delegación Cuauhtémoc, C.P. 06600 en la Ciudad de México.

14. CONVENIO DE CONFIDENCIALIDAD Y RESGUARDO DE LA INFORMACIÓN

El Proveedor de los **Servicios Administrados de Seguridad Integral 2021,** deberá suscribir el Convenio de Confidencialidad y Resguardo de Información correspondiente, mediante carta bajo protesta de decir verdad, firmada por su representante legal, en el que su representada o cualquiera de su personal asignado al proyecto por ningún motivo extraerán o divulgará el contenido de la información que se les entregará como parte del contrato.

La carta bajo protesta de decir verdad debe ir firmada por su representante legal, en la que manifieste, que se compromete a respetar y seguir los estándares tecnológicos, tanto de metodologías, procedimientos, hardware, como de software definidos por el Instituto.

Asimismo, en dicha carta el proveedor deberá indicar que se compromete a que toda la información que exista a la fecha de la adjudicación y aquella que desarrolle derivado del presente proyecto será propiedad intelectual y exclusiva de “EL INSTITUTO” y no podrá ser utilizada por el proveedor para otros fines.

Por lo que deberá considerar al menos los siguientes mecanismos de control de acceso a la información del Instituto:

- Se deberán establecer controles de acceso y privilegios restringidos al personal del Proveedor del SASI, a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del Instituto.
- Se deberá implantar y aceptar en todo momento el uso de controles que permitan registrar “Pistas de Auditoria” para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.
- La seguridad lógica deberá estar protegida mediante el uso de dispositivos de control de acceso (Firewalls), mecanismos de encriptación y seguridad física entre las redes del Proveedor del SASI y las del Instituto.
- Los empleados del Proveedor de SASI y sus sub-contratados, con acceso a la información sensible del Instituto, deberán firmar acuerdos de confidencialidad con este último.
- El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por el proveedor de los servicios SASI, observando los requisitos de seguridad y resguardo de la información.
- El Proveedor del SASI deberá permitir el acceso a información relacionada con el servicio prestado al Instituto para la realización de auditorías.
- El Proveedor SASI no deberá hacer uso indebido de la documentación, información, ni activos de TIC a los que tengan acceso o que se generen con motivo de la prestación del servicio.

15. PROPIEDAD INTELECTUAL

El proveedor se obliga durante la garantía de las licencias a liberar a “EL INSTITUTO” de toda responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione con motivo de la infracción de derechos de autor, patentes, marcas u otros derechos de propiedad industrial o intelectual a nivel Nacional o Internacional.

16. MÉTODO DE EVALUACIÓN DE PROPUESTAS

Se evaluará mediante el procedimiento de Puntos y Porcentajes y conforme a las características que presenten los proveedores en cuanto a funcionalidades en el Anexo Técnico como en el apéndice A del Anexo Técnico.

17. FUNCIONARIOS PÚBLICOS DE LA DIDT PARTICIPANTES EN EL PROCESO DE ADQUISICIÓN

a) Ing. Gabriel Barrón Montiel, Titular de la Coordinación Técnica de Seguridad de Tecnologías de Información y Comunicaciones.
b) Ing. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Integral.
c) Ing. Evelyn Jaimes Montes de la División de Seguridad Informática Integral.

18. VIGENCIA DEL CONTRATO

La vigencia del contrato será a partir de la firma y hasta el 31 de diciembre de 2021.

19. PLAZO DEL SERVICIO

La prestación de los servicios iniciará a partir del día hábil siguiente al de la notificación de la adjudicación y hasta el 31 de diciembre de 2021.

20. ADMINISTRADOR DEL CONTRATO

Conforme a las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto, el Administrador del Contrato, será el responsable de supervisar que se cumplan en tiempo y forma los compromisos contenidos en el contrato que para tal efecto se celebre, por lo tanto será el siguiente:

a) **Administrador del Contrato y Responsable Técnico**; Titular de la División de Seguridad Informática Integral.

b) **Supervisor del Contrato**; Titular de la Coordinación Técnica de Seguridad de Tecnologías de Información y Comunicaciones.

c) **Apoderado Legal;** Titular de la Coordinación de Mantenimiento y Operación de Servicios de Cómputo.

Los servicios a cargo del proveedor estarán bajo la administración y supervisión del responsable designado que para tal efecto será el Titular de la División de Seguridad Informática Integral.

21. MECANISMOS DE CONTROL PARA LA ADMINISTRACIÓN DEL CONTRATO

El Administrador del Contrato en conjunto con el Proveedor deberá generar el acta de entrega-recepción conforme a los entregables del Anexo Técnico.

MATRIZ DE PUNTOS Y PORCENTAJES "SERVICIOS ADMINISTRADOS DE SEGURIDAD INTEGRAL 2021"

Evaluación Técnica mediante el método de Puntos y Porcentajes

*La puntuación o unidades porcentuales a obtener en la propuesta técnica para ser considerada como solvente y, por tanto, no ser desechada, será de cuando menos **45 puntos de los 60 puntos** máximos posibles que se pueden obtener en su evaluación.*

Los licitantes deberán de considerar los siguientes criterios que evaluará el Instituto para establecer como solvente su propuesta:

Número	Rubros	Puntos Máximos Posibles	Puntos Obtenidos
1	Capacidad del Licitante	20.0	
2	Experiencia y especialidad del Licitante	18.0	
3	Propuesta de Trabajo	10.0	
4	Cumplimiento de Contratos	12.0	
	TOTAL:	**60.0**	

#	CARACTERÍSTICAS Servicios Administrados de Seguridad Integral 2021	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
1	**A) Capacidad del Licitante**			
	Consiste en los recursos con que cuente el licitante para la prestación de los servicios materia de la presente convocatoria, tales como: recursos humanos técnicamente aptos para prestar el servicio, así como los recursos económicos y de equipamiento que requiere el licitante para prestar los servicios en el tiempo, condiciones y niveles de calidad requeridos por la convocante; así como cualquier otro aspecto indispensable para que el licitante pueda cumplir con las obligaciones previstas en el contrato.			
	a) Capacidad de los recursos humanos.			
	Experiencia			
	• Manifestación escrita, firmada por el representante legal de la empresa licitante, en la que establezca que cuenta con al menos 1 (una) persona que se encuentren dentro de su plantilla; la cual deberá tener al menos 5 años de experiencia en proyectos de seguridad de la información, como responsable del Centro de Operaciones de Seguridad (SOC) y con la certificación solicitada en el Anexo Técnico • Manifestación escrita, firmada por el representante legal de la empresa licitante, en la que establezca que cuenta con al menos 3 (tres) recursos que se encuentren dentro de su plantilla; las cuales deberán tienen al menos 5 Años de experiencia en proyectos de seguridad de la información, como Administración y Operación de soluciones y herramientas tecnológicas y con la certificación solicitada en el Anexo Técnico • Manifestación escrita, firmada por el representante legal de la empresa licitante, en la que establezca que cuenta con al menos 2 (dos) recursos que se encuentren dentro de su plantilla; las cuales deberán tienen al menos 5 Años de experiencia en proyectos de seguridad de la información, como Analista de Seguridad y con la certificación solicitada en el Anexo Técnico. • Manifestación escrita, firmada por el representante legal de la empresa licitante, en la que establezca que cuenta con al menos 1 (un) recurso que se encuentre dentro de su plantilla; el cual deberá tener al menos 5 Años de experiencia en proyectos de seguridad de la información, como Líder de Proyecto y con la certificación solicitada en el Anexo Técnico. • Manifestación escrita, firmada por el representante legal de la empresa licitante, en la que establezca que cuenta con personal necesario dentro de su plantilla; el cual deberá tener al menos 5 Años de experiencia en proyectos de seguridad de la información, Operador de la Mesa del SOC y con la certificación solicitada en el Anexo Técnico. • Manifestación escrita, firmada por el representante legal de la empresa licitante, en la que establezca que cuenta con al menos 1 (un) recurso que se encuentre dentro de su plantilla; el cual deberá tener al menos 5 Años de experiencia en proyectos de seguridad de la información, como Consultor de Penetración y con la certificación solicitada en el Anexo Técnico. • Manifestación escrita, firmada por el representante legal de la empresa licitante, en la que establezca que cuenta con al menos 1 (un) recurso que se encuentre dentro de su plantilla; el cual deberá tener al menos 5 Años de experiencia en proyectos de seguridad de la información, como Consultor Forense de Cómputo y con la certificación solicitada en el Anexo Técnico. • Manifestación escrita, firmada por el representante legal de la empresa licitante, en la que establezca que cuenta con al menos 1 (un) recurso que se encuentre dentro de su plantilla; el cual deberá tener al menos 5 Años de experiencia en proyectos de seguridad de la información, como Arquitecto Especializado en Redes y Seguridad y con la certificación solicitada en el Anexo Técnico. • Los licitantes deberán presentar el currículum vitae del personal designado,		**1.6**	

#	CARACTERÍSTICAS Servicios Administrados de Seguridad Integral 2021	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
	los documentos que avalen sus conocimientos con los que se acredite la experiencia solicitada, así como copia simple de los contratos de trabajo u hojas de afiliación al Seguro Social. Nota: Se dará una puntuación de 0.16 puntos por cada una de las personas que cumplan con los años de experiencia solicitados, en caso de presentar la documentación de 10 personas solicitadas (A excepción de la Mesa SOC), **se dará la mayor puntuación que corresponde a 1.6**, en caso de no presentar la documentación correspondiente se considerará **como 0.00 la puntuación.**			
	Competencia o habilidad en el trabajo de acuerdo con sus conocimientos académicos o profesionales			
	• El licitante deberá comprobar que el personal solicitado, cuentan con cédula profesional en carreras afines a Tecnologías de Información y Comunicaciones: Nota: Por cada persona de las designadas en los puntos anteriores que acredite que cuenta con cédula profesional de al menos nivel licenciatura, se le otorgarán 0.48 puntos se le otorgara **un máximo de 4.8 puntos**; en caso de no entregar se le otorgaran 0 puntos		**4.8**	
	Dominio de Herramientas Relacionadas con el Servicio			
	Certificación con fabricantes • Escrito donde el representante legal de la empresa licitante manifieste cuantos años tiene de Socio (Partner) certificado con el fabricante de las soluciones de seguridad a implementar. Se otorgarán 0.177 puntos por cada 5 años que tenga el licitante de antigüedad por cada fabricante de la solución de seguridad que oferte (9 soluciones), **siendo el máximo de puntos a otorgar 1.6 puntos**; los licitantes deberán presentar el documento solicitado en este apartado. A los licitantes que no entreguen dicho documento **se les otorgará 0.00 puntos.**		**1.6**	
	b) Capacidad de Recursos Humanos y Equipamiento			
	• Servicios de Seguridad - Continuidad Operativa Son los servicios necesarios de seguridad perimetral (Firewalls, IPS, AntiDDoS, Filtrado Web, Firewall de Aplicaciones WEB, Firewall de base de datos, VPN, Gestión de Amenzas Unificadas.), que se requiere su implementación, puesta a punto y operación para que inmediatamente en donde lo requiera el Instituto se pueda continuar con la operación. Estos servicios serán bajo de manda conforme lo solicite el Instituto, los tiempos de entrega serán conforme al sitio y dependiendo del tipo de tecnología de acuerdo al Apéndice En donde se contemplan los tiempos de entrega y los tipos de modalidades como alta disponibilidad (HA), así como los Niveles de Servicio requeridos tanto para la implementación como la operación, incluyendo los temas de soporte y resolución de problemas e incidentes.			

#	CARACTERÍSTICAS Servicios Administrados de Seguridad Integral 2021	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
	• Servicios de Seguridad – Verificación / Calidad Son los elementos necesarios para que los servicios de calidad de la Seguridad de la Información se implementen, las pruebas estáticas y dinámicas de seguridad (revisiones de vulnerabilidades a los aplicativos y sistemas de información), temas de cumplimientos normativo (MAAGTICSI) y herramientas de seguridad, así como los Niveles de Servicio requeridos tanto para la implementación como la operación, incluyendo los temas de soporte y resolución de problemas e incidentes. • Servicios del Centro de Operaciones de Seguridad (SOC) El Instituto requiere que el proveedor del servicio cuente con un Centro de Operaciones de la Seguridad (SOC), que se encuentre físicamente en las instalaciones del proveedor. 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, que ejecute actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, análisis forense, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable. la gestión del centro de operaciones de seguridad (SOC) por sus siglas en inglés (análisis de bloqueos de seguridad, parches y actualizaciones de las firmas de las soluciones de seguridad funcionamiento 7x24x365, etc.), Al licitante que entregue toda la documentación técnica, datasheets, etc, (No se aceptaran cartas bajo protesta de decir verdad), donde se demuestre que cumplen con lo solicitado en el Anexo Técnico y su Apéndice, se le darán una **calificación máxima de 8 puntos**. Quien no presente la información completa solicitada donde se pueda comprobar su cumplimiento, **tendrá 0.00 puntos.**		**8**	
	Participación de discapacitados o empresas que cuenten con trabajadores con discapacidad Se otorgará puntaje al licitante que cuente cuando menos con el 5% de la totalidad de su plantilla de empleados con discapacidad, cuya antigüedad no sea inferior a seis meses, misma que se comprobará con la siguiente documentación: Aviso de alta al régimen obligatorio del Instituto Mexicano del Seguro Social, constancias o certificados de reconocimiento de discapacidad, expedidos por alguna institución del sector salud federal y cédula de determinación y comprobación de pago al IMSS correspondiente al mes de enero de 2018. Se asignará la mayor puntuación que **corresponde a 1.34**, al licitante que acredite tener el mayor número de trabajadores discapacitados en los términos señalados en el presente rubro. A partir del o los licitantes que hubieren obtenido mayor puntuación, se distribuirá, de manera proporcional la puntuación o unidades porcentuales a los demás licitantes, aplicando para ello una regla de tres.		**1.34**	
	Participación de MIPYME Se otorgará puntaje a la MIPYME participante que tenga alguna innovación tecnológica relacionada con alguno de los bienes o servicios que sean proporcionados con motivo del cumplimiento de las obligaciones contractuales para		**1.33**	

#	CARACTERÍSTICAS Servicios Administrados de Seguridad Integral 2021	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
	lo cual se presentará el siguiente documento: Constancia emitida por el instituto mexicano de la propiedad industrial, la cual no podrá tener una vigencia mayor a cinco años. Si el licitante presenta constancia emitida por el Instituto Mexicano de la Propiedad Industrial, **se le otorgarán 1.33 puntos**. Si el licitante no presenta constancia emitida por el Instituto Mexicano de la Propiedad Industrial, se le otorgarán 0.00 puntos.			
	Certificación de políticas y prácticas de igualdad de género. Se otorgarán puntos a las empresas que hayan aplicado políticas y prácticas de igualdad de género, conforme a la certificación correspondiente emitida por las autoridades y organismos facultados para tal efecto. En su caso, el licitante deberá presentar copia del certificado emitido por las autoridades de haber aplicado políticas y prácticas de igualdad de género. Al licitante que presente las políticas aplicadas **se le dará 1.33 puntos**. De no encontrarse la Licitante en el presente caso no será necesario entregar carta o documento alguno.		**1.33**	
	Total Puntos por este Rubro		**20**	
2	**B) Experiencia y especialidad del Licitante**			
	a) Experiencia			
	Deberá de entregar copia simple del acta constitutiva donde se demuestre que está constituido con el giro de proveeduría en servicios similares. Al licitante que demuestre su **experiencia** al estar constituido desde al menos hace 5 años con el giro de proveeduría en servicios similares se le **otorgarán 10 puntos**; al licitante que demuestre su experiencia al estar constituido desde hace 4 años con el giro de proveeduría en servicios similares **se le otorgarán 5 puntos**. Quien presente experiencia de 3 años se le **otorgaran 3 puntos**, quien presente experiencia de 2 años **se le otorgaran 2 puntos,** quien presente experiencia de 1 año **se le otorgara 1 punto y quien no presente información alguna tendrá 0.00 puntos**.		**10**	
	b) Especialidad del Licitante			
	Deberá de entregar copia simple de por lo menos 2 contratos y sus facturas correspondientes en donde se compruebe que se proporcionaron servicios similares. Al licitante que demuestre su **especialidad** entregando dos contratos con sus facturas correspondientes de más de 6 meses proporcionando servicios similares se le otorgarán **una calificación máxima de 8 puntos**; al licitante que demuestre su especialidad entregando un contrato de al menos 6 meses, **se le otorgaran 6 puntos**, al licitante que demuestre su especialidad entregando un contrato de tres meses proporcionando servicios similares **se le otorgarán 4 puntos**. Quien no presente información alguna **tendrá 0.00 puntos.**		**8**	

#	CARACTERÍSTICAS Servicios Administrados de Seguridad Integral 2021	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
	Total de Puntos por este rubro:		**18**	
3	**C) Propuesta de Trabajo**			
	a) Metodología, Plan de trabajo, Organigrama			
	El licitante se obliga a proporcionar al Instituto Una metodología donde se describa el mecanismo para la atención, solución, control, seguimiento de los casos de soporte, considerando la manera enunciativa mas no limitativa lo siguiente: 1. Las fallas o Problemas detectados serán reportados por: el Administrador del contrato y/o Personal de la División de Mesa de Servicios Tecnológicos, designado para dar seguimiento al soporte técnico. 2. Bajo el esquema 7 x 24 x 365 días para atención y seguimiento de fallas y/o problemas (disponibilidad las 24 horas, los 7 días de la semana los 365 días del año). a) Las fallas o problemas detectados, se reportarán principalmente a través de la Página web pública, para el registro y seguimiento de reportes de fallas y/o defectos de los productos En caso de contingencia se podrá utilizar alguno de los siguientes medios. b) Correo Electrónico c) Número 01800 3. El Instituto deberá de proporcionar en el reporte al menos lo siguiente: a) Tipo de falla b) Ambiente y Módulo en él que se presentó la falla Descripción de la falla c) Evidencia que el Instituto considere necesaria. d) severidad de la falla (Critica, Alta, Media o Baja) El soporte será provisto de la siguiente forma: 1. EL INSTITUTO podrá llevar a cabo levantamiento de reporte de fallas y/o defectos con disponibilidad de las 24 (veinticuatro) horas, los 7 (siete) días de la semana; 2. Vía Web: El proveedor deberá contar con una herramienta para el registro y seguimiento de los casos de soporte. 3. Vía Correo electrónico: El proveedor deberá proporcionar un correo electrónico, con disponibilidad de las 24 (veinticuatro) horas, los 7 (siete) días de la semana. 4. Vía telefónica: Mediante el número 01(800), EL INSTITUTO podrá llevar a cabo el seguimiento a reportes de fallas y/o defectos de los productos ofertados con disponibilidad de las 24 (veinticuatro) horas, los 7 (siete) días de la semana. 5. Vía Web: a través de la URL asignada por el proveedor, el Instituto realizará la descarga de actualizaciones (updates) y parches de los productos con disponibilidad de las 24 (veinticuatro) horas, los 7 (siete) días de la semana.		**1.5**	

#	CARACTERÍSTICAS Servicios Administrados de Seguridad Integral 2021	VERIFICACION REFERENCIA	PUNTOS MÁXIMOS	OBSERVACIONES
	Al licitante que entregue la metodología se le **otorgarán un máximo de 1.5 puntos**. Quien no presente la información completa solicitada **tendrá 0.00 puntos.**			
	El licitante se obliga a proporcionar al Instituto un plan de trabajo donde se describa los recursos de que dispone para prestar el servicio, cuándo y cómo llevará a cabo las actividades o tareas que implica el mismo. Al licitante que entregue el plan de trabajo se le **otorgarán un máximo de 2 puntos**. Quien no presente la información completa solicitada **tendrá 0.00 puntos.**		**2**	
	El licitante se obliga a proporcionar al Instituto el o los procedimientos para llevar a la práctica las actividades o habilidades y el esquema conforme al cual se estructurará la organización de los recursos humanos necesarios para cumplir con las obligaciones previstas en la convocatoria o invitación. Al licitante que entregue el o los procedimientos para llevar a la práctica las actividades o habilidades y el esquema conforme al cual se estructurará la organización de los recursos humanos se le **otorgarán un máximo de 1.5 puntos**. Quien no presente la información completa solicitada **tendrá 0.00 puntos.**		**1.5**	
	Organización			
	El licitante deberá proporcionar al Instituto una matriz con los niveles de escalamiento, tanto para la atención y solución de casos de soporte, indicando nombres y cargos de los responsables, teléfonos, e-mail y celulares. Quien presente dicha matriz se le **otorgará 5 puntos**. Quien no presente dicha matriz **tendrá 0.00 puntos.**		**5**	
	Total de Puntos por este rubro:		**10**	
4	**D) Cumplimiento de contratos**			
	Deberá de presentar cartas de satisfacción firmadas por el administrador del contrato o representante legal de la empresa, de los contratos presentados en el rubro de experiencia y especialidad donde se manifieste que cumplió con los servicios solicitados en tiempo y forma, y la liberación de las pólizas de cumplimiento de dichos contratos; se pueden presentar actas de entrega recepción o actas de cierre de proyecto, siempre y cuando estén firmadas por el administrador del contrato o representante legal de la empresa en donde se prestaron los servicios, en estas actas se debe manifestar que el licitante cumplió con los servicios solicitados en tiempo y forma. Al licitante que entregue al menos **tres cartas** de satisfacción y la liberación de las pólizas de cumplimiento no mayor a 5 años, se le otorgará **una calificación Máxima de 12 puntos**; al licitante que entregue carta de satisfacción y la liberación de la póliza de cumplimiento de 2 contratos, se le **otorgarán 8 puntos,** al licitante que entregue carta de satisfacción y la liberación de la póliza de cumplimiento de 1 contrato, se le **otorgarán 4 puntos** Quien no presente ninguna información **tendrá 0.00 puntos.**		**12**	
	Total de Puntos por este rubro:		**12**	
	TOTAL DE PUNTOS OBTENIDOS		**60**	

Anexo 3.- Escrito de acreditación legal y personalidad jurídica del licitante para comprometerse y suscribir propuestas.

Ciudad de México, a _____ de _____de 20__.

_____(Nombre)_____, manifiesto bajo protesta de decir verdad, que los datos aquí asentados son ciertos y han sido verificados, así como que cuento con facultades suficientes para ***comprometerme por mí o por mi representada y suscribir las propuestas*** en la presente licitación pública nacional Núm. _____, a nombre y representación de.__(Persona Física o Moral)___.

Datos Personas Morales y Físicas.

Registro Federal de Contribuyentes.	
Domicilio.	
Calle y Número.	
Colonia.	Demarcación Territorial o Municipio.
Código Postal.	Entidad Federativa.
Teléfono Fijo.	Teléfono Móvil.
Correo Electrónico.	
Apoderado Legal o Representante. (Nombre, Domicilio, Teléfonos y Correo Electrónico)	
Documento para Acreditar Personalidad y Facultades. (Escritura Pública y Modificaciones, Fecha, y Datos del Notario Público)	

Datos Personas Morales.

Número de la Escritura Pública en la que consta su Acta Constitutiva.		Fecha.
Nombre, Número y Domicilio del Notario Público (ante el cual se dio fe de la misma).		
Fecha y Datos de su Inscripción en el Registro Público de Comercio.		
Descripción del Objeto Social.		
Relación de Accionistas.		
Apellido Paterno	Apellido Materno	Nombre(s)
Reformas al Acta Constitutiva que incidan con el objeto del procedimiento (Señalar Nombre, Número y Circunscripción del Notario o Fedatario Público que las protocolizó, así como la Fecha y los datos de su Inscripción en el Registro Público de la Propiedad).		

Asimismo, manifiesto que los cambios o modificaciones que se realicen en cualquier momento a los datos o documentos contenidos en el presente documento y durante la vigencia del contrato que, en su caso, sea suscrito con el Instituto, deberán ser comunicados a éste, dentro de los cinco días hábiles siguientes a la fecha en que se generen.

Protesto lo necesario

_____

(Nombre y Firma del Apoderado o Representante Legal del Licitante)

Anexo 4.- Escrito de nacionalidad mexicana.

Ciudad de México, a _____ de _____de 20__.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones e Infraestructura
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

Me refiero al procedimiento _____(*licitación pública o invitación a cuando menos tres personas*)_____ No._____(*Número de Procedimiento*)____ en el que mi representada, la empresa _____(*nombre o razón social del licitante*)_____participa a través de la presente propuesta.

Sobre el particular, y en los términos de lo previsto en numeral 4.1.3, Documentación legal-administrativa, de las bases de la convocatoria de la licitación pública nacional citada en el párrafo anterior, manifiesto bajo protesta de decir verdad lo siguiente:

- Conforme al artículo 35 del Reglamento de la Ley, que mi representada es de nacionalidad mexicana, para participar en el procedimiento de licitación pública nacional.

- Conforme al artículo 39, fracción VIII del Reglamento de la Ley que el origen de los servicios que oferto, serán de origen nacional.

Protesto lo necesario

_____
(Nombre y Firma del Apoderado o Representante Legal del Licitante)

Anexo 5.- Escrito de cumplimiento de normas.

Ciudad de México, a _____ de _____de 20__.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones e Infraestructura
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

Me refiero al procedimiento _____(*licitación pública o invitación a cuando menos tres personas*)_____ No._____(*Número de Procedimiento*)____ en el que mi representada, la empresa _____(*nombre o razón social del licitante*)_____participa a través de la presente propuesta.

Sobre el particular, y en los términos de lo previsto en numeral 4.1.3, Documentación legal-administrativa, de las bases de la convocatoria de la licitación pública nacional citada en el párrafo anterior, manifiesto lo siguiente:

Que en caso de resultar adjudicado, los servicios propuestos cumplirán con las normas solicitadas en la presente convocatoria, de acuerdo con el Anexo [***] que se adjunta para tal efecto.

Protesto lo necesario

_____

(Nombre y Firma del Apoderado o Representante Legal del Licitante)

Anexo 6.- Escrito de no encontrarse en los supuestos de los artículos 50 y 60 de la LAASSP.

Ciudad de México, a ___ de _____de 20__.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones e Infraestructura
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

_____Nombre _____ en mi carácter de representante legal de la_(Persona Física o Moral)_. Declaro bajo protesta de decir verdad lo siguiente.

Que el suscrito (Solo Personas Morales. y las personas que forman parte de la sociedad y) de la propia empresa que represento, no se encuentra(n) en alguno de los supuestos señalados en los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, lo que manifiesto para los efectos correspondientes con relación a la licitación pública nacional número. _____.

Protesto lo necesario

_____
(Nombre y Firma del Apoderado o Representante Legal del Licitante)

Nota. En caso de que el licitante sea persona física, adecuar el formato

Anexo 7.- Declaración de integridad.

Ciudad de México, a _____ de _____de 20__.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones e Infraestructura
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

_____Nombre _____ en mi carácter de representante legal de la_(Persona Física o Moral), y en términos de la convocatoria de la licitación pública nacional número. _____. Declaro bajo protesta de decir verdad lo siguiente.

Que mi representada se abstendrá por si misma o a través de interpósita persona, de adoptar conductas para que los servidores públicos del Instituto, induzcan o alteren las evaluaciones de las proposiciones, el resultado del procedimiento, u otros aspectos que le otorguen condiciones más ventajosas con relación a los demás participantes.

Que en caso de resultar adjudicado, me obligo a liberar al Instituto de toda responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione con motivo de la infracción de derechos de autor, patentes, marcas u otros derechos de propiedad industrial o intelectual a nivel nacional o internacional.

Protesto lo necesario

_____

(Nombre y Firma del Apoderado o Representante Legal del Licitante)

Anexo 8.- Escrito de estratificación de MIPYME.

Ciudad de México, a_____ de _____ de _____ (1)

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones e Infraestructura
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

Me refiero al procedimiento de _____(3)_____ Núm. _____(4) _____ en el que mí representada, la empresa_____(5)_____, participa a través de la presente propuesta.

Al respecto y de conformidad con lo dispuesto por el artículo 34 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, manifiesto bajo protesta de decir verdad que mi representada está constituida conforme a las leyes mexicanas, con Registro Federal de Contribuyentes _____(6)_____, y asimismo que considerando los criterios (sector, número total de trabajadores y ventas anuales) establecidos en el Acuerdo por el que se establece la estratificación de las micro, pequeñas y medianas empresas, publicado en el Diario Oficial de la Federación el 30 de junio de 2009, mi representada tiene un Tope Máximo Combinado de _____(7)_____, con base en lo cual se estatifica como una empresa _____(8)_____.

De igual forma, declaro que la presente manifestación la hago teniendo pleno conocimiento de que la omisión, simulación o presentación de información falsa, son infracciones previstas por los artículos 69 y 81, ambos de la Ley General de Responsabilidades Administrativas, y demás disposiciones aplicables.

Protesto lo necesario

_____

(Nombre y Firma del Apoderado o Representante Legal del Licitante)

Anexo 8 Bis.- Instructivo de llenado para el escrito de estratificación de micro, pequeña o mediana empresa (MIPYMES).

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

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

1. Señalar la fecha de suscripción del documento.
2. Anotar el nombre de la convocante.
3. Precisar el procedimiento de contratación de que se trate (licitación pública o invitación a cuando menos tres personas).
4. Indicar el número de procedimiento de contratación asignado por CompraNet.
5. Anotar el nombre, razón social o denominación del licitante.
6. Indicar el Registro Federal de Contribuyentes del licitante.
7. Señalar el número que resulte de la aplicación de la expresión. Tope Máximo Combinado = (Trabajadores) x 10% + (Ventas anuales en millones de pesos) x 90%.

Para tales efectos puede utilizar la calculadora MIPYMES disponible en la página http://www.comprasdegobierNúm.gob.mx/calculadora
Para el concepto “Trabajadores”, utilizar el total de los trabajadores con los que cuenta la empresa a la fecha de la emisión de la manifestación.
Para el concepto “ventas anuales”, utilizar los datos conforme al reporte de su ejercicio fiscal correspondiente a la última declaración anual de impuestos federales, expresados en millones de pesos.

8. Señalar el tamaño de la empresa (Micro, Pequeña o Mediana), conforme al resultado de la operación señalada en el numeral anterior.
9. Anotar el nombre y firma del apoderado o representante legal del licitante.

Anexo 9.- Propuesta Económica.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones e Infraestructura
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

Razón social del licitante

DESCRIPCIÓN DEL BIEN O SERVICIO	Cantidad solicitada	Unidad de medida	Importe Mínimo	Importe Máximo
Servicios Administrados de Seguridad Integral 2021 (RESUMEN)	1	Servicio	$0.00	$0.00
		Subtotal:	$0.00	$0.00
		I.V.A.:	$0.00	$0.00
		Total:	$0.00	$0.00

DESGLOCE DE LOS BIENES O SERVICIOS

CONCEPTO	CANTIDAD MINIMA	CANTIDAD MAXIMA	PRECIO UNITARIO	TOTAL MIN	TOTAL MAX
I. Servicios de Seguridad - Continuidad Operativa					
1. Arquitectura de Firewall.	2	4		0	0
2. Prevención de Intrusiones (IPS)	2	4		0	0
3. Anti-denegación de servicios DDoS	2	4		0	0
4. Redes Privadas Virtuales	2	4		0	0
5. Filtrado de contenido web	2	4		0	0
6. Antispam	2	4		0	0
7. Firewall Especializado en Servicios Web	2	4		0	0
8. Firewall de Base de Datos	2	4		0	0
9. Gestión Unificada de Amenazas (UTM)	2	4		0	0
II.- Servicios de Seguridad – Verificación / Calidad					
1. Análisis de Vulnerabilidades	40	100		0	0
2. Pruebas de Penetración	40	100		0	0
3. Borrado Seguro de Información	25	50		0	0
4. Gestión de Dominios	1	1		0	0
5. Certificados Digitales SSL	4	6		0	0
6. Análisis Forense	1	2		0	0
7. Sistema de Gestión de Seguridad de la Información (SGSI)	1	1		0	0
III.- Servicios del Centro de Operaciones de				0	0

Seguridad (SOC)					
1. Servicios del Centro de Operaciones de Seguridad (SOC)	1	1			
				0	0
			Subtotal:	0	0
			I.V.A.:	0	0
				$ -	

Lugar y fecha

Representante Legal del Licitante

Nombre y Firma

Anexo 10.- Relación de documentos a presentar.

Fecha
Licitación Pública Nacional Electrónica (Número y Carácter)
Razón Social y Dirección Completa
Teléfonos y Correo Electrónico
Nombre del Representante

Referencia	Documento legal-administrativo	Presentado	
		Si	No
Anexos 1 y 2	4.1.1 Propuesta técnica. Deberá incluir la descripción amplia y detallada del servicio, para lo cual el licitante deberá cumplir con las especificaciones contenidas en el Anexo 1 y Anexo 2 de la presente convocatoria, así como anexar a su propuesta los documentos solicitados en dichos anexos		
Anexo 3	4.1.3.1 Escrito bajo protesta de decir verdad que cuenta con facultades suficientes para comprometerse por sí o por su representada, de acuerdo con el Anexo 3. Acompañándose de copia simple por ambos lados de su identificación oficial vigente con fotografía, (cartilla del servicio militar nacional, pasaporte, credencial para votar ó cédula profesional), tratándose de personas físicas, y en el caso de personas morales, de la persona que firme la propuesta.		
Anexo 4	4.1.3.2 Escrito bajo protesta de decir verdad, que el licitante es de nacionalidad mexicana, de acuerdo con el Anexo 4.		
Anexo 5	4.1.3.3 Escrito en el que manifieste que en caso de resultar adjudicado, los servicios propuestos cumplirán con las normas solicitadas en la presente convocatoria, de acuerdo con el Anexo 5.		
Anexo 6	4.1.3.4 Escrito bajo protesta de decir verdad, que no se ubica en los supuestos establecidos en los artículos 50 y 60 de la LAASSP, de acuerdo con el Anexo 6.		
Anexo 7	4.1.3.5 Declaración de integridad, en la que el licitante manifieste, bajo protesta de decir verdad que se abstendrán de adoptar conductas, por si o a través de interpósita persona, para que los servidores públicos del IMSS 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, de acuerdo con el Anexo 7.		
Anexo 8	4.1.3.6 En su caso, escrito bajo protesta de decir verdad que el licitante cuenta con estratificación como micro, pequeña o mediana empresa, de acuerdo con el Anexo 8.		
Escrito CompraNet	4.1.3.7 Escrito libre en el que manifieste su aceptación de que se tendrán como no presentadas sus proposiciones y, en su caso, la documentación requerida, cuando el archivo electrónico en el que se contengan las proposiciones y/o demás información no pueda abrirse por tener algún virus informático o por cualquier otra causa ajena al IMSS, en términos de lo dispuesto por el numeral 29 del “Acuerdo por el que se establecen las disposiciones que deberán observar para la utilización del sistema electrónico de información pública gubernamental, denominado CompraNet”.		
Anexo 11	Escrito para solicitar la clasificación de la información entregada por el licitante.		
Anexo 15	Modelo de convenio de proposición conjunta.		
Referencia	**Documento de la propuesta económica**	**Presentado**	
		Si	**No**
Anexo 9	Formato de propuesta Económica.		

Anexo 11.- Formato información reservada y confidencial.

Ciudad de México, a __ de _____ de 20__.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones e Infraestructura
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

___(Nombre) , en mi carácter de _____, de la ___(Persona Física o Moral)___, manifiesto por medio de la presente que los documentos contenidos en mi propuesta y remitida a la convocante para la licitación pública nacional Núm. _____que contiene a su vez información de carácter Reservada y Confidencial con fundamento en términos de lo dispuesto por los artículos 97, 98, 110 fracción XIII, 111 y 113 de la Ley Federal de Transparencia y Acceso a la Información Pública, deberá indicar si en los documentos que proporcionan al IMSS se contiene información de carácter confidencial o comercial reservada, señalando los documentos o las secciones de éstos que la contengan, así como el fundamento por el cual considera que tengan ese carácter.

(El licitante deberá señalar y fundamentar los numerales de su proposición administrativa-legal y/o técnica que considere información confidencial y/o comercial reservada.). Cabe señalar que de no clasificarse la información por parte del licitante en los términos señalados, la información presentada como parte de su proposición técnica – legal - económica tendrá tratamiento de información de carácter público.

Relación de documentos:

Ejemplos:

Protesto lo necesario

_____
(Nombre y Firma del Apoderado o Representante Legal del Licitante)

Anexo 12.- Escrito de manifestación 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.

(Escrito en original, preferentemente en papel membretado y firma autógrafa del licitante o representante legal)

Ciudad de México, a _____ de _____de 2020.

Instituto Mexicano del Seguro Social
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
P r e s e n t e

PROCEDIMIENTO No. _____

PARA PERSONAS MORALES:

_____, en mi carácter de _____, de la ___(Persona Moral)___, manifiesto bajo protesta de decir verdad que los siguientes socios o accionistas

1.
2.
3.

No desempeñan empleo, cargo o comisión en el servicio público y no se actualiza un Conflicto de Interés.

(En caso de algún socio o accionista desempeñe empleo, cargo o comisión en el servicio público, se deberá indicar el nombre del socio o accionista)

1.
2.
3.

Independientemente de desempeñar empleo, cargo o comisión en el servicio público, con la formalización del contrato correspondiente, no se actualiza un Conflicto de Interés.

PARA PERSONA FÍSICAS:

_____, manifiesto bajo protesta de decir verdad que no desempeño empleo, cargo o comisión en el servicio público y no se actualiza un Conflicto de Interés.

O

_____, manifiesto bajo protesta de decir verdad que a pesar de desempeñar empleo, cargo o comisión en el servicio público y no se actualiza un Conflicto de Interés.

_____

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

Anexo 13.- Escrito de interés.

Ciudad de México, a _____ de _____de 20__

____(Nombre)_____ manifiesto bajo protesta de decir verdad, que se tiene interés en participar en la presente Licitación Pública Nacional Electrónica Núm. _____ y en su caso ***solicitar aclaraciones*** a los aspectos contenidos en la convocatoria, por si o a nombre y representación de.__(Persona Física o Moral)__.

Datos Personas Morales y Físicas.

Registro Federal de Contribuyentes.	
Domicilio.	
Calle y Número.	
Colonia.	Demarcación Territorial o Municipio.
Código Postal.	Entidad Federativa.
Teléfono Fijo.	Teléfono Móvil.
Correo Electrónico.	
Apoderado Legal o Representante. (Nombre, Domicilio, Teléfonos y Correo Electrónico)	
Documento para Acreditar Personalidad y Facultades. (Escritura Pública y Modificaciones, Fecha, y Datos del Notario Público)	

Datos Personas Morales.

Número de la Escritura Pública en la que consta su Acta Constitutiva.		Fecha.
Nombre, Número y Domicilio del Notario Público (ante el cual se dio fe de la misma).		
Fecha y Datos de su Inscripción en el Registro Público de Comercio.		
Descripción del Objeto Social.		
Relación de Accionistas.		
Apellido Paterno	Apellido Materno	Nombre(s)
Reformas al Acta Constitutiva que incidan con el objeto del procedimiento (Señalar Nombre, Número y Circunscripción del Notario o Fedatario Públicos que las protocolizó, así como la Fecha y los datos de su Inscripción en el Registro Público de la Propiedad)		

Protesto lo necesario

_____

(Nombre y firma del apoderado o representante legal del licitante)

Anexo 13.1- Formato de solicitud de aclaraciones.

PROCEDIMIENTO:		**FECHA:**	
NOMBRE O RAZÓN SOCIAL DEL LICITANTE			
DOMICILIO			
R.F.C.			
TELÉFONO			
CORREO ELECTRÓNICO			

No. de pregunta	Numeral de la Convocatoria	Pregunta y/o aclaración	Respuesta IMSS
1.-			
2.-			
3.-			
4.-			
5.-			
6.-			
7.-			
8.-			
9.-			
10.-			

Instructivo de llenado

Concepto	Descripción
No. de pregunta	**Se refiere al número consecutivo de la pregunta o aclaración formulada por el licitante**
Numeral de la convocatoria.	**Los licitantes deberán indicar el numeral específico de la convocatoria sobre el cual deseen formular preguntas o solicitar aclaraciones.**
Pregunta y/o aclaración	**Las preguntas o solicitudes de aclaración versarán exclusivamente sobre el contenido de la convocatoria podrán agregar filas al formato de acuerdo al número de solicitudes de solicitudes de aclaración.**

Representante Legal
del Licitante

_____
Nombre Y Firma

Anexo 14.- Modelo de contrato.

Contrato (indicar en su caso, si se trata de un contrato Abierto o Plurianual) para la prestación de Servicios Administrados de Seguridad Integral, que celebran, por una parte, el **INSTITUTO MEXICANO DEL SEGURO SOCIAL**, que en lo sucesivo se denominará **"EL INSTITUTO"**, representado en este acto por el **Dr. Alberto Flavio Balderas Hernández**, en su carácter de Apoderado (a) Legal, y, por la otra parte, la empresa denominada _____, a quien en lo sucesivo se le denominará **"EL PROVEEDOR"**, representada por _____, en su carácter de Representante Legal, y a quienes en forma conjunta se les denominará **"LAS PARTES",** al tenor de las Declaraciones y Cláusulas siguientes:

(en caso de participación conjunta, de deberá cambiar la redacción a: y, por la otra, _____ representada por el/la C._____ en su carácter de Representante Legal, en participación conjunta con _____, representada por el/la C. _____, en su carácter de Representante Legal, a quienes en forma conjunta o individualmente de les denominará en lo sucesivo **"EL PROVEEDOR"** y en forma conjunta con **"EL INSTITUTO"** se les denominará **"LAS PARTES"**, al tenor de las Declaraciones y Cláusulas siguientes:)

D E C L A R A C I O N E S

I.- "EL INSTITUTO" declara, a través de su Apoderado (a) Legal que:

I.1.- Es un Organismo Descentralizado de la Administración Pública Federal con personalidad jurídica y patrimonio propios, que tiene a su cargo la organización y administración del Seguro Social, como un servicio público de carácter nacional, en términos de los artículos 4º y 5º de la Ley del Seguro Social.

I.2.- Está facultado para contratar los servicios necesarios, en términos de la legislación vigente, para la consecución de los fines para los que fue creado, de conformidad con el artículo 251, fracción IV de la Ley del Seguro Social.

I.3.- El Dr. Alberto Flavio Balderas Hernández, en su carácter de Titular de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos, cuenta con las facultades suficientes para suscribir el presente instrumento jurídico en su calidad de Apoderado Legal, de conformidad con lo establecido en el artículo 268 A de la Ley de Seguro Social, y acredita su personalidad mediante el testimonio de la Escritura Pública número ___ de fecha _____, otorgada ante la fe del Licenciado _____, Titular de la Notaría Pública Número ___ del _____, e inscrita en el Registro Público de Organismos Descentralizados bajo el folio número _____, de fecha _____; manifiesta bajo protesta de decir verdad que las facultades que le fueron conferidas no le han sido revocadas, modificadas, ni restringidas en forma alguna en cumplimiento a los artículos 24 y 25 de la Ley Federal de las Entidades Paraestatales.

NOTA: *En tratándose de contratos plurianuales que deba suscribir el Director General del Instituto, deberá insertarse, en sustitución del párrafo que antecede, el texto siguiente:*

El Dr. Alberto Flavio Balderas Hernández, se encuentra facultado para suscribir el presente instrumento jurídico en representación de ***"EL INSTITUTO"*** *con fundamento en los artículos 268, fracción III, y 277 F, cuarto párrafo, de la Ley del Seguro Social y 66, fracción I del Reglamento Interior del Instituto Mexicano del Seguro Social, y acredita su personalidad mediante el testimonio de la Escritura Pública número _____, de fecha _____ de _____de _____, pasada ante la fe del _____, titular de la Notaría Pública número __ de la _____, en la que consta la protocolización de su nombramiento como Director General de "****EL INSTITUTO****", para celebrar en forma indelegable, contratos plurianuales, cuya prestación genere una obligación de pago para "****EL INSTITUTO****", igual o mayor a 190,150 veces la Unidad de Medida y Actualización (UMA), en alguno de sus años de vigencia y manifiesta bajo protesta de decir verdad, que las facultades que le fueron conferidas no le han sido revocadas, modificadas, ni restringidas en forma alguna.*

El *Nombramiento,* se encuentra inscrito en el Registro Público de Organismos Descentralizados *bajo el folio número _____, de fecha _____, y manifiesta bajo protesta de decir verdad que las facultades que le fueron conferidas no le han sido revocadas, modificadas, ni restringidas en forma alguna.*

I.4.- El Dr. Alberto Flavio Balderas Hernández, Titular de la Coordinación Técnica de Adquisición de Bienes de Inversión y Activos de **"EL INSTITUTO"**, funge como Administrador del presente contrato, responsable de dar seguimiento y verificar el cumplimiento de los derechos y obligaciones establecidos en este instrumento jurídico, de conformidad con lo dispuesto en el artículo 84 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

NOTA: En contratos plurianuales en los que su administración se ejerza en Órganos de Operación Administrativa Desconcentrada, se insertará la siguiente declaración del IMSS[1]:

El C. _____, en su calidad de Titular de la Delegación (Estatal o Regional) del IMSS en _____ y como superior jerárquico de los servidores públicos encargados de administrar el presente instrumento jurídico suscrito dentro de la circunscripción territorial de dicha Delegación, suscribe el presente instrumento jurídico con las facultades que le confieren los artículos 2, fracción IV, inciso a), 8, 139, 141, 144 fracciones I y XXIII, y 155 fracción___, del Reglamento Interior del Instituto Mexicano del Seguro Social, y de acuerdo con el poder que le fue conferido en la Escritura Pública número _____, de fecha _____, otorgada ante la fe del Licenciado_____, Notario Público número _____, de la Ciudad de _____, inscrita en el Registro Público de Organismos Descentralizados, con el número de folio _____, de fecha _____, en cumplimiento a los artículos 24 y 25, fracción IV, de la Ley Federal de las Entidades Paraestatales.

[1] Adecuar en UMAES.

I.5.- Para el cumplimiento de sus funciones y la realización de sus actividades, se requiere de la prestación de Servicios Administrados de Seguridad Integral, solicitado por el Coordinador de Mantenimiento y Operación de Servicios de Cómputo.

I.6.- Para cubrir las erogaciones que se deriven del presente contrato, cuenta con los recursos disponibles suficientes, no comprometidos, en la cuenta número _____ de conformidad con el Dictamen de Disponibilidad Presupuestal Previo con número de folio 0000001073-2021, emitido por la Titular de la División de Control y Seguimiento al Gasto de Operación de fecha _____, mismo que se agrega al presente contrato como **Anexo _ (__)**.

NOTA: En aquellos contratos que sean suscritos en un ejercicio presupuestario anterior al del inicio de su vigencia, de conformidad con lo dispuesto en el artículo 25, segundo párrafo de la LAASSP, deberá agregarse el siguiente párrafo:

Los recursos presupuestarios a ejercer con motivo del presente instrumento jurídico, quedan sujetos para fines de ejecución y pago, a la disponibilidad presupuestaria con que cuente **"EL INSTITUTO"**, conforme al Presupuesto de Egresos de la Federación que apruebe la H. Cámara de Diputados del Congreso de la Unión, sin responsabilidad alguna para **"EL INSTITUTO"**.

NOTA: En tratándose de aquellos contratos que rebasen las asignaciones del ejercicio presupuestario correspondiente, de conformidad con lo dispuesto en el artículo 277 F, de la Ley del Seguro Social, se deberá insertar el texto siguiente:

Los compromisos excedentes no cubiertos durante el presente ejercicio, quedan sujetos para fines de ejecución y pago, a la disponibilidad presupuestaria con que cuente **"EL INSTITUTO"**, conforme al Presupuesto de Egresos de la Federación que apruebe la H. Cámara de Diputados del Congreso de la Unión, sin responsabilidad alguna para **"EL INSTITUTO"**.

NOTA: Incluir como **declaración** opcional del IMSS, los datos de autorización del Consejo Técnico, tratándose de contratos plurianuales, conforme a lo siguiente:

*De conformidad con lo dispuesto en el artículo 277 F, primer párrafo, de la Ley del Seguro Social, el Consejo Técnico de **"EL INSTITUTO"**, autorizó la celebración del presente contrato plurianual, y el presupuesto a ejercer en el mismo, conforme al Acuerdo _____, emitido por el citado Órgano de Gobierno, el día ___ de _____ de ____.*

I.7.- Con fecha _____, la Coordinación Técnica de _____, a través de la División de _____, mediante (acta de _____ u oficio de _____), notificó a **"EL PROVEEDOR"** la adjudicación del procedimiento de Licitación Pública Nacional Electrónica número LA-050GYR019-E__-2021, con fundamento en lo dispuesto en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos y de conformidad con los artículos 26, fracción I, 26 Bis fracción II y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, los relativos de su

Reglamento y demás disposiciones aplicables en la materia, como se detalla en el **Anexo _ (__)**, del presente instrumento jurídico.

I.8.- De conformidad con lo previsto en el artículo 81, fracción IV del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en caso de discrepancia entre el contenido en la _____ y el presente instrumento jurídico, prevalecerá lo establecido en la _____ y, en su caso, la junta de aclaraciones respectiva. (En su caso).

I.9.- Señala como su domicilio para todos los efectos de este acto jurídico, el ubicado en Calle Durango número 291, piso PH, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, en la Ciudad de México.

II.- "EL PROVEEDOR" declara, a través de su Representante Legal, que:

EN CASO DE SER PERSONA FÍSICA:

II.1.- Acredita su personalidad para la firma de este contrato, mediante copia certificada de su _____ (Acta de nacimiento, carta de naturalización), folio número _____, expedida por _____ de fecha _____ e identificación oficial consistente en el documento _____ expedido por _____, con número _____, de fecha o año de registro _____.

II.2.- Se encuentra Inscrita en el Régimen de _____, y su actividad económica consiste en _____ (actividades vinculantes al objeto del contrato).

EN CASO DE PERSONA MORAL.

II.1.- Es una persona moral constituida de conformidad con las leyes de los Estados Unidos Mexicanos, según consta en la Escritura Pública número _____ de fecha _____, pasada ante la fe del (la) Licenciado (a) _____, Titular de la Notaría Pública número ___ de ___, e inscrita en el Registro Público de la Propiedad y de Comercio de _____, con el folio mercantil número _____.

II.2.- _____, acredita su personalidad en términos de la Escritura Pública número ___ de fecha _____, pasada ante la fe del (la) Licenciado (a) _____, Titular de la Notaría Pública número ____ de _____, e inscrita en el Registro Público de la Propiedad y de Comercio de _____, con el folio mercantil número _____, y manifiesta bajo protesta de decir verdad que las facultades que le fueron conferidas no le han sido revocadas, modificadas ni restringidas en forma alguna.

II.3.- De acuerdo con sus Estatutos, su objeto social consiste, entre otros en: _____.

II.4.- Cuenta con los registros siguientes:

- Registro Federal de Contribuyentes número: _____.
- Registro Patronal ante **"EL INSTITUTO"** y **EL INFONAVIT** número: _____.

EN CASO DE QUE EL MONTO DEL CONTRATO SEA MAYOR A $300,000.00 SIN I.V.A., SE DEBEN SEÑALAR LAS DECLARACIÓNES CORRESPONDIENTES A LA OPINIÓN DE CUMPLIMIENTO EN MATERIA FISCAL Y DE SEGURIDAD SOCIAL (SAT E IMSS).

II.5.- Cuenta, al igual que su subcontratante, con el documento vigente expedido por el Servicio de Administración Tributaria (SAT), de opinión de cumplimiento de obligaciones fiscales en sentido positivo, de conformidad con el artículo 32 D del Código Fiscal de la Federación, así como a lo dispuesto por las Reglas 2.1.31 y 2.1.39 de la Resolución Miscelánea Fiscal para 2019, publicada el 29 de abril de 2019, del cual (de los cuales) presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.
(Lo resaltado en amarillo solo se debe incluir cuando exista subcontratación).

II.6.- Sus trabajadores se encuentran inscritos en el régimen obligatorio del Seguro Social, y al corriente en el pago de las cuotas obrero patronales a que haya lugar, conforme a lo dispuesto en la Ley del Seguro Social, cuyas constancias correspondientes debidamente emitidas por **"EL INSTITUTO"** exhibe para efectos de la suscripción del presente instrumento jurídico. (En caso de aplicar)

II.7.- Cuenta, al igual que su subcontratante, con el documento correspondiente, vigente, expedido por **"EL INSTITUTO"** sobre el cumplimiento de sus obligaciones fiscales en materia de seguridad social, conforme al Acuerdo ACDO.SA1.HCT.101214/281.P.DIR dictado por el H. Consejo Técnico de **"EL INSTITUTO"** en la sesión ordinaria celebrada el 10 de diciembre de 2014, publicado en el Diario Oficial de la Federación el 27 de febrero de 2015 y su modificación publicada en el mismo de fecha 3 de abril de 2015, del cual (de los cuales) presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.
(Lo resaltado en amarillo solo se debe incluir cuando exista subcontratación).

En caso de incumplimiento en sus obligaciones en materia de seguridad social, solicita se apliquen los recursos derivados del presente contrato, contra los adeudos que, en su caso, tuviera a favor de **"EL INSTITUTO".** (En caso de aplicar)

II.8.- Cuenta, al igual que su subcontratante, con el documento correspondiente, vigente, expedido por el INFONAVIT en los términos del Acuerdo del H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores por el que se emiten las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos, publicado en el Diario Oficial de la Federación el 28 de junio de 2017, del cual (de los cuales) presenta copia a **"EL INSTITUTO"** para efectos de la suscripción del presente contrato.
(Lo resaltado en amarillo solo se debe incluir cuando exista subcontratación).

II.9.- Manifiesta bajo protesta de decir verdad, no encontrarse en los supuestos de los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En caso de que **"EL PROVEEDOR"** se encuentre en los supuestos señalados anteriormente, el contrato será nulo previa determinación de la autoridad competente de

conformidad con lo establecido en el artículo 15 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

II.10.- Conforme a lo previsto en los artículos 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 107 de su Reglamento, **"EL PROVEEDOR"**, en caso de auditorías, visitas o inspecciones que practique la Secretaría de la Función Pública y el Órgano Interno de Control en **"EL INSTITUTO",** deberá proporcionar la información relativa al presente contrato que en su momento se requiera.

II.11.- Reúne las condiciones de organización, experiencia, personal capacitado y demás recursos técnicos, humanos y económicos necesarios, así como con la capacidad legal suficiente para cumplir con las obligaciones que contrae en el presente contrato.

II.12.- Para efectos legales y de notificación relacionados con el presente contrato señala como domicilio para oír y recibir toda clase de notificaciones y documentos, el ubicado en _____ número _____, Colonia _____, Demarcación Territorial_____, Código Postal _____, Ciudad de México, teléfonos _____, correo electrónico: _____.

Hechas las declaraciones anteriores, **"LAS PARTES"** convienen en otorgar el presente contrato, de conformidad con las siguientes:

EN CASO DE QUE SE HAYA ADJUDICADO A UN PROVEEDOR EN PARTICIPACIÓN CONJUNTA, SE INCLUIRÁ EL SIGUIENTE TEXTO:

III.- "EL PROVEEDOR", declara conjuntamente que:

III.1.- Han celebrado convenio de participación conjunta, cuyas obligaciones deberán cumplirse en términos del mismo, el cual se integra al presente instrumento jurídico como **Anexo __ (__)**.

III.2.- Conocen el contenido y los requisitos que establece la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento, la Convocatoria y sus Anexos.

C L Á U S U L A S

PRIMERA.- OBJETO DEL CONTRATO.- "EL PROVEEDOR" se obliga a prestar el servicio de Servicios Administrados de Seguridad Integral, cuyas características, cantidades, alcances y especificaciones se describen en los **Anexos** _ **(__)** y __ **(__)** del presente instrumento jurídico, así como a las condiciones de la Convocatoria, Junta de Aclaraciones y Acta de _____del procedimiento del cual deriva el presente contrato, disponibles para su consulta en el Portal de Compras Gubernamentales Compranet.

REDACCIÓN PARA CONTRATO CERRADO

SEGUNDA.- IMPORTE DEL CONTRATO.- El importe del presente contrato es por la cantidad de **$_____.00 (_____ 00/100 M.N.)**, (en caso de aplicar) más/incluye el Impuesto al Valor Agregado (I.V.A.) o en su defecto (la tasa

aplicable correspondiente al Impuesto al Valor Agregado (I.V.A.) es 0%), de conformidad con los precios unitarios que se indican en el **Anexo _ (___)** del presente contrato.

"LAS PARTES" convienen que el presente contrato se celebra bajo la modalidad de precios fijos, de acuerdo con los precios unitarios pactados, por lo que el monto de los mismos no cambiará durante la vigencia del presente instrumento jurídico.

REDACCIÓN PARA CONTRATO ABIERTO

SEGUNDA.- IMPORTE DEL CONTRATO.- El importe del presente contrato es por la cantidad mínima de **$_____.00 (_____PESOS 00/100 M.N.)**, (en caso de aplicar) más/incluye el Impuesto al Valor Agregado (I.V.A.) o en su defecto (la tasa aplicable correspondiente al Impuesto al Valor Agregado (I.V.A.) es 0%), y por la cantidad máxima de **$_____.00 (_____PESOS 00/100 M.N.)** (en caso de aplicar) más/incluye el Impuesto al Valor Agregado (I.V.A.) o en su defecto (la tasa aplicable correspondiente al Impuesto al Valor Agregado (I.V.A.) es 0%), de conformidad con los precios unitarios que se indican en el **Anexo _ (__)** del presente contrato.

"LAS PARTES" convienen que el presente contrato se celebra bajo la modalidad de precios fijos, de acuerdo con los precios unitarios pactados, por lo que el monto de los mismos no cambiará durante la vigencia del presente instrumento jurídico.

EN CASO DE TRATARSE DE UN CONTRATO PLURIANUAL, SE TENDRÁN QUE SEÑALAR LOS IMPORTES A EJERCER POR CADA EJERCICIO FISCAL.

TERCERA.- FORMA Y CONDICIONES DE PAGO.- Se efectuarán pagos _____ a **"EL PROVEEDOR"** una vez proporcionado los servicios, de conformidad con lo dispuesto en los artículos 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 93 de su Reglamento, así como por lo establecido en los Términos y Condiciones que se agregan al presente contrato en el **Anexo _ (_)**.

El pago del servicio se realizará en _____de **"EL INSTITUTO"**, cuyos domicilios se relacionan en el **Anexo _ (__)** del presente contrato, una vez que el servicio haya sido proporcionado conforme a _____:

(Agregar párrafos correspondientes a pago conforme a cada caso en particular)

El pago se realizará en pesos mexicanos, en los plazos normados por la Dirección de Finanzas en el "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos", sin que éstos rebasen los 20 (veinte) días naturales posteriores a aquel en que **"EL PROVEEDOR"** presente en las áreas de trámite de erogaciones la representación impresa del Comprobante Fiscal Digital por Internet (CFDI), siempre y cuando se cuente con la suficiencia presupuestal, así como con la documentación comprobatoria que acredite la prestación de los servicios, y se indique en dicha documentación los servicios proporcionados, número de proveedor, número de contrato, número de fianza y denominación social de la afianzadora, en su caso.

"EL PROVEEDOR" deberá expedir sus CFDI, en el esquema de facturación electrónica, con las especificaciones normadas por el Servicio de Administración Tributaria (SAT) a nombre del Instituto Mexicano del Seguro Social, con Registro Federal de Contribuyentes IMS421231I45, domicilio en Avenida Paseo de la Reforma número 476, Colonia Juárez, Código Postal 06600, Demarcación Territorial Cuauhtémoc, en la Ciudad de México.

"EL PROVEEDOR", para cada uno de los pagos que efectivamente reciba, de acuerdo con esta cláusula, deberá de expedir a nombre de **"EL INSTITUTO"**, el "CFDI con complemento para la recepción de pagos", también denominado "recibo electrónico de pago", el cual elaborará dentro de los plazos establecidos por las disposiciones fiscales vigentes y lo cargará en el portal de servicios a proveedores de la página de **"EL INSTITUTO"**.

Para la validación de dichos comprobantes **"EL PROVEEDOR"** deberá cargar en internet, a través del portal de servicios a proveedores de la página de **"EL INSTITUTO"** el archivo en formato XML, la validez de los mismos será determinada durante la carga y únicamente los comprobantes válidos serán procedentes para pago.

El pago se realizará mediante transferencia electrónica de fondos, a través del esquema electrónico interbancario que **"EL INSTITUTO"** tiene en operación; para tal efecto, **"EL PROVEEDOR"** proporcionará con oportunidad su número de cuenta, CLABE, banco y sucursal, a menos que **"EL PROVEEDOR"** acredite en forma fehaciente la imposibilidad para ello.

El pago se depositará en la fecha programada, a través del esquema interbancario si la cuenta bancaria de **"EL PROVEEDOR"** está contratada con BANORTE, BBVA BANCOMER, HSBC, SCOTIABANK INVERLAT o a través del esquema interbancario vía SPEI (Sistema de Pagos Electrónicos Interbancarios), si la cuenta pertenece a un banco distinto a los antes mencionados.

El administrador del contrato será quien dará la autorización para que la Dirección de Finanzas proceda a su pago de acuerdo con lo normado en el anexo "Cuentas Contables" del "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos".

En ningún caso se deberá autorizar el pago de los servicios, sí no se ha determinado, calculado y notificado a **"EL PROVEEDOR"** las penas convencionales o deducciones pactadas en el presente contrato, así como su registro y validación en el Sistema PREI Millenium.

"EL PROVEEDOR" se obliga a no cancelar ante el SAT los CFDI a favor de **"EL INSTITUTO"** previamente validados en el portal de servicios a proveedores, salvo justificación y comunicación por parte del mismo al administrador del contrato para su autorización expresa, debiendo éste informar a las áreas de trámite de erogaciones de dicha justificación y reposición del CFDI en su caso.

"EL PROVEEDOR" deberá entregar el CFDI a favor de **"EL INSTITUTO"** por el importe de la aplicación de la pena convencional por atraso.

Las Unidades Responsables del Gasto (URG) deberán registrar el contrato y su dictamen presupuestal en el Sistema PREI Millenium para el trámite de pago correspondiente.

"EL PROVEEDOR", durante la vigencia del presente contrato, se obliga a presentar a **"EL INSTITUTO"**, junto con el CFDI respectivo la constancia positiva y vigente emitida por el INFONAVIT y la "Opinión de cumplimiento de obligaciones en materia de seguridad social", vigente y positiva, la cual puede ser consultada a través de la página electrónica http://www.imss.gob.mx/tramites/cumplimiento-obligaciones, en los términos requeridos por **"EL INSTITUTO"**. (En caso de aplicar)

Los servicios cuya recepción no genere alta a través del SAI ni realice al PREI Millenium de manera electrónica, deberán contener la firma de recepción y de autorización para el trámite de pago de acuerdo a lo establecido en el "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos" vigente, así como el Acta de Entrega-Recepción (en caso de aplicar).

Para que **"EL PROVEEDOR"** pueda celebrar un contrato de cesión de derechos de cobro, deberá notificarlo por escrito a **"EL INSTITUTO"** con un mínimo de 5 días naturales anteriores a la fecha de pago programada; el administrador del contrato o, en su caso, el Titular del Área Requirente, deberá entregar los documentos sustantivos de dicha cesión al área responsable de realizar el proceso, conforme al "Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos".

De igual forma procederá en caso de que celebre contrato de cesión de derechos de cobro a través de factoraje financiero conforme al Programa de Cadenas Productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo.

En caso de que **"EL PROVEEDOR"** reciba pagos en exceso deberá reintegrar las cantidades pagadas en exceso más los intereses correspondientes, conforme a la tasa que establezca la Ley de Ingresos de la Federación, en los casos de prórroga para el pago de créditos fiscales. Los intereses se calcularán sobre las cantidades en exceso 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 **"EL INSTITUTO"**.

En caso de que **"EL PROVEEDOR"** presente su CFDI con errores o deficiencias, conforme a lo previsto en los artículos 89 y 90 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"EL INSTITUTO"** dentro de los 3 (tres) días hábiles siguientes a la recepción de la misma, indicará por escrito a **"EL PROVEEDOR"** las deficiencias o errores que deberá corregir. El periodo que transcurra a partir de la entrega del citado escrito y hasta que **"EL PROVEEDOR"** presente las correcciones no se computará dentro del plazo estipulado para el pago.

El administrador del contrato llevará a cabo la valoración de la procedencia del pago por concepto de gastos no recuperables conforme a lo previsto en los artículos 101 y 102 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en relación con los artículos 38, 46, 54 Bis y 55 Bis, segundo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, previa solicitud por escrito a **"EL PROVEEDOR"**, acompañada de los documentos siguientes:

• Copia de la identificación oficial vigente con fotografía y firma de la persona que haya realizado los trámites relacionados con el procedimiento de contratación.

• El CFDI que reúna los requisitos de los artículos 29 y 29-A del CFF, 37 al 40 del RCFF y, en su caso, la Resolución de la Miscelánea Fiscal del Ejercicio que corresponda.

• La solicitud la realizará al administrador del contrato para la determinación de la procedencia del pago y, en su caso, elaborar el finiquito y remitirlo para el pago respectivo a la Coordinación de Contabilidad y Trámite de Erogaciones, dependiente de la Dirección de Finanzas, o ante la Jefatura de Servicios de Finanzas o de la UMAE correspondiente. (Eliminar lo marcado cuando el pago se efectúe a Nivel Central o ante los Órganos de Operación Administrativa Desconcentrada).

El pago de los servicios quedará condicionado proporcionalmente al pago que **"EL PROVEEDOR"** deba efectuar por concepto de penas convencionales por atraso y/o por concepto de deducciones. En ambos casos, **"EL INSTITUTO"** realizará las retenciones correspondientes sobre el CFDI que se presente para pago. En el entendido de que en el supuesto de que sea rescindido el contrato, no procederá el cobro de dichas penalizaciones, ni la contabilización de las mismas para hacer efectiva la garantía de cumplimiento, de conformidad con lo establecido por el artículo 95 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

PÁRRAFO PARA EN CASO DE QUE EXISTA PARTICIPACIÓN CONJUNTA.

Para efectos del cobro de sus CFDI, deberá presentarse por **"EL PROVEEDOR"** que se haya establecido en el convenio de participación conjunta, el cual se agrega al presente instrumento jurídico como **Anexo __ (____)**, en el entendido de que **"EL INSTITUTO"** no será responsable de la manera en que hayan acordado la distribución del pago.

CUARTA.- PLAZO, LUGAR Y CONDICIONES DE LA PRESTACIÓN DEL SERVICIO.- "EL PROVEEDOR" se obliga a prestar a **"EL INSTITUTO"** el servicio que se menciona en la Cláusula Primera del presente instrumento jurídico, conforme a lo establecido en el Anexo Técnico y en los Términos y Condiciones integrados en el **Anexo __ (___)** de contrato, apegándose a las condiciones, alcances y características detalladas en la Convocatoria, Junta de Aclaraciones (en su caso) y Acta de Fallo del procedimiento del cual deriva el presente contrato, disponibles para su consulta en el Portal de Compras Gubernamentales CompraNet, y de acuerdo con lo siguiente:

PLAZO DE LA PRESTACIÓN DEL SERVICIO.- El servicio iniciará a partir del día hábil siguiente a la notificación de adjudicación y hasta el 31 de diciembre de 2021.

EN CASO DE APLICAR Lo anterior de conformidad con los artículos 46 de la LAASSP y 84 de su Reglamento.

LUGAR DE LA PRESTACIÓN DEL SERVICIO.- "EL PROVEEDOR" se obliga expresamente a prestar el servicio en _____.

CONDICIONES DE LA PRESTACIÓN DEL SERVICIO.- "EL PROVEEDOR" se obliga con **"EL INSTITUTO"** a cumplir con las condiciones del servicio, de acuerdo a lo establecido en los Términos y Condiciones que se integran en el presente contrato como **Anexo** _ **(__)**, así como a lo ofrecido en sus propuestas técnica y económica que se agregan en el **Anexo** __ **(__)**.

EN CASO DE EXISTA PARTICIPACIÓN CONJUNTA

"EL PROVEEDOR" convino en conjuntar sus recursos técnicos, legales, administrativos, económicos y financieros por lo que se obliga a proporcionar los servicios objeto del presente contrato en términos del convenio de participación conjunta, integrado en el **Anexo** __ **(___)**, del presente contrato.

"EL PROVEEDOR" conviene que en el supuesto de que cualquiera se declare en quiebra o suspensión de pagos, no los libera de cumplir con sus obligaciones, por lo que cualquiera de ellas que subsista, acepta y se obliga expresamente a responder solidariamente de las obligaciones contractuales a que hubiere lugar.

Cabe resaltar que mientras no se cumpla con las condiciones de la prestación del servicio establecidas, **"EL INSTITUTO"** no dará por aceptado el servicio objeto de este contrato.

QUINTA.- VIGENCIA.- "LAS PARTES" convienen que la vigencia del presente contrato será a partir de la firma y hasta el 31 de diciembre de 2021.

SEXTA.- TRANSFERENCIA DE DERECHOS DE COBRO.- "EL PROVEEDOR" se obliga a no transferir o ceder por ningún título, en forma total o parcial, a favor de cualquier otra persona física o moral, sus derechos y obligaciones que se deriven del presente contrato; a excepción de los derechos de cobro, debiendo, en este caso, solicitar por escrito el consentimiento de **"EL INSTITUTO"** a través del administrador del presente contrato para tal efecto.

"EL PROVEEDOR" deberá presentar la solicitud correspondiente dentro de los 5 (cinco) días naturales anteriores a la fecha de pago programada, a la que deberá adjuntar una copia de los contra-recibos cuyo importe transfiere, y demás documentos sustantivos de dicha transferencia, lo cual será necesario para efectuar el pago correspondiente.

Si con motivo de la transferencia de los derechos de cobro solicitada por **"EL PROVEEDOR"** se origina un retraso en el pago, no procederá el pago de los gastos financieros a que hace referencia el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

SÉPTIMA.- RESPONSABILIDAD.- Conforme a lo previsto en el artículo 53 de la LAASSP, **"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, llegue a causar a **"EL INSTITUTO"** y/o a terceros. Asimismo, se obliga a cumplir cabalmente el objeto del presente contrato y a entera satisfacción de **"EL INSTITUTO"**; por lo que responderá de los defectos y vicios ocultos que afecten la calidad de los servicios entregados, tanto durante el tiempo de vigencia de este contrato como durante la vida útil del bien, así como a responder de cualquier otra responsabilidad en que hubiere incurrido en los términos señalados en el Código Civil Federal.

Lo anterior, de acuerdo a la Garantía del Servicio descrita en la Cláusula _____, inciso ___ del presente contrato. (En caso de aplicar).

OCTAVA.- CONTRIBUCIONES.- Los impuestos y/o derechos que procedan con motivo del servicio objeto del presente contrato, serán pagados por **"EL PROVEEDOR"** conforme a la legislación aplicable en la materia.

"EL INSTITUTO" sólo cubrirá el Impuesto al Valor Agregado (I.V.A.), de acuerdo con lo establecido en las disposiciones fiscales vigentes en la materia. (EN CASO DE APLICAR).

"EL PROVEEDOR", en su caso, cumplirá con la inscripción de sus trabajadores en el régimen obligatorio del Seguro Social, así como con el pago de las cuotas obrero-patronales a que haya lugar, conforme a lo dispuesto en la Ley del Seguro Social. **"EL INSTITUTO",** a través del Área fiscalizadora competente, podrá verificar en cualquier momento el cumplimiento de dicha obligación.

"EL PROVEEDOR" que tenga cuentas líquidas y exigibles a su cargo por concepto de cuotas obrero patronales, conforme a lo previsto en el artículo 40 B de la Ley del Seguro Social, acepta que **"EL INSTITUTO"** las compense con el o los pagos que tenga que hacerle por concepto de contraprestación por la contratación del servicio.

NOVENA.- PROPIEDAD INTELECTUAL, PATENTES Y/O MARCAS.- "EL PROVEEDOR" se obliga para con **"EL INSTITUTO"**, a responder por los daños y/o perjuicios que pudiera causar a **"EL INSTITUTO"** y/o a terceros, si con motivo de la prestación del servicio se violan derechos de autor, de patentes y/o marcas u otro derecho reservado a nivel Nacional o Internacional.

Por lo anterior, **"EL PROVEEDOR"** manifiesta en este acto bajo protesta de decir verdad, no encontrarse en ninguno de los supuestos de infracción a la Ley Federal del Derecho de Autor, ni a la Ley de la Propiedad Industrial.

En caso de que sobreviniera alguna reclamación en contra de **"EL INSTITUTO"** por cualquiera de las causas antes mencionadas, la única obligación de éste será la de dar aviso en el domicilio previsto en este instrumento jurídico a **"EL PROVEEDOR"**, para que éste lleve a cabo las acciones necesarias que garanticen la liberación de **"EL INSTITUTO"** de cualquier controversia o responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione.

Lo anterior de conformidad a lo establecido en el artículo 45, fracción XX de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

(SÓLO EN CASO DE APLICAR)
Asimismo, **"LAS PARTES"** se obligan a lo señalado en el numeral __ de los Términos y Condiciones que se agregan en el **Anexo __ (__)** del presente contrato.

DÉCIMA.- GARANTÍAS.- "EL PROVEEDOR" se obliga a entregar a **"EL INSTITUTO"** las garantías que a continuación se indican:

a) **DEL SERVICIO.- "EL PROVEEDOR"** se obliga a entregar al Administrador del Contrato, escrito preferentemente en papel membretado, en el cual garantice _____, firmado por su representante legal. (ADECUAR CONFORME PROCEDIMIENTO DE CONTRATACIÓN)

b) **DE CUMPLIMIENTO DEL CONTRATO.- "EL PROVEEDOR"** se obliga a entregar a más tardar dentro de los 10 (diez) días naturales posteriores a la firma de este instrumento jurídico (VERIFICAR PLAZO DE ENTREGA SEÑALADO EN EL PROCEDIMIENTO DE CONTRATACIÓN), en términos de la fracción II del artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, una garantía de cumplimiento de todas y cada una de las obligaciones a su cargo derivadas del presente contrato, mediante fianza expedida por compañía autorizada en los términos de la Ley de Instituciones de Seguros y de Fianzas a favor del "Instituto Mexicano del Seguro Social" por un monto equivalente al 10% (diez por ciento) sobre el importe total ó máximo que se indica en la Cláusula Segunda del presente contrato, sin considerar el Impuesto al Valor Agregado (I.V.A.), en Moneda Nacional.

EN CASO DE CONTRATOS PLURIANUALES:
La garantía de cumplimiento del contrato podrá ser por el 10% del monto total (o máximo si fuese contrato abierto) a erogar en el ejercicio fiscal de que se trate y que deberá ser renovada cada ejercicio por el monto que se ejercerá en el mismo, entregándose dentro de los primeros 10 días naturales del ejercicio que corresponda conforme lo prevé el artículo 87 del Reglamento de la LAASSP.

"EL PROVEEDOR" queda obligado a entregar a **"EL INSTITUTO"** la póliza de fianza antes señalada, en la División de Contratos, ubicada en Calle Durango número 291, 10º piso, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, en la Ciudad de México, apegándose al formato que para tal efecto se entregará en la referida División.

VERIFICAR VIGENCIA DE LA GARANTÍA EN LOS TÉRMINOS Y CONDICIONES.

Dicha póliza de garantía de cumplimiento del contrato se liberará de forma inmediata a **"EL PROVEEDOR"** una vez que **"EL INSTITUTO"** le otorgue autorización por escrito, para que éste pueda solicitar a la afianzadora

correspondiente la cancelación de la fianza, autorización que se entregará a **"EL PROVEEDOR"** siempre que demuestre haber cumplido con la totalidad de las obligaciones adquiridas por virtud del presente contrato; para lo anterior, deberá presentar mediante escrito la solicitud de liberación de la fianza en la División de Contratos, misma que llevará a cabo el procedimiento para su liberación y entrega.

ENDOSO DE LA GARANTÍA DE CUMPLIMIENTO.- En el supuesto de que **"EL INSTITUTO"** y por así convenir a sus intereses, decidiera modificar en cualquiera de sus partes el presente contrato**, "EL PROVEEDOR"** se obliga a otorgar el endoso de la póliza de garantía originalmente entregada, en el que conste las modificaciones o cambios en la respectiva fianza, observándose los mismos términos y condiciones señalados en la presente cláusula para la entrega de la garantía de cumplimiento, debiéndola entregar **"EL PROVEEDOR"** a más tardar dentro de los 10 (diez) días naturales posteriores a la firma del convenio respectivo.

(EN EL CASO DE APLICAR DE ACUERDO AL MONTO)

No obstante lo anterior, y toda vez que el monto del presente contrato es menor a 900 (novecientos) días de Unidad de Medida y Actualización (UMA), **"EL PROVEEDOR"** podrá presentar la garantía de cumplimiento de las obligaciones estipuladas, mediante cheque certificado, por un importe equivalente al 10% (diez por ciento) del monto total, sin considerar el Impuesto al Valor Agregado, en favor de **"EL INSTITUTO",** siendo necesario considerar lo siguiente:

a) El cheque debe expedirse a nombre del "Instituto Mexicano del Seguro Social".

b) Dicho cheque deberá ser resguardado, a título de garantía, por **"EL INSTITUTO"** en la _____.

c) El cheque será devuelto a solicitud, por escrito de **"EL PROVEEDOR"** el segundo día hábil posterior a que **"EL INSTITUTO"** constate el cumplimiento del presente instrumento, previa validación del Administrador del Contrato.

DÉCIMA PRIMERA.- EJECUCIÓN DE LA GARANTÍA DE CUMPLIMIENTO DE ESTE CONTRATO.- "EL INSTITUTO" llevará a cabo la ejecución de la garantía de cumplimiento de contrato en los casos siguientes:

a) Se rescinda administrativamente el presente contrato.

b) Durante su vigencia se detecten deficiencias, fallas o calidad inferior del servicio prestado, en comparación con lo ofertado.

c) Cuando en el supuesto de que se realicen modificaciones al contrato, **"EL PROVEEDOR"** no entregue en el plazo pactado el endoso o la nueva garantía, que ampare el porcentaje establecido para garantizar el cumplimiento del presente instrumento, de conformidad con la Cláusula ____, inciso __).(VERIFICAR)

d) Por cualquier otro incumplimiento de las obligaciones contraídas en este contrato

De conformidad con el artículo 81, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, la aplicación de la garantía de cumplimiento se hará efectiva _____
de manera proporcional al monto de las obligaciones incumplidas o
por el monto total de las obligaciones garantizadas. (Dependiendo del caso concreto)

DÉCIMA SEGUNDA.- PENAS CONVENCIONALES.- De conformidad con lo establecido en los artículos 45, fracción XIX, 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 95 y 96 de su Reglamento, la pena convencional aplicable a **"EL PROVEEDOR"**, por atraso en el cumplimiento de la prestación del servicio será del 0.2% (cero punto dos por ciento) por cada día de atraso, sin considerar el I.V.A., hasta el cumplimiento de su totalidad se calculará, conforme a lo señalado en el numeral ___ de los Términos y Condiciones incluidos en el **Anexo** _ **(___)** del presente contrato.

PARA EL CASO DE QUE EXISTAN VARIOS PORCENTAJES DE PENAS CONVENCIONALES, SE DEBERÁ USAR LA SIGUIENTE REDACCIÓN:
DÉCIMA SEGUNDA.- PENAS CONVENCIONALES.- De conformidad con lo establecido en los artículos 45, fracción XIX, 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 95 y 96 de su Reglamento, la pena convencional aplicable a **"EL PROVEEDOR"**, por atraso en el cumplimiento de la prestación del servicio será conforme a los conceptos y porcentajes señalados en el numeral ___de los Términos y Condiciones incluidos en el **Anexo** _ **(__)** del presente contrato.

El Administrador del presente contrato será el responsable de determinar, calcular y aplicar las penas convencionales, vigilando los correspondientes registro o captura y validación en el sistema PREI Millenium, así como de notificarlas a **"EL PROVEEDOR"** por escrito, por medios electrónicos u ópticos.

"EL INSTITUTO" descontará las cantidades que resulten de aplicar la pena convencional, sobre los pagos que deba cubrir a **"EL PROVEEDOR"**. Por lo tanto, **"EL PROVEEDOR"** autoriza a descontar las cantidades que resulten de aplicar las sanciones señaladas en párrafos anteriores, sobre los pagos que éste deba cubrirle a **"EL INSTITUTO"** durante el período en que incurra y/o se mantenga en atraso con motivo de la prestación del servicio.

Para autorizar el pago del servicio, previamente **"EL PROVEEDOR"** tiene que haber cubierto las penas convencionales aplicadas conforme a lo dispuesto en el presente contrato. El administrador del presente contrato será el responsable de verificar que se cumpla esta obligación, dentro de los 5 (cinco) hábiles siguientes a la conclusión del atraso.

DÉCIMA TERCERA.- DEDUCCIONES.- Con fundamento en lo dispuesto en los artículos 53 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento, **"EL PROVEEDOR"**, por la entrega parcial o deficiente del servicio, se hará acreedor a una sanción equivalente al __% (___ por ciento) del valor de lo

Durango No. 291, 5to. Piso, Col. Roma Norte, Alcaldía Cuauhtémoc, C. P. 06700, CDMX.
www.imss.gob.mx

incumplido, conforme a lo señalado en el numeral ____ de los Términos y Condiciones que se integran en el **Anexo** __ **(___)** del presente contrato.

PARA EL CASO DE QUE EXISTAN VARIOS PORCENTAJES DE PENAS CONVENCIONALES, SE DEBERÁ USAR LA SIGUIENTE REDACCIÓN:

DÉCIMA TERCERA.- DEDUCCIONES.- Con fundamento en lo dispuesto en los artículos 53 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento, **"EL PROVEEDOR"**, por la entrega parcial o deficiente del servicio, se hará acreedor a una sanción conforme los conceptos y porcentajes señalados en el numeral ___ de los Términos y Condiciones que se integran en el **Anexo** __ **(__)** del presente contrato.

El administrador del presente contrato será responsable del cálculo, aplicación y seguimiento de las deducciones. El monto máximo de aplicación de las deducciones no podrán ser mayor al que resulte de aplicar el porcentaje de la garantía de cumplimiento del presente contrato.

En caso de que se exceda se podrá proceder a la rescisión del contrato.

DÉCIMA CUARTA.- TERMINACIÓN ANTICIPADA DEL CONTRATO.- De conformidad con lo establecido en el artículo 54 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 102 de su Reglamento, **"EL INSTITUTO"** podrá dar por terminado anticipadamente el presente contrato sin responsabilidad para éste y sin necesidad de que medie resolución judicial alguna, cuando concurran razones de interés general o bien cuando por causas justificadas se extinga la necesidad de requerir el servicio, objeto del presente contrato, y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas se ocasionaría algún daño o perjuicio a **"EL INSTITUTO"** o se determine la nulidad de los actos que dieron origen al presente instrumento jurídico, con motivo de la resolución de una inconformidad o intervención de oficio emitida por la Secretaría de la Función Pública.

La terminación anticipada del presente contrato se sustentará mediante dictamen que precise las razones o las causas justificadas que den origen a la misma. Los gastos no recuperables por la terminación anticipada serán pagados siempre que éstos sean razonables, estén comprobados y se relacionen directamente con el presente instrumento jurídico.

DÉCIMA QUINTA.- SUSPENSIÓN DEL SERVICIO.- En caso fortuito o fuerza mayor, bajo su responsabilidad, **"EL INSTITUTO"** podrá suspender la prestación del servicio en términos del artículo 55 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en cuyo caso únicamente se pagarán aquéllos que hubiesen sido efectivamente prestados.

Cuando la suspensión obedezca a causas imputables a **"EL INSTITUTO"**, se pagarán previa solicitud de **"EL PROVEEDOR"** los gastos no recuperables de conformidad con el artículo 102, fracción II, del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, para lo cual deberá presentar su solicitud a **"EL INSTITUTO"** para su revisión y validación, una relación pormenorizada de los gastos, los

cuales deberán estar debidamente justificados, sean razonables, se relacionen directamente con el objeto del servicio contratado y a entera satisfacción del administrador del presente contrato.

DÉCIMA SEXTA.- CAUSALES DE RESCISIÓN ADMINISTRATIVA DEL CONTRATO.- "EL INSTITUTO" podrá rescindir administrativamente este contrato sin más responsabilidad para el mismo y sin necesidad de resolución judicial, cuando **"EL PROVEEDOR"** incurra en cualquiera de las causales que se señalan a continuación:

1. Cuando no entregue la garantía de cumplimiento del presente contrato, a más tardar dentro de los 10 (diez) días naturales posteriores a la firma del mismo.

2. Cuando incurra en falta de veracidad total o parcial respecto a la información proporcionada para la celebración del presente contrato.

3. Cuando incumpla, total o parcialmente, con cualesquiera de las obligaciones establecidas en el presente contrato y sus anexos.

4. Cuando se compruebe que el servicio ha sido prestado con alcances y características distintas a las pactadas.

5. Cuando se transmitan total o parcialmente, bajo cualquier título y a favor de otra persona física o moral, los derechos y obligaciones a que se refiere el presente documento, con excepción de los derechos de cobro, previa autorización de **"EL INSTITUTO"**.

6. Si la autoridad competente declara el concurso mercantil o cualquier situación análoga o equivalente que afecte el patrimonio de **"EL PROVEEDOR"**.

7. Cuando de manera reiterativa y constante, **"EL PROVEEDOR"** sea sancionado por parte de **"EL INSTITUTO"** con penalizaciones y/o deducciones sobre el mismo concepto de los servicios que proporciona, o por ubicarse en los límites de incumplimientos previstos en la cláusula de penas convencionales y/o deducciones del presente instrumento.

8. Cuando se sitúe en alguno de los supuestos previstos en el artículo 50 de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público.

9. En el supuesto de que la Comisión Federal de Competencia Económica, de acuerdo con sus facultades, notifique a **"EL INSTITUTO"** la sanción impuesta a **"EL PROVEEDOR"** con motivo de la colusión de precios en que hubiese incurrido durante el procedimiento de contratación, en contravención a lo dispuesto en los artículos 9 de la Ley Federal de Competencia Económica y 34 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. (En caso de aplicar)

10. Si **"EL PROVEEDOR"** no permite a **"EL INSTITUTO"** la administración y verificación a que se refiere la cláusula correspondiente del presente contrato.

11. EN CASO DE TRATARSE DE UN CONTRATO PLURIANUAL, SE DEBERÁ MENCIONAR COMO CAUSAL, LA NO ENTREGA DE LA RENOVACIÓN DE LA GARANTÍA CORRESPONDIENTE AL EJERCICIO FISCAL DE QUE SE TRATE EN EL PLAZO SEÑALADO EN LA CLÁUSULA DE GARANTÍAS.

DÉCIMA SÉPTIMA.- RESCISIÓN ADMINISTRATIVA DEL CONTRATO.- "EL INSTITUTO", en términos de lo dispuesto en el artículo 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, podrá rescindir administrativamente el presente contrato en cualquier momento, cuando **"EL PROVEEDOR"** incurra en incumplimiento de cualquiera de las obligaciones a su cargo, de conformidad con el procedimiento siguiente:

a) Si **"EL INSTITUTO"** considera que **"EL PROVEEDOR"** ha incurrido en alguna de las causales de rescisión que se consignan en la Cláusula que antecede, lo hará saber a **"EL PROVEEDOR"** de forma indubitable por escrito, a efecto de que éste exponga lo que a su derecho convenga y aporte, en su caso, las pruebas que estime pertinentes, en un término de 5 (cinco) días hábiles, a partir de la notificación de la comunicación de referencia.

b) Transcurrido el término a que se refiere el inciso anterior, se resolverá considerando los argumentos y pruebas que hubiere hecho valer.

c) La determinación de dar o no por rescindido administrativamente el presente contrato, deberá ser debidamente fundada, motivada y comunicada por escrito a **"EL PROVEEDOR"** dentro de los 15 (quince) días hábiles siguientes, al vencimiento del plazo señalado en el inciso a), de esta Cláusula.

En el supuesto de que se rescinda este contrato, **"EL INSTITUTO"** no aplicarán las penas convencionales, ni su contabilización para hacer efectiva la garantía de cumplimiento de este instrumento jurídico.

En caso de que **"EL INSTITUTO"** determine dar por rescindido el presente contrato, se deberá formular y notificar un finiquito dentro de los 20 (veinte) días naturales siguientes a la fecha en que se notifique la rescisión, de conformidad con el artículo 99 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en el que se hagan constar los pagos que, en su caso, deba efectuar **"EL INSTITUTO"** por concepto de la prestación del servicio por **"EL PROVEEDOR"** hasta el momento en que se determine la rescisión administrativa.

Iniciado un procedimiento de conciliación **"EL INSTITUTO"**, bajo su responsabilidad, podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido este contrato, **"EL PROVEEDOR"** presta el servicio, el procedimiento iniciado quedará sin efectos, previa aceptación y verificación de **"EL INSTITUTO"** por escrito, de que continúa vigente la necesidad de contar con el servicio y aplicando, en su caso, las penas convencionales correspondientes.

"EL INSTITUTO" podrá determinar no dar por rescindido este contrato, cuando durante el procedimiento advierta que dicha rescisión pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, **"EL INSTITUTO**" 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.

De no darse por rescindido este contrato, **"EL INSTITUTO"** establecerá, con **"EL PROVEEDOR"**, un nuevo plazo para el cumplimiento de aquellas obligaciones que se hubiesen dejado de cumplir, a efecto de que **"EL PROVEEDOR"** subsane el incumplimiento que hubiere motivado el inicio del procedimiento de rescisión. Lo anterior se llevará a cabo a través de un convenio modificatorio en el que se atenderá a las condiciones previstas en los dos últimos párrafos del artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

DÉCIMA OCTAVA.- RELACIÓN LABORAL.- "LAS PARTES" convienen en que **"EL INSTITUTO"** no adquiere ninguna obligación de carácter laboral para con **"EL PROVEEDOR"** ni para con los trabajadores que el mismo contrate para la realización del objeto del presente instrumento jurídico, toda vez que dicho personal depende exclusivamente de **"EL PROVEEDOR"**.

Por lo anterior, no se le considerará a **"EL INSTITUTO"** como patrón, ni aún substituto, y **"EL PROVEEDOR"** expresamente lo exime de cualquier responsabilidad de carácter civil, fiscal, de seguridad social, laboral o de otra especie, que en su caso pudiera llegar a generarse.

"EL PROVEEDOR" se obliga a liberar a **"EL INSTITUTO"** de cualquier reclamación de índole laboral o de seguridad social que sea presentada por parte de sus trabajadores, ante las autoridades competentes.

EN CASO DE APLICAR, CONFORME A TÉRMINOS Y CONDICIONES AGREGAR **DÉCIMA _____.- CONFIDENCIALIDAD.-**

DÉCIMA NOVENA.- MODIFICACIONES.- De conformidad con lo establecido en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"EL INSTITUTO"** podrá celebrar por escrito Convenio Modificatorio, al presente contrato dentro de la vigencia del mismo. Para tal efecto, **"EL PROVEEDOR"** se obliga a entregar, en su caso, la modificación de la garantía, en términos del artículo 103, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

PRÓRROGAS.- Asimismo, se podrán acordar prórrogas al plazo originalmente pactado por caso fortuito, fuerza mayor o por causas atribuibles a **"EL INSTITUTO"**, lo cual deberá estar debidamente acreditado en el expediente de contratación respectivo. **"EL PROVEEDOR"** puede solicitar la modificación del plazo originalmente pactado cuando se actualicen y se acrediten los supuestos de caso fortuito o de fuerza mayor.

Cualquier modificación a los derechos y obligaciones estipuladas por **"LAS PARTES"** en el presente contrato, deberá formalizarse mediante convenio y por escrito, mismo que

será suscrito por los servidores públicos que lo hayan hecho en el contrato, quienes los sustituyan o estén facultados para ello.

VIGÉSIMA.- ADMINISTRACIÓN Y VERIFICACIÓN.- El Dr. Alberto Flavio Balderas Hernández, Titular de la Coordinación Técnica de Adquisiciones de Bienes de Inversión y Activos, funge como administrador del contrato, responsable de dar seguimiento y verificar el cumplimiento de los derechos y obligaciones establecidos en el mismo, de conformidad con lo establecido en el documento de designación de administrador del contrato que se agrega al presente como **Anexo __ (__)** y el artículo 84 penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En el caso de que se lleve a cabo un relevo institucional temporal o permanente con dicho servidor público de **"EL INSTITUTO"** tendrá carácter de ADMINISTRADOR DEL CONTRATO la persona que sustituya al servidor público en el cargo, conforme a la designación correspondiente.

VIGÉSIMA PRIMERA.- PROCEDIMIENTO DE CONCILIACIÓN.- En cualquier momento durante la vigencia del presente Contrato, **"EL PROVEEDOR"** o **"EL INSTITUTO"** podrán presentar ante el Órgano Interno de Control en **"EL INSTITUTO"** solicitud de conciliación por desavenencias, derivadas del presente instrumento jurídico, conforme a lo dispuesto por los artículos 77 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 128 de su Reglamento.

EN CASO DE PARTICIPACIÓN CONJUNTA, SE DEBERÁ AGREGAR LA SIGUIENTE CLÁUSULA:

VIGÉSIMA XXXXXX.- OBLIGACIÓN SOLIDARIA O MANCOMUNADA.- "LAS PARTES" que suscriben el presente contrato en su carácter de **"EL PROVEEDOR"**, asumen las obligaciones materia de este instrumento jurídico en forma *mancomunada o solidaria* conforme a lo estipulado en el convenio de participación conjunta, que se agrega al presente contrato en el **Anexo __ (__)**.

VIGÉSIMA SEGUNDA.- RELACIÓN DE ANEXOS.- Los anexos que se relacionan a continuación forman parte integrante del presente contrato.

Anexo 1 (uno) _____

Anexo 2 (dos) _____

Anexo 3 (tres) _____

Anexo 4 (cuatro) _____

(ADECUAR LOS ANEXOS CONFORME A LA DOCUMENTACIÓN DE CADA PROCEDIMIENTO DE CONTRATACIÓN)

VIGÉSIMA TERCERA.- LEGISLACIÓN APLICABLE.- "LAS PARTES" se obligan a sujetarse estrictamente para el cumplimiento del presente contrato, a todas y cada una de las cláusulas del mismo, así como a lo establecido en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y supletoriamente al Código Civil Federal, a la Ley Federal de Procedimiento Administrativo, al Código Federal de Procedimientos Civiles y demás ordenamientos aplicables en la materia.

VIGÉSIMA CUARTA.- JURISDICCIÓN.- Para la interpretación y cumplimiento de este instrumento jurídico, así como para todo aquello que no esté expresamente estipulado en el mismo, **"LAS PARTES"** se someten a la jurisdicción de los Tribunales Federales competentes de la Ciudad de México, renunciando a cualquier otro fuero presente o futuro que por razón de su domicilio les pudiera corresponder.

Previa lectura y debidamente enteradas **"LAS PARTES"** del contenido, alcance y fuerza legal del presente contrato, en virtud de que se ajusta a la expresión de su libre voluntad y que su consentimiento no se encuentra afectado por dolo, error, mala fe, ni otros vicios de la voluntad, lo firman y ratifican en todas sus partes, por quintuplicado, en la Ciudad de México, el _____, quedando un ejemplar en poder de **"EL PROVEEDOR"** y los restantes en poder de **"EL INSTITUTO"**.

"EL INSTITUTO" **INSTITUTO MEXICANO DEL SEGURO SOCIAL**	**"EL PROVEEDOR"** _____
_____ Alberto Flavio Balderas Hernández Apoderado(a) Legal	_____ _____ Representante Legal

ADMINISTRADOR DEL CONTRATO

_____

C. _____

_____

Durango No. 291, 5to. Piso, Col. Roma Norte, Alcaldía Cuauhtémoc, C. P. 06700, CDMX.
www.imss.gob.mx

Anexo 15.- Modelo de convenio de proposición conjunta.

CONVENIO DE PROPOSICIÓN CONJUNTA QUE CELEBRAN POR UNA PARTE _____, REPRESENTADA POR _____ EN SU CARÁCTER DE _____, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "EL PARTICIPANTE A", Y POR OTRA _____, REPRESENTADA POR _____, EN SU CARÁCTER DE _____, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "EL PARTICIPANTE B", Y CUANDO SE HAGA REFERENCIA A LOS QUE INTERVIENEN SE DENOMINARÁN "Las Partes", AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS.

1.1. "EL PARTICIPANTE A", DECLARA QUE.:

1.1.1 ES UNA SOCIEDAD LEGALMENTE CONSTITUIDA, DE CONFORMIDAD CON LAS LEYES MEXICANAS, SEGÚN CONSTA EN EL TESTIMONIO DE LA ESCRITURA PÚBLICA (PÓLIZA) NÚMERO ____, DE FECHA ____, OTORGADA ANTE LA FE DEL LIC. ____ NOTARIO (CORREDOR) PÚBLICO NÚMERO ____, DEL ____, E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DE COMERCIO DE _____, EN EL FOLIO MERCANTIL ____ DE FECHA _____.

EL ACTA CONSTITUTIVA DE LA SOCIEDAD ____ (SI/NO) HA TENIDO REFORMAS Y MODIFICACIONES.

Nota. En su caso, se deberán relacionar las escrituras en que consten las reformas o modificaciones de la sociedad.

LOS NOMBRES DE SUS SOCIOS SON:

_____ CON REGISTRO FEDERAL DE CONTRIBUYENTES _____.

1.1.2 TIENE LOS SIGUIENTES REGISTROS OFICIALES. REGISTRO FEDERAL DE CONTRIBUYENTES NÚMERO___ Y REGISTRO PATRONAL ANTE EL INSTITUTO MEXICANO DEL SEGURO SOCIAL NÚMERO __.

1.1.3 SU REPRESENTANTE LEGAL CON EL CARÁCTER YA MENCIONADO, CUENTA CON LAS FACULTADES NECESARIAS PARA SUSCRIBIR EL PRESENTE CONVENIO, DE CONFORMIDAD CON EL CONTENIDO DEL TESTIMONIO DE LA ESCRITURA PÚBLICA NÚMERO ____ DE FECHA ____, OTORGADA ANTE LA FE DEL LIC. ____ NOTARIO PÚBLICO NÚMERO ___, DEL _____ E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DE COMERCIO, EN EL FOLIO MERCANTIL NÚMERO _____ DE FECHA ____, MANIFESTANDO "BAJO PROTESTA DE DECIR VERDAD", QUE DICHAS FACULTADES NO LE HAN SIDO REVOCADAS, NI LIMITADAS O MODIFICADAS EN FORMA ALGUNA, A LA FECHA EN QUE SE SUSCRIBE EL PRESENTE INSTRUMENTO JURÍDICO.

EL DOMICILIO DEL REPRESENTANTE LEGAL ES EL UBICADO EN: _____.

1.1.4 SU OBJETO SOCIAL, ENTRE OTROS CORRESPONDE A. _____; POR LO QUE CUENTA CON LOS RECURSOS FINANCIEROS, TÉCNICOS, ADMINISTRATIVOS Y HUMANOS PARA OBLIGARSE, EN LOS TÉRMINOS Y CONDICIONES QUE SE ESTIPULAN EN EL PRESENTE CONVENIO.

1.1.5 SEÑALA COMO DOMICILIO LEGAL PARA TODOS LOS EFECTOS QUE DERIVEN DEL PRESENTE CONVENIO, EL UBICADO EN:

2.1 "EL PARTICIPANTE B", DECLARA QUE:

2.1.1 ES UNA SOCIEDAD LEGALMENTE CONSTITUIDA DE CONFORMIDAD CON LAS LEYES DE LOS ESTADOS UNIDOS MEXICANOS, SEGÚN CONSTA EL TESTIMONIO (PÓLIZA) DE LA ESCRITURA PÚBLICA NÚMERO ___, DE FECHA ___, PASADA ANTE LA FE DEL LIC. ____ NOTARIO (CORREDOR) PÚBLICO NÚMERO ___, DEL __, E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DEL COMERCIO, EN EL FOLIO MERCANTIL NÚMERO ____ DE FECHA ____.

EL ACTA CONSTITUTIVA DE LA SOCIEDAD __ (SI/NO) HA TENIDO REFORMAS Y MODIFICACIONES.

Nota. En su caso, se deberán relacionar las escrituras en que consten las reformas o modificaciones de la sociedad.

LOS NOMBRES DE SUS SOCIOS SON:

_____ CON REGISTRO FEDERAL DE CONTRIBUYENTES ____.

2.1.2 TIENE LOS SIGUIENTES REGISTROS OFICIALES. REGISTRO FEDERAL DE CONTRIBUYENTES NÚMERO _____ Y REGISTRO PATRONAL ANTE EL INSTITUTO MEXICANO DEL SEGURO SOCIAL NÚMERO _____.

2.1.3 SU REPRESENTANTE LEGAL, CON EL CARÁCTER YA MENCIONADO, CUENTA CON LAS FACULTADES NECESARIAS PARA SUSCRIBIR EL PRESENTE CONVENIO, DE CONFORMIDAD CON EL CONTENIDO DEL TESTIMONIO DE LA ESCRITURA PÚBLICA NÚMERO ____ DE FECHA _____, PASADA ANTE LA FE DEL LIC. _____ NOTARIO PÚBLICO NÚMERO _____, DEL _____ E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DEL COMERCIO, EN EL FOLIO MERCANTIL NÚMERO _____ DE FECHA ____, MANIFESTANDO "BAJO PROTESTA DE DECIR VERDAD" QUE DICHAS FACULTADES NO LE HAN SIDO REVOCADAS, NI LIMITADAS O MODIFICADAS EN FORMA ALGUNA, A LA FECHA EN QUE SE SUSCRIBE EL PRESENTE INSTRUMENTO JURÍDICO.

EL DOMICILIO DE SU REPRESENTANTE LEGAL ES EL UBICADO EN _____.

2.1.4 SU OBJETO SOCIAL, ENTRE OTROS CORRESPONDE A. _____; POR LO QUE CUENTA CON LOS RECURSOS FINANCIEROS, TÉCNICOS, ADMINISTRATIVOS Y HUMANOS PARA OBLIGARSE, EN LOS TÉRMINOS Y CONDICIONES QUE SE ESTIPULAN EN EL PRESENTE CONVENIO.

2.1.5 SEÑALA COMO DOMICILIO LEGAL PARA TODOS LOS EFECTOS QUE DERIVEN DEL PRESENTE CONVENIO, EL UBICADO EN. _____. (MENCIONAR E IDENTIFICAR A CUÁNTOS INTEGRANTES CONFORMAN LA PROPOSICIÓN CONJUNTA PARA LA PRESENTACIÓN DE PROPUESTAS).

3.1. "Las Partes" DECLARAN QUE:

3.1.1. CONOCEN LOS REQUISITOS Y CONDICIONES ESTIPULADAS EN LA CONVOCATORIA A LA LICITACIÓN PÚBLICA NACIONAL_____.

3.1.2. MANIFIESTAN SU CONFORMIDAD EN FORMALIZAR EL PRESENTE CONVENIO, CON EL OBJETO DE PARTICIPAR CONJUNTAMENTE EN LA LICITACIÓN, PRESENTANDO PROPUESTA TÉCNICA Y ECONÓMICA, CUMPLIENDO CON LO ESTABLECIDO EN LA CONVOCATORIA DE LA LICITACIÓN Y CON LO DISPUESTO EN LOS ARTÍCULOS 34, DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO Y 44 DE SU REGLAMENTO.

EXPUESTO LO ANTERIOR, LAS PARTES OTORGAN LAS SIGUIENTES.

CLÁUSULAS

PRIMERA.- OBJETO: "PROPOSICIÓN CONJUNTA".

"Las Partes" CONVIENEN, EN CONJUNTAR SUS RECURSOS TÉCNICOS, LEGALES, ADMINISTRATIVOS, ECONÓMICOS Y FINANCIEROS PARA PRESENTAR PROPUESTA TÉCNICA Y ECONÓMICA EN LA LICITACIÓN PÚBLICA NACIONAL NÚMERO _____ Y EN CASO DE SER ADJUDICATARIO DEL CONTRATO, SE OBLIGAN A OTORGAR EL SERVICIO CONTRATADO OBJETO DEL CONVENIO, CON LA PARTICIPACIÓN SIGUIENTE.

PARTICIPANTE "A". (DESCRIBIR LA PARTE QUE SE OBLIGA A SUMINISTRAR).

(CADA UNO DE LOS INTEGRANTES QUE CONFORMAN LA PROPOSICIÓN CONJUNTA PARA LA PRESENTACIÓN DE PROPUESTAS DEBERÁ DESCRIBIR LA PARTE QUE SE OBLIGA A ENTREGAR).

SEGUNDA.-REPRESENTANTE COMÚN Y OBLIGADO SOLIDARIO.

"Las Partes" ACEPTAN EXPRESAMENTE EN DESIGNAR COMO REPRESENTANTE COMÚN AL _____, A TRAVÉS DEL PRESENTE INSTRUMENTO, OTORGÁNDOLE PODER AMPLIO Y SUFICIENTE, PARA ATENDER TODO LO RELACIONADO CON LAS PROPUESTAS TÉCNICA Y ECONÓMICA EN EL PROCEDIMIENTO DE LICITACIÓN, ASÍ COMO PARA SUSCRIBIR DICHAS PROPUESTAS.

ASIMISMO, CONVIENEN ENTRE SI EN CONSTITUIRSE EN FORMA CONJUNTA Y SOLIDARIA PARA COMPROMETERSE POR CUALQUIER RESPONSABILIDAD DERIVADA DEL CUMPLIMIENTO DE LAS OBLIGACIONES ESTABLECIDAS EN EL PRESENTE CONVENIO, CON RELACIÓN AL CONTRATO QUE SUS REPRESENTANTES LEGALES FIRMEN CON EL INSTITUTO MEXICANO DEL SEGURO SOCIAL (IMSS), DERIVADO DEL PROCEDIMIENTO DE CONTRATACIÓN _____, ACEPTANDO EXPRESAMENTE EN RESPONDER ANTE EL IMSS POR LAS PROPUESTAS QUE SE PRESENTEN Y, EN SU CASO, DE LAS OBLIGACIONES QUE DERIVEN DE LA ADJUDICACIÓN DEL CONTRATO RESPECTIVO.

TERCERA.- DEL COBRO DE LAS FACTURAS.

"Las Partes" CONVIENEN EXPRESAMENTE, QUE "EL PARTICIPANTE_____ (LOS PARTICIPANTES, DEBERÁN INDICAR CUÁL DE ELLOS ESTARÁ FACULTADO PARA REALIZAR EL COBRO), PARA EFECTUAR EL COBRO DE LAS FACTURAS RELATIVAS AL SERVICIO QUE SE PROPORCIONE AL IMSS, CON MOTIVO DEL CONTRATO QUE SE DERIVE DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO _____.

CUARTA.- VIGENCIA.

"Las Partes" CONVIENEN, EN QUE LA VIGENCIA DEL PRESENTE CONVENIO SERÁ EL DEL PERÍODO DURANTE EL CUAL SE DESARROLLE EL PROCEDIMIENTO DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO _____, INCLUYENDO, EN SU CASO, DE RESULTAR ADJUDICADOS DEL CONTRATO, EL PLAZO QUE SE ESTIPULE EN ÉSTE Y EL QUE PUDIERA RESULTAR DE CONVENIOS DE MODIFICACIÓN.

QUINTA.-OBLIGACIONES.

"Las Partes" CONVIENEN EN QUE EN EL SUPUESTO DE QUE CUALQUIERA DE ELLAS QUE SE DECLARE EN QUIEBRA O EN SUSPENSIÓN DE PAGOS, NO LAS LIBERA DE CUMPLIR CON SUS OBLIGACIONES, POR LO QUE CUALQUIERA DE ELLAS QUE SUBSISTA, ACEPTA Y SE OBLIGA EXPRESAMENTE A RESPONDER SOLIDARIAMENTE DE LAS OBLIGACIONES CONTRACTUALES A QUE HUBIERE LUGAR.

"Las Partes" ACEPTAN Y SE OBLIGAN A PROTOCOLIZAR ANTE NOTARIO PÚBLICO EL PRESENTE CONVENIO, EN CASO DE RESULTAR ADJUDICADOS DEL CONTRATO QUE SE DERIVE DEL FALLO EMITIDO EN LA LICITACIÓN PÚBLICA NACIONAL NÚMERO _____ EN QUE PARTICIPAN Y, QUE EL PRESENTE INSTRUMENTO, DEBIDAMENTE PROTOCOLIZADO, FORMARÁ PARTE INTEGRANTE DEL CONTRATO QUE SUSCRIBAN LOS REPRESENTANTES LEGALES DE CADA INTEGRANTE Y EL IMSS.

LEÍDO QUE FUE EL PRESENTE CONVENIO POR "Las Partes" Y ENTERADOS DE SU ALCANCE Y EFECTOS LEGALES, ACEPTANDO QUE NO EXISTIÓ ERROR, DOLO, VIOLENCIA O MALA FE, LO RATIFICAN Y FIRMAN, DE CONFORMIDAD EN LA CIUDAD DE MÉXICO, EL DÍA _____ DE _____ DE 20___.

"EL PARTICIPANTE A"	"EL PARTICIPANTE B"
_____	_____
NOMBRE Y CARGO DEL APODERADO LEGAL	NOMBRE Y CARGO DEL APODERADO LEGAL

Anexo 16.- Glosario.

Para efectos de ésta convocatoria, se entenderá por:

Administrador del contrato: Servidor(es) público(s) en quien recae la responsabilidad de dar seguimiento al cumplimiento de las obligaciones establecidas en el contrato.

ALSC: Administración Local de Servicios al Contribuyente.

Área contratante: La facultada en la dependencia o entidad para realizar procedimientos de contratación a efecto de adquirir o arrendar bienes o contratar la prestación de servicios que requiera la dependencia o entidad de que se trate;

Área requirente: La que en la dependencia o entidad, solicite o requiera formalmente la adquisición o arrendamiento de bienes o la prestación de servicios, o bien aquella que los utilizará;

Área técnica: La responsable de elaborar las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, de responder las preguntas que sobre estos aspectos técnicos realicen los licitantes; así como de coadyuvar en la evaluación de las proposiciones.

CABCS: Coordinación de Adquisición de Bienes y Contratación de Servicios.

CECOBAN: Centro de Compensación Bancaria.

CNBV: Comisión Nacional Bancaria y de Valores.

COMPRANET: El Sistema Electrónico de información pública gubernamental sobre adquisiciones, arrendamientos, servicios, obras públicas y servicios relacionados con las mismas con dirección electrónica en Internet: http//compranet.funcionpublica.gob.mx.

Contrato: Documento a través del cual se formalizan los derechos y obligaciones derivados del Fallo del procedimiento de contratación de la adquisición o la prestación de los servicios.

DOF: Diario Oficial de la Federación.

EMA (Entidad Mexicana de Acreditación): Entidad de gestión privada en nuestro país, que tiene como objetivo acreditar a los Organismos de la Evaluación de la Conformidad que son los laboratorios de ensayo, laboratorios de calibración, laboratorios clínicos, unidades de verificación (organismos de inspección) y organismos de certificación.

IMSS o Instituto: Instituto Mexicano del Seguro Social.

INFONAVIT: Instituto del Fondo Nacional de la Vivienda para los Trabajadores.

Investigación de mercado: La verificación de la existencia de bienes, arrendamientos o servicios, de proveedores a nivel nacional o internacional y del precio estimado basado en la información que se obtenga en la propia dependencia o entidad, de organismos públicos o privados, de fabricantes de bienes o prestadores del servicio, o una combinación de dichas fuentes de información.

IVA: Impuesto al Valor Agregado.

LAASSP: Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Medio de Identificación Electrónica: Conjunto de datos electrónicos asociados con documentos que son utilizados para reconocer a su autor, y que legitiman el consentimiento de éste para obligarlo a las manifestaciones que en él se contienen, de conformidad con el artículo 27 de la LAASSP.

Medios remotos de comunicación electrónica: Los dispositivos tecnológicos para efectuar transmisión de datos e información a través de computadoras, líneas telefónicas, enlaces dedicados, microondas y similares.

MIPYMES: Las micro, pequeñas y medianas empresas de nacionalidad mexicana a que hace referencia la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa;

Normas: Las Normas Oficiales Mexicanas, las Normas Mexicanas, según proceda, y a falta de éstas, con las Normas Internacionales, de conformidad con lo dispuesto por los artículos 53 y 55 de la Ley Federal sobre Metrología y Normalización; en su caso, las normas de referencia o especificaciones a que se refiere el artículo 67 de la Ley citada.

OIC: Órgano Interno de Control en el IMSS.

Partida o concepto.- La división o desglose de los bienes a adquirir y/o arrendar o de los servicios a contratar, contenidos en un procedimiento de contratación o en un contrato, para diferenciarlos unos de otros, clasificarlos o agruparlos.

POBALINES.- Las políticas, bases y lineamientos a que se refieren el párrafo sexto del artículo 1 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Proveedor: La persona que celebre contratos de adquisiciones, arrendamientos o servicios.

Reglamento: Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Resolución miscelánea: Publicación anual en el DOF que agrupa disposiciones de carácter general, aplicables a impuestos, productos, aprovechamientos, contribuciones de mejoras y derechos federales, excepto a los relacionados con el comercio exterior.

RFC.- Registro Federal de Contribuyentes.

SAT: El Servicio de Administración Tributaria.

SFP: Secretaría de la Función Pública.

Sobre cerrado: Cualquier medio que contenga la proposición del licitante, cuyo contenido solo puede ser conocido en el Acto de Presentación y Apertura de Proposiciones, en términos de la Ley.

SSA: Secretaría de Salud.