Lotería Nacional

Subdirección General de Administración y Finanzas

Dirección de Recursos Materiales y Servicios Generales

Gerencia de Adquisiciones

Avenida Insurgentes Sur 1397 piso 6, Colonia Insurgentes Mixcoac, Demarcación Territorial Benito Juárez, Código Postal 03920 en la Ciudad de México

Licitación Pública Nacional

Número: LA-06-HJY-006HJY001-N-220-2026

"SERVICIO INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN PARA LOTERÍA NACIONAL (SISI)"

Convocatoria aprobada por el Subcomité Revisor de Convocatorias en la Trigésima Sesión de fecha 20 de octubre de 2026.

ÍNDICE

GLOSARIO 4

1. IDENTIFICACIÓN DE LA LICITACIÓN. 6

1.1. Datos de identificación. 6
1.2. Medio y carácter de la Licitación. 6
1.3. Número de identificación de la Licitación. 6
1.4. Indicación de los ejercicios fiscales para la contratación. 6
1.5. Idioma. 6
1.6. Disponibilidad presupuestaria. 7
1.7. Oferta Subsecuente de Descuento. 7

2. OBJETO Y ALCANCE DE LA LICITACIÓN. 7

2.1. Objeto de la contratación. 7
2.2. Indicación de agrupamiento. 7
2.3. Precio máximo de referencia 7
2.4. Normas Oficiales Mexicanas, Normas Mexicanas, Internacionales, calidad, Referencia o Especificaciones. 7
2.5. Pruebas e institución pública o privada que lo realizará. 8
2.6. Tipo de contratación. 8
2.7. Criterios Específicos de Evaluación. 8
2.8. Forma de adjudicación. 8
2.9. Modelo del contrato. 8
2.10. Terminación de la relación contractual. 8
2.11. Contribuciones. 9
2.12. Discrepancias y Controversias. 9

3. FORMA Y TÉRMINOS QUE REGIRÁN LOS DIVERSOS ACTOS DE LA LICITACIÓN. 9

3.1. Fecha, hora y lugar para los actos de la Licitación. 10
3.2. Junta de Aclaraciones 10
3.3. Acto de Presentación y Apertura de Proposiciones. 11
3.4. Proposiciones conjuntas. 12
3.5. Envío de una sola proposición. 13
3.6. Presentación de la documentación distinta a la propuesta técnica y propuesta económica. 13
3.7. Acreditamiento de personalidad jurídica. 13
3.8. Acto de Fallo y Firma de Contrato. 13

4. REQUISITOS QUE LAS O LOS LICITANTES DEBEN CUMPLIR. 18

4.1. Documentación legal y Administrativa. 18
4.2. Propuesta técnica 21
4.3. Propuesta económica 23
4.4. Causales expresas de desechamiento. 24

5. CRITERIOS ESPECÍFICOS CONFORME A LOS CUALES SE EVALUARÁN LAS PROPOSICIONES. 26

5.1. Evaluación legal. 26
5.2. Evaluación de la propuesta técnica. 27
5.3. Evaluación de la propuesta económica. 36

6. INCONFORMIDADES. 37

7. CANCELACIÓN DE LA LICITACIÓN, PARTIDA(S), O CONCEPTOS INCLUIDOS EN ÉSTA. 38

8. DECLARACIÓN DE LICITACIÓN DESIERTA. 38
9. FORMATOS QUE FACILITARÁN Y AGILIZARÁN LA PRESENTACIÓN Y RECEPCIÓN DE LAS PROPOSICIONES. ... 38
10. NOTA INFORMATIVA OCDE. 39
ANEXO I ANEXO TÉCNICO 40
ANEXO II ACREDITAMIENTO DE PERSONALIDAD JURÍDICA PERSONA FÍSICA 169
ANEXO III ACREDITAMIENTO DE PERSONALIDAD JURÍDICA PERSONA MORAL 170
ANEXO IV ESCRITO DE LOS SUPUESTOS ESTABLECIDOS EN LOS ARTÍCULOS 71 Y 90 DE LA LEY 172
ANEXO V ESCRITO DE DECLARACIÓN DE INTEGRIDAD 173
ANEXO VI ESCRITO DE NACIONALIDAD 174
ANEXO VII ACEPTACIÓN DE CONDICIONES DE LA PLATAFORMA 175
ANEXO VIII MANIFESTACIÓN DE VÍNCULOS 176
ANEXO IX MANIFESTACIÓN DE BENEFICIOS O VENTAJAS 177
ANEXO X MANIFESTACIÓN DE SUBCONTRATACIÓN 178
ANEXO XI ESTRATIFICACIÓN DE LAS MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS 179
ANEXO XII FORMATO DE INFORMACIÓN RESERVADA Y CONFIDENCIAL 180
ANEXO XIII NOTA OCDE 181
ANEXO XIV PROPUESTA ECONÓMICA 184
ANEXO XV ACUSE DE RECEPCIÓN DE LA DOCUMENTACIÓN CONFORME A LOS NUMERALES 4.1, 4.2 Y 4.3 DE LA CONVOCATORIA 191
ANEXO XVI ESCRITO DE MANIFIESTACIÓN 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. 195
ANEXO XVII MODELO DE CONTRATO 196
ANEXO XVIII FORMA DE REDACCIÓN DE LA PÓLIZA QUE GARANTICE EL CUMPLIMIENTO DEL CONTRATO 218

GLOSARIO

Para efectos de la presente **Convocatoria**, se entenderá por:

Acuerdo:	Acuerdo por el que se establecen las disposiciones que se deberán observar para la utilización del Sistema Electrónico de Información Pública Gubernamental denominado **CompraNet**, publicado en el Diario Oficial de la Federación el 28 de junio de 2011.
Administrador del contrato:	De conformidad con lo establecido en los artículos 2 fracción IV y 129 penúltimo párrafo del Reglamento, la persona responsable de administrar y verificar el cumplimiento del Contrato que se derive del presente procedimiento de contratación, de conformidad con el apartado Responsable de administrar y verificar el contrato o pedido los bienes, arrendamientos o servicios del Anexo Técnico.
Área Requirente:	Gerencia de Telecomunicaciones y Seguridad Informática.
Área Contratante:	Subdirección General de Administración y Finanzas, a través de la Gerencia de Adquisiciones, de conformidad con el numeral 5.6 Inciso a). de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de Lotería Nacional.
Área Técnica:	Gerencia de Telecomunicaciones y Seguridad Informática.
Anexo Técnico:	El apartado de la presente **Convocatoria** que contiene las características, especificaciones técnicas y alcances de la contratación del **Servicio** solicitado.
Contrato:	El (los) instrumento (s) jurídicos que regulará (n) los derechos y obligaciones entre la **LN** y la o el (las o los) licitante(s) que resulten adjudicado(a) (s), derivado (s) de la presente Licitación.
Convocante:	La Lotería Nacional a través de la Subdirección General de Administración y Finanzas. por conducto de la Gerencia de Adquisiciones de la Dirección de Recursos Materiales y Servicios Generales
Convocatoria:	El documento en el cual se establecen las bases en que se desarrollará el procedimiento y en el cual se describen los requisitos de participación para la contratación del **Servicio** objeto de esta **Licitación**.
D.O.F.:	El Diario Oficial de la Federación.
Escrito libre:	El documento que deberá cumplir como mínimo con los datos requeridos en la Convocatoria, no importando el orden y/o ubicación del contenido.
Identificación Oficial Vigente:	La credencial de elector, pasaporte o cartilla del Servicio Militar Nacional liberada.
I.V.A.:	Impuesto al Valor Agregado.
Licitación:	La Licitación Pública Nacional número LA-06-HJY-006HJY001-N-220-2026.
Ley o LAASSP:	La Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
Licitante(s):	La(s) persona(s) física(s) o moral(es) que participa(n) en este procedimiento de **Licitación.**
Licitante(s) Adjudicado(as):	La(s) persona(s) física(s) o moral(es) que resulte(n) adjudicada(s) por haber cumplido con todos los requisitos técnicos, económicos, administrativos y legales, que presente(n) las **Proposiciones** solventes, conforme a los criterios de adjudicación; con la(s) que se celebrará(n) el(los) **Contratos.**
LN y/o Lotería	Lotería Nacional.
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.
OIC:	Órgano Interno de Control en la **LN.**
Partida:	La división o desglose de los servicios a contratar, contenidos en un procedimiento de contratación o en un contrato, para diferenciarlos unos de otros, clasificarlos o agruparlos.
Plataforma	La Plataforma Digital de Contrataciones Públicas Compras MX

Proposiciones:	Conjunto integrado por la **Propuesta Técnica** y la **Propuesta Económica** que presente(n) el(los) **Licitante(s)**. La propuesta técnica incluye la documentación Legal y Administrativa.
Propuesta Económica:	El documento que contiene la información proporcionada por las o los **Licitante(s)** con los costos que ofertarán a la **Convocante** para efectos del presente procedimiento de **Licitación**, mismo que deberá realizarse conforme a los términos y condiciones contenidos en la presente **Convocatoria** y su **Anexo Técnico**.
Propuesta Técnica:	El documento que contiene la información proporcionada por las o los **Licitante(s)** con las características y especificaciones del **Servicio** que ofertan para efectos del presente procedimiento de **Licitación**, mismo que deberá realizarse conforme a los términos y condiciones contenidos en la presente **Convocatoria** y su **Anexo Técnico**, así como la documentación Legal y Administrativa.
Proveedor:	La persona física o moral que celebre el contrato.
Reglamento o RLAASSP:	El **Reglamento** de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
SAT:	El Servicio de Administración Tributaria.
SABG o Secretaría:	Secretaría Anticorrupción y Buen Gobierno.
Servicio:	Servicio Integral de Seguridad de la Información para Lotería Nacional (SISI) objeto de esta **Licitación**, descrito en el **Anexo Técnico** de la presente **Convocatoria**.

CONVOCATORIA

En observancia al párrafo sexto del artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, de conformidad con los artículos 33, 35 fracción I, 36, 39 fracción I, 40, 41, 42 segundo párrafo y 47 segundo párrafo de la Ley; así como los artículos 83 y 86 de su Reglamento, se convoca a participar en el presente procedimiento de contratación a las personas físicas y/o morales de nacionalidad mexicana, cuya actividad económica u objeto social esté relacionado con el objeto de esta Licitación.

1. IDENTIFICACIÓN DE LA LICITACIÓN.

1.1. Datos de identificación.

Convocante:	Lotería Nacional.
Área contratante:	Subdirección General de Administración y Finanzas, a través de la Gerencia de Adquisiciones.
Domicilio:	Avenida Insurgentes Sur 1397 piso 6, Colonia Insurgentes Mixcoac, Demarcación Territorial Benito Juárez, Código Postal 03920 en la Ciudad de México.
Área Requirente:	Gerencia de Telecomunicaciones y Seguridad Informática.

1.2. Medio y carácter de la Licitación.

La Licitación Pública conforme al medio utilizado es "**Electrónica**"; por lo cual las o los licitantes deberán enviar su proposición a través de la Plataforma de conformidad con lo dispuesto en el artículo 36 de la Ley.

En las proposiciones remitidas a través de la Plataforma deberán emplearse los medios de identificación electrónica que establezca la SABG, los cuales producirán los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio, lo anterior conforme a lo establecido en el artículo 37 último párrafo de la Ley y 95 de su Reglamento.

Por lo anterior, aquellos(as) interesados(as) en participar en esta Licitación que requieran asesoría o presenten situaciones particulares sobre el manejo de la Plataforma, deberán dirigirse con el personal de la SABG; los datos de contacto podrán ser localizados en la página web https://comprasmx.buengobierno.gob.mx/

El carácter del presente procedimiento de contratación es **Nacional,** de conformidad con lo dispuesto en el artículo 39 fracción I de la Ley.

1.3. Número de identificación de la Licitación.

LA-06-HJY-006HJY001-N-220-2026.

1.4. Indicación de los ejercicios fiscales para la contratación.

Esta contratación es para los ejercicios fiscales 2026, 2027 y 2028.

1.5. Idioma.

Las proposiciones deberán presentarse únicamente en idioma español, en caso de presentar documentación adicional en idioma distinto, deberá acompañarse de su correspondiente traducción simple al español, de conformidad con el artículo 40 fracción IV de la Ley.

1.6. Disponibilidad presupuestaria.

Se cuenta con la autorización de la Directora General de Lotería Nacional de fecha 24 de marzo de 2026, en los términos del artículo 148 del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.

Por lo que los recursos para el contrato que derive de la presente Licitación Pública, estarán sujetos a la disponibilidad presupuestaria del año en el que se prevé su vigencia.

Por lo anterior, y conforme al artículo 33 de la Ley, se contará con suficiencia presupuestal en la partida presupuestal número:

31904 Servicios integrales de infraestructura de Cómputo.

La Convocante cuenta con disponibilidad presupuestaria para cubrir las obligaciones derivadas de la presente contratación correspondientes al ejercicio fiscal 2026, con cargo a la partida específica del Clasificador por Objeto del Gasto vigente **31904,** según consta en la solicitud de suficiencia presupuestal número de folio; 1910 de fecha 20 de julio de 2026.

1.7. Oferta Subsecuente de Descuento.

No aplica para la presente Licitación.

2. OBJETO Y ALCANCE DE LA LICITACIÓN.

2.1. Objeto de la contratación.

Proporcionar de manera integrada y unificada las especificaciones, requerimientos técnicos y funcionalidades de los servicios y soluciones requeridas para el "SERVICIO INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN (SISI)". "LOTERÍA", a través de la Subgerencia de Seguridad Informática requiere contar con servicios que permitan robustecer y complementar la Seguridad de la Información para salvaguardar la integridad y confidencialidad de la información.

Lo anterior, conforme a la descripción amplia y detallada del **Servicio** a contratar, los Términos y Condiciones, los lugares de prestación del **Servicio**, las especificaciones y los requisitos que están señalados en el **Anexo Técnico** de la presente Convocatoria

2.2. Indicación de agrupamiento.

NO aplica para la presente Licitación.

2.3. Precio máximo de referencia

NO aplica para la presente Licitación.

2.4. Normas Oficiales Mexicanas, Normas Mexicanas, Internacionales, calidad, Referencia o Especificaciones.

De conformidad a lo establecido en el **Anexo Técnico**

2.5. Pruebas e institución pública o privada que lo realizará.

De conformidad a lo establecido en el Anexo Técnico

2.6. Tipo de contratación.

Contrato abierto por monto de conformidad con el artículo 68 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

2.7. Criterios Específicos de Evaluación.

Criterio de evaluación por puntos y porcentajes.

2.8. Forma de adjudicación.

El contrato se adjudicará por la **partida única completa** a la o el licitante cuya proposición resulte solvente porque cumple con los requisitos administrativos-legales, técnicos y económicos a criterio de lo resultante de la evaluación por puntos y porcentajes establecidos en esta Convocatoria, de conformidad con los numerales 4.1, 4.2 y 4.3 y **"Anexo Técnico"** de la presente Convocatoria,

2.9. Modelo del contrato.

Con fundamento en lo dispuesto por los artículos 40 fracción XIX y 66 de la Ley; así como 83 fracción II inciso i) y 126 antepenúltimo párrafo de su Reglamento se adjunta a la presente Licitación, el modelo de contrato que forma parte integrante de la misma **Anexo XVII** el cual se elaboró de conformidad al modelo de contrato aprobado por la Secretaría Anticorrupción y Buen Gobierno, mismo que se encuentra publicado en Compras MX, la Convocatoria y las demás disposiciones legales aplicables. En caso de discrepancia entre el modelo de contrato en relación con la Convocatoria y sus juntas de aclaraciones, prevalecerá lo estipulado en estas últimas.

2.10. Terminación de la relación contractual.

I. Rescisión administrativa del contrato.

La **LN** podrá en cualquier momento rescindir administrativamente el contrato cuando el proveedor incumpla total o parcialmente con cualquiera de las obligaciones establecidas en la Convocatoria y en el Contrato y su Anexo Técnico respectivo, de conformidad con el artículo 77 de la Ley.

Con independencia de lo anterior, son causas específicas de rescisión contractual la actualización de alguno de los siguientes supuestos:

- Si el "proveedor" se declara en concurso mercantil;
- Si el "proveedor" transfiere en forma parcial o total a terceras personas, físicas o morales, los derechos y obligaciones derivados del Contrato correspondiente con excepción de los derechos de cobro;
- Si el "proveedor" no permite a la **LN** la administración y verificación a que se refiere la Cláusula **DÉCIMA SEGUNDA** de cada uno de los Contratos;

- Si el "proveedor" no entrega la garantía de cumplimiento y póliza de responsabilidad civil, dentro del plazo establecido en la Cláusula **NOVENA** y **DÉCIMA SEXTA** del contrato respectivo**.**

II. Terminación anticipada.

La **LN** podrá dar por terminado anticipadamente el contrato, sin responsabilidad para ésta y sin necesidad de que medie resolución judicial y/o administrativa alguna, cuando concurran razones de interés general o bien cuando por causas justificadas se extinga la necesidad de requerir los servicios objeto del contrato y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas se ocasionaría un daño o perjuicio a la **LN** o se determine la nulidad total o parcial de los actos que dieron origen al instrumento jurídico con motivo de la resolución de una inconformidad, de conformidad con el artículo 78 de la Ley.

III. Nulidades.

Aquellos actos, contratos y convenios que se realicen o celebren en contravención a lo dispuesto por la Ley, su Reglamento y las demás disposiciones aplicables, serán nulos previa determinación de la autoridad competente.

2.11. Contribuciones.

Las contribuciones que se generen con motivo de la prestación de los servicios objeto de la presente contratación serán cubiertas por la **LN** y por el proveedor, de acuerdo con la legislación impositiva vigente.

La **LN** entregará el importe por concepto de Impuesto al Valor Agregado a el proveedor adjudicado, el cual lo enterará a la oficina recaudadora, conforme a la legislación fiscal vigente. Cualquier otro impuesto o derecho de carácter federal o local, distinto al antes señalado, deberá ser cubierto por la o el licitante adjudicado.

2.12. Discrepancias y Controversias.

La convocatoria, el contrato y su Anexo Técnico son los instrumentos que vinculan a las partes en sus derechos y obligaciones. Las estipulaciones establecidas en el contrato no deberán modificar las condiciones previstas en la convocatoria y su Junta de Aclaraciones, en caso de discrepancias prevalecerá lo estipulado en éstas, de conformidad con lo dispuesto por el artículo 66 de la Ley y fracción IV del artículo 126 de su Reglamento.

Para la resolución de cualquier controversia que se pudiera derivar de la interpretación y cumplimiento del contrato que se derive del procedimiento, las partes convienen en someterse a la jurisdicción de los Tribunales Federales, con residencia en la Ciudad de México, por lo que renuncian expresamente a cualquier otro fuero que pudiera corresponderles por la ubicación de sus domicilios presentes o futuros, o por cualquier otra causa de conformidad con lo dispuesto en el artículo 66 de la Ley.

3. FORMA Y TÉRMINOS QUE REGIRÁN LOS DIVERSOS ACTOS DE LA LICITACIÓN.

La presente licitación se lleva a cabo sin reducción en plazos con fundamento en los artículos 42 primer y segundo párrafo de la Ley.

3.1. Fecha, hora y lugar para los actos de la Licitación.

EVENTOS	FECHA	HORA	LUGAR
Publicación de la Convocatoria en la Plataforma.	26/octubre/2026	No aplica	Los actos se realizarán de conformidad con lo establecido en el artículo 36 de la Ley, a través de la Plataforma. Al tratarse de una Licitación electrónica, las o los licitantes únicamente podrán participar a través de la Plataforma.
Envío del Resumen de la publicación al DOF.	26/octubre/2026	No aplica	
Junta de Aclaraciones a la Convocatoria.	04/noviembre/2026	11:00	
Acto de Presentación y Apertura de Proposiciones.	11/noviembre/2026	11:00	
Acto de Fallo.	17/noviembre/2026	17:00	

Los eventos a través de medios electrónicos se realizarán en el domicilio de la convocante, señalado en el numeral 1.1. de la presente convocatoria.

3.2. Junta de Aclaraciones

La Junta de Aclaraciones se llevará a cabo conforme a lo dispuesto en los artículos 44 de la Ley, 90 y 91 del Reglamento, por lo que las o los licitantes que manifiesten su interés en participar en la licitación deberán realizarlo utilizando para tal caso la **plantilla disponible en la Plataforma**, con el cual serán considerados como licitantes y tendrán derecho a formular solicitudes de aclaración utilizando para tal caso la **plantilla disponible en formato Excel en la Plataforma.**

En su caso, las o los licitantes que deseen enviar solicitudes de aclaración deberán realizarlas 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. Las solicitudes que no cumplan con los requisitos señalados serán desechadas por la convocante, de conformidad con lo señalado en el séptimo párrafo del artículo 90 del Reglamento.

El plazo para enviar dichas solicitudes será a más tardar **veinticuatro horas antes** de la fecha y hora en que se realice la Junta de Aclaraciones, de conformidad con lo establecido en el artículo 44 de la Ley cuarto párrafo.

La convocante procederá a enviar a través de la Plataforma las contestaciones a las solicitudes de aclaración recibidas, por lo que todos las o los licitantes se darán por notificados a través de este medio. Las solicitudes de aclaración que sean recibidas con posterioridad al plazo antes previsto no serán contestadas por resultar extemporáneas de conformidad con lo establecido en el artículo 91 fracción IV del Reglamento.

Cuando en razón del número de solicitudes recibidas o algún otro factor no imputable a la convocante y que sea acreditable, el servidor público que presida la Junta de Aclaraciones informará a las o los licitantes si éstas serán enviadas conforme lo programado o si se suspenderá la sesión para reanudarla en hora o fecha posterior a efecto de que se remitan las respuestas en forma.

Con el envío de las respuestas a que se refiere el párrafo anterior, la convocante informará a las o los licitantes, atendiendo al número de solicitudes de aclaración contestadas, el plazo que estos tendrán para formular las preguntas que consideren necesarias en relación con las respuestas remitidas. Dicho plazo no podrá ser inferior a seis ni superior a cuarenta y ocho horas. Una vez recibidas las preguntas a las respuestas otorgadas

por la convocante, ésta informará a las o los licitantes el plazo máximo en el que enviará las contestaciones correspondientes.

Cualquier modificación a la Convocatoria realizada en los tiempos establecidos para tal efecto en la Ley y las que resulten de la o las Juntas de Aclaraciones, formarán parte de la presente Convocatoria y deberán ser consideradas por las o los licitantes en la elaboración de su proposición.

El contenido del Acta de la Junta de Aclaraciones se difundirá a través de la Plataforma el mismo día en que se emita, lo anterior para efectos de notificación a las o los licitantes en el entendido de que este procedimiento sustituye a la notificación personal, con fundamento en lo establecido en el artículo 50 de la Ley y 94 segundo párrafo del Reglamento.

De conformidad con el primer párrafo del artículo 50 de la Ley, las actas de las juntas de aclaraciones serán firmadas por los licitantes que hubieran enviado preguntas, sin que la falta de firma de alguno de ellos reste validez o efectos a las mismas.

No se omite señalar que con fundamento en el artículo 35 décimo párrafo de la Ley, a los actos del procedimiento de licitación pública podrá asistir cualquier persona en calidad de observador, bajo la condición de registrar su asistencia y abstenerse de intervenir en cualquier forma en los mismos.

3.3. Acto de Presentación y Apertura de Proposiciones.

El acto de Presentación y Apertura de Proposiciones se llevará a cabo en términos de los artículos 45 y 46 de la Ley, 92, 93, 94 segundo párrafo y 99 primer y segundo párrafo del Reglamento, conforme a lo dispuesto en el numeral 3.1 de la convocatoria. Las proposiciones se recibirán a través de la Plataforma, por lo que se estará a lo dispuesto en el Acuerdo y el soporte documental deberá remitirse de forma legible (en archivo PDF sin utilizar baja resolución, formato imagen jpg o equivalente).

Asimismo, se precisa que en la documentación técnica, legal y económica que integre la proposición remitida a través de la Plataforma se deberán emplear los medios establecidos en el artículo 83 de la Ley.

Si por causas ajenas a la voluntad de la SABG o de la convocante, no fuera posible abrir los archivos que contengan las propuestas enviadas por medios remotos de comunicación electrónica, el acto se reanudará a partir de que se restablezcan las condiciones que dieron origen a la interrupción.

Una vez recibidas las proposiciones que hayan sido enviadas a través de la Plataforma, se procederá a la apertura de todas y cada una de ellas, haciéndose constar la documentación presentada, sin que ello implique la evaluación de su contenido, por lo que, en el caso de que algún licitante omita la presentación de algún documento o algún requisito, no serán desechadas en ese momento, haciéndose constar ello en el formato de recepción de los documentos que integran la propuesta conforme al **Anexo XV Acuse de recepción de la documentación conforme a los numerales 4.1, 4.2 y 4.3 de la Convocatoria**, lo anterior de conformidad con lo establecido el artículo 95 del Reglamento.

Se informa que por tratarse de una licitación electrónica, en términos de los artículos 36 y 85 segundo párrafo, inciso d) de la Ley y en concordancia con el numeral 24 del Acuerdo, las proposiciones recibidas en dicha Plataforma no se imprimirán en su totalidad, toda vez que se generará un expediente (sobre digital), el cual contendrá toda la información del presente procedimiento, por lo que la convocante procederá a descargar la proposición misma que consta de la propuesta técnica y económica, cabe aclarar que la propuesta técnica incluye la documentación legal y administrativa; proposición que se grabará en medio digital (Disco compacto) y únicamente se imprimirá la propuesta económica, que será rubricada por el servidor público que presida el acto de Presentación y Apertura de Proposiciones.

El servidor público que presida el acto, atendiendo al número de proposiciones presentadas y a las partidas licitadas, podrá optar entre dar lectura al precio unitario de cada una de las partidas que integran las proposiciones, o anexar copia de la propuesta económica de las o los licitantes al acta respectiva, debiendo en este último caso, dar lectura al importe total de cada proposición. En ambos supuestos el análisis detallado de las proposiciones se efectuará posteriormente por la convocante, al realizar la evaluación de las mismas, de conformidad con el artículo 92 sexto y séptimo párrafo del Reglamento de la Ley.

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

Sin perjuicio de lo anterior, en caso de presentarse alguna inconformidad respecto de la partida adjudicada, la cotización estará vigente hasta en tanto ésta no sea resuelta.

No se omite señalar que con fundamento en el artículo 35 décimo párrafo de la Ley, a los actos del procedimiento de licitación pública podrá asistir cualquier persona en calidad de observador, bajo la condición de registrar su asistencia y abstenerse de intervenir en cualquier forma en los mismos.

3.4. Proposiciones conjuntas.

Se aceptan proposiciones conjuntas, de conformidad con el artículo 45 cuarto párrafo de la Ley y 88 del Reglamento, para lo cual la o el representante común de la agrupación deberá señalar que la proposición se presenta en forma conjunta. **El convenio de Participación Conjunta** se presentará con la proposición y, en caso, de que a las o los licitantes que la hubieren presentado se les adjudique el contrato, dicho convenio, formará parte integrante del mismo como uno de sus anexos, para lo cual deberán de firmar todos los representantes de las personas morales que hayan firmado el convenio de participación conjunta, o el representante de la nueva sociedad, lo cual deberá de constar en escritura pública.

Cualquiera de los integrantes de la agrupación, podrá presentar el escrito mediante el cual manifieste su interés en participar en la Junta de Aclaraciones y en el procedimiento de contratación.

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

a) Nombre, domicilio y Registro Federal de Contribuyentes de las personas integrantes, señalando, en su caso, los datos de los instrumentos públicos con los que se acredita la existencia legal de las personas morales y, de haberlas, sus reformas y modificaciones, así como el nombre de los socios que aparezcan en éstas;

b) Nombre y domicilio de los representantes de cada una de las personas agrupadas, señalando, en su caso, los datos de las escrituras públicas con las que acrediten las facultades de representación;

c) Designación de un representante común, otorgándole poder amplio y suficiente, para atender todo lo relacionado con la proposición y con el procedimiento de licitación pública;

d) Descripción de las partes objeto del contrato que corresponderá cumplir a cada persona integrante, así como la manera en que se exigirá el cumplimiento de las obligaciones, y

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

f) Precisar si la proposición conjunta es ofertada por grandes empresas o sin identificación de la estratificación de sus integrantes, si se trata de una proposición conjunta sostenible, o bien, si se trata de una proposición conjunta sostenible estratégica, adjuntando la documentación que lo avale.

En caso de exhibir propuesta conjunta, se deberá de presentar el convenio de Participación Conjunta. **Para cada una de las personas agrupadas deberá presentar en forma individual los siguientes escritos:** además del Convenio de Participación Conjunta**,** Acreditamiento de personalidad jurídica persona física o persona moral (**ANEXO II o III**), Escrito de los supuestos establecidos en los artículos 71 y 90 de la Ley (**Anexo IV**), Declaración de Integridad **(Anexo V),** Escrito de Nacionalidad **(Anexo VI),** Escrito de Aceptación de condiciones de la Plataforma **(Anexo VII),** Manifestación de vínculos **(Anexo VIII),** Manifestación de beneficios o ventajas **(Anexo IX),** Manifestación de subcontratación **(Anexo X),** en su caso la estratificación de las micro, pequeñas o medianas empresas (**Anexo XI),** además deberán de presentar Identificación oficial vigente del representante legal, pasaporte vigente, cartilla del Servicio Militar Nacional liberada, credencial para votar vigente y las opiniones de cumplimiento de obligaciones de cada uno de los integrantes de la propuesta conjunta.

3.5. Envío de una sola proposición.

Las o los licitantes sólo podrán presentar una proposición para esta Licitación, de conformidad con el artículo 35 noveno párrafo de la Ley.

3.6. Presentación de la documentación distinta a la propuesta técnica y propuesta económica.

La o el licitante podrá presentar a su elección, dentro o fuera de los parámetros técnicos y económicos la documentación distinta a la propuesta técnica y propuesta económica, misma que invariablemente forma parte de su proposición.

3.7. Acreditamiento de personalidad jurídica.

Las o los licitantes deberán presentar acreditamiento de personalidad jurídica persona física **(ANEXO II)** o acreditamiento de personalidad jurídica persona moral **(ANEXO III)**, según corresponda, debidamente requisitado.

3.8. Acto de Fallo y Firma de Contrato.

a) Acto de Fallo

El Fallo se emitirá de conformidad con el artículo 49 de la Ley, en la fecha, lugar y hora establecidas en el numeral 3.1 de esta Convocatoria o en el acta de presentación y apertura de proposiciones, en caso de que en la fecha originalmente prevista no se pueda emitir, el mismo podrá ser diferido hasta por veinte días naturales posteriores a la fecha señalada.

El contenido de dicho Fallo se difundirá a través de la Plataforma el mismo día en que se emita, en el entendido de que esta publicación sustituye a la notificación personal, conforme lo establecido en el artículo 50 segundo párrafo de la Ley.

b) Firma de Contrato

Previamente a la firma del instrumento jurídico, el licitante adjudicado deberá presentar dentro de los 2 días hábiles posteriores a la notificación del fallo mediante escrito en la Gerencia de Adquisiciones de la Dirección de Recursos Materiales y Servicios Generales, ubicada en Avenida Insurgentes Sur 1397, Colonia Insurgentes Mixcoac, Demarcación Territorial Benito Juárez, Código Postal, 03920, Ciudad de México, con teléfono 555482-0000, extensión 5700, de 9:00 a 14:00 horas, la documentación que se enlista a continuación en original para cotejo y 1 (copia) tamaño carta acompañado de un checklist para persona física o en su caso para persona moral".

DOCUMENTACIÓN QUE DEBE(N) PRESENTAR LA (LAS) O EL (LOS) LICITANTE (S) QUE RESULTE(N) ADJUDICADO(S) O ADJUDICADA(S).

La o el licitante adjudicado(a) deberá presentar a la Gerencia de Adquisiciones a partir del día siguiente hábil del Acto de Fallo, teniendo un término de 2 días hábiles, los siguientes documentos (NO deberán integrarse en la proposición a fin de agilizar la recepción de las proposiciones):

Checklist persona física

GERENCIA DE ADQUISICIONES			
No. DE CONTRATO			
PROVEEDOR			
OBJETO DEL CONTRATO			
PROCEDIMIENTO			
DOCUMENTACIÓN QUE SE ANEXA			
ANEXOS	DOCUMENTO	SI / NO	NO APLICA (NA)
1	Constancia de Situación Fiscal		
2	Clave Única de Registro de Población		
3	Acta de nacimiento o en su caso, carta de naturalización respectiva, expedida por la autoridad competente.		
4	Identificación oficial vigente con fotografía de la persona física		
5	Comprobante de Domicilio (actualizado, no mayor a tres meses)		
6	Carta de pago interbancario o de estado de cuenta (actualizado no mayor a tres meses)		
7	Carta original bajo protesta de decir verdad que no se encuentra en los supuestos señalados en los artículos 71 y 90 de la LAASSP.		
8	Carta original bajo protesta de decir verdad, en el que manifieste no encontrarse dentro del supuesto establecido en el artículo 49 fracción IX, de la Ley General de Responsabilidades Administrativas.		
9	Carta original bajo protesta de decir verdad, en la que manifieste que cumplirá con la regla 2.1.28 primer párrafo de la Resolución Miscelánea Fiscal para el año 2026.		

10	Documento vigente expedido por el SAT, en el que se emita la opinión positiva del cumplimiento de sus obligaciones fiscales.		
11	Documento expedido por el Instituto Mexicano del Seguro Social en el que, emita opinión de cumplimiento positiva respecto al cumplimiento de sus obligaciones fiscales en materia de seguro social.		
12	Constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos sin adeudo o con garantía, expedida por el Instituto de Fondo Nacional de la Vivienda para los Trabajadores.		
13	Inscripción en el Registro de Prestadoras de Servicios Especializados u Obras Especializadas, mismo que deberá estar vigente.		
Fecha de Recepción de documentos			

Checklist persona moral

GERENCIA DE ADQUISICIONES			
No. DE CONTRATO			
PROVEEDOR			
OBJETO DEL CONTRATO			
PROCEDIMIENTO			
DOCUMENTACIÓN QUE SE ANEXA			
ANEXOS	DOCUMENTO	SI / NO	NO APLICA (NA)
1	Constancia de Situación Fiscal		
2	Escritura pública en la que conste que fue constituida conforme a las Leyes Mexicanas y que tiene su domicilio en Territorio Nacional con la constancia de inscripción en el Registro Público de Comercio y en su caso, sus reformas o modificaciones que haya sufrido, siendo que el objeto del mismo este directamente relacionado con el suministro objeto de la contratación y que contenga el poder que se otorgue al representante legal, para la celebración de actos de administración o poder especial para suscribir instrumento jurídico o contratos o bien para llevar a cabo todos los tramites derivados de procedimientos o adjudicación en el Gobierno Federal o su equivalente.		
3	Identificación oficial vigente con fotografía del Representante Legal		
4	Comprobante de Domicilio (actualizado, no mayor a tres meses)		
5	Carta de Pago Interbancario o Estado de Cuenta (actualizado no mayor a tres meses)		
6	Instrumento Notarial con el cual el representante legal acredite su personalidad.		

7	Carta original bajo protesta de decir verdad que no se encuentra en los supuestos señalados en los artículos 71 y 90 de la LAASSP.		
8	Carta original bajo protesta de decir verdad, en el que manifieste no encontrarse dentro del supuesto establecido en el artículo 49 fracción IX, de la Ley General de Responsabilidades administrativas.		
9	Carta original bajo protesta de decir verdad, en la que manifieste que cumplirá con la regla 2.1.28 primer párrafo de la Resolución Miscelánea Fiscal para el año 2026.		
10	Documento vigente expedido por el SAT, en el que se emita la opinión positiva del cumplimiento de sus obligaciones fiscales.		
11	Documento expedido por el Instituto Mexicano del Seguro Social en el que, emita opinión de cumplimiento positiva respecto al cumplimiento de sus obligaciones fiscales en materia de seguro social.		
12	Constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos sin adeudo o con garantía, expedida por el Instituto de Fondo Nacional de la Vivienda para los Trabajadores.		
13	Inscripción en el Registro de Prestadoras de Servicios Especializados u Obras Especializadas, mismo que deberá estar vigente.		
Fecha de recepción de documentos			

La vigencia del contrato será de veinticuatro **(24) meses** contados a partir del día hábil siguiente a la fecha de la notificación del fallo.

a) Opinión positiva de cumplimiento de obligaciones fiscales emitida por el SAT vigente a la firma del contrato, cuando el monto exceda de $300,000.00 (trescientos mil pesos 00/100 M.N.) sin incluir el IVA, la o el licitante que resulte adjudicado deberá hacer pública la opinión del cumplimiento de obligaciones fiscales, lo anterior, de conformidad con lo establecido en el artículo 32-D del Código Fiscal de la Federación, en relación con las disposiciones 2.1.24. y 2.1.28 de la Resolución Miscelánea Fiscal para 2026, publicada en el Diario Oficial de la Federación el 28 de diciembre de 2025, requisito sin el cual tampoco es factible la formalización del instrumento correspondiente.

b) Opinión positiva de cumplimiento de obligaciones en materia de seguridad social vigente a la firma del contrato, emitida por el IMSS, cuando el monto exceda de $300,000.00 (trescientos mil pesos 00/100 M.N.) sin incluir el IVA, en términos del artículo 32-D del Código Fiscal de la Federación y del Acuerdo ACDO.AS2.HCT.300925/288.P.DIR publicado en el DOF el 06 de octubre de 2025.

Así mismo, deberá de considerar lo señalado en el "**ANEXO II**" de las "**Disposiciones transitorias aplicables a las "Reglas de carácter general para la obtención de la opinión del cumplimiento de obligaciones fiscales en materia de seguridad social", aprobadas y reformadas por el H. Consejo Técnico del Instituto Mexicano del Seguro Social.**", publicado en el DOF el día 06 de octubre de 2025, que a la letra cita:

Primera. *La opinión del cumplimiento de obligaciones fiscales en materia de seguridad social se considerará válida durante los plazos de quince días hábiles o de veinte días hábiles -tratándose de contrataciones derivadas de procedimientos consolidados-, previstos en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público o de quince días naturales en tratándose de la Ley de Obras Públicas y Servicios Relacionados con las Mismas, que la persona contribuyente tiene para la formalización de las contrataciones referidas en el artículo 32-D del Código Fiscal de la Federación.*

Segunda. *Para efectos de lo previsto en la disposición anterior, la persona contribuyente deberá acreditar ante el ente público contratante que la opinión del cumplimiento de obligaciones fiscales en materia de seguridad social fue obtenida durante los plazos que la persona contribuyente tiene para la formalización del contrato correspondiente, en términos de las disposiciones jurídicas aplicables.*

c) Opinión en el que conste que se encuentra al corriente de cumplimiento de obligaciones en materia de aportaciones patronales y entero de descuentos del Instituto del Fondo Nacional de la Vivienda para los Trabajadores emitida por el INFONAVIT, en términos del artículo 32-D del Código Fiscal de la Federación y del "**AVISO por el que se hace del conocimiento del público en general las modificaciones al 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 el 10 de noviembre de 2025), por lo que en caso de no presentarla o presentar una opinión negativa o un documento apócrifo, no se llevará a cabo la formalización del instrumento jurídico correspondiente.

d) Escrito en el cual el particular manifieste **bajo protesta de decir verdad** que no desempeña empleo, cargo o comisión en el servicio público o, en su caso que, a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un Conflicto de Interés. En caso de que la o el licitante que resulte adjudicado sea persona moral, dichas manifestaciones deberán presentarse respecto a los socios o accionistas que ejerzan control sobre la sociedad, de conformidad con los artículos 71 y 90 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. **Anexo XVI.**

e) Se solicita a la o el licitante que resulte adjudicado(a), remita a más tardar el día hábil siguiente a la notificación del acto de Fallo, la propuesta técnica y económica presentada en el acto de Presentación y Apertura de Proposiciones, en medio electrónico y editable, lo anterior para que se agilice y facilite el manejo de la información requerida por la Gerencia de Adquisiciones para la elaboración del instrumento contractual derivado del presente procedimiento de contratación.

La firma del contrato se llevará a cabo dentro de los 15 días hábiles posteriores a la notificación del fallo, invariablemente a través del Módulo de Formalización de Instrumentos Jurídicos (incluye presentación de garantías no fiscales, entregables de cumplimiento contractual, convenios modificatorios, entre otros) mismo que deberá ser consultado tanto proveedores como administradores de los contratos, en la siguiente dirección electrónica: https://comprasmx.buengobierno.gob.mx/mfij, en consecuencia, el Administrador del Contrato deberá solicitar su registro a la Dirección de Recursos Materiales y Servicios por única ocasión, siendo indispensable tener actualizada su firma electrónica avanzada proporcionada por el Servicio de Administración Tributaria (SAT).

No se omite señalar, que el incumplimiento a lo anterior dará como consecuencia las responsabilidades administrativas que correspondan.

Conforme a lo establecido en el artículo **67** de la LAASSP, los derechos y obligaciones que se deriven del instrumento jurídico respectivo no podrán ser transferidos por el licitante adjudicado en favor de cualquier otra

persona, con excepción de los derechos de cobro, en cuyo caso se deberá contar con el consentimiento de la Convocante.

4. REQUISITOS QUE LAS O LOS LICITANTES DEBEN CUMPLIR.

Con fundamento en los artículos 36 y 45 de la Ley, las o los licitantes deberán remitir a través de la Plataforma, su proposición, misma que consta de la propuesta técnica y económica, cabe aclarar que la propuesta técnica incluye la documentación legal y administrativa, firmada con la firma electrónica avanzada que emitió el SAT en favor de la o el licitante y/o representante común de ser el caso de participación conjunta, para el cumplimiento de sus obligaciones fiscales.

En caso de que no se presente propuesta técnica o propuesta económica, no será objeto de evaluación la propuesta presentada y será motivo de desechamiento de conformidad con el numeral 4.4 de la presente Convocatoria.

De acuerdo con lo dispuesto en el artículo 95 del Reglamento, los/as licitantes deberá foliar cada uno de los documentos que integren la proposición y aquéllos distintos a ésta, en todas y cada una de las hojas que los integren.

Al efecto, se deberán numerar de manera individual la propuesta técnica (establecida en los numerales 4.1 y 4.2 de la presente) y económica (establecida en el numeral 4.3 de la presente), así como el resto de los documentos que entreguen los/as licitantes. La falta total de folios no afecta la solvencia de las proposiciones, en el caso de que alguna o algunas hojas o la totalidad de los documentos carezcan de folio y se constate que la o las hojas no foliadas mantienen continuidad, no será causa de desechamiento. Lo anterior de conformidad a lo previsto en el Artículo 95 del Reglamento.

De conformidad a lo dispuesto en el artículo 86 de la Ley, las personas físicas y morales interesadas en participar en el presente procedimiento de contratación, deberá inscribirse en el registro electrónico de personas físicas y morales, y mantener actualizada la información que le sea requerida, conforme a los lineamientos que establezca la Secretaría.

Por ser una Licitación electrónica, podrá enviarse en varios archivos electrónicos.

4.1. Documentación legal y Administrativa.

La o el licitante deberá presentar los siguientes documentos debidamente requisitados, los cuales se consideran **indispensables para la evaluación de la proposición** y, en consecuencia, su incumplimiento afectaría su solvencia y motivaría su desechamiento:

a) Acreditamiento de Personalidad Jurídica.

Escrito **Bajo Protesta de Decir Verdad**, en el que manifieste que cuenta con facultades suficientes para comprometerse por sí o por su representada señalando su actividad comercial o su objeto social, según corresponda, así como el domicilio para el cumplimiento de las obligaciones derivadas del presente procedimiento. **ANEXO II o III.**

b) Acta constitutiva

Documento legal donde se estipulan todos los aspectos fundamentales de la empresa, y se regulan tanto la estructura como el control quiénes son los miembros que la forman.

c) Identificación Oficial.

Identificación oficial vigente por ambos lados de quien firma la proposición, la que deberá contener firma y fotografía, debiendo ser únicamente: pasaporte, cartilla del Servicio Militar Nacional liberada, credencial para votar. Para el caso de personas morales, la identificación deberá corresponder al Representante legal.

d) Escrito de los supuestos establecidos en los artículos 71 y 90 de la Ley.

Escrito **bajo protesta de decir verdad**, que no se ubica en los supuestos establecidos en los artículos 71 y 90 de la Ley, de acuerdo con el **Anexo IV** de la Convocatoria.

e) Escrito de Declaración de Integridad.

Declaración de integridad, en la que la o el licitante manifieste, **bajo protesta de decir verdad** que por sí mismo (persona física) o la empresa que representa se abstendrá por sí misma o a través de interpósita persona (persona moral), de adoptar conductas para que los servidores públicos, induzcan o alteren las evaluaciones de las proposiciones, el resultado del procedimiento u otros aspectos que le otorguen condiciones más ventajosas con relación a los demás participantes, así como de incorporar durante la vigencia de los contratos a personas que se encuentren inhabilitadas conforme al **Anexo V** de la Convocatoria.

f) Escrito de Nacionalidad.

Escrito de la o el licitante en el cual manifieste **bajo protesta de decir verdad** que es de nacionalidad mexicana y cumplen con lo establecido en el artículo 39, fracción I de Ley, así como el artículo 58 de su Reglamento, para lo cual deberá requisitar el **Anexo VI.**

g) Convenio de participación conjunta.

En caso de exhibir propuesta conjunta, se deberá de presentar el Convenio de Participación Conjunta. **Para cada una de las personas agrupadas deberá presentar en forma individual los siguientes escritos:** además del Convenio de Participación Conjunta, Acreditamiento de personalidad jurídica persona física o persona moral (**ANEXO II o III**), Escrito de los supuestos establecidos en los artículos 71 y 90 de la Ley (**Anexo IV**), Declaración de Integridad **(Anexo V),** Escrito de Nacionalidad **(Anexo VI),** Escrito de Aceptación de condiciones de la Plataforma **(Anexo VII),** Manifestación de vínculos **(Anexo VIII),** Manifestación de beneficios o ventajas **(Anexo IX),** Manifestación de subcontratación **(Anexo X),** en su caso la estratificación de las micro, pequeñas o medianas empresas **(Anexo XI),** además deberán de presentar Identificación oficial vigente del representante legal, pasaporte vigente, cartilla del Servicio Militar Nacional liberada, credencial para votar vigente.

h) Escrito de aceptación de las condiciones de la Plataforma.

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 la proposición y/o demás información no pueda abrirse por tener algún virus informático o por cualquier otra causa ajena a la **LN**, en términos de lo dispuesto por el numeral 29 del Acuerdo, para lo cual podrá utilizar el **Anexo VII** Escrito de Aceptación de condiciones de la Plataforma.

i) Manifestación de vínculos.

Escrito de la o el licitante afirme o niegue, **bajo protesta de decir verdad,** los vínculos o relaciones de negocios, laborales, profesionales, personales o de parentesco con consanguinidad o afinidad hasta el cuarto grado de las personas servidoras públicas que establece el Protocolo de Actuación en Contrataciones, para lo cual deberá requisitar el **Anexo VIII**.

j) Manifestación de beneficios o ventajas.

Escrito de la o el licitante, **bajo protesta de decir verdad,** manifestando que no ejecuta con otro licitante acciones que impliquen o tengan por objeto obtener un beneficio o ventaja indebida en el procedimiento, para lo cual deberá requisitar el **Anexo IX**.

k) Manifestación de subcontratación.

Escrito de la o el licitante, **bajo protesta de decir verdad,** manifestando que, en caso de resultar ganador, no podrá subcontratar a otro licitante que haya presentado proposición en el presente procedimiento, para lo cual deberá requisitar el **Anexo X**.

l) Manifestación de Correo Electrónico

Escrito de la o el licitante, **bajo protesta de decir verdad,** donde señala una cuenta de correo electrónico oficial como domicilio electrónico válido para recibir notificaciones, avisos, requerimientos y comunicaciones derivadas de la presente licitación.

m) Escrito de estratificación de las micro, pequeñas y medianas empresas.

Escrito en el que la o el licitante indique que cuenta con estratificación como micro, pequeña o mediana empresa, de acuerdo con el Anexo XI de la Convocatoria.

n) Información reservada y confidencial.

Escrito mediante el cual la o el licitante deberá indicar si en los documentos que proporciona a la LN se contiene información de carácter confidencial o reservada, señalando los documentos o las secciones de éstos que la contengan, así como el fundamento y motivación por los cuales considera que tengan ese carácter, conforme al Anexo XII Información Reservada y Confidencial. Cabe señalar que de no clasificarse la información por parte de la o el licitante en los términos señalados, o no señalar motivo y fundamento de la clasificación, la información presentada como parte de su propuesta técnica y económica, aclarando que la propuesta técnica incluye la documentación legal y administrativa tendrá tratamiento de información de carácter público de conformidad con el artículo 115 de la Ley General de Transparencia y Acceso a la Información Pública en vigor.

Adicionalmente, la o el licitante podrá presentar los siguientes documentos, los cuales no afectan la solvencia y por lo tanto el incumplimiento no será causa de desechamiento:

o) Opinión de obligaciones SAT.

Opinión positiva de cumplimiento de obligaciones fiscales emitida por el SAT vigente a la fecha de presentación y apertura de proposiciones del presente procedimiento de contratación, cuando el monto exceda de $300,000.00 (trescientos mil pesos 00/100 M.N.) sin incluir el IVA, la o el licitante que resulte adjudicado deberá hacer pública la opinión del cumplimiento de obligaciones fiscales, lo anterior, de conformidad con lo establecido en el artículo 32-D del Código Fiscal de la Federación, en relación con las disposiciones 2.1.24. y 2.1.28 de la Resolución Miscelánea Fiscal para 2026, publicada en el Diario Oficial de

la Federación el 28 de diciembre de 2025, requisito sin el cual tampoco es factible la formalización del instrumento correspondiente.

p) Opinión de obligaciones IMSS.

Opinión positiva de cumplimiento de obligaciones en materia de seguridad social vigente a la fecha de presentación y apertura de proposiciones del presente procedimiento de contratación, emitida por el IMSS, cuando el monto exceda de $300,000.00 (trescientos mil pesos 00/100 M.N.) sin incluir el IVA, en términos del artículo 32-D del Código Fiscal de la Federación y del Acuerdo ACDO.AS2.HCT.300925/288.P.DIR publicado en el DOF el 06 de octubre de 2025.

q) Opinión de obligaciones INFONAVIT

Opinión en el que conste que se encuentra al corriente de cumplimiento de obligaciones en materia de aportaciones patronales y entero de descuentos del Instituto del Fondo Nacional de la Vivienda para los Trabajadores emitida por el INFONAVIT, vigente a la fecha de presentación y apertura de proposiciones del presente procedimiento de contratación, en términos del artículo 32-D del Código Fiscal de la Federación y del "AVISO por el que se hace del conocimiento del público en general las modificaciones al 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, en los términos que se indican." (Publicado el 10 de noviembre de 2025) por lo que en caso de no presentarla o presentar una opinión negativa o un documento apócrifo, no se llevará a cabo la formalización del instrumento jurídico correspondiente.

4.2. Propuesta técnica

"LOS LICITANTES" deberán presentar su propuesta técnica conforme a la descripción amplia y detallada contenidas en el presente numeral, en el Anexo Técnico y deberán incluir la siguiente documentación:

A. Propuesta Técnica en hoja membretada firmada por el Representante Legal en el que se describa ampliamente los (bienes y/o servicios) que ofrece, en concordancia con lo señalado en el presente Anexo Técnico, dando cumplimiento a todas y cada una de las especificaciones técnicas establecidas.

B. Escrito en hoja membretada firmado por el Representante Legal, en el cual manifieste que cuentan con capacidad de respuesta inmediata, así como con los recursos técnicos, financieros y demás que sean necesarios, y cuyas actividades comerciales o profesionales estén relacionadas con la prestación del servicio, entrega de los bienes o arrendamiento. (ANEXO B).

C. Escrito de no existencia de conflicto de interés: los licitantes deberán entregar dentro de su propuesta técnica escrito firmado por el representante legal manifestando la no existencia de conflicto de interés al no prestar o desarrollar servicios o bien de estar relacionado con una empresa o filial que actualmente preste o desarrolle servicios de operación y seguridad en las TIC's de "LOTERÍA".

D. EL LICITANTE deberá presentar las siguientes cartas firmadas por el representante legal del fabricante de los productos que actualmente tiene Lotería Nacional, lo anterior, en apego a los artículos 54 y 55 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, toda vez que el área requirente verificó que estos requerimientos guardan relación directa con el objeto de la contratación y no limitan la libre participación, concurrencia o competencia económica. Derivado de la verificación efectuada por el área requirente, se determina que, por la naturaleza técnica, operativa y sensible de los servicios requeridos, resultan necesarias estos requisitos para que EL LICITANTE acredite contar con los conocimientos, habilidades y controles suficientes para garantizar la correcta prestación del servicio, la

calidad en su ejecución y la protección de la información que sea tratada, procesada, almacenada o administrada con motivo del contrato. que oferte, donde cumpla con lo siguiente:

- Nivel mínimo Expert para las licencias de Trend Micro propiedad de Lotería.
- Nivel mínimo Advanced para los equipos Firewall Fortinet propiedad de Lotería.

Aunado a lo anterior, deberá presentar:

- Carta del representante legal del Fabricante, que es Socio de Negocio de las tecnologías ofertadas para dar cumplimiento a los servicios a ser implementados y que mientras se tenga licenciamiento y soporte vigente contarán con apoyo técnico del mismo en caso de ser requerido para los siguientes servicios:
    - Protección de Información en Correo Electrónico
    - Visibilidad y Monitoreo de los Usuarios
    - Segmentación Zero Trust
    - Protección de Endpoint de siguiente generación (EDR)
    - Entorno de ataque cambiante (EAC)
    - Servicio de Diagnóstico y Reparación de Configuraciones Erróneas
    - Servicio de Firewall de Siguiente Generación (NGFW)
    - Servicio de Protección a Aplicaciones Móviles
    - Servicio de Correlación de Eventos
    - Servicio de Orquestación, Automatización y Respuesta de Seguridad
    - Servicio de Ciberinteligencia
    - Gestión de vulnerabilidades para endpoints y servidores
- Carta firmada por el representante legal del fabricante del producto ofertado indicando que cuentan con al menos el segundo nivel más alto de partner para los siguiente servicios:
    - Protección de Información en Correo Electrónico
    - Visibilidad y Monitoreo de los Usuarios
    - Segmentación Zero Trust
    - Protección de Endpoint de siguiente generación (EDR)
    - Entorno de ataque cambiante (EAC)
    - Servicio de Diagnóstico y Reparación de Configuraciones Erróneas
    - Servicio de Firewall de Siguiente Generación (NGFW)
    - Servicio de Protección a Aplicaciones Móviles
    - Servicio de Correlación de Eventos
    - Servicio de Orquestación, Automatización y Respuesta de Seguridad
    - Servicio de Ciberinteligencia

E. Copia de los certificados vigentes a nombre DEL LICITANTE, los cuales deberán ser emitidos por una autoridad certificadora reconocida y avalada para la emisión de certificaciones en las normas ISO ISO/IEC 27001:2022, ISO/IEC 20000-1:2018, ISO 22301:2019, ISO 9001:2015 e ISO 37001:2016.

F. EL LICITANTE deberá presentar una carta, en papel membretado y firmada por su representante legal donde especifique lo siguiente:

- Que cualquier software, marca y/o patente de algún sistema, aplicativo o programa que sea utilizado para la prestación del servicio objeto de la presente licitación, ha sido adquirido y/o se encuentra licenciado debidamente, cumpliendo con todas las disposiciones legales pertinentes en México.

- Que, en caso de infracción o reclamación relacionada con derechos de autor, marcas, patentes o cualquier otro derecho de propiedad intelectual vinculado con el software, sistemas, aplicativos o programas utilizados para la prestación del servicio, [Nombre de la Empresa o Licitante] se compromete a:

    a) Defender, indemnizar y mantener indemne a "LOTERÍA", contra cualquier reclamación, demanda, acción legal, daño, pérdida, costo o gasto, incluyendo honorarios legales, derivados de dicha infracción o reclamación.

b) Tomar las medidas necesarias para garantizar la continuidad de la prestación del servicio a "LOTERÍA", sin que ello implique un costo adicional para la misma

G. Documentación que EL LICITANTE deberá presentar por cada uno de sus recursos humanos enlistados para el cumplimiento del subrubro "PERFIL REQUERIDO" del Anexo Técnico es la siguiente:

1) Currículum vitae que cumpla con el perfil y certificaciones solicitadas, el cual debe de incluir:
   - Nombre completo.
   - Escolaridad.
   - Años de experiencia.
   - Teléfono.
   - Correo electrónico.

Descripción de certificado(s) requerido (s) en el ANEXO TÉCNICO.

1) Acreditar la relación laboral con "EL LICITANTE" presentando copia simple del último pago ante el IMSS y/o documento afiliatorio ante el IMSS, pudiendo testar información sensible.
2) Presentar copia simple de la identificación oficial vigente del personal propuesto.

H. Currículo Empresarial donde se describen las actividades y los clientes de la empresa.

I. "EL LICITANTE" deberá presentar al menos 3 contratos en copia simple, celebrados con Dependencias y/o Entidades Públicas o Sector Privado, demostrando experiencia mínima de 3 años en la prestación de servicios similares a los requeridos en el Anexo Técnico

4.3. Propuesta económica

La o el licitante deberá presentar su propuesta económica debidamente firmada y requisitada con la información solicitada en el numeral 4.3 y el Anexo **XIV**, en caso de no usar el **Anexo XIV**, el documento que se remitido podrá usar otro formato. Para ambos casos deberá contener la información señalada en los incisos del **A.** hasta el **H**. del presente numeral

Para efectos de agilizar el procedimiento se solicita a la o el licitante su propuesta económica en versión editable word o excel.

La propuesta económica deberá cumplir con lo siguiente:

A. Señalar el número del presente procedimiento.

B. Fecha de emisión de la propuesta económica, misma que deberá ser entre el periodo comprendido entre la fecha de la conclusión de la última Junta de Aclaraciones y la fecha del Acta de Presentación y Apertura de Proposiciones.

C. Se deberá cotizar en moneda nacional y a dos decimales.

D. Deberá cotizar el precio unitario de cada uno de los conceptos indicados del servicio objeto de la presente Licitación, sin IVA, establecer el importe, subtotal, IVA y total; así mismo deberá de requisitar el cuadro resumen, para lo cual podrá utilizar el **Anexo XIV**.

E. La vigencia de la cotización será de 60 (sesenta) días naturales; Los precios serán fijos durante la vigencia del contrato, así como su conformidad a las condiciones de pago establecidas en el Anexo Técnico,

aceptando que en caso de que la Secretaría Anticorrupción y Buen Gobierno, derivado de una inconformidad, decrete la suspensión del procedimiento, la proposición enviada permanecerá vigente.

F. Deberá Indicar que los precios serán fijos durante la vigencia del contrato.

G. Manifestar su conformidad con las condiciones de pago establecidas en esta convocatoria.

H. Folio en la propuesta económica.

Se precisa que **no será objeto de evaluación** la información capturada en el apartado "**Parámetros Económicos**" de la Plataforma.

4.4. Causales expresas de desechamiento.

Será causal de desechamiento:

a) Cuando la actividad económica u objeto social de la o el licitante manifestada en los Acreditamientos de personalidad jurídica persona física (**ANEXO II**) o Acreditamiento de personalidad jurídica persona moral (**ANEXO III**), según corresponda, no se encuentren relacionada con el objeto de contratación de la presente Convocatoria.

b) Cuando no presente escrito **"Bajo protesta de decir verdad"**, de que la o el licitante no se ubica en los supuestos establecidos en los artículos 71 y 90 de la Ley, de acuerdo con el **Anexo IV** de la Convocatoria.

c) Cuando de la consulta al directorio de proveedores y contratistas sancionados de la SABG, se advierta que la o el licitante se encuentra enlistado como **inhabilitado** en dicho directorio.

d) Cuando no presente escrito **"Bajo protesta de decir verdad"** que la persona física o la empresa que representa se abstendrá por sí misma o a través de interpósita persona, de adoptar conductas para que los servidores públicos de la **LN**, 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, así como de incorporar durante la vigencia de los contratos a personas que se encuentren inhabilitadas, conforme al **Anexo V** de la Convocatoria.

e) Cuando no presente Identificación Oficial o bien, cuando la identificación oficial presentada no reúna alguno de los requisitos solicitados tales como la fotografía, firma, no esté vigente o para el caso de personas morales no corresponda al representante legal de la persona moral que firma la proposición.

f) Si se comprueba que algún licitante ha acordado con otro u otros elevar el costo del **Servicio** objeto de la Convocatoria, o cualquier otro acuerdo que tenga como fin obtener una ventaja sobre los demás licitantes.

g) La falta de presentación de los escritos o manifestaciones "**bajo protesta de decir verdad"**, que se soliciten como requisito de participación en la Convocatoria será motivo de desechamiento, por incumplir las disposiciones jurídicas que los establecen, conforme al artículo 83 antepenúltimo párrafo del Reglamento.

h) La falta absoluta de folio en la documentación que integre la propuesta técnica, económica, así como el resto de los documentos que entregue la o el licitante, sin embargo, en el caso de que alguna o

algunas hojas o la totalidad de los documentos carezcan de folio y se constate que la o las hojas no foliadas mantienen continuidad, no será causa de desechamiento.

i) Que no cumplan con alguno de los requisitos establecidos en esta Convocatoria contenidos en los numerales **4.1 del inciso a) a la k), 4.2, 4.3 o Anexo Técnico,** así como los que se deriven del Acto de la Junta de Aclaraciones.

j) Cuando la o el licitante presente más de una proposición.

k) Será causa de desechamiento cuando el servicio ofertado incumpla las especificaciones técnicas, alcances, condiciones o requerimientos mínimos establecidos en la convocatoria y su Anexo Técnico, de manera que afecte la solvencia de la proposición.

l) Cuando los documentos que exhiban las o los licitantes no sean legibles imposibilitando el análisis integral de la proposición.

m) Cuando no exista correspondencia, resulten incompletos o incongruentes los datos asentados en su propuesta económica **Anexo XIV**.

n) Cuando la proposición de la o el licitante se remita en una versión que no puede ser descargada de la Plataforma y/o visualizada por encontrarse dañado el archivo o los archivos.

o) La falta de señalamiento de que es de nacionalidad mexicana.

p) Presentar documentación en idioma diverso al español, sin traducción simple al español**.**

q) Cuando las proposiciones conjuntas, no cumplan con uno o más de los requisitos establecidos en el numeral 3.4. Proposiciones conjuntas y 4.1 Inciso g), de la presente Convocatoria.

r) En caso de que el nombre de la o el licitante con el que presenta su proposición en la Plataforma no coincida con el nombre de este en la acreditación de personalidad o en cualquier otro documento que forme parte de la proposición, sin que medie la indicación de que sea una propuesta conjunta**.**

s) Cuando se verifique que la o el licitante se encuentra listado en la relación de contribuyentes con operaciones presuntamente inexistentes, de acuerdo con el SAT.

t) Cuando la información presentada en la proposición contenga información contradictoria, en uno o más documentos,

u) Cuando no se coticen la totalidad de los conceptos o contenidos en la **partida** para la que participa en el **Anexo XIV.**

v) Cuando sólo se presente la propuesta técnica y no se presente la propuesta económica, o viceversa o, la falta de ambas propuestas.

w) Cuando se acredite fehacientemente que el licitante se encuentre en alguno de los supuestos establecidos en el artículo 71 de la LAASSP.

x) En caso de que los precios no sean convenientes o se determine que son no aceptables o cuando el monto ofertado en el procedimiento de contratación exceda el presupuesto autorizado para la contratación de la dependencia o entidad contratante.

y) Cuando los escritos o manifestaciones presentadas no cubran la totalidad de los requisitos solicitados en el Anexo que corresponda, mismo que están referenciados en los "Formatos que facilitarán y agilizarán la presentación y recepción de las proposiciones".

5. CRITERIOS ESPECÍFICOS CONFORME A LOS CUALES SE EVALUARÁN LAS PROPOSICIONES.

5.1. Evaluación legal.

La evaluación legal será realizada por el Área Contratante, verificando que la documentación presentada por la o el licitante cumpla con los requisitos solicitados en el numeral 4.1 de la presente convocatoria, así como los que se deriven del acto de la Junta de Aclaraciones, observando que exista congruencia en la información proporcionada.

Se verificará que la o el licitante no se encuentre listado en la Relación de contribuyentes con operaciones presuntamente inexistentes, de acuerdo con el SAT y en el Directorio de proveedores y contratistas sancionados de la SABG, en caso de encontrarse listado se procederá en términos del numeral 4.4 de la presente convocatoria.

Se verificará que el objeto social de la o el licitante manifestado en el Acreditamiento de personalidad jurídica persona física **(ANEXO II)** o Acreditamiento de personalidad jurídica persona moral **(ANEXO III)**, según corresponda, se encuentre relacionada con el objeto de la contratación de la presente licitación, de no ser así será causa de desechamiento.

Se comprobará que la identificación se encuentre vigente, y que contenga firma y fotografía.

Se verificará el Directorio de proveedores y contratistas sancionados de la SABG, y que corresponda con la manifestación presentada en cumplimiento al inciso c) del numeral 4.1.

Se verificará que los documentos solicitados en los incisos a) al k) del numeral 4.1., se presenten y que estos estén debidamente requisitados.

Para el caso de la fracción VIII del artículo 71 de la Ley, verificar que las o los licitantes no se encuentren vinculados entre sí por algún socio o asociado y de contar con la certeza de la existencia de dicho vínculo, se deberán desechar las proposiciones que en su caso se encuentren vinculadas, debiendo comunicar dicha circunstancia al Órgano Interno de Control, para que dicha autoridad determine si se actualiza lo dispuesto en la fracción IV del artículo 90 de la LAASSP.

En caso de que se presente proposición conjunta, se verificará que el convenio presentado; cumpla con la información señalada en el artículo 88 del Reglamento. El Área Contratante evaluará los términos legales del convenio, y el Área Técnica, la descripción de las partes objeto del Contrato que corresponderá cumplir a cada integrante, en términos del numeral 4.2.2.1.15 del Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Se verificará que la documentación presentada se encuentre foliada de manera continua, sin embargo, en el caso de que alguna o algunas hojas o la totalidad de los documentos carezcan de folio y se constate que la o las hojas no foliadas mantienen continuidad, no será causa de desechamiento.

En caso de no cumplir con alguno de los requisitos establecidos en el presente apartado, se procederá de conformidad con el numeral 4.4 **Causales expresas de desechamiento**.

5.2. Evaluación de la propuesta técnica.

Se empleará el criterio de evaluación por puntos y porcentajes en el presente procedimiento de contratación, conforme a lo establecido en el artículo 47 tercer párrafo de la Ley y 100 de su Reglamento

Se verificará por parte del área técnica que los Licitantes cumplan con las condiciones y requerimientos solicitados en el numeral 4.2. y en el anexo técnico de esta Convocatoria y los que deriven del o los actos de solicitud de aclaraciones.

La Convocante se reserva el derecho de verificar la veracidad o autenticidad de la información y documentación presentada por el Licitante.

Se verificará que la documentación presentada en la propuesta técnica se encuentre foliada de manera continua, no siendo válido el folio que contiene el propio documento.

El total de puntuación asignada a la propuesta técnica de los licitantes será de 60 puntos de acuerdo con lo siguiente.

NÚMERO	RUBRO	PUNTUACIÓN PARA OTORGAR
1	Capacidad del licitante	24
2	Experiencia y especialidad del licitante	6
3	Propuesta de Trabajo	18
4	Transferencia de conocimientos	2
4	Cumplimiento de Contratos	10
	TOTAL	**60**

TABLA DE PUNTOS Y PORCENTAJES				
CAPACIDAD DEL LICITANTE (24 PUNTOS)				
No. DE RUBRO	**RUBRO / SUBRUBRO / CARACTERÍSTICAS**		**PUNTOS / PORCENTAJE MÍNIMO / MÁXIMO A OBTENER**	**RESULTADO DE LA EVALUACIÓN**
1	**CAPACIDAD DEL LICITANTE**		**RUBRO (24 PUNTOS)**	
1	**1.1.**	**CAPACIDAD DE LOS RECURSOS HUMANOS**	**SUB RUBRO (14 PUNTOS)**	
1	**1.1.1.**	**EXPERIENCIA DEL PERSONAL**	**ASPECTO (4.2 PUNTOS)**	
1	1.1.1.1	**EXPERIENCIA**	"EL LICITANTE" deberá acreditar una experiencia de 3 y 5 años del personal propuesto respectivamente de conformidad con lo solicitado en el punto "PERFIL REQUERIDO" del Anexo Técnico, para garantizar el cumplimiento de los servicios objeto de la presente licitación. Documentación que el licitante deberá presentar por cada uno de sus recursos humanos enlistados para el cumplimiento del sub rubro es la siguiente:	Se deberán presentar los siguientes perfiles: Se otorgarán **0.50 puntos** al licitante que presente la documentación de los numerales 1, 2 y 3, que avale contar con al menos **1 (una)** persona para el perfil:

			1) Currículum vitae que cumpla con el perfil y certificaciones solicitadas, el cual debe de incluir: • Nombre completo. • Escolaridad. • Años de experiencia. • Teléfono. • Correo electrónico. Descripción de certificado(s) requerido (s) en el ANEXO TÉCNICO. 2) Acreditar la relación laboral con "EL LICITANTE" presentando copia simple del último pago ante el IMSS y/o documento afiliatorio ante el IMSS, pudiendo testar información sensible. 3) Presentar copia simple de la identificación oficial vigente del personal propuesto.	**Administrador del Centro de Detección, Análisis y Respuesta Gestionada (MDR)** Se otorgarán **0.50 puntos** al licitante que presente la documentación de los numerales 1, 2 y 3, que avale contar con al menos **2 (dos)** personas para el perfil: **Administración y Operación de soluciones y herramientas tecnológicas** Se otorgarán **0.50 puntos** al licitante que presente la documentación de los numerales 1, 2 y 3, que avale contar con al menos **1 (una)** persona para el perfil: **Coordinador (MDR)** Se otorgarán **0.35 puntos** al licitante que presente la documentación de los numerales 1, 2 y 3, que avale contar con al menos **4 (cuatro)** personas para el perfil: **Analista del Centro de Detección, Análisis y Respuesta Gestionada (MDR)** de no presentar al menos cuatro personas no se otorgarán puntos. Se otorgará **1 punto** al licitante que presente la documentación de los numerales 1, 2 y 3, que avale contar con al menos **1 (una)** persona para el perfil: **Líder de proyecto** Se otorgarán **0.75 puntos** al licitante que presente la documentación de los numerales 1, 2 y 3, que avale contar con al menos **1 (una)** persona para el perfil: **Consultor especializado en protección de datos** Se otorgarán **0.40 puntos** al licitante que presente la documentación de los numerales 1, 2 y 3, que avale contar con al menos **1 (una)** persona para el perfil: **Consultor especializado en continuidad operativa y seguridad de la información** Se otorgarán **0.20 puntos** al licitante que presente la documentación de los numerales 1, 2 y 3, que avale contar con al menos **1 (una)** persona para el perfil: **Consultor especializado en la herramienta ITSM**
1	**1.1.2.**	**COMPETENCIA Y HABILIDADES**	**ASPECTO (7 PUNTOS)**	
1	1.1.2.1	**NIVEL ACÁDEMICO**	Para el cumplimiento de Competencia y Habilidades, "EL LICITANTE" deberá presentar copia simple del Título y/o Cédula Profesional a nivel licenciatura o ingeniería en carreras como: Comunicaciones, Electrónica, Sistemas Computacionales, Físico Matemáticas, Industrial Electrónica, Telemática, Ciencias de la Informática, Computación, Redes Computacionales o afines a TIC´´´´´´´´´´´´´´´S en donde demuestre que todo el personal propuesto para el	Se otorgarán **6 puntos** para el licitante que demuestre que todo el personal propuesto para el cumplimiento del Apartado **"1.1.1. EXPERIENCIA DEL PERSONAL"** cuenta con estudios profesionales. En caso de no cumplir totalmente con alguno los puntos solicitados no se le otorgarán puntos.

			cumplimiento del Apartado **"1.1.1. EXPERIENCIA DEL PERSONAL"** cuenta con estudios profesionales. Adicional, para el perfil "Líder de Proyecto" deberá acreditar mediante la presentación de copia simple del Título y/o Cédula Profesional estudios a nivel maestría en Tecnologías de Información y Comunicación.	Se otorgará **1 punto** para el licitante que presente copia simple del Título y/o Cédula Profesional estudios a nivel maestría en Tecnologías de Información y Comunicación para el perfil de "Líder de proyecto. En caso de no presentar este requisito, no se le otorgarán puntos.
1	**1.1.3.**	**DOMINIO DE HERRAMIENTAS RELACIONDAS CON EL SERVICIO**	**ASPECTO (2.8 PUNTOS)**	
1	1.1.3.1	**DOMINIO DE HERRAMIENTAS**	"EL LICITANTE" deberá presentar copia simple de los certificados del personal solicitado en el Apartado **"1.1.1. EXPERIENCIA DEL PERSONAL"** para garantizar el cumplimiento de los servicios objeto de la presente licitación. 1 (una) persona como Administrador del Centro de Detección, Análisis y Respuesta Gestionada (MDR), deberá presentar las siguientes certificaciones vigentes: ✓ CISSP (Certified Information Systems Security Professional) ✓ ITIL V4 Foundation Certificate in IT Service Management 2 (dos) personas en la Administración y Operación de soluciones y herramientas tecnológicas, deberá presentar la siguiente certificación vigente: Certificado del fabricante de las soluciones propuestas para al menos los siguientes servicios: ✓ Protección de Información en Correo Electrónico ✓ Visibilidad y Monitoreo de los Usuarios ✓ Segmentación zero trust ✓ Protección de Endpoint de siguiente generación (EDR) ✓ Protección para Servidores ✓ Protección de Endpoint de siguiente generación en Equipos de Cómputo ✓ Entorno de ataque cambiante (EAC) ✓ Servicio de Firewall de Siguiente Generación (NGFW) ✓ Servicio de Protección a Aplicaciones Móviles ✓ Servicio de Correlación de Eventos ✓ Servicio de Orquestación, Automatización y Respuesta de Seguridad 1 (una) persona como Coordinador (MDR), deberá presentar las siguientes certificaciones vigentes: ✓ EC-Council Certified Incident Handler ✓ EC-Council CEH (Certified Ethical Hacker) 4 (cuatro) personas como Analista del Centro de Detección, Análisis y Respuesta Gestionada (MDR), deberán presentar la siguiente certificación vigente: ✓ ITIL V4 Foundation Certificate 1 (una) persona como Líder de proyecto, deberá presentar las siguientes certificaciones vigentes: ✓ PMP (Project Management Professional), PMI	Se otorgarán **2.8 puntos** por el total de cumplimiento. En caso de no cumplir totalmente con alguno los puntos solicitados no se le otorgarán puntos.

			✓ CRISC (Certified in Risk and Information Systems Control) ✓ ITIL 4 Master 1 (una) persona como Consultor especializado en protección de datos, deberá presentar las siguientes certificaciones vigentes: ✓ CISM Certified Information Security Manager ✓ CISSP (Certified Information Systems Security Professional) ✓ CRISC (Certified in Risk and Information Systems Control) 1 (una) persona como Consultor especializado en continuidad operativa y seguridad de la información, deberá presentar una de las siguientes certificaciones vigentes: ✓ Certified ISO/IEC 27001 Information Security Associate. ó ✓ Certificado ISO/IEC 27001:2022 Lead Auditor ó ✓ Certificado ISO 22301:2019 Lead Auditor 1 (una) persona como Consultor especializado en la herramienta ITSM, deberá presentar una de las siguientes certificaciones vigentes: ✓ Certificado del fabricante de la solución propuesta de la herramienta de ITSM ó ✓ Certificado Auditor Líder 22301:2019	
TOTAL, DEL SUBRUBRO				**14 PUNTOS.**
1	**1.2**	**CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO**	**ASPECTO (9.2 PUNTOS)**	
1	1.2.1	**CAPACIDAD DE LOS RECURSOS ECONÓMICOS**	"EL LICITANTE" deberá acreditar la capacidad económica de sus ingresos equivalentes hasta el 20% del monto total de su oferta económica, para demostrar que se encuentra al corriente en sus obligaciones fiscales deberá presentar la última declaración fiscal anual del impuesto sobre la renta, así como copia de la declaración provisional del mes inmediato anterior a la fecha de presentación y apertura de propuestas, integrando su respectivo acuse de pago bancario y el acuse que emite el SAT. Las declaraciones deberán estar firmadas por el apoderado o representante legal del Licitante o en su caso el representante común que firme las propuestas.	Por el cumplimiento total del punto se otorgarán **2.2 Puntos.** En caso de no cumplir totalmente con alguno los puntos solicitados no se le otorgarán puntos.
1	1.2.2	**CAPACIDAD DE LOS RECURSOS DE EQUIPAMIENTO**	"EL LICITANTE" deberá presentar copia de los certificados de las normas **ISO/IEC 27001:2022, ISO/IEC 20000-1:2018 e ISO 22301:2019** vigentes y a su nombre y demostrar por lo menos 20 procesos en cada uno, siendo indispensable cumplir con los siguientes procesos similares en las 3 (tres) certificaciones: • Gestión de Incidentes • Gestión de Cambios • Gestión de Continuidad de Negocio • Gestión de Activos	Se asignarán **7 puntos** al licitante que dé cumplimiento total a lo solicitado. En caso de no cumplir totalmente con alguno los puntos solicitados no se le otorgarán puntos.

			• Monitoreo y Revisiones • Gestión Requerimientos • Gestión del Conocimiento • Respuesta a Incidentes de Seguridad • Atención y Resolución de Problemas "EL LICITANTE" deberá presentar copia del certificado **ISO 9001:2015** "Sistema de Gestión de Calidad" vigente y a su nombre, demostrando por lo menos 20 procesos. "EL LICITANTE" deberá acredita contar con un Sistema de Gestión Antisoborno, presentando copia de la certificación ISO 37001:2016 vigente y a su nombre. "EL LICITANTE" deberá presentar documento comprobatorio en el que se demuestre que es miembro activo del Foro Global de Equipos de Respuesta a Incidentes y Seguridad (FIRST por sus siglas en inglés) con una antigüedad mínima de 5 años a la fecha del acto de presentación y apertura de proposiciones.	
TOTAL, DEL SUBRUBRO				**9.2 PUNTOS**
		PARTICIPACIÓN DE TRABAJADORES CON DISCAPACIDAD	**SUBRUBRO (0.2 PUNTOS)**	**0.2 PUNTOS**
1	**1.3.**	PARTICIPACIÓN DE TRABAJADORES CON DISCAPACIDAD	"EL LICITANTE" deberá presentar carta firmada por el representante o apoderado legal, en el que manifieste que es una empresa que cuenta con personal con discapacidad en una proporción de al menos 5% de la totalidad de la plantilla de empleados con una antigüedad mayor de seis meses dada de alta en el régimen obligatorio del Instituto Mexicano del Seguro Social. Antigüedad que se comprobará con original o copia certificada para su cotejo y copia simple del aviso de alta al régimen obligatorio del Instituto Mexicano del Seguro Social.	Se otorgarán **0.2 puntos** al licitante que acredite contar por lo menos con el 5% por ciento de trabajadores discapacitados en los términos señalados en el párrafo anterior. En caso de no acreditar lo requerido no se otorgarán puntos.
TOTAL, DEL SUBRUBRO				**0.2 PUNTOS**
1	**1.4.**	**IMPLEMENTACIÓN DE POLÍTICAS Y PRÁCTICAS DE IGUALDAD DE GÉNERO**	**SUBRUBRO (0.2 PUNTOS)**	**0.2 PUNTOS**
1	1.4.1	IGUALDAD DE GÉNERO EN EL ENTORNO LABORAL	"EL LICITANTE" deberá presentar certificación que acredite haber aplicado políticas y prácticas de igualdad de género, conforme a la NMX-R-025-SCFI-2015, en Igualdad Laboral y No Discriminación, emitida por las autoridades y organismos facultados para tal efecto, vigente y a nombre de la empresa licitante en términos de lo dispuesto por el artículo 18 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público inciso c).	Se otorgarán **0.2 puntos** al licitante que presente certificación que acredite haber aplicado políticas y prácticas de igualdad de género conforme lo requerido. En caso de no acreditar lo requerido no se otorgarán puntos.
TOTAL, DEL SUBRUBRO				**0.2 PUNTOS**

1	**1.5.**	**PARTICIPACIÓN DE MIPYMES QUE PRODUZCAN BIENES CON INNOVACIÓN TECNOLÓGICA**	**SUBRUBRO (0.20 PUNTOS)**	**0.20 PUNTOS**
1	1.5.1	MIPYMES QUE PRODUZCAN BIENES CON INNOVACIÓN TECNOLÓGICA	Para la participación de MIPYMES que produzcan bienes con innovación tecnológica relacionados directamente con la prestación del servicio que se licita, "EL LICITANTE" presentará: Copia del documento expedido por el instituto mexicano de la propiedad industrial (IMPI) de dicha innovación tecnológica con el cual se otorgó la patente, registro o autorización correspondiente, en términos de lo dispuesto por el segundo párrafo del artículo 14 de la LAASSP, la cual no podrá tener una vigencia mayor a cinco años.	Se otorgarán **0.20 puntos** al licitante que presente la documentación que acredite haber producido servicios que estén relacionados con la prestación del servicio objeto del presente procedimiento de contratación. En caso de no acreditar lo requerido no se otorgarán puntos.
TOTAL, DEL SUBRUBRO				**0.20 PUNTOS**
1	**1.6.**	**PARTICIPACIÓN DE EMPRESAS QUE CUENTEN CON CERTIFICADOS EN MATERIA AMBIENTAL**	**SUBRUBRO (0.20 PUNTOS)**	**0.20 PUNTOS**
1	1.6.1	PARTICIPACIÓN DE EMPRESAS QUE CUENTEN CON CERTIFICADOS EN MATERIA AMBIENTAL.	Al Licitante (persona física o moral) que acredite contar con alguno de los certificados vigentes en materia de autorregulación y auditoría ambiental emitidos conforme al Reglamento aplicable. Se asignarán 0.2 Al Licitante que omita presentar el certificado solicitado, lo presente incompleto o no se encuentre vigente a la fecha de presentación y apertura de proposiciones. No se asignarán puntos Este rubro será evaluado con la presentación del anexo de MYPIMES y la presentación de la constancia emitida por el Instituto Mexicano de la Propiedad Industrial en términos de lo dispuesto por el segundo párrafo del artículo 14 de la Ley de Adquisiciones.	Al Licitante que demuestre el cumplimiento del requisito a través de la entrega de la totalidad de la documentación especificada. **Se asignarán 0.2 puntos.** Al Licitante que omita presentar la documentación incompleta o no presentada. **No se asignarán puntos.**
TOTAL, DEL SUBRUBRO				**0.20 PUNTOS**
TOTAL, DEL RUBRO				**24 PUNTOS**

EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE (6 PUNTOS)				
No. DE RUBRO	**RUBRO / SUBRUBRO / CARACTERÍSTICA**		**PUNTOS / PORCENTAJE MÍNIMO / MÁXIMO A OBTENER**	**RESULTADO DE LA EVALUACIÓN**
2	**EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE**		**RUBRO (6 PUNTOS)**	
2	**2.1.**	**EXPERIENCIA**	**SUBRUBRO (3 PUNTOS)**	**3 PUNTOS**
2	2.1.1.	MAYOR TIEMPO PRESTANDO SERVICIOS SIMILARES A LOS REQUERIDOS	"EL LICITANTE" deberá acreditar mediante copia simple de contratos celebrados con Dependencias y/o Entidades Públicas o Sector Privado, una experiencia mínima de 3 años en la prestación de servicios similares a los requeridos en el Anexo Técnico, los cuales deberán cumplir con lo siguiente: Cada contrato deberá estar debidamente formalizado y completo incluyendo sus anexos. Se podrán presentar contratos vigentes y/o concluidos. Los contratos no deberán tener una antigüedad mayor de 10 años de haber sido celebrados previo a la fecha del acto de presentación y apertura de proposiciones.	Se otorgará **3 puntos** al licitante que acredite más de 5 años de experiencia Se otorgará **2 puntos** al licitante que acredite al menos 5 años de experiencia. Se otorgará **1 puntos** al licitante que acredite al menos 4 años de experiencia. En caso de no acreditar por lo menos 4 años de experiencia conforme a lo solicitado, no se otorgarán puntos.

			El cómputo del tiempo de experiencia se realizará considerando solamente el tiempo calendario efectivamente prestado (todos los traslapes se contabilizarán solo una vez) Cada contrato deberá tener servicios similares a los requeridos en el Anexo Técnico y tener una vigencia mínima de 6 meses. Se aceptará la presentación de contratos plurianuales.	
TOTAL, DEL SUBRUBRO				**3 PUNTOS**
2	**2.2.**	**ESPECIALIDAD**	**SUBRUBRO (3 PUNTOS)**	**3 PUNTOS**
2	2.2.1	MAYOR NÚMERO DE CONTRATOS PRESTANDO SERVICIOS SIMILARES A LOS REQUERIDOS	"EL LICITANTE" deberá presentar copia simple de contratos celebrados con Dependencias y/o Entidades Públicas o Sector Privado, con los cuales se acredite que cuenta con la especialidad requerida en el Anexo Técnico (mínimo 3 contratos), los cuales deberán cumplir con lo siguiente: Cada contrato deberá estar debidamente formalizado y completo incluyendo sus anexos. Cada contrato deberá estar concluido a la fecha del acto de presentación y apertura de proposiciones. Los contratos no deberán tener una antigüedad mayor de 10 años ni menor a seis meses de haber sido celebrados, previos a la fecha del acto de presentación y apertura de proposiciones. Cada contrato deberá tener servicios similares a los requeridos en el Anexo Técnico y tener una vigencia mínima de 6 meses. Se aceptará la presentación de contratos plurianuales.	Se otorgará 3 **puntos** al licitante que acredite el cumplimiento de 5 o más contratos (deberán ser los mismos contratos presentados en el rubro 4. Cumplimiento de contratos) Se otorgará 2 **puntos** al licitante que acredite el cumplimiento de 4 contratos (deberán ser los mismos contratos presentados en el rubro 4. Cumplimiento de contratos) Se otorgará 1 **puntos** al licitante que acredite el cumplimiento de 3 contratos (deberán ser los mismos contratos presentados en el rubro 4. Cumplimiento de contratos) En caso de no acreditar por lo menos 3 contratos conforme a lo solicitado, no se otorgarán puntos.
TOTAL, DEL SUBRUBRO				**3 PUNTOS**
TOTAL, DEL RUBRO				**6 PUNTOS**

PROPUESTA DE TRABAJO (18 PUNTOS)				
No. DE RUBRO	**RUBRO / SUBRUBRO / CARACTERÍSTICA**		**PUNTOS / PORCENTAJE MÍNIMO / MÁXIMO A OBTENER**	**RESULTADO DE LA EVALUACIÓN**
3	**PROPUESTA DE TRABAJO**		**RUBRO (18 PUNTOS)**	
3	**3.1.**	**METODOLOGÍA PARA LA PRESTACIÓN DEL SERVICIO**	**SUBRUBRO (2 PUNTO)**	**2 PUNTOS**
3	3.1.1.	METODOLOGÍA	"EL LICITANTE" A fin de acreditar la metodología para la implementación y administración de servicios, deberá de presentar como parte de su propuesta técnica documento descriptivo, firmado por el representante o apoderado legal, la metodología a utilizar para cada una de las etapas del proyecto.	Se otorgará **2 puntos** al licitante que presente la metodología en cumplimiento a lo solicitado. Por la omisión parcial o total en la presentación de este documento o algún requisito no se le otorgarán puntos.

TOTAL, DEL SUBRUBRO				**2 PUNTOS**
3	**3.2.**	**PLAN DE TRABAJO PROPUESTO POR EL LICITANTE**	**SUBRUBRO (3 PUNTOS)**	**3 PUNTOS**
3	3.2.1.	PLAN DE TRABAJO	"EL LICITANTE" deberá presentar un Plan de Trabajo que debe incluir como mínimo lo siguiente: 1. Actividades 2. Proyección de calendario de tiempos 3. Responsables 4. Cabe mencionar que el Plan de trabajo detallado en el Cronograma de Actividades es de carácter enunciativo más no limitativo, por lo que la propuesta del licitante puede ser más amplia y detallada y deberá estar firmado autógrafamente por el apoderado o representante legal del licitante y por el Líder de proyecto propuesto.	Se otorgarán **3 puntos** a licitante que presente el plan de trabajo conforme a lo solicitado. Por la omisión parcial o total en la presentación de este documento o algún requisito no se le otorgarán puntos.
TOTAL, DEL SUBRUBRO				**3 PUNTOS**
3	**3.3.**	**ESQUEMA ESTRUCTURAL DE LA ORGANIZACIÓN DE LOS RECURSOS HUMANOS**	**SUBRUBRO (1 PUNTO)**	**1 PUNTO**
3	3.3.1	ORGANIZACIÓN DE LOS RECURSOS HUMANOS	"EL LICITANTE" a fin de acreditar el esquema estructural de la organización de los recursos humanos, deberá entregar documento firmado por el representante o apoderado legal del licitante, con el organigrama y la descripción de las funciones del personal que se presenta en la propuesta. (El personal deberá ser el mismo que se menciona en el punto 1.1.3. DOMINIO DE HERRAMIENTAS RELACIONDAS CON EL SERVICIO)	Se otorgará **1 punto** para aquella propuesta que cumpla con lo solicitado. Por la omisión parcial o total en la presentación de este documento o algún requisito no se le otorgarán puntos.
3	**3.4.**	**PLAN DETALLADO PARA ETAPA INICIAL**	**SUBRUBRO (5 PUNTOS)**	**5 PUNTOS**
3	3.4.1	PLAN DETALLADO PARA ETAPA INICIAL	Para la Etapa Inicial, en su propuesta técnica EL LICITANTE deberá entregar el Plan de Trabajo General para la implementación de los servicios solicitados de acuerdo con las fases de la metodología del PMI, Scrum o Lean, el cual deberá contener al menos: • Servicio a implementar • Componentes tecnológicos • Ruta crítica de instalación / actualización / configuración • Pruebas • Fecha de puesta en operación • Requerimientos El Plan de Trabajo General no deberá exceder 120 días naturales contados a partir de la notificación del fallo.	Se otorgarán **5 puntos** para aquella propuesta que cumpla con lo solicitado. Por la omisión parcial o total en la presentación de este documento o algún requisito no se le otorgarán puntos.
3	**3.5.**	**PLAN DETALLADO PARA FASE OPERATIVA**	**SUBRUBRO (7 PUNTO)**	**7 PUNTOS**

3	3.5.1	**PLAN DETALLADO PARA FASE OPERATIVA**	EL LICITANTE deberá presentar el Plan de Trabajo General para dar atención a la totalidad de requerimientos del Anexo Técnico correspondientes a la fase operativa. Contenido del Plan de Trabajo General mínimo: Para cada servicio a implementar: • Componentes tecnológicos propuestos • Actualización / sustitución / incorporación de componentes tecnológicos. • Ruta crítica de instalación / actualización / sustitución / configuración • Pruebas a realizar • Riesgos operativos identificados • Plan de mitigación • Requerimientos • Tiempo para puesta en operación	Se otorgarán **7 puntos** para aquella propuesta que cumpla con lo solicitado. Por la omisión parcial o total en la presentación de este documento o algún requisito no se le otorgarán puntos.
TOTAL, DEL SUBRUBRO				**1 PUNTO**
TOTAL, DEL RUBRO				**18 PUNTOS**

TRANSFERENCIA DE CONOCIMIENTOS (2 PUNTOS)				
No. DE RUBRO	**RUBRO / SUBRUBRO / CARACTERÍSTICA**		**PUNTOS / PORCENTAJE MÍNIMO / MÁXIMO A OBTENER**	**RESULTADO DE LA EVALUACIÓN**
4	**TRANSFERENCIA DE CONOCIMIENTOS**		**RUBRO (2 PUNTOS)**	
4	**4.1**	**TRANSFERENCIA DE CONOCIMIENTOS**	**SUBRUBRO (2 PUNTO)**	**2 PUNTOS**
4	4.1.1.	TRANSFERENCIA DE CONOCIMIENTOS	"EL LICITANTE" deberá incluir en su propuesta la transferencia de conocimiento técnica necesaria al personal designado por el Administrador del Contrato, mediante escrito o correo electrónico, a fin de que esté en condiciones de realizar la correcta administración y supervisión del proyecto sobre los bienes y/o servicios suministrados, dicha transferencia de conocimiento será para mínimo cinco (5) personas y máximo quince (15), por cada una de las tecnologías suministradas.	Se otorgará **2 puntos** al licitante que presente la transferencia de conocimientos para 15 personas. Se otorgará 1 **punto** al licitante que presente la transferencia de conocimientos para 5 personas Por la omisión parcial o total en la presentación de este documento o algún requisito no se le otorgarán puntos.
TOTAL, DEL SUB RUBRO				**2 PUNTOS**
TOTAL, DEL SUB RUBRO				**2 PUNTOS**
TOTAL, DEL RUBRO				**2 PUNTOS**

CUMPLIMIENTO DE CONTRATOS (10 PUNTOS).				
No. DE RUBRO	**RUBRIO / SUBRUBRO / CARACTERÍSTICA**		**PUNTOS / PORCENTAJE MÍNIMO / MÁXIMO A OBTENER**	**RESULTADO DE LA EVALUACIÓN**
5	**CUMPLIMIENTO DE CONTRATOS**		**RUBRO (10 PUNTOS)**	
5	**5.1.**	**CUMPLIMIENTO DE CONTRATOS**	**SUBRUBRO (10 PUNTOS)**	**10 PUNTOS**

5	5.1.1.	CUMPLIMIENTO SATISFACTORIO DE CONTRATOS	"EL LICITANTE" deberá comprobar el cumplimiento de mínimo 3 contratos con el documento que acredite su cumplimiento, los contratos deberán ser los mismos presentados en el subrubro 2.2 ESPECIALIDAD y cumplir con lo siguiente: Los contratos deberán ser celebrados con Dependencias y/o Entidades Públicas o Sector Privado. Deberán presentar documento mediante el cual se haga constar la cancelación de la garantía y/o liberación de fianza de cumplimiento y su respectiva fianza(s) y/o carta de satisfacción del contrato. Dicho escrito deberá contener mínimo la siguiente información: • Fecha de emisión. • Nombre y cargo del servidor público y/o persona autorizada que firma el documento de cumplimiento del contrato • Número de contrato. • Que indique que se han cumplido con las obligaciones establecidas en el contrato (en su caso)	Se asignará **10 puntos** al licitante que acredite el cumplimiento de 5 o más contratos con su respectivo documento de cumplimiento. Se asignará **7 puntos** al licitante que acredite el cumplimiento de 4 contratos con su respectivo documento de cumplimiento. Se asignará **4 puntos** al licitante que acredite el cumplimiento de 3 contratos con su respectivo documento de cumplimiento. En caso de no acreditar el cumplimiento de por lo menos 3 contratos, o bien que no coincidan con los presentados en el subrubro de especialidad no le serán otorgados puntos.
TOTAL, DEL SUBRUBRO				**10 PUNTOS**
TOTAL, DEL RUBRO				**10 PUNTOS**
TOTAL, DE PUNTOS ACUMULADOS				**60 PUNTOS**

5.3. Evaluación de la propuesta económica.

La evaluación de las propuestas económicas será realizada por el Área Contratante, verificando que la documentación presentada por la persona licitante cumpla con los requisitos solicitados en la Convocatoria y su Anexo Técnico, así como los que se deriven del acto de solicitud de aclaraciones y que no incurran en los supuestos establecidos en el numeral 4.4 incisos j) y u).

En caso de que derivado de la evaluación legal-administrativa y técnica, la propuesta sea considerada como no solvente, no se llevará a cabo la evaluación de la propuesta económica.

Para efectos de la evaluación de la propuesta económica, sólo se considerará el subtotal de la propuesta.

El total de puntuación asignada a la propuesta económica de los licitantes será de 40 puntos, por lo que a la propuesta económica que resulte ser la más baja de las técnicamente aceptadas y que cuenten con la totalidad de la información (documentación legal – administrativa), se le asignará la puntuación o unidades porcentuales máximas.

Para determinar la puntuación que corresponda a la propuesta económica de cada participante aplicará la siguiente fórmula:

$$PPE = \frac{MPEMB}{MPI} \times 40$$

Donde:
PPE = puntos de la propuesta económica

MPEMB= monto de la proposición más baja
40 = total de puntuación máxima asignado a la propuesta económica
MPI = monto de la proposición que se analiza

Por lo que la proposición más conveniente será aquella que reúna la mayor puntuación o unidades porcentuales, conforme a la siguiente fórmula:

PUNTOS TOTALES DE LA PROPOSICIÓN	=	PUNTOS PROPUESTA TÉCNICA	+	PUNTOS PROPUESTA ECONÓMICA

Se tomarán en consideración para efectos de comparación, a fin de determinar la propuesta económica más baja, la sumatoria de los costos totales de los conceptos referidos en la propuesta económica antes de I.V.A. contenidos en la Partida única, conforme a lo solicitado en el Anexo XIV de la presente convocatoria.

Cuando se presente un error de cálculo en la propuesta económica, solo habrá lugar a su rectificación por parte de la convocante, cuando la corrección no implique la modificación de precios unitarios, lo que se hará constar en el dictamen que sustente el fallo. Si la o el licitante no acepta la corrección de la propuesta, se desechará la misma. Lo anterior, con fundamento en el artículo 103 del Reglamento. Lo que se hará constar en el dictamen que sustente el fallo.

Para efectos de proceder a la evaluación de la propuesta económica, solo serán considerados los precios unitarios sin considerar el impuesto al valor agregado (I.V.A.).

En el supuesto de existir empate entre dos o más propuestas se dará preferencia en primer término Mipymes nacionales cooperativas, organismos del sector social de la economía certificados por el Instituto Nacional de la Economía Social, incluyendo aquellos cuyo objeto sea la inclusión laboral de mujeres y personas vulnerables y las constituidas o conformadas por grupos de atención prioritaria, que cuenten con documento de constitución y registro emitido conforme a las disposiciones jurídicas aplicables.

Se verificará que la documentación presentada en la propuesta económica se encuentre foliada de manera continua.

En caso de no cumplir con alguno de los requisitos establecidos en el presente apartado, se procederá de conformidad con el numeral 4.4 Causales expresas de desechamiento

6. INCONFORMIDADES.

De acuerdo con lo dispuesto en los artículos 95 y 96 de la Ley, las o los licitantes podrán interponer inconformidad, presentándola directamente por escrito en el O.I.C. de la Secretaría Anticorrupción y Buen Gobierno en Av. de los Insurgentes Sur 1735, Demarcación Álvaro Obregón, Col. Guadalupe Inn, C.P.01020, Ciudad de México, teléfono: 55 2000 3000, en días y horas hábiles, en el O.I.C. en Lotería Nacional, ubicado en el piso 8 del edificio sede en Av. Insurgentes Sur 1397, Col. Insurgentes Mixcoac, Demarcación Benito Juárez, C.P. 03920, Ciudad de México, Teléfono: 55 54-82-00-60 en un horario de 8:00 a 18:00 en días hábiles, así como en la dirección electrónica de ComprasMX (antes CompraNet): https://upcp-compranet.buengobierno.gob.mx/X por cualquier acto del procedimiento de contratación que contravenga las disposiciones de la Ley y su Reglamento.

Asimismo, se señala que tales inconformidades podrán presentarse mediante la Plataforma en la dirección electrónica https://comprasmx.buengobierno.gob.mx/, lo anterior, contra actos del procedimiento de contratación que contravengan las disposiciones que rigen las materias objeto del mencionado ordenamiento.

7. CANCELACIÓN DE LA LICITACIÓN, PARTIDA(S), O CONCEPTOS INCLUIDOS EN ÉSTA.

Con fundamento en el artículo 51 cuarto párrafo de la Ley, la Convocante podrá cancelar la presente Licitación, partida, o conceptos incluidos en ésta, hasta antes de emitir el fallo, por caso fortuito o fuerza mayor; de igual manera se podrá cancelar cuando existan circunstancias debidamente justificadas que provoquen la extinción de la necesidad de los bienes, arrendamientos o servicios, y que de continuarse con el procedimiento de contratación se pudiera ocasionar un daño o perjuicio a la **LN**.

8. DECLARACIÓN DE LICITACIÓN DESIERTA.

De conformidad con lo establecido en los artículos 51 primer párrafo de la Ley y 106 del Reglamento el presente procedimiento de contratación se declarará desierto cuando:

a. No se presenten proposiciones en el acto de Presentación y Apertura de Proposiciones.

b. Al analizar cualitativamente las propuestas técnicas y económicas, así como la demás documentación solicitada, ninguna cumpla con todos los requisitos establecidos en esta convocatoria y la documentación que la integra.

c. Cuando los precios de los servicios no resulten aceptables; cuando el monto ofertado en el procedimiento de contratación, exceda el presupuesto autorizado para la contratación de la dependencia o entidad contratante o convenientes.

9. FORMATOS QUE FACILITARÁN Y AGILIZARÁN LA PRESENTACIÓN Y RECEPCIÓN DE LAS PROPOSICIONES.

Número	Descripción
Anexo I	Anexo Técnico
Anexo II	Acreditamiento de personalidad jurídica persona física
Anexo III	Acreditamiento de personalidad jurídica persona moral
Anexo IV	Escrito de los supuestos establecidos en los artículos 71 y 90 de la Ley
Anexo V	Escrito de Declaración de Integridad.
Anexo VI	Escrito de Nacionalidad
Anexo VII	Aceptación de condiciones de la Plataforma
Anexo VIII	Manifestación de Vínculos
Anexo IX	Manifestación de beneficios o ventajas
Anexo X	Manifestación de Subcontratación
Anexo XI	Estratificación de las micro, pequeñas y medianas empresas
Anexo XII	Formato de Información reservada y confidencial
Anexo XIII	Nota OCDE
Anexo XIV	Propuesta económica
Anexo XV	Acuse de recepción de la documentación conforme a los numerales 4.1, 4.2 y 4.3 de la Convocatoria

Número	Descripción
Anexo XVI	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.
XVII	Modelo de contrato
XVIII	Forma de redacción de la póliza que garantice el cumplimiento del contrato

10. NOTA INFORMATIVA OCDE.

Nota informativa para participantes de países miembros de la Organización para la Cooperación y el Desarrollo Económico (OCDE) y firmantes de la Convención para Combatir el Cohecho de Servidores Públicos Extranjeros en Transacciones Comerciales Internacionales.

Esta nota es de carácter informativa por lo que no deberá incluirse en la proposición y no será causal de desechamiento la no presentación de la misma. **Anexo XIII.**

El lenguaje empleado en el presente documento no busca generar ninguna distinción ni marcar diferencias entre hombres y mujeres, por lo que las referencias o alusiones en la redacción hechas hacia un género representan a ambos sexos.

ÁREA CONVOCANTE

_____
LIC. CARLOS ALBERTO GAMA MORALES
Gerente de Adquisiciones

ÁREA JURÍDICA

_____
LIC. GUILLERMO GARDUÑO AGUILAR
Subdirector General de Asuntos Jurídicos
Por los aspectos legales

ÁREA REQUIRENTE

_____
LIC. ARMANDO CARDENAS REYES
Gerente de Telecomunicaciones y Seguridad Informática

ANEXO I
ANEXO TÉCNICO

SERVICIO INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN PARA LOTERÍA NACIONAL(SISI)	
LA ENTIDAD:	Lotería Nacional. "LOTERÍA"
Fecha de elaboración:	22 de octubre de 2026
Área requirente y Área técnica	LIC. ARMANDO CARDENAS REYES Gerencia de Telecomunicaciones y Seguridad Informática o quien lo sustituya en el cargo
Administrador del contrato:	Ing. DANIEL ALEJANDRO TOLEDO ALDARACA Titular de la Subgerencia de Seguridad Informática o quien lo sustituya en el cargo
Clave CUCOP:	31900004 "Servicios a centros de datos"
Partida presupuestal:	31904, "Servicios Integrales de Infraestructura de Cómputo"

ESPECIFICACIONES DE LOS BIENES, ARRENDAMIENTOS O SERVICIOS

Objetivo de la contratación

Proporcionar de manera integrada y unificada las especificaciones, requerimientos técnicos y funcionalidades de los servicios y soluciones requeridas para el "**SERVICIO INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN (SISI)**". "LOTERÍA", a través de la Subgerencia de Seguridad Informática requiere contar con servicios que permitan robustecer y complementar la Seguridad de la Información para salvaguardar la integridad y confidencialidad de la información.

Objetivos Estratégicos de Seguridad Institucional y Operativa de "LOTERÍA"

La contratación del **SERVICIO INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN (SISI),** en lo subsecuente nombrado como "SERVICIO INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN PARA LOTERÍA NACIONAL (SISI)", así como también "SISI", es crucial para mantener la integridad digital de "LOTERÍA", así como la confidencialidad, integridad y disponibilidad de su información y para garantizar la continuidad de los servicios tecnológicos que automatizan las funciones sustantivas y administrativas de la Entidad, con lo cual se busca:

- Proteger la infraestructura crítica y los activos informáticos, que son esenciales para la operación de las áreas sustantivas y administrativas de "LOTERÍA".
- Asegurar la continuidad de los servicios tecnológicos que respaldan las funciones sustantivas, administrativas, operativas y de sorteos, previniendo interrupciones que puedan afectar la prestación de los servicios.
- Identificar y mitigar riesgos tecnológicos, implementando soluciones avanzadas de ciberseguridad como monitoreo constante y control de acceso.
- Atender las observaciones en materia de ciberseguridad que en su caso determinen los Órganos de Fiscalización, en las posibles revisiones de acuerdo con el programa de supervisión de dichos órganos.
- Alinear los servicios con estándares internacionales (ISO/IEC 27001:2022)
- Actualizar el Sistema de Gestión de Seguridad de la Información que refuerce las políticas de seguridad y minimice riesgos, cumpliendo con estándares globales en materia de ciberseguridad.
- Cumplir con marco normativo alineando los servicios solicitados en el AT con la Estrategia Digital y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, garantizando que "LOTERÍA" opere dentro del marco legal y técnico correspondiente.

Antecedentes

"LOTERÍA" requiere que el servicio a contratar tenga la capacidad y flexibilidad de incorporar soluciones robustas de seguridad con servicios ordinarios y bajo demanda de acuerdo con las necesidades operativas de "LOTERÍA"; dichos servicios deben brindarse de manera unificada con estándares de calidad, seguridad, niveles de servicio y servicios administrados, que garanticen la continuidad administrativa y de operativa de negocio mediante:

- Servicios de seguridad, en materias específicas relacionadas con las Tecnologías de la Información, Comunicaciones y seguridad de la Información, incluyendo servicios especializados.
- Servicios que brinden protección de la información mediante soluciones especializadas.
- Administrar diversas soluciones tecnológicas de seguridad mediante personal técnico certificado y especialistas en la materia.
- Fortalecer los procesos y capacidades en materia de seguridad de la información a través de la implementación de controles con base en mejores prácticas y estándares que permitan lograr un nivel de riesgo aceptable.
- Implementar los controles tecnológicos de seguridad de la información requeridos en el presente Anexo Técnico para monitorear y proteger los activos de TIC, con la finalidad de incrementar la integridad, confidencialidad y disponibilidad de la información sensible de "LOTERÍA".

Alcance

"LOTERÍA" requiere del "SERVICIO INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN PARA LOTERÍA NACIONAL(SISI)", con el objetivo de robustecer, fortalecer y complementar el esquema institucional de seguridad de la información, a fin de salvaguardar la integridad, confidencialidad y disponibilidad de la información de la entidad.

Es importante señalar que Lotería Nacional necesita contar con un servicio que tenga la capacidad y flexibilidad de incorporar soluciones robustas de seguridad bajo un esquema por demanda conforme Lotería Nacional 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 Lotería Nacional 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 de Lotería Nacional.

El servicio deberá contemplar un esquema integral y transversal de protección, que no se limite a plataformas individuales, sino que cubra la totalidad del tráfico de red, la superficie de ataque completa y todos los vectores de amenaza, internos y externos, garantizando visibilidad, control y respuesta en tiempo real sobre todo lo que ingresa, circula y sale de la infraestructura institucional, mediante la provisión de soluciones y servicios de seguridad especializados orientados a la protección de la información, usuarios, aplicaciones, equipos de cómputo, servidores, comunicaciones de datos, directorio activo, servicios de correo electrónico y demás plataformas tecnológicas institucionales que generen syslog o permitan su integración con tecnologías de monitoreo, así como servicios especializados en materia de seguridad de la información.

Asimismo, las soluciones y servicios considerados dentro del presente servicio deben cubrir y proteger la infraestructura, plataformas y soluciones tecnológicas instaladas en las sedes de "LOTERÍA" en la Ciudad de México y oficinas regionales, así como la infraestructura ubicada en los centros de datos externos, primario y de respaldo, incluyendo los componentes de red, seguridad y cómputo asociados a dichos entornos y de los que disponga "LOTERÍA" se integren a este servicio, por mencionar algunos: servidores, equipos de comunicación (routers, switches y demás dispositivos de red) instalados tanto en las sedes de "LOTERÍA", como en centros de datos remotos.

De igual forma, el alcance del servicio deberá contemplar:

- **Usuarios, identidades y dispositivos:** protección de endpoints, dispositivos móviles y accesos remotos, independientemente de la ubicación del usuario.

- **Aplicaciones y servicios digitales: i**ncluyendo correo electrónico institucional, herramientas de colaboración, aplicaciones web y servicios en la nube.
- **Infraestructura de red y comunicaciones:** servidores, equipos de comunicación (routers, switches y demás dispositivos de red y conectados a la misma con registro de logs), instalados tanto en las sedes centros de datos centrales como en centros de datos remotos.
- **Centros de datos:** infraestructura tecnológica ubicada en las sedes de "LOTERÍA", como en centros de datos remotos.
- **Seguridad perimetral:** sedes centrales y regionales de "LOTERÍA", incluyendo la operación, monitoreo, gestión y transición tecnológica de las soluciones de Firewall de Nueva Generación (FWNG) con los que cuenta "LOTERÍA" y demás herramientas de seguridad perimetral solicitadas en el Anexo Técnico, en lo sucesivo AT.
- **Directorio Activo y gestión de identidades**: con controles de acceso basados en el principio de mínimo privilegio y modelo Zero Trust.

El alcance del servicio comprenderá la infraestructura, plataformas y soluciones tecnológicas instaladas en las sedes de "LOTERÍA" en la Ciudad de México, así como la infraestructura ubicada en los centros de datos de externos, incluyendo los componentes de red, seguridad y cómputo asociados a dichos entornos.
De esta forma, se establece un esquema integral de seguridad, que permita la protección transversal de los activos de información, infraestructura tecnológica y servicios digitales de "LOTERÍA" de tal forma que, todas las soluciones y servicios incluidos en este Anexo Técnico, en lo sucesivo "AT", deben operar de forma integrada con las plataformas empresariales de ciberseguridad que ofrezca EL LICITANTE como parte de su solución, la cual debe integrar en su operación inteligencia artificial que centralice la detección, análisis, gestión de riesgos y respuesta a amenazas en un solo entorno, compartiendo telemetría, correlacionando alertas y permitiendo respuestas coordinadas desde una consola única de operación.
EL LICITANTE deberá considerar dentro del alcance del servicio los mecanismos de intercambio de información con la Agencia de Transformación Digital y Telecomunicaciones (ATDT), el Centro Nacional de Respuesta a Incidentes de Seguridad Informática de la Administración Pública Federal y las dependencias y Centros de Atención a Incidentes de Seguridad gubernamentales en cumplimiento a la "Política General de Ciberseguridad para la Administración Pública Federal". Estos mecanismos serán definidos en conjunto con los entes previamente mencionados una vez que se determine su alcance por parte de la ATDT.
Como parte de los alcances del presente Anexo Técnico, se incluyen los siguientes:

- **Servicios de Seguridad - Continuidad Operativa**

  Son los servicios necesarios de seguridad para la protección de la información (Protección de Información en Correo Electrónico, Visibilidad y Monitoreo de los Usuarios, Segmentación Zero Trust, Protección de Endpoint de siguiente generación (EDR). Entorno de ataque cambiante (EAC) Servicio de Firewall de Siguiente Generación y Servicio de Protección a Aplicaciones Móviles), que se requiere su implementación, puesta a punto y su operación.

  Con estadísticas de reducción de superficie tanto dentro como fuera y con control de todo lo que entra y sale.
  Hay algunas solicitudes que lo hacen vago o en realidad no protegen como solicita esta parte. En particular protecciones solo a plataformas. Lo ideal sería proteger todo el tráfico y toda la superficie no plataformas.

- **Centro de Detección, Análisis y Respuesta Gestionada (MDR)**

  "LOTERÍA" requiere que EL LICITANTE cuente con un Centro de Operaciones de la Seguridad (SOC), a través del cual brinde el servicio de Centro de Detección, Análisis y Respuesta Gestionada (MDR) por sus siglas en inglés, el cual debe encontrarse físicamente en las instalaciones DEL LICITANTE bajo un esquema de operación 24x7

(las 24 horas del día, los 7 días de la semana y durante la vigencia del contrato). El objetivo de este centro deberá de ser la gestión proactiva de la seguridad y responsable de la administración, operación, monitoreo, soporte, atención a fallas de los componentes de las soluciones de seguridad del presente anexo técnico y de respuesta avanzada. El centro deberá realizar actividades de **Threat Hunting proactivo** para identificar amenazas que evaden los controles tradicionales, ejecutar actividades de detección, análisis y respuesta a incidentes, notificación de alertas y vulnerabilidades para los equipos de cómputo personal de la Entidad incluyendo análisis forense digital y respuesta dirigida (Containment) ante incidentes confirmados.

Vigencia

La vigencia del servicio o contrato será de veinticuatro (24) meses contados a partir del día hábil siguiente a la fecha de la notificación del fallo.

Especificaciones técnicas

Generalidades

Como parte del "SISI", EL LICITANTE que resulte adjudicado, en lo subsecuente EL LICITANTE, debe proporcionar:

- La instalación, configuración, puesta a punto, operación, mantenimiento preventivo y correctivo de todos los elementos solicitados dentro del presente Anexo Técnico.
- EL LICITANTE debe garantizar que los componentes que forman parte de su propuesta sean compatibles e interoperables con las plataformas actuales con que operan los sistemas de "LOTERÍA" y debe realizar la instalación, configuración y pruebas de integración y compatibilidad para validar la correcta operación de la totalidad de las soluciones requeridas en este Anexo Técnico.
- EL LICITANTE debe considerar dentro de su propuesta la totalidad de funcionalidades especificadas en el presente Anexo Técnico. El lictante podrá utilizar la infraestructura y aplicaciones propietarias de "LOTERÍA" enlistadas en el Apartado A "COMPONENTES DE SEGURIDAD CON LOS QUE CUENTA "LOTERÍA"", de acuerdo con lo establecido en el rubro "**CONDICIONES DE USO DE LA INFRAESTRUCTURA EXISTENTE".**
- Como parte del servicio, durante la vigencia del servicio "EL LICITANTE" deberá mantener vigente todo el licenciamiento considerado dentro de su propuesta, así como el soporte técnico, componentes y refacciones necesarias por parte de los fabricantes para la adecuada operación de la infraestructura y aplicaciones propuestas.
- Durante la Etapa Inicial, esto es, a partir del inicio de vigencia del contrato y hasta el inicio de la Etapa de Operación, el PRESTADOR DEL SERVICIO deberá tomar la operación de la infraestructura de ciberseguridad actual de "LOTERÍA". Durante esta etapa, el PRESTADOR DEL SERVICIO deberá contar con el soporte para la actualización de versiones, firmas y demás insumos indispensables para la operación de los componentes descritos en el Apartado A "COMPONENTES DE SEGURIDAD CON LOS QUE CUENTA "LOTERÍA"", considerando el cambio de partes en caso de ser requeridos.
- La gestión y operación del "SISI", se regirá bajo un esquema de Servicio Administrado, por lo que es necesario que EL LICITANTE cuente con la infraestructura, la cobertura, la experiencia, el personal técnico especializado, el software y el soporte necesario y suficiente para poder dar un servicio de la más alta calidad en tiempo, forma y a entera satisfacción de "LOTERÍA".
- "LOTERÍA" tendrá acceso sin cargo adicional, a las versiones (de firmware y software) que se liberen de los productos solicitados en el presente Anexo Técnico durante la vigencia del servicio o contrato. Todo el software y/o firmware proporcionado, deberá contar con licencia de uso en su versión comercial (no demostración o evaluación). Así también, EL LICITANTE será directamente responsable de proveer el soporte

técnico necesario para toda la infraestructura, componentes de la solución propuesta por EL LICITANTE debiendo realizar tareas de remediación en todo momento a fin de dar solución a eventos, incidentes, mitigación de riesgos en la infraestructura de "LOTERÍA" derivadas de amenazas o vulnerabilidades que pudieran tener los servicios del presente servicio o los activos que protege este, proponer soluciones, mejores prácticas y así mejorar la postura de seguridad de la Secretaría.

- Como parte de su propuesta, "EL LICITANTE", debe proporcionar el personal en sitio certificado de acuerdo con las especificaciones del apartado SOPORTE TÉCNICO del Anexo Técnico para cumplir con las tareas de soporte y atención a fallas de acuerdo con las necesidades de la Entidad.
- "EL LICITANTE" debe incluir en su propuesta el soporte técnico y gestión del "SISI" bajo un esquema de operación 7x24x365 (7 días a la semana las 24 horas del día, 365 días al año) mediante alertas de la mesa de servicio para todos los componentes tecnológicos propuestos y administrados durante la vigencia del servicio.
- EL LICITANTE debe garantizar que se brinden los accesos necesarios como administrador, al personal designado por "LOTERÍA" para facilitar las evaluaciones y validaciones. Dichos accesos estarán controlados garantizando el monitoreo de logs para temas de no repudio y trazabilidad, asegurando la confidencialidad y seguridad de la información de "LOTERÍA". Toda vez que la operación del "SISI" es responsabilidad de EL LICITANTE, los accesos provistos a "LOTERÍA" deberán ser debidamente acotados o monitoreados para no poner en riesgo la operación de los servicios.
- La solicitud de accesos necesarios será realizada por EL LICITANTE directamente a través del personal autorizado por el Administrador del contrato por parte de "LOTERÍA", designado como responsable de la supervisión y coordinación de estas solicitudes, asegurando que los procedimientos de seguridad y confidencialidad sean respetados.
- Como parte del "SISI", EL LICITANTE debe incluir en su propuesta los recursos técnicos y humanos especializados para realizar las actividades estipuladas en el Anexo Técnico; así como para la elaboración y cumplimiento de la documentación requerida en la ejecución de las actividades y seguimiento general del proyecto.
- "EL LICITANTE" deberá incluir en su propuesta el equipamiento, accesorios, refacciones, hardware, software con licenciamiento, y lo necesario para su correcta instalación y configuración para la puesta en marcha de cada uno de los componentes de hardware y software ofertados; así como la puesta a punto, el soporte técnico y el mantenimiento de estos durante la vigencia del servicio.

Etapa inicial

El día hábil posterior a la fecha de notificación del fallo, EL LICITANTE deberá acudir a las oficinas de la Subgerencia de Seguridad Informática, ubicadas en Av. Insurgentes Sur No. 1397 Piso 1, Insurgentes Mixcoac, Benito Juárez, 03920 Ciudad de México, para la reunión de inicio del servicio con el Administrador del Contrato. En esta sesión de inicio del servicio, "LOTERÍA" hará entrega de los accesos a las herramientas, consolas y demás elementos requeridos por EL LICITANTE y EL LICITANTE deberá tomar la operación de la infraestructura y servicios con que cuenta actualmente "LOTERÍA" descrita en el Apartado A.

EL LICITANTE en la reunión de inicio del servicio deberá presentar al personal propuesto para soporte en sitio y a partir de la conclusión de la reunión de inicio, será responsabilidad total de EL LICITANTE la operación de la infraestructura y servicios con que cuenta actualmente "LOTERÍA".

Durante la etapa inicial, "LOTERÍA" coadyuvará en la operación de la infraestructura con que cuenta actualmente, sin que esto implique la transferencia de responsabilidades al personal de "LOTERÍA".

"LOTERÍA" proporcionará las facilidades necesarias en los sitios que se definen en la APARTADO A, "Unidades Administrativas de "LOTERÍA"" para dar mantenimiento y/o instalar la infraestructura tecnológica de ciberseguridad propuesta por EL LICITANTE como parte de su solución de acuerdo con la siguiente estrategia:

- En su propuesta técnica EL LICITANTE deberá entregar el **Plan de Trabajo General** para la implementación de los servicios solicitados de acuerdo con las fases de la metodología del PMI, Scrum o Lean, el cual deberá contener al menos:
  - Servicio a implementar
  - Componentes tecnológicos
  - Ruta crítica de instalación / actualización / configuración
  - Pruebas
  - Fecha de puesta en operación
  - Requerimientos

  El **Plan de Trabajo General** no deberá exceder 120 días naturales contados a partir de la notificación del fallo.

- Duración de la **Fase inicial**, cuya duración máxima será de 120 días. EL LICITANTE deberá operar la infraestructura y servicios con que actualmente cuenta "LOTERÍA", bajo condiciones óptimas y vigentes. Todos los servicios durante la fase inicial deberán operar con los mismos niveles de servicio solicitados en el presente Anexo Técnico y deberán proteger la infraestructura, servicios e información de "LOTERÍA" de acuerdo con lo establecido por el mismo fabricante para los equipos y versiones de software que tiene disponibles "LOTERÍA".
- La fase inicial será pagada mensualmente de acuerdo con cada servicio soportado y en cumplimiento a lo establecido al presente Anexo Técnico, una vez recibidos los entregables correspondientes y de acuerdo con las condiciones generales de pago.
- Paso a **Fase de Operación**. EL LICITANTE podrá entregar de forma individual cada uno de los servicios solicitados a "LOTERÍA", quién otorgará su autorización para que pase a Fase de Operación, debiendo cumplir todos los criterios y requerimientos solicitados en el presente Anexo Técnico. Previo a la pasar a Fase de Operación, cada servicio deberá cubrir las pruebas operativas y de integración necesarias para mantener a salvo la infraestructura, servicios e información de "LOTERÍA".
- Cada servicio que pase a Fase de Operación dejará de ser cubierta como Fase Inicial y será pagada como Fase de Operación. En caso de que un servicio pase a Fase de Operación en día distinto a fin de mes, se computarán los días efectivamente prestados como Fase Inicial y como Fase de Operación para su pago correspondiente.

Plan de Trabajo Detallado

EL LICITANTE deberá presentar el Plan de Trabajo Detallado para dar atención a la totalidad de requerimientos del presente Anexo Técnico dentro de los 10 días naturales posteriores al fallo. "LOTERÍA" analizará y en su caso autorizará la ejecución de dicho plan en un plazo máximo de 5 días. En caso de que "LOTERÍA" tenga observaciones, EL LICITANTE tendrá un plazo máximo de 3 días naturales a partir de la recepción de las observaciones para subsanarlas en su totalidad.
La duración de las actividades contempladas en el Plan de Trabajo Detallado no deberá exceder 120 días naturales posteriores al fallo y deberá considerar las pruebas operativas previas para su implementación.
La ejecución del Plan de Trabajo Detallado deberá realizarse de acuerdo con lo planificado. Sólo se podrá modificar el mismo por Caso Fortuiro o Fuerza Mayor y por autorización expresa del Administrador del Contrato.
Contenido del Plan de Trabajo Detallado mínimo:

- Para cada servicio a implementar:
  - Componentes tecnológicos actuales
  - Actualización / sustitución / incorporación de componentes tecnológicos.

- Ruta crítica de instalación / actualización / sustitución / configuración
- Pruebas a realizar
- Riesgos operativos identificados
- Plan de mitigación
- Requerimientos
- Fecha de puesta en operación

Uso de Equipos Actuales

- Los equipos existentes (firewalls, consolas, etc.) serán utilizados inicialmente en la puesta en marcha del servicio.
- EL LICITANTE deberá realizar una evaluación técnica inicial dentro de los primeros 5 días naturales posteriores a la fecha de adjudicación para reconocer el estado de operación de los equipos en uso, a fin de que tome la administración correspondiente y garantice la misma durante la vigencia del servicio, conforme a los términos de administración y/o gobernanza que establezcan para tal fin el proveedor y Lotería.
- Así mismo, El LICITANTE, previo al terminado del periodo de tiempo establecido para la fase inicial 120 días, debe sustituir los equipos Firewall tipo 1, FortiGate 1500D y Gatwey Pc | Dell modelo optiplex 9020; para el caso de los equipos de Dell EMC, se debe evaluar su configuración, dentro de los primeros 5 días, para que, previo al término del periodo de tiempo establecido para la fase inicial, se restaurare la conexión SAN con la configuración más conveniente para el almacenamiento de información objeto del servicio.
  El PROVEEDOR debe sustituir, sin generar erogaciones adicionales a las contractualmente establecidas para "LOTERÍA".
  Los equipos suministrados en sustitución deben ser nuevos de fábrica y cumplir, como mínimo, con las especificaciones, capacidades, funcionalidades y requerimientos técnicos establecidos en el presente Anexo Técnico. No se aceptarán equipos usados, reacondicionados, remanufacturados o que hayan sido previamente puestos en operación.
  Asimismo, los equipos propuestos como sustitución deberán encontrarse dentro de un ciclo de vida vigente y contar, a la fecha de su instalación, con una expectativa de disponibilidad comercial y soporte por parte del fabricante por un periodo mínimo de treinta y seis meses posteriores a la fecha de fin de soporte del equipo sustituido.
- EL LICITANTE, tres días naturales posteriores a la fecha de adjudicación debe llevar a cabo un análisis de configuración y políticas de seguridad, cuyo objetivo será hacer más eficiente los procesos de detección de amenazas, así como las acciones de remediación, y presentar a más tardar, 15 días hábiles de iniciada la vigencia del servicio, las propuestas de mejora a los reportes y tableros con los que se cuenta.
- Plan de actualización de Equipos
- EL LICITANTE debe entregar a más tardar, 15 días hábiles de iniciada la vigencia del servicio un informe detallado de la vigencia de soporte de los equipos, así como de su estado de salud. El informe incluirá:
  - Equipo analizado
  - Modelo del equipo propuesto (cuando aplique).
  - Fecha de fin de vigencia de soporte de los equipos.
  - Estado de salud general.
  - Deficiencias identificadas.
  - Recomendaciones.
  - Fechas de reemplazo (cuando aplique) y cronograma.
- El administrador del contrato autorizará el reemplazo de equipos a conveniencia de Lotería y la prestación del servicio.

Condiciones de uso de la infraestructura existente

Todos los servicios solicitados por "LOTERÍA" en el presente Anexo Técnico deberán ser provistos por EL LICITANTE y podrá utilizar la infraestructura con que cuenta actualmente "LOTERÍA" como parte de su oferta técnica. Todos los equipos, software y componentes tecnológicos que utilice EL LICITANTE para la provisión del servicio deberán contar con soporte de fabricante y no se podrán utilizar componentes, equipos o software fuera de su vida útil considerada por el fabricante (End of Life).

Todos los equipos, software y componentes tecnológicos que integre el LICITANTE para la prestación de los servicios requeridos por Lotería, para agregar funcionalidades, complementar o sustituir la infraestructura con que cuenta actualmente Lotería, deberán ser nuevos, no reacondicionados, no remanufacturados y su fecha de fin de venta o de soporte, anunciada por el fabricante no deberá estar dentro de la vigencia del contrato o dentro de los 36 meses posteriores al término de la vigencia del contrato.

En caso de que, durante la vigencia del contrato, algún equipo propiedad de "EL LICITANTE" alcance su fecha de fin de soporte por parte del fabricante, "EL LICITANTE" debe prever y realizar oportunamente las acciones de actualización, adecuación, sustitución de componentes, licenciamiento o cualquier otra actividad técnicamente necesaria para garantizar la continuidad operativa, compatibilidad, seguridad y correcto funcionamiento del equipo, sin que ello genere erogaciones adicionales para LOTERÍA, debiendo considerar lo siguiente:

- El equipo de remplazo debe ser de especificaciones técnicas iguales o superiores a las presentadas en la sección de REQUERIMIENTOS TÉCNICOS.
- Como parte del remplazo "EL LICITANTE" debe incluir el todo licenciamiento necesario para asegurar que la funcionalidad de la solución sea igual o mayor.
- El equipo de remplazo debe ser nuevo de fábrica, especificado en los requerimientos técnicos (no usado, no reacondicionado, no remanufacturado y que su fecha de fin de venta o de soporte, anunciada por el fabricante, no esté dentro de la vigencia del contrato o dentro de los 36 meses posteriores al término de la vigencia del contrato, para lo cual, "EL LICITANTE" deberá entregar carta emitida por el fabricante donde se indique la fecha que compruebe lo anterior y condiciones del nuevo equipo.
- La funcionalidad de la solución de la cual forma parte el equipo remplazado deberá ser igual o mejorada.
- La fecha de fin de soporte del equipo suministrado en sustitución no deberá estar dentro de la vigencia del contrato o dentro de los 36 meses posteriores al término de la vigencia del contrato.
- Es responsabilidad de "EL LICITANTE" la configuración, instalación y puesta en operación del equipo de remplazo, asegurando que las funcionalidades de la solución sean iguales o superiores.
- La infraestructura tecnológica propuesta por "EL LICITANTE" debe incluir los arneses, cables y demás componentes necesarios para la puesta en operación de esta infraestructura tecnológica.

Lotería, como parte del servicio cuenta con infraestructura y licenciamiento de aplicaciones o soluciones de seguridad, especificadas en el Apartado A, y que fueron heredadas del servicio proporcionado con anterioridad y con los que Lotería sigue administrando los servicios de seguridad, infraestructura y soluciones que se pone a disposición de EL LICITANTE para la ejecución del presente servicio, sin que esto condiciones o limite al LICITANTE para proporcionar el servicio conforme se solicita, proveyendo soluciones diferentes o adicionales, de así requerirlo, siempre y cuando cumplan con las especificaciones descritas en el presente Anexo Técnico.

Por lo anterior, EL LICITANTE debe mantener vigente el licenciamiento, garantías, pólizas de soporte y refacciones necesarias por parte de los fabricantes, aplicable a infraestructura y soluciones de seguridad, durante la vigencia del contrato para cubrir los niveles de servicios establecidos durante la vigencia del servicio, considerando el cambio de partes en caso de ser requeridos, aplicando tanto a los equipos que tomará en control inicialmente propiedad de "LOTERÍA", como para aquellos que proveerá como nuevos.

Servicios de seguridad bajo demanda – continuidad operativa

Protección de Información en Correo Electrónico

Descripción del servicio:

En apego a la Política publicada por la ATDT, y de acuerdo con el Principio Rector "Valor público y derechos digitales", Objetivo Específico 3.1 Fortalecer la protección de infraestructura y servicios críticos y la Acción Operativa 08 Fortalecer el e-mail, se considera esencial y necesario cubrirlo como a continuación se describe.
El servicio tiene como objetivo proteger la plataforma de correo electrónico institucional contra amenazas avanzadas, garantizando la confidencialidad, integridad y disponibilidad de la información, mediante la prevención, detección, análisis y respuesta ante incidentes de seguridad derivados del uso del correo electrónico como vector de ataque.
"LOTERÍA" requiere, controlar el uso y acceso a los datos e información alojada en las estaciones de trabajo, supervisar el acceso de los usuarios a los datos confidenciales para identificar las conductas de riesgo o los peligros en la seguridad, controlar el acceso a la información confidencial, facilidad en la gestión de incidentes y las políticas de pérdida de datos en el Correo Electrónico.
EL LICITANTE deberá brindar el presente servicio en la modalidad bajo demanda conforme lo siguiente:

- La solución deberá incluir motores especializados en la detección de **Business Email Compromise (BEC)** mediante inteligencia artificial para identificar anomalías de lenguaje y suplantación de identidad ejecutiva.

Detalles del Servicio:

Arquitectura e Implementación

La solución debe ofrecer flexibilidad de despliegue y operación en múltiples entornos.

Modalidades de instalación

- Basada en appliance físico de propósito específico para ambientes on-premise.
- Instalación en nubes privadas:
  - VMware ESXi
  - Microsoft Hyper-V
  - KVM
  - Citrix XenServer
- Capacidad de operar como:
  - Gateway SMTP para servidores de correo existentes.
  - MTA (Mail Transfer Agent).
  - Proxy SMTP transparente para análisis de correo saliente.
  - Cliente WCCP para recibir y analizar correo mediante este protocolo.
  - Servidor de correo independiente (MTA server mode) con buzones locales accesibles vía Webmail, POP3 o IMAP.

Integración y APIs

- API REST para monitoreo, automatización y orquestación.
- Integración avanzada con Microsoft 365 mediante API nativa para:
  - Detección de amenazas posteriores a la entrega.
  - Recuperación de mensajes.
  - Políticas basadas en palabras clave, nombre de archivo o tipo de contenido.

- Licenciamiento alternativo para:
  - Escaneo en tiempo real de buzones de Microsoft 365.
  - Escaneo programado.
  - Recuperación de amenazas descubiertas posteriormente.

Gestión de Tráfico y Políticas de Correo

Control de flujo y entrega

- Soporte para múltiples dominios.
- Políticas por destinatario, dominio, tráfico entrante o saliente.
- Entrega basada en usuarios existentes en LDAP.
- Relay configurable según IP origen.
- Capacidad de retrasar el envío de correos sobredimensionados.
- Mantenimiento de cola de correo ante fallos de conexión o errores de entrega.
- Validación de destinatarios para buzones válidos.

Listas y reputación

- Listas blancas y negras por usuario, dominio y globales.
- Reputación de remitente basada en:
  - Número de virus enviados.
  - Cantidad de spam generado.
  - Destinatarios incorrectos.
- Detección de IPs falsificadas (Forged IP).
- Compatibilidad con DNSBL, SURBL y listas grises (IPv4 e IPv6).
- Control DNS reverso para protección contra spoofing.
- Identificación de altos volúmenes de conexiones y aplicación de límites por IP o remitente.

Cuarentena, Archivado y Almacenamiento

- Cuarentena por usuario, accesible vía Web y POP3.
- Gestión individual de mensajes en cuarentena (liberar/eliminar).
- Programación de informes de cuarentena.
- Archivado de correo basado en políticas de envío/recepción, con soporte para almacenamiento remoto.
- Almacenamiento local o remoto de correo y cuarentena.
- Sincronización de mensajes en cuarentena en escenarios de alta disponibilidad.

Autenticación y Administración

Autenticación

- SMTP Auth mediante LDAP, RADIUS, POP3 o IMAP.
- Doble factor de autenticación para administradores.

Administración y acceso

- Configuración vía interfaz web (HTTP/HTTPS).
- Creación de administradores por dominio.
- Restricción de acceso por IP y máscara.

- Niveles de acceso: lectura/escritura y solo lectura.
- Perfiles de configuración granular (antispam, antivirus, autenticación, etc.).
- Asistente (wizard) para aprovisionamiento inicial.

Alta Disponibilidad

- Soporte para HA en modos Activo-Activo y Activo-Pasivo.
- Conmutación por falla de red.
- Sincronización de configuraciones y mensajes.
- Detección y reporte de fallas.
- Hasta 24 miembros en clúster Activo-Pasivo.

Seguridad de Correo: Antispam, Antivirus, Antiphishing y Sandboxing

Antispam

La solución debe incluir un conjunto amplio de técnicas:

- Análisis heurístico con umbrales configurables.
- Análisis bayesiano.
- Detección de newsletters.
- Greylisting.
- Filtrado basado en URLs del cuerpo del mensaje.
- Análisis de palabras prohibidas (Banned Words).
- Diccionarios predefinidos y personalizados con pesos configurables.
- Listas blancas y negras de palabras.
- Análisis de imágenes (GIF, JPEG, PNG) para identificar spam.
- Análisis de imagen y PDF para detección de spam.
- Soporte para DNSBL, SURBL y listas grises.
- Detección de URLs maliciosas mediante base de reputación del fabricante.
- Selección de categorías de URL permitidas o bloqueadas.
- Detección de spam nuevo mediante correlación global de eventos.

Acciones posibles ante spam:

- Aceptar.
- Rechazar (Reject).
- Descartar (Discard).
- Cuarentena personal.
- Cuarentena del sistema.
- Sobrescritura.

Antivirus / Antimalware

- Inspección de archivos adjuntos y contenido.
- Análisis de archivos comprimidos: ZIP, PKZIP, LHA, ARJ, RAR.
- Base de datos de malware del fabricante y terceros, actualizable.
- Acciones ante malware:
    - Reject.
    - Discard.

  - Cuarentena de dominio.
  - Cuarentena del sistema.
  - Reescritura de dirección del destinatario.
- Análisis de imágenes para detectar contenido inapropiado para adultos.

Sandboxing

- Evaluación de amenazas avanzadas y día cero mediante sandboxing.
- Soporte para sandboxing on-premise y en la nube.

Protecciones Adicionales

- Protección contra ataques de denegación de servicio (Mail Bomb).
- Inspección minuciosa de encabezados.
- Detección de spoofing mediante DNS reverso.
- Conexión en tiempo real con base de datos del fabricante para actualizaciones antispam.

Compatibilidad con Estándares de Autenticación

- SPF
- DKIM
- DMARC

Sincronización y Servicios en Modo Servidor

- Sincronización de contactos y calendarios con clientes MUA.
- Soporte para WebDAV o CalDAV para publicación y sincronización de calendarios.

Prevención de Fuga de Información (DLP)

La solución debe incorporar un sistema DLP robusto, capaz de detectar, controlar y proteger información sensible que pueda filtrarse a través del correo electrónico.

Capacidades de detección

- Definición de información sensible mediante:
  - Palabras clave.
  - Frases.
  - Expresiones regulares.
  - Diccionarios predefinidos y personalizados.
- Lista predefinida de tipos de información sensible, incluyendo:
  - Números de tarjetas de crédito.
  - Identificadores personales (PII).
  - Datos financieros (PCI).
  - Identificadores nacionales como CURP, RFC, SIN, SSN, etc.
- Plantillas de protección de datos por país o región.
- Diccionarios predefinidos para cumplimiento normativo:
  - HIPAA, GLB, SOX.
  - Canadian SIN, US SSN, Credit Card, ABA Routing, CUSIP, ISIN.
- Diccionarios y listas de expresiones personalizables.
- Escaneo completo del mensaje:

  - Encabezado.
  - Asunto.
  - Cuerpo.
  - Archivos adjuntos.
- Capacidad de inspeccionar archivos protegidos por contraseña mediante:
  - Contraseñas predefinidas.
  - Listas de contraseñas.
  - Búsqueda de la palabra “password” en el cuerpo del mensaje.

Análisis y acciones automatizadas

La solución debe analizar contenido y adjuntos para determinar si un correo debe ser:

- Puesto en cuarentena.
- Cifrado.
- Archivado.
- Bloqueado.
- Etiquetado (tagging).
- Sobrescrito.
- Reenviado a otro host.

Fingerprinting

- Creación y almacenamiento de fingerprints de documentos.
- Fingerprints para archivos adjuntos de correo electrónico.
- Capacidad de almacenar fingerprints de archivos antiguos y nuevos (actualizados).
- Filtros basados en tipos de archivo.

Manejo de contenido malicioso

- Remoción o neutralización de contenido potencialmente malicioso.
- Capacidad de reconstrucción posterior del archivo.
- Aplicable a archivos MS Office, PDF y otros que contengan:
  - Macros.
  - Java.
  - HTML con URLs maliciosas.

Cifrado de Correo Electrónico

La solución debe ofrecer múltiples métodos de cifrado para garantizar la confidencialidad de la información.

Cifrado mediante políticas DLP

- Cifrado automático basado en reglas de DLP.

Identity Based Encryption (IBE)

- Cifrado basado en identidad sin necesidad de PSK o certificados previos.
- Soporte para métodos:
  - **Push:** el mensaje cifrado se envía como adjunto.
  - **Pull:** el mensaje cifrado se almacena en la plataforma y se accede mediante autenticación.
- En ambos métodos:
  - El destinatario debe estar registrado en la plataforma.
  - Se requiere autenticación para visualizar mensajes cifrados.

Otros métodos de cifrado

- Soporte para cifrado S/MIME.
- Soporte para SMTPS y SMTP sobre TLS.

Portales y experiencia del usuario

- Portal seguro para terceros con acceso mediante usuario y contraseña.
- Notificaciones automáticas de correos bloqueados.
- Portal personal de cuarentena para usuarios finales.

Registro, monitoreo y reportes

Registro de eventos

- Almacenamiento local de registros y eventos.
- Envío de logs a servidores remotos mediante Syslog.

Análisis y visualización

- Análisis de actividad y eventos.
- Presentación de resultados en:
    - Tablas.
    - Gráficas.

Informes

- Generación de informes bajo demanda.
- Programación de informes en intervalos específicos.
- Exportación de informes en formato PDF o HTML.

Protección contra amenazas

- Antivirus embebido sin necesidad de software adicional.
- Sandboxing para archivos y amenazas día cero (sin firmas).
- Detección de malware avanzado y enlaces maliciosos.
- Bloqueo automático de IPs por spam o ataques tipo DHA.

Filtrado y validación de correo

- Técnicas antispam (firmas, heurística, patrones, filtrado de URL).
- Validación de dominios con SPF, DKIM y DMARC.
- Protección contra spoofing y phishing (bloqueo, reglas de dominio, educación al usuario).
- Inspección y advertencia sobre URLs sospechosas o no categorizadas.
- Inclusión de disclaimers en correos salientes.

Gestión y administración

- Consola web para gestión, administración y reportes.
- Dashboards de seguridad, correo entrante y correo saliente.
- Menú rápido para creación de políticas, ejecución de reportes y búsqueda de logs.
- Monitoreo de logs en tiempo real (estatus de mensajes, conexiones y entregas).
- Flexibilidad para configurar políticas por usuarios, grupos o dominios.

Integración y compatibilidad

- Integración con plataformas de mensajería vía SMTP.

- Soporte de LDAP (Active Directory y genérico).
- Compatibilidad con cifrado TLS.

Concienciación y educación del usuario

- Módulo de formación para identificar correos de phishing.
- Notificaciones y mensajes educativos en correos sospechosos

EL LICITANTE deberá garantizar la actualización constante de cada servicio y herramienta descritos en este servicio, asegurando la aplicación de parches de seguridad, mejoras de funcionalidad y compatibilidad con nuevas versiones.
Asimismo, el prestador de servicio será responsable de realizar las actualizaciones de manera oportuna y sin afectar la continuidad del servicio.
En caso de que no sea posible la aplicación de actualizaciones por impactos operativos, deberá documentarse y ser autorizado por LOTERIA.
Las actualizaciones críticas, debidas a vulnerabilidades de día cero, deberán aplicarse de forma inmediata, salvo en los casos expresados en el párrafo anterior.
En caso de que se materialicen ataques o vulnerabilidades debido al uso de versiones obsoletas no atendidas sin la documentación y autorización correspondiente, se determinarán las responsabilidades correspondientes y se aplicarán las penas establecidas en el contrato.

Cumplimiento de RFCs

- Debe soportar el RFC 1213 (Management Information Base for Network Management of TCP/IP-based Internets: MIB-II)
- Debe soportar el RFC 1918 (Address Allocation for Private Internets)
- Debe soportar el RFC 1985 (SMTP Service Extension for Remote Message Queue Starting)
- Debe soportar el RFC 2034 (SMTP Service Extension for Returning Enhanced Error Codes)
- Debe soportar el RFC 2045 (Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies)
- Debe soportar el RFC 2505 (Anti-Spam Recommendations for SMTP MTAs)
- Debe soportar el RFC 2634 (Enhanced Security Services for S/MIME)
- Debe soportar el RFC 2920 (SMTP Service Extension for Command Pipelining)
- Debe soportar el RFC 3207 (SMTP Service Extension for Secure SMTP over TLS)
- Debe soportar el RFC 3461 (SMTP Service Extension for Delivery Status Notifications DSNs)
- Debe soportar el RFC 3463 (Enhanced Mail System Status Codes)
- Debe soportar el RFC 3464 (Extensible Message Format for Delivery Status Notifications)
- Debe soportar el RFC 3635 (Definitions of Managed Objects for the Ethernet-like Interface Types)
- Debe soportar el RFC 4954 (SMTP Service Extension for Authentication)
- Debe soportar el RFC 5321 (SMTP)
- Debe soportar el RFC 5322 (Internet Message Format)
- Debe soportar el RFC 6376 (DomainKeys Identified Mail (DKIM) Signatures)
- Debe soportar el RFC 6522 (Multipart/Report Content Type for the Reporting of Mail System Administrative Messages)
- Debe soportar el RFC 6409 (Message Submission)
- Debe soportar el RFC 7208 (Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail)
- Debe soportar el RFC 2088 (IMAP4 Non-synchronizing Literals)
- Debe soportar el RFC 2177 (IMAP4 Idle Command)

- Debe soportar el RFC 2221 (Login Referrals)
- Debe soportar el RFC 2342 (IMAP4 Namespace)
- Debe soportar el RFC 2683 (IMAP4 Implementation Recommendations)
- Debe soportar el RFC 2971 (IMAP4 ID Extension)
- Debe soportar el RFC 3348 (IMAP4 Child Mailbox Extension)
- Debe soportar el RFC 3501 (IMAP4 rev1)
- Debe soportar el RFC 3502 (IMAP Multiappend Extension)
- Debe soportar el RFC 3516 (IMAP4 Binary Content Extension)
- Debe soportar el RFC 3691 (Unselect Command)
- Debe soportar el RFC 4315 (UIDPLUS Extension)
- Debe soportar el RFC 4469 (Catenate Extension)
- Debe soportar el RFC 4731 (Extension to SEARCH Command for Controlling What Kind of Information Is Returned)
- Debe soportar el RFC 4959 (Extension for Simple Authentication and Security Layer (SASL) Initial Client Response)
- Debe soportar el RFC 5032 (WITHIN Search Extension)
- Debe soportar el RFC 5161 (Enable Extension)
- Debe soportar el RFC 5182 (Extension for Referencing the Last SEARCH Result)
- Debe soportar el RFC 5255 (IMAP Internationalization)
- Debe soportar el RFC 5256 (Sort and Thread Extensions)
- Debe soportar el RFC 5258 (List Command Extensions)
- Debe soportar el RFC 5267 (Contexts for IMAP4)
- Debe soportar el RFC 5819 (Extension for Returning STATUS Information in Extended LIST)
- Debe soportar el RFC 6154 (LIST Extension for Special-Use Mailboxes)
- Debe soportar el RFC 6851 (MOVE extension)
- Debe soportar el RFC 7162 (IMAP Extensions: Quick Flag Changes Resynchronization (CONDSTOR) and Quick Mailbox Resynchronization (QRESYNC))
- Debe soportar el RFC 1939 (POP3)
- Debe soportar el RFC 2449 (POP3 Extension Mechanism)
- Debe soportar el RFC 1155 (Structure and Identification of Management Information for TCP/IP-based Interface)
- Debe soportar el RFC 1157 (SNMP v1)
- Debe soportar el RFC 1213 (MIB 2)
- Debe soportar el RFC 2578 (Structure of Management Information Version 2)
- Debe soportar el RFC 2579 (Textual Conventions for SMIv2)
- Debe soportar el RFC 2595 (Using TLS with IMAP, POP3 and ACAP)
- Debe soportar el RFC 3410 (SNMP v3)
- Debe soportar el RFC 3416 (SNMP v2)

Administración de la Plataforma

EL LICITANTE deberá administrar integralmente la plataforma considerando lo siguiente:

Administración

- Administrar, configurar y operar de manera continua la solución de protección de correo electrónico.
- Gestionar políticas de seguridad alineadas a los requerimientos operativos y normativos de “LOTERÍA”.
- Mantener la disponibilidad, integridad y correcto funcionamiento de la plataforma.

Gestión de Amenazas y Protección

- Aplicar las configuraciones y mecanismos de protección solicitadas para esta herramienta.
- Administrar listas de reputación, dominios permitidos/bloqueados y reglas anti-spam.
- Habilitar y optimizar el análisis de URLs en tiempo real (time-of-click).

Análisis Avanzado y Sandboxing

- Administrar y operar las capacidades de sandbox para análisis de archivos adjuntos.
- Investigar correos sospechosos y determinar su nivel de riesgo.
- Generar evidencias técnicas derivadas de los análisis realizados.

Protección contra Suplantación de Identidad

- Configurar y monitorear controles de autenticación de correo.
- Detectar y mitigar intentos de suplantación de dominios o identidad institucional.

Prevención de Fuga de Información (DLP)

- Implementar, administrar y afinar políticas de DLP.
- Clasificar información sensible y definir reglas de protección.
- Ejecutar acciones de bloqueo, cuarentena o cifrado conforme a políticas.

Cifrado de Correo Electrónico

- Configurar mecanismos de cifrado automático basados en reglas.
- Asegurar la protección de información sensible en tránsito.

Monitoreo y Atención de Incidentes

- Monitorear eventos de seguridad de correo en esquema 24x7.
- Detectar, analizar y atender incidentes de manera oportuna.
- Escalar eventos críticos al SOC conforme a los procedimientos establecidos.
- Registrar todos los eventos e incidentes en la herramienta ITSM.

Gestión Operativa y Mejora Continua

- Realizar tuning periódico de reglas para reducir falsos positivos/negativos.
- Mantener actualizadas firmas, motores de detección e inteligencia de amenazas.
- Proponer mejoras continúas basadas en tendencias de ataque.

Integración con el Ecosistema de Seguridad

- Integrar la solución con el MDR.
- Asegurar el envío de logs y eventos para correlación.

Reporteo y Evidencia

- Entregar los reportes periódicos solicitados en el presente anexo técnico.
- Proporcionar evidencia técnica de incidentes relevantes.
- Generar reportes ejecutivos y técnicos conforme a requerimientos.

Visibilidad y Monitoreo de los Usuarios

En apego a la reciente política publicada por la ATDT y de acuerdo con el Principio Rector "Resiliencia operativa", Objetivo Específico 4.1 Consolidar capacidades es de monitoreo y respuesta y la Acción Operativa 03 Mecanismos de correlación, este servicio se considera esencial y es necesario cubrirlo como a continuación se describe.

Descripción del servicio:

"LOTERÍA" requiere identificar las conductas de riesgo o los peligros en la seguridad, controlar el acceso a la información confidencial, mediante la visibilidad y monitoreo de los usuarios.
EL LICITANTE deberá brindar el presente servicio en la modalidad bajo demanda conforme lo siguiente:

- EL LICITANTE debe considerar todo el equipamiento, licencias, implementación, puesta a punto, administración y monitoreo de los componentes tecnológicos que componen la protección del servicio.
- La solución debe tener un portal de administración basado en SaaS.
- El portal de administración debe admitir la autenticación de múltiples factores a través de un autenticador de terceros o por correo institucional. También debe de tener la opción de utilizar tecnologías SSO.
- El punto final no debe requerir reiniciarse después de la instalación.
- El punto final debe tener comunicación con la infraestructura del fabricante a través del canal de cifrado de un extremo a otro.
- El portal de administración debe proporcionar los últimos paquetes de terminales junto con las últimas notas de la versión.
- La interfaz de usuario de administración debe tener documentación en línea sobre el producto y las funcionalidades.
- La solución debe tener la capacidad de agregar / eliminar nuevos usuarios para acceder al portal de administración.
- La solución debe proporcionar diferentes niveles de acceso / roles en el portal de administración.
- Capacidad para restablecer la autenticación de dos factores en caso de emergencia.
- La solución debe proporcionar la capacidad de restablecer la contraseña sin la necesidad de abrir un caso de soporte con EL LICITANTE.
- Posibilidad de cambiar la contraseña a través del portal de administración.
- La solución debe proporcionar una vista de alto nivel de la actividad del usuario.
- Los paneles de investigación deben proporcionar detalles adicionales útiles para los analistas. Además debe permitir la creación de tableros personalizados.
- Capacidad para filtrar solo las alertas que tienen una puntuación de alto riesgo.
- La solución debe proporcionar agregación de eventos a nivel de usuario entre otros criterios a través del monitoreo o reporte de eventos.
- La solución debe tener una investigación en profundidad sobre la actividad del usuario, los datos y el tiempo, la aplicación, el canal monitoreado, el origen y el destino.
- La solución debe proporcionar atributos de Active Directory a través de la integración con AD como nombre, apellido, correo, hostname.

- La solución debe tener un agente de punto final para recopilar las actividades del usuario y correlacionarlo con el comportamiento del usuario.
- La solución debe contar con las capacidades de analizar canales de comunicación para monitorear la actividad de usuario de al menos los siguientes medios:
    - Grabación de Pantalla
    - Aplicaciones
    - Páginas Web
    - Correo
    - Audio
    - Reuniones en Línea
    - Mensajería Instantánea
    - Uso de Teclado
    - Impresión
    - Geolocalización
    - Uso de Cámara
    - Registros de Windows
- El punto final debe tener un soporte completo para los canales de Windows.
- El punto final debe tener un soporte completo para los canales de MacOS.
- El punto final no debe depender de las extensiones del navegador para analizar las actividades del tráfico web.
- La solución debe tener la capacidad de grabar audio y video del escritorio de los usuarios finales configurable mediante políticas con la capacidad de tomar control del equipo sin la necesidad de utilizar RDP u otro software de terceros. También debe contar con la capacidad de bloquear el teclado y mouse del usuario en tiempo real en caso de anomalías detectadas como acceso no autorizado o sospechoso.
- La solución debe tener la capacidad de analizar eventos sin procesar para identificar operaciones comerciales comprometidas, detección de anomalías o infracciones
- La solución debe tener un motor de políticas para recopilar y correlacionar eventos continuamente con el fin de detectar comportamientos sospechosos.
- La solución debe tener la capacidad de crear de reglas granulares para automatizar los casos de uso únicos de monitoreo de usuarios que requiera LN.
- La solución debe tener capacidades de detección de anomalías para la identificación de conductas de riesgo.
- La solución debe tener la capacidad de establecer una línea de base de la actividad del usuario para comprender el comportamiento del usuario durante un período de tiempo.
- La solución debe proporcionar un cálculo de riesgo basado en el tipo de detección de manera cualitativa, es decir, sin riesgo, bajo, medio, alto o crítico.
- El cálculo del puntaje de riesgo debe tener parámetros específicos y el método debe ser de conocimiento común para la creación de reglas personalizadas basadas en actividades granulares de usuario.
- La solución debe tener un cálculo de riesgo en tiempo real en el endpoint.
- La solución debe proporcionar diferentes tipos de gravedad para los eventos de riesgo del usuario.
- La solución debe tener la funcionalidad de DLP para poder aplicar políticas de punto final DLP basadas en las características del usuario mediante reglas y control de acciones sobre datos.
- La solución debe de utilizar Inteligencia Artificial para realizar consultas personalizadas (prompts) sobre la información recolectada de LN con la finalidad de agilizar el trabajo de análisis al generar nuevos tableros para analizar la información.

EL LICITANTE deberá garantizar la actualización constante de cada servicio y herramienta descritos en este servicio, asegurando la aplicación de parches de seguridad, mejoras de funcionalidad y compatibilidad con nuevas versiones.

Asimismo, el prestador de servicio será responsable de realizar las actualizaciones de manera oportuna y sin afectar la continuidad del servicio. En caso de que se materialicen ataques o vulnerabilidades debido al uso de versiones obsoletas, se determinarán las responsabilidades correspondientes y se aplicarán las penas establecidas en el contrato.

Administración y operación de la Plataforma

"EL LICITANTE" deberá administrar integralmente las funcionalidades de la plataforma que requiere "LOTERÍA" de acuerdo con lo siguiente:

Administración de la Plataforma

- Configurar, operar y mantener la plataforma conforme a mejores prácticas.
- Gestionar usuarios, roles, accesos y políticas de seguridad.
- Asegurar la disponibilidad, integridad y correcta operación del servicio.

Gestión de Superficie de Ataque (Attack Surface Management)

- Identificar y monitorear activos expuestos (internos y externos).
- Detectar vulnerabilidades, configuraciones erróneas y riesgos de exposición.
- Priorizar riesgos con base en criticidad e impacto al negocio.

Gestión de Riesgos (Cyber Risk Exposure)

- Analizar continuamente el nivel de riesgo de la organización.
- Correlacionar vulnerabilidades, amenazas e indicadores de compromiso (IoC).
- Generar recomendaciones de remediación basadas en riesgo.

Monitoreo y Detección de Amenazas

- Supervisar eventos de seguridad generados por la plataforma.
- Detectar actividades sospechosas y comportamientos anómalos.
- Integrar eventos con MDR para su atención.

Respuesta y Contención

- Ejecutar acciones de contención inicial conforme a la integración con el SOAR.
- Escalar incidentes al SOC o equipos correspondientes.
- Dar seguimiento hasta su cierre documentado.

Integración y Correlación

- Asegurar la integración con:
  - Herramientas de endpoint, red, correo y cloud
  - MDR

Afinación Continua (Tuning)

- Ajustar reglas, políticas y umbrales para reducir falsos positivos/negativos.
- Optimizar continuamente la postura de seguridad.

Reporteo y Visibilidad

- Generar los reportes ejecutivos y técnicos periódicos solicitados en el presente Anexo Técnico.
- Proveer tableros de control actualizados.

Gestión de Actualizaciones

- Asegurar que la plataforma opere con las versiones más actualizadas de firmas y software.
- Validar nuevas funcionalidades incluidas en los productos ofertados.

Segmentación Zero Trust

En apego a la reciente política publicada por la ATDT y de acuerdo con el Principio Rector "Ciberseguridad por diseño", Objetivo Específico 5.1 Garantizar accesos seguros y confiables en toda la APF y la Acción Operativa 03 ZERO TRUST, este servicio se considera esencial y es necesario cubrirlo como a continuación se describe.

Descripción del Servicio

EL LICITANTE deberá proporcionar una solución tecnológica integral bajo demanda de segmentación definida por software bajo el modelo de Zero Trust, desacoplada de la infraestructura de red tradicional, que permita la segmentación hasta el nivel de aplicación, garantizando que las políticas de seguridad sigan al flujo de las aplicaciones independientemente de la infraestructura donde se encuentre alojada.
La solución deberá permitir la protección de recursos institucionales mediante controles de acceso basados en identidad, contexto y postura de seguridad, alineándose con los principios del modelo Zero Trust Architecture (ZTA).
Asimismo, la solución deberá permitir la automatización y orquestación de controles de seguridad, así como proveer mecanismos avanzados para la detección de comportamientos maliciosos y prevención de amenazas.
La solución deberá incluir como mínimo:

- Firewall de inteligencia de amenazas para detección y bloqueo de tráfico malicioso.
- Capacidades de engaño dinámico (deception) para identificar movimientos laterales.
- Análisis de reputación basado en firmas para detección de procesos o tráfico malicioso.
- API REST abierta para facilitar integraciones con plataformas institucionales.
- EL LICITANTE deberá considerar todos los componentes necesarios para la operación del servicio, incluyendo:
    - Licenciamiento
    - Equipamiento requerido
    - Implementación
    - Configuración y puesta en operación
    - Administración y monitoreo de la solución

Objetivo del Servicio

Implementar una arquitectura de seguridad basada en Zero Trust que permita fortalecer la protección de los recursos tecnológicos institucionales mediante:

- Control de acceso basado en identidad
- Segmentación lógica de la infraestructura
- Eliminación de confianza implícita por ubicación de red
- Reducción del movimiento lateral dentro de la red
- Monitoreo continuo de accesos y comportamiento de usuarios

La solución deberá alinearse con los principios definidos en el estándar:
NIST SP 800-207 – Zero Trust Architecture.

Requerimientos Generales

EL LICITANTE deberá ofertar una solución tecnológica que permita la adopción progresiva de una Arquitectura Zero Trust dentro de la infraestructura tecnológica institucional, operando bajo el principio:
"Never Trust, Always Verify".
La solución deberá validar de forma continua:

- Identidades
- Dispositivos
- Aplicaciones
- Contexto de acceso

antes de permitir el acceso a los recursos institucionales.

Características Técnicas de la Solución

Acceso Seguro a Recursos
La solución deberá garantizar:

- Acceso seguro a recursos institucionales basado en políticas de seguridad.
- Eliminación del movimiento lateral dentro de la red (tráfico este-oeste).
- Comunicación cifrada mediante criptografía fuerte.
- Conexión únicamente a recursos autorizados.
- Inaccesibilidad a recursos no autorizados.

Asimismo, deberá:

- Establecer túneles de comunicación seguros.
- Permitir acceso a múltiples sitios con una sola autenticación (Single Sign-On).
- Soportar conectividad entre diferentes centros de datos, oficinas y entornos híbridos.
- Funcionar sin requerir modificaciones en la infraestructura de red existente (switches, routers o firewalls).
- Tener la capacidad de re-enrutar tráfico entre el cliente y el recurso protegido.
- Soportar IPv4 e IPv6.

La solución deberá contar con mecanismos que garanticen que el componente de autenticación no responda a tráfico proveniente de hosts no enrolados en la solución.

Control Basado en Zero Trust

La solución deberá soportar las siguientes capacidades:

- Políticas de acceso basadas en usuario o grupo de usuarios.
- Control del tráfico DNS.
- Ofuscación de red para agentes.
- Firewall de aplicaciones con estado (Stateful Firewall).
- Protección contra ataques de denegación de servicio (DoS).

Requisitos Funcionales de la Solución

Control de Identidad y Acceso

La solución deberá:

- Integrarse con sistemas de gestión de identidad institucional.
- Permitir autenticación multifactor (MFA).
- Realizar verificación continua de identidad durante la sesión.
- Permitir políticas de acceso basadas en atributos (ABAC).
- Permitir autenticación basada en riesgo.

Evaluación del Estado de Seguridad del Dispositivo

La solución deberá:

- Validar el estado de seguridad de los dispositivos antes de permitir acceso.
- Verificar cumplimiento de políticas de seguridad del endpoint.
- Identificar dispositivos administrados y no administrados.
- Integrarse con soluciones existentes de seguridad de endpoints.

Control Dinámico de Acceso

La solución deberá permitir aplicar políticas basadas en contexto considerando:

- Ubicación geográfica
- Dirección IP
- Estado del dispositivo
- Nivel de riesgo del usuario
- La solución deberá permitir revocar o modificar accesos en tiempo real ante cambios en el nivel de riesgo.

Microsegmentación de Infraestructura

La solución deberá permitir:

- Segmentación lógica de la red institucional.
- Definición de políticas de comunicación entre aplicaciones.
- Restricción del movimiento lateral dentro de la red.
- Protección granular de aplicaciones críticas.

Protección de Aplicaciones

La solución deberá:

- Controlar el acceso a aplicaciones web y sistemas internos.
- Permitir acceso seguro a recursos en entornos:
    - On-premise
    - Nube
    - Infraestructura híbrida
- Implementar autenticación y autorización centralizada.

Monitoreo y Visibilidad

La solución deberá permitir:

- Registro de eventos de autenticación y acceso.
- Integración con plataformas SIEM institucionales.
- Generación de reportes de auditoría.

- Detección de comportamientos anómalos.

Integración con Infraestructura Existente

La solución deberá integrarse con:

- Firewalls institucionales
- Sistemas IDS/IPS
- SIEM institucional
- Plataformas de monitoreo de seguridad
- Sistemas de protección de aplicaciones web (WAF)

La integración deberá realizarse sin afectar la operación de los servicios institucionales.

Implementación del Servicio

EL LICITANTE deberá presentar como parte de su propuesta técnica:
Diseño de Arquitectura
Documento que contemple:

- Arquitectura Zero Trust propuesta
- Componentes tecnológicos
- Integración con infraestructura institucional
- Identificación de puntos de control

Plan de Implementación

EL LICITANTE deberá presentar:

- Estrategia de adopción gradual de Zero Trust
- Cronograma de implementación
- Identificación de recursos técnicos
- Estrategia de mitigación de riesgos

Administración y Operación

La solución deberá permitir:

- Administración centralizada
- Dashboards de monitoreo
- Reportes periódicos de cumplimiento
- Auditoría de accesos a recursos

Acceso Seguro Basado en ZTNA

La solución deberá incluir capacidades de:
Zero Trust Network Access (ZTNA) para permitir:

- Acceso seguro a aplicaciones sin exponer la red interna
- Acceso basado en identidad y contexto
- Autenticación fuerte
- Acceso granular a aplicaciones específicas
- Reducción de la superficie de ataque
- Acceso para usuarios internos y terceros autorizados

Inventario y Clasificación de Activos

La solución deberá permitir:

- Identificación de activos tecnológicos
- Clasificación de activos críticos
- Identificación de flujos de datos
- Aplicación de políticas basadas en criticidad
- Protección de datos sensibles

Evaluación de Madurez Zero Trust

EL LICITANTE deberá realizar un diagnóstico inicial de madurez de seguridad, considerando:

- Identidades
- Dispositivos
- Redes
- Aplicaciones
- Datos
- Monitoreo de seguridad

Posteriormente deberá presentar una hoja de ruta de adopción Zero Trust que incluya:

- Etapas de implementación
- Priorización de activos
- Identificación de brechas
- Recomendaciones de mejora

Automatización y Respuesta ante Incidentes

La solución deberá permitir:

- Integración con herramientas de monitoreo
- Automatización de respuestas ante incidentes
- Aislamiento de dispositivos comprometidos
- Revocación automática de accesos
- Entregar información relativa a procesos de conexión, que incluyan evidencias de no-repudio, con una retención de 3 meses en línea y 1 año fuera de línea.
- Aplicación dinámica de controles de seguridad

Continuidad Operativa

La solución deberá contemplar la implementación de un nodo local de control (on-premise) que permita:

- Operación local en caso de pérdida de conectividad con la nube
- Sincronización automática de políticas
- Continuidad en autenticación y autorización
- Registro de eventos durante contingencias
- Replicación posterior de logs a plataformas centrales

La arquitectura deberá contemplar:

- Alta disponibilidad
- Tolerancia a fallos
- Resiliencia operativa

Gestión de Identidad de Usuarios

La solución deberá permitir:

- Definición de políticas de acceso basadas en identidad
- Control de comunicación entre usuarios y recursos autorizados

Integración con proveedores de identidad mediante:

- SAML
- LDAP
- LDAPS

Asimismo, deberá permitir:

- Registro de logs de acceso
- Envío de logs a servidores centralizados
- Registro de tráfico permitido y denegado

Gestión y Administración de la Solución

La solución deberá permitir:

- Control de acceso basado en roles (RBAC)
- Respaldos de configuración sin reinicio de servicios
- Instalación de agentes mediante línea de comandos
- Integración con entornos híbridos
- Incorporación de nuevos recursos sin afectar la disponibilidad

Actualizaciones y Mantenimiento

EL LICITANTE deberá garantizar:

- Actualización constante de componentes y herramientas
- Aplicación oportuna de parches de seguridad
- Actualizaciones sin afectar la continuidad del servicio

En caso de incidentes derivados del uso de versiones obsoletas, se determinarán las responsabilidades correspondientes conforme a lo establecido en el contrato.

Protección de Endpoint de siguiente generación (EDR)

Protección para Servidores

Descripción del servicio:

El servicio requerido bajo demanda debe contar con capacidades para manejar todo el ciclo de vida de las amenazas cibernéticas hacia los usuarios finales y activos de cómputo de la entidad; debe contar con capacidades de retroalimentación a las fuentes de amenazas directamente, así mismo permita la actualización de agentes en el entorno interno o externo de la entidad como usuarios móviles o remotos.

EL LICITANTE deberá considera la protección de al menos 136 servidores. Esta cantidad podrá incrementarse durante la vigencia del servicio a solicitud del Administrador del Contrato.
EL LICITANTE deberá realizar las siguientes actividades:

- Aprovisionamiento de una consola para "LOTERÍA" que permita integrar los repositorios necesarios, mínimo dos, que actualiza en línea directamente con el fabricante durante la vigencia del contrato.
- Instalación
- Configuración
- Puesta en operación
- Capacitación, para todas las soluciones tecnológicas ofertadas tales como appliances y soluciones de software de seguridad informática por parte del fabricante.
- Entrega de credenciales de acceso
- Soporte técnico durante la vigencia del contrato

Detalles del Servicio:

Respecto a la Protección de Endpoint de siguiente generación en Servidores, el servicio requerido debe contar con las siguientes características técnicas y funcionales; debe ser capaz de:

Proveer la consola de administración centralizada on premise o en la nube, con conexión directa a el fabricante para actualizaciones, soporte y para una administración más eficiente de todos los componentes de protección en el panorama de amenazas en constante cambio

- La solución contemplada deberá contar con una protección de firewall de host, prevención de intrusos, antimalware, monitoreo de integridad, inspección de bitácoras y control de aplicaciones en cada equipo ya sea físico, virtual para al menos los siguientes sistemas operativos, donde aplique en los esquemas mencionados:
    - Windows Server
        - Windows Server 2008 (32- and 64-bit)
        - Windows Server 2008 R2 (64-bit)
        - Windows Server 2012 (64-bit)
        - Windows Server 2012 R2 (64-bit)
        - Windows Server 2016 (LTSC, version 1607) (64-bit)
        - Windows Serve Corer, SAC version 1709 (64-bit)
        - Windows Server 2019 (64-bit)
        - Windows Server 2022 (64-bit)
    - Solaris:
        - Solaris 10 Updates 4-10 (64-bit, SPARC or x86)
        - Solaris 10 Update 11 (1/13) (64-bit, SPARC or x86)
        - Solaris 11.0 (1111), 11.1 (64-bit, SPARC or x86)
        - Solaris 11.2, 11.3 (64-bit, SPARC or x86)
        - Solaris 11.4 (64-bit, SPARC or x86)
    - Linux:
        - Red Hat® Enterprise 5 (32/64 bit), 6 (32/64 bit), 7 (64 bit), 8 (64 bit)
        - SUSE® Enterprise 11 (32/64 bit)
        - SUSE® Enterprise 12 (64 bit)
        - SUSE® Enterprise 15 (64 bit)
        - CentOs 5 y 6 (32/64 bit)

- CentOs 7 y 8 (64 bit)
- Oracle Linux 5 y 6 (32/64bit)
- Oracle Linux 7, 8 (64 bit)
- Debian 6, 7, 8, 9, 10 (64 bit)
- Ubuntu 10.04, 12.04, 14.04, 16.04, 18.04, 20.04 (64-bit)

La solución deberá considerar la prevención de intrusos, antimalware, monitoreo de integridad, reputación web, control de aplicaciones, monitoreo de bitácoras del sistema sean provistos mediante un solo agente, y estos a su vez sean administrados mediante una consola de administración, misma que deberá tener la capacidad de integrarse nativamente con una consola central para la visualización de eventos de seguridad.
La solución deberá tener la capacidad de poder crear grupos para llevar a cabo una agrupación que permita la administración y visibilidad de los servidores con base a una serie de criterios como nombre, Sistema Operativo, Versión, parámetros de nubes públicas como AWS, Azure.
La solución deberá tener la capacidad de ejecutar tareas de descarga, activación, aplicación de políticas de seguridad del agente.
La solución deberá permitir etiquetar eventos importantes de seguridad y duplicar esas etiquetas para eventos futuros.
La solución deberá contener un firewall que proteja servidores físicos y virtuales administrados desde la misma consola, permitiendo sólo las comunicaciones requeridas entre ellos. Este filtrado debe ser bidireccional y hacerse al menos sobre los siguientes parámetros:

- Protocolos: ICMP, IGMP, TCP, UDP, TCP+UDP
- Direcciones MAC
- Direcciones IP
- Puertos TCP & UDP
- Plantillas con reglas predefinidas para plataformas comunes

La solución deberá poder identificar las interfaces de red sobre los servidores, además de permitir la definición del tipo de interfaz para la aplicación de la política sobre múltiples interfaces con base a la cadena o patrón de texto que se establezca.

IPS de Host

- La solución deberá ser capaz de realizar una inspección profunda de los paquetes para analizar y prevenir ataques a vulnerabilidades en las aplicaciones instaladas en cada servidor, incluidas vulnerabilidades de día cero.
- La solución deberá monitorear el tráfico para registrar algún ataque, y además tener la capacidad de realizar acciones de bloqueo.
- La solución deberá de incluir protección inmediata de vulnerabilidades para aplicaciones y sistemas operativos, incluidas bases de datos, sitios Web, correo electrónico, entre otras.
- La solución deberá contar con firmas y reglas que permitan la protección de vulnerabilidades del sistema operativo y/o aplicaciones, sin la necesidad de modificar archivos a nivel del sistema.
- La solución deberá poder realizar un escaneo que permita ejecutar acciones dependiendo del comportamiento detectado.
- La solución deberá proteger ataques de tipo inyección de SQL, secuencias de comandos de sitios cruzados (Cross-Site Scripting) y otras vulnerabilidades de las aplicaciones Web.
- La solución deberá ser capaz de bloquear el tráfico de aplicaciones no deseadas como P2P, mensajería instantánea, navegadores web, y muchas otras, definidas por aplicación y no por puerto, de forma tal que otras aplicaciones que usan el o los mismos puertos puedan funcionar de manera normal.
- La solución deberá ser capaz de inspeccionar y bloquear tráfico malicioso que tenga como objetivo servicios o aplicaciones sobre contenedores Docker.

- La solución deberá prevenir la explotación de vulnerabilidades sobre los hosts de Docker y contenedores mediante la protección de parcheo virtual.

Protección Antimalware

- Garantizar la exploración en tiempo real, programada y manual de todos los archivos para la detección de malware.
- Los escaneos en tiempo real, los escaneos programados y los escaneos bajo demanda deben contar con la posibilidad de manejar excepciones en función de: tipos de archivos y rutas.
- Protección mediante la detección de antimalware en tiempo real para los sistemas de archivos utilizados en los hosts y contenedores de Dockers en ejecución.
- Proteger y detectar malwares como virus, trojanos, backdoors, rootkits, pakers, spyware/grayware, entre otras amenazas.
- Capacidades de detección que utilicen tecnología Deep para realizar un análisis en profundo sobre las potenciales amenazas desconocidas o ataques de día cero.
- Deberá contar con la capacidad Threat Intelligence que permita un análisis avanzado de las amenazas mediante la integración con la tecnología de sandboxing.
- Deberá contar con controles para la detección de amenazas ransomware, con la capacidad de terminar el proceso de cifrado.
- Deberá contar con un motor de recuperación de datos que pueda crear copias de archivos que están siendo cifrados por un ransomware.
- Deberá contar con una funcionalidad anti-exploit que realice el monitoreo de procesos que puedan tener comportamientos sospechosos. Esta funcionalidad deberá ocupar mecanismos como Data Execution Prevention (DEP), Structured Exception Handling Overwrite Protection (SEHOP) y heap spray prevention.

Reputación Web

- La solución deberá de incluir en la integración con los servicios de reputación (del mismo fabricante) para mejorar la protección contra amenazas, incluyendo servicio de reputación de archivo y reputación de URL’s.
- La solución deberá de contemplar la funcionalidad de reputación de URL’s debe evitar la conexión a sitios de mala reputación que puedan poner en riesgo la información que reside en los servidores.
- La solución deberá de tener la funcionalidad de reputación de URL’s debe permitir el manejo de excepciones.

Monitoreo de cambios de archivos y carpetas criticas

- La solución deberá identificar los cambios en archivos críticos, cambios a la configuración de archivos, carpetas, servicios y llaves de registro tanto del sistema operativo como de las aplicaciones instaladas en el servidor. Bajo las plataformas de Windows y Linux soportadas es necesario la identificación en tiempo real.
- La solución deberá ser capaz de identificar y aplicar automáticamente reglas de monitoreo sobre cambios realizados en archivos, carpetas críticas del sistema operativo, procesos o servicios ejecutándose dentro del equipo.
- La solución deberá permitir identificar el usuario que realice cambios sobre los archivos, servicios o llaves de registros dentro del servidor.
- La solución deberá de contar con reglas que permitan monitorear rutas y directorios de aplicaciones como Kubernetes y Dockers.

Control de Aplicaciones

- Debe de ser capaz de una vez habilitado el componente, realizar un escaneo que permita buscar el inventario de programas instalados para crear un conjunto de reglas locales, permitiendo la ejecución de los programas identificados.
- Debe de monitorear de forma continua con el fin de detectar cualquier cambio tanto a nivel del kernel y archivos de sistema realizados por los programas al momento de la instalación o nuevas ejecuciones.
- Debe de ser capaz de identificar si un software es nuevo o cambió para decidir si bloquea o permite la ejecución. Los parámetros que se usan para comparar son sha-256 y tamaño del archivo.
- Debe de crear reglas para permitir o bloquear un software específico cuando intenta iniciarse. Igualmente, se debe de tener la capacidad de editar o eliminar reglas utilizando el editor del conjunto de reglas o el registro de decisiones.
- Debe de detectar como software:
    - Aplicaciones Windows (.exe, .com, .dll, .sys), librerías Linux (.so), entre otros binarios y librerías.
    - Archivos Java .jar and .class.
    - PHP, Python, y shell scripts, y otras aplicaciones web y scripts que se interpretan o compilan.
    - Scripts de Windows Powershell, batch files (.bat) y otros scripts específicos de Windows (.wsf, .vbs, .js).

Monitoreo de bitácoras del sistema operativo y aplicaciones

- La solución debe inspeccionar bitácoras de sistema operativo y aplicaciones para identificar eventos de seguridad que se consideren relevantes o críticos.
- Capacidad de crear reglas personalizadas para el monitoreo de bitácoras.
- Capacidad de inspeccionar eventos generados por aplicaciones los cuales sean almacenados en archivos de bitácoras.
- La solución deberá de contar con reglas que permitan monitorear rutas eventos de aplicaciones como Kubernetes y Dockers.
- La solución debe tener la capacidad de inspeccionar logs de eventos generados como:
- En el visor de eventos para los servidores de plataformas Windows.
- En el syslog de servidores con sistema operativo Linux.
- Inyección procesos
- Intento cambio de password
- Eliminar usuario
- Asignación de privilegios a un nuevo inicio de sesión.

REST API

- La solución deberá tener documentado un API pública que permita automatizar tareas administrativas, incluyendo funcionalidades de autenticación, administración cuentas, eventos, monitoreo como al menos:
    - Modificar Cuentas Administrador
    - Eliminar Cuentas Administrador.
    - Listar Servidores.
    - Buscar Servidor.
    - Crear Grupo de Servidores.
    - Asignación y administración de políticas.
    - Búsqueda y Listado de Reportes
    - Crear una tarea basada en eventos.
    - Crear una tarea programada

- Integración con la Plataforma de Investigación y Respuesta a incidentes (EDR):

- Deberá poder en los servidores definidos permitir el envío de telemetría hacia la plataforma EDR, permitiendo enviar la información con la actividad a nivel de procesos, archivos, red, registros (Windows), conexiones, peticiones de dominio, modificación de procesos al menos.
- Deberá tener la capacidad de consumir los indicadores de compromiso u objetos sospechosos generados por la Plataforma EDR.

Integración con la Plataforma de Investigación y Respuesta a Incidentes (EDR)

Respecto a la Protección de Endpoint de siguiente generación en la Plataforma de Investigación y respuesta (EDR), el servicio debe tener la capacidad de:

- Aplicar técnicas de inteligencia artificial y analítica experta sobre los datos recolectados y telemetría enviada desde los sensores de endpoints y servidores con el fin de generar alertas de alta fidelidad.
- Mostrar los resultados de una investigación, donde permita visualizar el perfil de ejecución, alcance del impacto y ejecutar acciones de respuesta y contención.
- Contar con aplicaciones dentro de la plataforma al menos de:
  - Administración Modelos de Detección.
  - Técnicas de Ataques Observadas.
  - Inteligencias de Amenazas
  - Workbench
  - Administración de repuesta a incidentes
  - Aplicación de Búsqueda
  - Inventario de Endpoints
- La solución deberá contar con modelos de detección correlacionados automatizados, los cuales correlacionan eventos entre capas de seguridad para encontrar ataques no descubiertos. Los modelos de detección, que generan los activadores de alerta, combinan múltiples reglas y filtros utilizando una variedad de técnicas de análisis que incluyen el apilamiento de datos y el aprendizaje automático para detectar amenazas o comportamientos.
- La solución deberá permitir realizar búsquedas a través de los datos recopilados del endpoint y servidores mediante un simple generador de consultas.
- La solución deberá realizar búsquedas personalizadas o de barrido de IoC utilizando varios parámetros y filtre las cosas agregando criterios de búsqueda adicionales.
- La solución deberá contemplar dentro de la aplicación de Búsqueda diferentes métodos de búsqueda, filtros y un lenguaje de consulta similar a Kibana para identificar, categorizar y recuperar los resultados de una investigación.
- La solución deberá tener un apartado donde se publiquen los últimos indicadores de compromiso publicados por las áreas de investigación del fabricante o de fuentes externas como corporaciones de seguridad, agencias de gobierno (Norte América, Europa), entre otras fuentes.
- La solución deberá generar y permitir visualizar al análisis causa raíz o RCA en donde se incluya el detalle de los procesos, objetos y direcciones que se detectaron durante la ejecución maliciosa de la amenaza.
- La solución deberá mapear las técnicas utilizadas con base al framework de MITRE ATT&CK.
- La solución deberá permitir generar respuestas para una acción rápida tomada directamente desde la plataforma en el workbench o dentro de los resultados de búsqueda de la búsqueda sobre la data de endpoints y servers como:
  - Terminar el proceso activo sobre el equipo y el resto de endpoints.
  - Aislar endpoint afectado de la red excepto la comunicación con la plataforma de detección y respuesta.
  - Restaurar conectividad de un endpoint después de haber sido aislado.

  - Permitir una conexión a un endpoint monitoreado permitiendo ejecutar comandos remotos para actividades de investigación.
  - Ejecución de script customizado.
- La solución deberá contar con un API pública que permita integrarse con varias herramientas SIEM y SOAR.

Administración y Gestión Centralizada

Este servicio debe:

- Proporcionar funciones de administración central en términos de registros y estado de productos que sean registrados.
- Capacidad habilitada para administrar e implementar centralmente actualizaciones de productos del agente, incluidos parches, revisiones y actualizaciones de firmware para la protección de los usuarios.
- Proporcionar un control de acceso basado en roles para fines de administración, investigación y operación.
- Proporcionar la función de registro de auditoría para una vista histórica de las actividades del usuario.
- Capacidad habilitada para generar informes descargables a partir de plantillas existentes y personalizables.
- Deberá poder integrarse con Active Directory para importar los grupos de AD adicionales a los usuarios.
- Deberá contar con un dashboard que muestre la relación entre updates, detecciones críticas, estatus de componentes, entre otros.
- Deberá permitir a los administradores el dar de alta políticas desde un único punto para la configuración y habilitación de los diferentes controles de seguridad del servicio de protección avanzada en endpoints.
- Deberá poder ser el repositorio de logs de las consolas de gestión de los servicios de protección de endpoint, servidores, entre otros del mismo fabricante.
- Deberá poder generar reportes desde templates estáticos o customizados con la información requerida para asegurar la protección.
- Deberá tener la funcionalidad de log de auditoría que permita monitorear los comandos ejecutados desde la consola central.
- Deberá poder permitir la descarga de los paquetes de instalación de los agentes de protección avanzada en endpoint desde la consola central.
- Deberá poder realizar notificaciones vía correo, Windows Syslog, SNMP trap o alguna aplicación estandarizada de la industria utilizada por el “LOTERÍA”.
- Deberá poder contar con un API para el reenvío de detecciones en formato CEF, eventos de auditoría de productos, estados de actualización del patrón del agente de seguridad o estados de actualización del motor del agente de seguridad a los servidores SIEM.
- Deberá poder generar notificaciones a una persona o grupo con los eventos detectados por las soluciones. Las categorías de eventos son:
  - Actividad de Amenazas Avanzadas
  - Violación Políticas de contenido
  - Actualizaciones
  - Actividad Amenazas Conocidas.

Protección de Endpoint de siguiente generación en Equipos de Cómputo personal

Compatibilidad y Requerimientos del Agente

Sistemas Operativos Soportados

La solución deberá garantizar compatibilidad plena con los sistemas operativos descritos, asegurando operación estable, telemetría completa y soporte continuo.

Windows Desktop

- Windows XP SP2, 7, 8, 8.1, 10 y 11 (32 y 64 bits).

Windows Server

- Windows Server 2003 SP2, 2008 SP1/R2 SP2, 2012/2012 R2, 2016, 2019, 2022 y 2025.

macOS

- Versiones desde El Capitan (10.11) hasta Sequoia (15).

Linux

- RedHat Enterprise Linux y CentOS 6.8+, 7.2+, 8+, 9+.
- Ubuntu LTS 16.04.5+, 18.04, 20.04 y 22.04.
- Oracle Linux 6.10, 7.7+, 8.2+.
- Amazon Linux AMI 2.
- SUSE SLES 12 SP5 y 15; OpenSUSE Leap 15.2.

Infraestructura VDI

- VMware Horizon 6 y 7.
- Citrix XenDesktop 7.

Dispositivos Móviles

- Android 9.0 o superior.
- iOS 15.0 o superior.

Requerimientos de Consumo

La solución deberá operar con impacto mínimo en el rendimiento del endpoint:

- Consumo máximo de memoria RAM: **350 MB**.
- Consumo promedio de CPU: **< 2%**.
- Espacio en disco requerido: **≤ 1 GB**.

Instalación, Actualización y Administración

La solución deberá:

- Permitir despliegue masivo mediante SCCM, JAMF u otras herramientas equivalentes.
- Actualizarse sin intervención del usuario y sin requerir reinicios.
- Incorporar mecanismos Anti-Tamper en el agente.
- Permitir la generación de instaladores preconfigurados sin interacción del usuario.
- Operar detrás de servidores proxy.
- Permitir la protección mediante contraseña para la desinstalación del agente.

Capacidades de Detección (EDR)

Telemetría y Monitoreo

El agente deberá registrar en tiempo real:

- Creación, terminación e interacción entre procesos.
- Cambios en el registro de Windows.
- Solicitudes DNS generadas por el dispositivo.
- Conexiones de red salientes y entrantes.
- Actividad sospechosa asociada a DLL.
- Usuario asociado a cada evento.

Inteligencia y Técnicas de Detección

La solución deberá:

- Detectar amenazas sin depender de firmas hash locales.
- Integrar inteligencia de amenazas actualizable diariamente.
- Incorporar técnicas MITRE ATT&CK y mostrar las técnicas detectadas.
- Identificar actividad maliciosa conocida.

Capacidades de Threat Hunting

La plataforma deberá permitir:

- Búsqueda por IoCs en Windows y Linux (archivos, procesos, red, logs, registro).
- Consultas de texto libre.
- Almacenamiento de consultas para reutilización futura.
- Búsqueda por acciones específicas (creación/eliminación de archivos, eventos de red, eventos de registro, etc.).

Convivencia con Otras Soluciones

- La solución deberá coexistir con antivirus tradicionales o NGAV.
- Deberá permitir excepciones por archivo o carpeta para el motor de NGAV.

Prevención de Malware (NGAV)

Prevención Proactiva

La solución deberá:

- Bloquear la ejecución de archivos maliciosos.
- Incorporar un motor NGAV basado en kernel con capacidades de Machine Learning.
- Controlar dispositivos USB con excepciones basadas en:

  - nombre del dispositivo
  - vendor
  - número serial
  - combinaciones de los anteriores
- Crear excepciones para procesos legítimos monitoreados.

Protección Contra Ransomware

La solución deberá:

- Bloquear procesos asociados a ransomware.
- Realizar respaldo automático de archivos cifrados.
- Inspeccionar comportamiento de procesos para identificar anomalías.
- Bloquear exploits que permitan la ejecución o propagación de ransomware.
- Prevenir cifrado de disco y modificaciones no autorizadas.

Políticas y Modos de Operación

La plataforma deberá permitir:

- Políticas en estado Activa, Desactivada o Solo Log.
- Modo simulación sin bloqueo.
- Configuración granular de reglas (solo registrar o bloquear).
- Escaneos periódicos, programados o bajo demanda.

Difusión y Contención (Post-Infección)

La solución deberá:

- Aislar automáticamente endpoints comprometidos.
- Modificar políticas asignadas según la actividad detectada.
- Bloquear actividades maliciosas en ejecución.
- Crear excepciones basadas en:
  - ruta de archivo
  - destino del tráfico
  - usuario ejecutor
  - IP, aplicaciones o protocolos
- Gestionar falsos positivos de forma manual y automática.

Respuesta a Incidentes

Retención y Forense

La solución deberá:

- Mantener histórico mínimo de 30 días.
- Almacenar metadata para análisis forense.
- Obtener capturas instantáneas de memoria (memory dumps).

Integraciones

La plataforma deberá:

- Integrarse con SIEM vía Syslog.
- Integrarse mediante Open Ticket
- Exponer API para consulta de datos de eventos.

Acciones de Remediación

La solución deberá permitir:

- Terminación de procesos maliciosos.
- Eliminación de archivos.
- Restauración de configuración del registro.
- Aislamiento de dispositivos.
- Restricción de acceso según clasificación del evento.
- Limpieza automática y reversión de cambios.
- Envío de ejecutables a sandbox.

Control de Vulnerabilidades y Comunicación

La solución deberá:

- Identificar aplicaciones que representen riesgo por su comunicación en red.
- Aplicar parcheo virtual sin agentes adicionales.
- Reducir superficie de ataque basada en CVE y reputación.
- Prevenir comunicación de aplicaciones no autorizadas.
- Crear políticas basadas en versión de aplicación.
- Identificar y reportar aplicaciones que generan tráfico y sus destinos.
- Crear listas de aplicaciones bloqueadas por política.

Escenarios de Ataque Cubiertos

La solución deberá:

- Identificar y prevenir intentos de escalación de privilegios.
- Bloquear ransomware conocido.
- Controlar dispositivos USB.

- Automatizar investigación con mínima interrupción.
- Desactivar amenazas automáticamente.
- Proveer visibilidad completa de la cadena de ataque.
- Conservar snapshots de memoria para análisis.

Funcionalidades Adicionales de Protección de Endpoint

La solución deberá:

- Proveer consola centralizada.
- Detectar y responder automáticamente a malware avanzado y ataques fileless.
- Integrar control de aplicaciones, control de dispositivos y antimalware en un solo agente.
- Permitir integración vía API con terceros.
- Incluir Firewall basado en host.

Tanto la solución de la Protección para Servidores como la solución de la Protección de Endpoint de siguiente generación en Equipos de Cómputo deberán estar integrados al Centro de detección, análisis y respuesta gestionada (MDR)

EL LICITANTE deberá garantizar la actualización constante de cada servicio y herramienta descritos en este servicio, asegurando la aplicación de parches de seguridad, mejoras de funcionalidad y compatibilidad con nuevas versiones. Asimismo, el prestador de servicio será responsable de realizar las actualizaciones de manera oportuna y sin afectar la continuidad del servicio. En caso de que se materialicen ataques o vulnerabilidades debido al uso de versiones obsoletas, se determinarán las responsabilidades correspondientes y se aplicarán las penas establecidas en el contrato.

Entorno de ataque cambiante (EAC)

El servicio de Entorno de Ataque Cambiante (EAC) deberá proporcionar **capacidades avanzadas de prevención, detección, investigación, respuesta y recuperación** bajo demanda frente a amenazas sofisticadas, particularmente ataques del tipo ransomware. Este servicio automatizará de forma extensa el ciclo completo de respuesta a incidentes mediante tecnología basada en protección de memoria polimórfica AMTD – Defensa Automatizada de Objetivos Móviles.
EAC deberá transformar la superficie de ataque de un sistema en un objetivo dinámico e impredecible, rompiendo la ventaja estratégica del atacante. En lugar de basarse en la detección de amenazas conocidas (como hacen los antivirus o EDR), EAC utiliza la mutación para que las vulnerabilidades de un sistema sean imposibles de explotar. Este enfoque proactivo permitirá ayudar a bloquear ataques desconocidos e indetectables, reduciendo significativamente el riesgo cibernético y fortaleciendo la resiliencia operativa a nivel de máquina.

La solución deberá mantener análisis continuo, visibilidad en tiempo real y notificación proactiva 24/7, garantizando la confidencialidad, integridad y disponibilidad de la información. Asimismo, deberá ser capaz de identificar y bloquear ataques de ransomware en sus primeras fases, priorizar eventos de forma autónoma y orquestar acciones de respuesta inmediata.

Tecnología de Defensa de Objetivo en Movimiento

La tecnología AMTD deberá:

- Crear una superficie de ataque dinámica en la memoria de ejecución, imposible de mapear por actores maliciosos.

- Aleatorizar continuamente la memoria de aplicaciones, APIs y recursos del sistema operativo.
- Insertar señuelos que permitan detectar accesos indebidos.
- Capturar código malicioso para análisis forense y generar alertas oportunas.
- Impedir la reutilización de vectores de ataque en cualquier punto final.

Incluso si un atacante identifica una puerta real esta ya no existirá cuando intente reutilizarla, imposibilitando la repetición del ataque.

Capacidades del Servicio EAC

1. Protección avanzada contra ransomware

- Prevención integral desde el acceso inicial hasta la fase de encriptación.
- Bloqueo en tiempo real sin necesidad de firmas, patrones o IoAs.
- Resiliencia y continuidad operativa mediante la prevención del secuestro de datos en tiempo real a nivel de memoria, impidiendo que los procesos de ransomware inicien o completen la fase de cifrado en los endpoints y servidores institucionales.

2. Protección contra robo de credenciales

- Defensa contra ataques orientados a la sustracción de información sensible.

3. Prevención proactiva

- Identificación de errores de configuración en endpoints.
- Detección de sistemas en fin de vida útil.
- Identificación de plugins maliciosos en navegadores.
- Prevención de exfiltración de datos.

4. Eficiencia operativa

- Instalación sencilla, sin impacto significativo en el rendimiento.
- Sin necesidad de personal adicional.
- Reducción de costos y tiempos de clasificación de alertas.

5. Priorización de vulnerabilidades basada en riesgo

- Gestión de exposición mediante priorización efectiva de parches.
- Protección sin parches impulsada por EAC.

6. Despliegue flexible

- Plataforma SaaS, multi-tenant, administrada por API.
- Agente ultraligero (<9 MB).
- Sin requerir conexión a internet.
- Despliegue sin reinicios ni interrupciones.
- Protección para endpoints físicos y virtuales (incluyendo VDI, VMware Horizon View y Citrix).
- Sin monitoreo ni recopilación de datos personales.

EAC para Puntos Finales en Windows

La solución deberá:

- Detener ataques avanzados y evasivos, complementando NGAV, EPP y EDR/XDR.
- Proporcionar visibilidad continua del inventario de aplicaciones.
- Priorizar vulnerabilidades según riesgo.
- Administrarse completamente desde la nube.
- Proteger endpoints físicos y virtuales sin configuración adicional.

Funciones de Gestión de la Plataforma

La plataforma deberá ofrecer un conjunto completo de capacidades de administración, monitoreo, auditoría y control, incluyendo una Interfaz gráfica de usuario (GUI) que incluya:

Paneles e indicadores

- Eventos totales.
- Eventos bloqueados.
- Eventos por rango temporal.
- Dispositivos monitoreados.
- Dispositivos sin comunicación.
- Dispositivos que requieren actualización.

Visibilidad de riesgos y vulnerabilidades

- Panel de vulnerabilidades por equipo (workstations y servidores), con:
- Número de aplicaciones vulnerables.
- Puntuación de riesgo.
- Número de CVEs.
- Nivel de criticidad por host.
- Inventario de software con información del ciclo de vida (incluyendo fin de soporte).
- Página de aplicaciones vulnerables con EPSS, CVSS, CVEs y hosts afectados.
- Página de configuraciones incorrectas con recomendaciones de remediación.
- Página de software de alto riesgo, incluyendo herramientas LoTL usadas en los últimos 14 días.
- Visibilidad de extensiones instaladas en navegadores.

Gestión de eventos

- Página principal con eventos críticos.
- Detalles del evento: fecha, ID de amenaza (hash), nombre y tamaño del archivo, usuario, acción.
- Correlación con la matriz MITRE ATT&CK.
- Registro de IP del equipo afectado y del usuario activo.
- Cadena completa de procesos.
- DLLs cargadas y sus trayectorias.

Configuración y administración

- Registro y gestión de usuarios con roles diferenciados.
- Configuración para envío de registros vía feed.
- Registro de proveedor de identidad mediante OpenID o SAML.
- Personalización del mensaje mostrado al usuario durante confinamiento.
- Configuración del intervalo de comunicación (keep-alive).
- Control de versión del agente desde la consola.

- Menú centralizado de información sobre actualizaciones y avisos de inteligencia.
- Autenticación de segundo factor.
- Gestión de usuarios: creación, modificación, eliminación, permisos y usuarios de solo lectura.
- Desinstalación remota del agente.
- Eliminación automática de agentes inactivos tras un periodo definido.
- Anonimización opcional de registros exportados.

Exportación e integración

- Exportación de informes:
- Informe de Riesgos Ejecutivos
- Informe de Vulnerabilidades
- Informe de Incidentes
- Informe de Uso de Licencias
- Informe Ejecutivo Operativo
- Exportación de registros de auditoría (CSV y JSON).
- Envío de correos electrónicos de alerta.
- Envío de registros a sistemas externos.
- Integración mediante Open API con ámbitos y permisos personalizables.

EL LICITANTE deberá:

- Presentar carta del fabricante de la solución ofertada.
- Garantizar actualizaciones constantes de servicios y herramientas.
- Aplicar parches de seguridad y mejoras de funcionalidad.
- Mantener compatibilidad con nuevas versiones.
- Realizar actualizaciones sin afectar la continuidad del servicio.
- Asumir responsabilidades y penalizaciones en caso de incidentes derivados de versiones obsoletas.

Servicio de Diagnóstico y Reparación de Configuraciones Erróneas

Características técnicas requeridas

Los errores de configuración en los sistemas operativos de equipos de usuario final de “LOTERÍA” constituyen una amenaza significativa y constante para la seguridad. Estas fallas pueden generar vulnerabilidades que comprometan las actividades operativas, los procesos internos y la imagen institucional de la organización.
La herramienta requerida bajo demanda debe permitir la corrección de problemas desde una interfaz centralizada ubicada en la nube como servicio SaaS, operando de forma protegida y sin afectar el funcionamiento de los sistemas. Cuando sea requerido, la plataforma debe facilitar la reversión de modificaciones realizadas en los equipos designados de manera sencilla. Asimismo, es fundamental que el servicio incorpore evaluaciones de profesionales especializados en ciberseguridad, proporcionando un análisis experto sobre las posibles consecuencias de las correcciones en los recursos tecnológicos. Este enfoque permitirá que los responsables de los sistemas y aplicaciones en “LOTERÍA” puedan tomar decisiones fundamentadas sobre las modificaciones que se implementarán en su infraestructura mediante este servicio.
La implementación de un servicio gestionado para la identificación y corrección de problemas de configuración resulta fundamental para descubrir, solucionar y evitar estas vulnerabilidades de manera anticipada. Esto permitirá disminuir considerablemente los puntos de exposición a ataques y fortalecer el nivel de protección integral de “LOTERÍA”, mediante:

a. Una plataforma centralizada y especializada en la remediación configuraciones erróneas, con la capacidad de analizar el impacto y la viabilidad de los cambios a realizar a través de esta, y que incluso, pueda automatizar ciertos tipos de tareas.
b. Una plataforma que realice los cambios a través de un agente ligero que tenga el menor impacto promedio dentro de los equipos donde se encuentra instalado.
c. Un servicio de diagnóstico y reparación de plataforma de remediación de configuraciones erróneas que añada el análisis experto y la información contextual.
d. Un mapeo de los hallazgos con marcos de referencia conocidos como CIS, NIST, MITRE, entre otros.

La propuesta del servicio deberá contemplar un servicio de diagnóstico y reparación de malas configuraciones administrado que contemple los siguientes aspectos:

a. EL PRESTADOR DEL SERVICIO deberá incluir los elementos necesarios acorde a la topología y arquitectura de la red de “LOTERÍA”.
b. El servicio deberá contemplar el despliegue agentes ligeros para los endpoints de usuarios de “LOTERÍA”, además de la integración con directorio activo.
c. EL LICITANTE deberá proporcionar las guías de mercado de Gartner de las soluciones tecnológicas a desplegar.
d. Deberá considerar soporte técnico del servicio y la tecnología utilizada durante la vigencia del contrato.
e. Para que “LOTERÍA” verifique el cumplimiento de todos los aspectos técnicos planteados en el presente anexo, el concursante deberá respaldarlo con la documentación técnica del servicio propuesto en donde se pueda verificar cada requerimiento técnico solicitado.

“LOTERÍA” proporcionará los insumos necesarios para que el PRESTADOR DEL SERVICIO proporcione el servicio de manera óptima en beneficio de “LOTERÍA”:

1. “LOTERÍA” gestionará la creación de un Grupo de Remediaciones conformado por el administrador del contrato, personal del área de seguridad de la información de “LOTERÍA”, especialista de la plataforma designado por el PRESTADOR DEL SERVICIO y el dueño y/o administrador de los servidores críticos dentro del alcance del contrato. El Grupo de Remediaciones tendrá las siguientes responsabilidades:
    a. Evaluar el impacto al negocio que podrían tener las acciones de remediación proporcionadas por el servicio de diagnóstico y reparación de configuraciones erróneas sobre los activos dentro del alcance del contrato. Esta acción debe ser ejecutada por todos los miembros del Grupo de Remediaciones. El resultado determina la posibilidad o imposibilidad de efectuar cambios en los activos con base en criterios de negocio y seguridad de “LOTERÍA”.
    b. Aprobar o determinar la imposibilidad de ejecución de las acciones de recomendación proporcionadas por el servicio de diagnóstico y reparación de configuraciones erróneas sobre los activos dentro del alcance del contrato, con base en el análisis de impacto al negocio determinado previamente por el Grupo de Remediaciones. Esta acción debe ser ejecutada por los miembros del Grupo de Remediaciones que pertenecen a “LOTERÍA”.
    c. Si la acción de remediación proporcionada por el servicio de diagnóstico y reparación de configuraciones erróneas sobre los activos dentro del alcance del contrato es aprobada, entonces el personal calificado del PRESTADOR DEL SERVICIO deberá ejecutar la acción de remediación desde la plataforma propuesta.
    d. Si la acción de remediación implica algún cambio manual, y se aprueba su ejecución por parte del Comité, entonces el dueño y/o administrador del servidor deberá ejecutar el proceso de cambio con

base en el resultado de la evaluación del impacto al negocio, siguiendo los lineamientos internos de "LOTERÍA".

e. Si la acción de remediación aplicada genera un impacto no esperado en el algún activo dentro del alcance, a pesar de la evaluación y aprobación por parte del Comité, entonces el PRESTADOR DEL SERVICIO debe revertir la acción de remediación de la configuración desde la plataforma propuesta de acuerdo con los niveles de servicio del contrato. En caso de que la acción de remediación haya sido ejecutada completa o parcialmente de manera manual, el personal designado por "LOTERÍA" sobre ese activo deberá realizar las acciones de corrección.

f. Si se determina la imposibilidad de realizar la ejecución proporciona por el servicio de diagnóstico y reparación de configuraciones erróneas sobre los activos dentro del alcance del contrato, se deberá documentar dicha decisión, y en caso de que aplique, analizar otros controles de seguridad compensatorios. Esta acción debe ser ejecutada por todos los miembros del Grupo de Remediaciones.

g. Llevar a cabo reuniones periódicas de revisión de las remediaciones emitidas aplicadas por el servicio de diagnóstico y reparación de configuraciones erróneas, con el objetivo de mejorar el servicio en beneficio de "LOTERÍA". La periodicidad deberá ser determinada por el administrador del contrato, con base en la disponibilidad de los dueños y/o administradores de los activos dentro del alcance del contrato.

h. Integrarse a otros espacios dentro de "LOTERÍA" que tengan como objetivo la reducción de la superficie de ataque, mejorar la postura de seguridad o robustecer los controles de seguridad de "LOTERÍA". Esto debe ser determinado por el administrador del contrato.

i. Generar minutas de cada sesión convocada por el Grupo de Remediaciones. Las minutas se deben de distribuir a todos los miembros posterior al cierre de cada sesión, máximo el siguiente día hábil. Esta acción deberá ser efectuada por el PRESTADOR DEL SERVICIO.

2. "LOTERÍA" proporcionará al PRESTADOR DEL SERVICIO la información interna necesaria de "LOTERÍA" para materializar los objetivos del contrato. Por ejemplo, dicha información puede ser lineamientos para controles de cambio, inventarios de activos, gestión de reuniones con dueños de aplicaciones, etc.

Descripción del Servicio

El servicio administrado de diagnóstico y reparación de configuraciones erróneas deberá permitir la **remediación orquestada** de configuraciones fuera de cumplimiento (Hardening). Cada acción de remediación deberá contar con una fase de **simulación de impacto (Dry-Run)** y una validación automática post-ejecución para asegurar que el sistema regresó al **estado de cumplimiento (Baseline)** definido por el estándar CIS o NIST. Esto con el objetivo de mejorar la postura de seguridad de "LOTERÍA" al reducir la superficie de ataque de los dispositivos críticos como lo son los diferentes endpoints dentro de "LOTERÍA".

El servicio solicitado debe contar con lo siguiente:

- Escanear los activos dentro del alcance para detectar configuraciones erróneas, desviaciones de políticas, y vulnerabilidades en todos los equipos, servidores y dispositivos de red soportados por la plataforma tecnológica.
- Permitir la remediación con "un solo clic" para agilizar la operación y reducir la carga de trabajo a administradores de TI.
- Evaluar consecuencias potenciales antes de aplicar los cambios desde la plataforma, minimizando que no haya disrupciones en los servicios.
- Capacidad de revertir los cambios realizados a través de "un solo clic".

- Monitorear continuamente las configuraciones de los dispositivos soportados, identificando riesgos y áreas de oportunidad antes de que se conviertan en causas de incidentes de seguridad.
- Asignar una puntuación a las configuraciones erróneas para priorizar esfuerzos basados en el impacto potencial.
- Capacidad de configurar remediaciones automáticas basadas en políticas predefinidas, mejorando la postura de seguridad sin intervención manual.
- Capacidad de asegurar que las configuraciones de los dispositivos se alinean con marcos de referencia de seguridad como NIS2, CISI/2, NIST, PCI, HIPPA, etc.
- Proveer opciones de remediación inmediata para mantener el cumplimiento y reducir riesgos de seguridad.
- Capacidad de definir marcos de referencia personalizados de acuerdo con diferentes criterios de seguridad.
- Identificar debilidades de seguridad en GPO de directorio activo con alineamiento a las mejores prácticas de seguridad.
- Monitorear y alertar de desviaciones de configuración dentro de las políticas de directorio activo.

Los servicios administrados de diagnóstico y reparación de configuraciones erróneas deben de proveer los siguientes servicios:

- Monitoreo de configuraciones erróneas e informes de seguridad 24x7x365.
- Acompañamiento por parte de un equipo especializado en la diagnóstico y reparación de la plataforma con conocimiento de seguridad,
- “LOTERÍA” creará un Comité de Remediación conformado por personal de “LOTERÍA” e invitará a personal designado del PRESTADOR DEL SERVICIO. El objetivo de este Comité de Remediación será evaluar el impacto de las configuraciones erróneas y sus posibles remediaciones en los servicios de los activos dentro del alcance. “LOTERÍA” será quien determine la aplicación de las remediaciones en los activos dentro del alcance.
- Soporte técnico avanzado de la plataforma tecnológica utilizada.
- Apoyo en la diagnóstico y reparación de remediación de configuraciones erróneas que requieran algún grado de asistencia manual. La ejecución de estas acciones de remediación serán responsabilidad de “LOTERÍA”.

Funcionalidades del Servicio

- El servicio de remediación de configuraciones erróneas debe de proporcionarse en la nube como servicio SaaS.
- El servicio debe operar sin agentes tradicionales para realizar las tareas de remediación dentro de los equipos y servidores dentro del alcance del servicio. La funcionalidad de remediación debe de ser proporcionada a través de una tarea programada que se ejecute una vez al día con impacto mínimo en el uso de CPU, minimizando la no degradación del desempeño de los equipos o servidores.
- El servicio debe soportar acciones de remediación sobre ambientes Windows, Linux y MacOS, haciendo uso de las debidas credenciales.
- El servicio debe no solo detectar configuraciones erróneas y desviaciones de cumplimiento de marcos de referencia de seguridad, sino también, automatizar la remediación, reduciendo el trabajo manual del equipo de “LOTERÍA”.
- El servicio debe identificar las acciones de remediación que pueden ser aplicadas con riesgo mínimo de afectación dentro de los sistemas de “LOTERÍA”.
- El servicio debe identificar las acciones de remediación que implican la evaluación por parte del equipo de trabajo designado por “LOTERÍA” antes de su aplicación.

- El servicio debe proporcionar las instrucciones para aplicar las acciones de remediación manual, en caso de ser necesario.
- El servicio debe proporcionar la capacidad de revertir las acciones de remediación (rollback), permitiendo cambios seguros y controlados.
- Debe identificar configuraciones erróneas interdependientes y recomendar acciones de remediación que reduzcan la superficie de ataque de “LOTERÍA”.
- Debe proporcionar un mecanismo para determinar el riesgo obtenido después de aplicar las acciones de remediación.
- Debe proporcionar un mecanismo para determinar el valor monetario ahorrado que se obtiene después de aplicar las acciones de remediación, a partir de costos proporcionados por “LOTERÍA”.
- El servicio debe proveer integración API para que la plataforma tecnológica sea capaz de integrase con diferentes herramientas de “LOTERÍA” para flujos de seguridad específicos en concordancia de las políticas de seguridad de “LOTERÍA”.
- La solución debe permitir crear grupos de agente ligeros con base en criterios de segregación por parte del personal de “LOTERÍA”, además de los grupos por defecto con los que cuenta la solución.
- La solución debe mostrar dashboards ejecutivos que contengan información sobre el estado de remediación de las configuraciones erróneas, donde muestre tendencias de alertas, número de acciones de remediación realizadas, logros y proyecciones de estimados de ahorro en términos de tiempo y monetarios, entre otras métricas relevantes para el equipo de seguridad de “LOTERÍA”. Esto con base en las alertas de configuraciones erróneas, que son generadas y atendidas durante un periodo determinado, en los activos dentro del alcance del contrato.
- La solución debe mostrar dashboards ejecutivos que contengan el detalle sobre el estado del cumplimiento de controles de marcos de referencia como CIS, que permitan ayudar a determinar cuál es la postura de seguridad de “LOTERÍA”. Esto con base en las alertas de configuraciones erróneas, que son generadas y atendidas durante un periodo determinado, en los activos dentro del alcance del contrato.
- Los dashboards ejecutivos deben ser exportables a PDF desde la plataforma de la solución del servicio.
- La solución deberá llevar una bitácora de las acciones relevantes que se realizan en la plataforma por parte de los usuarios que proporcionan el servicio o tienen a la consola de administración.
- La solución debe permitir generar roles y usuarios, con permisos de administrados o sólo lectura.
- La solución debe contar con integración SAML para gestionar el acceso de los usuarios a la plataforma de la solución del servicio.

Diagnóstico y reparación de configuraciones erróneas

- La solución del servicio debe proporcionar en un dashboard de la consola de administración, la cantidad de agente ligeros instalados por tipo de sistema operativo en los activos dentro del alcance.
- La solución del servicio debe tener la capacidad de calcular la cantidad monetaria que la empresa está ahorrando en términos del salario total de un ingeniero de soporte técnico o de administración de infraestructura. Debe estimar el tiempo y el costo total que ha ahorrado, y también, el tiempo y costos que pueden ser potencialmente ahorrados con base en la información proporcionada por “LOTERÍA”.
- La solución del servicio debe ser capaz de dar una vista rápida al top 5 de los potenciales vectores de ataque derivados de las configuraciones erróneas, en los cuales, debe permitir aplicar filtros en los dispositivos y categorías que se requiere visualizar.

- La plataforma de solución debe categorizar los posibles vectores de ataque derivados de las configuraciones erróneas en diferentes clasificaciones. La siguiente lista contiene (mas no limita) los vectores de ataque como:
    - Navegadores
    - Credenciales
    - Movimiento Lateral
    - Protocolos Legados
    - Software Obsoleto
    - Ejecución de Código Remoto
    - Escalación de Privilegios
- La plataforma de la solución debe ofrecer una descripción concisa de la afectación derivado de las configuraciones erróneas, junto con recomendaciones claras para su remediación, su categoría y nivel de criticidad, así como su puntuación en el impacto de la configuración equivocada. Además, debe incluir un gráfico que visualice el total de dispositivos afectados, detallando cuántos de ellos presentan la vulnerabilidad. También debe proporcionar información sobre cada dispositivo afectado, e incluir un botón que permita automatizar el proceso de remediación, facilitando la corrección inmediata de la configuración equivocada. Así mismo, gracias a la calculadora de retorno de inversión, debe ser capaz de dar información sobre el ahorro monetario que genera a “LOTERÍA” a través de sus acciones.
- La solución debe diferenciar de manera automática, hace cuanto han sido utilizados los componentes del sistema que son afectados por configuraciones erróneas. Esto con la finalidad de indicar al Comité de Remediación, que remediaciones se pueden aplicar sin afectación dentro de cada servidor o equipo dentro del alcance del contrato.
- La solución debe programar las siguientes posibles acciones sobre las alertas de configuraciones erróneas a través del agente ligero:
    - Remediar
    - Auto remediar (en caso de que el usuario revierta el cambio de manera manual)
    - Silenciar alerta
- La solución debe proporcionar los pasos manuales o configuraciones adicionales, a seguir en caso de que clasifique a la configuración equivocada como compleja, y que, por ello, requiera de un análisis profundo por parte de “LOTERÍA”.
- La solución debe proporcionar información sobre las actualizaciones y novedades más recientes relacionadas con las mejoras en la plataforma propuesta. Así también el cronograma para las nuevas funcionalidades que se integrarán a la plataforma propuesta.

Cumplimiento de Seguridad y Administración de la Solución

- La solución debe proporcionar recomendaciones de fortalecimiento alineadas con las directrices del Center for Internet Security (CIS-8) y el National Institute of Standards and Technology (NIST 800-53). Los puntos de referencia de la industria sirven como directrices completas para configurar una variedad de software, sistemas operativos y dispositivos lo cual reduce los riesgos en estos sistemas contra vulnerabilidades conocidas.
- La solución debe mostrar la metodología de mapeo de cumplimiento, el cual ayuda a localizar las tareas abiertas a los controles dentro de los marcos que se establezcan. Se puede vincular tareas abiertas o

pendientes a los controles del CIS, ayudando a organizar y gestionar el cumplimiento en beneficio de "LOTERÍA".

- La solución no solo debe mapear los controles CIS a las tareas, sino que también podrá extender este mapeo a otros marcos regulatorios, usando los controles del CIS como intermediarios. Esto significa que se puede ver cómo esos controles se alinean con otras normativas o sistemas de cumplimiento. Esto podrá generar marcos de referencia personalizados o conocidos como MITRE, PCI, HIPPAA, etc.
- El mapeo de controles de seguridad debe mostrar los equipos afectados al hacer el desglose de cualquier control dentro de la consola de la solución.
- La solución debe contar con CIS Controls, que es una lista de controles priorizada de medidas de seguridad prácticas diseñadas por el Center for Internet Security. Estos controles abarcan una amplia gama de aspectos de ciberseguridad, ofreciendo a las organizaciones una hoja de ruta clara para mejorar sus prácticas de ciberseguridad, las cuales se actualizan regularmente para abordar amenazas emergentes e incorporar las mejores prácticas de la industria. Al adherirse a estos controles y puntos de referencia, las organizaciones pueden establecer una base sólida de ciberseguridad y mitigar diversos riesgos cibernéticos.
- La solución debe proporcionar los puntos de referencia de los Niveles 1 y 2 de CIS que proporcionan directrices específicas como controles de configuración para asegurar los sistemas contra vulnerabilidades comunes, siendo el Nivel 1 una oferta de medidas de seguridad básicas y el Nivel 2 requisitos más estrictos. El Security Technical Implementation Guide (STIG) proporciona una guía detallada adicional para asegurar sistemas y aplicaciones.
- La plataforma de la solución debe permitir exportar los mapeos de las configuraciones erróneas con los controles de los estándares de ciberseguridad mostrados dentro de su consola.
- La solución debe proporcionar visibilidad y ayudar a administrar la configuración de seguridad dentro de Active Directory y las Políticas de Grupo en "LOTERÍA", así como abordar problemas de seguridad y operativos que puedan presentarse.
- La solución debe proveer información sobre varios aspectos, incluyendo grupos de administradores, rutas de archivos vulnerables dentro de los GPOs, Identificadores de Seguridad (SIDs) con control total sobre las Unidades Organizativas (OUs), Nombres Principales de Servicio (SPNs), entre otros. El módulo pretende demostrar lo que un atacante podría acceder antes de proceder a un movimiento lateral o elevar sus permisos dentro de la red.
- La solución debe ofrecer recomendaciones para mejorar la administración de Directorio Activo y las GPOs, así como ayudar a localizar las GPOs que no están vinculadas a ninguna unidad organizacional, configuraciones duplicadas eliminando redundancia, identificación y gestión de cuentas obsoletas, marcar los sistemas operativos antiguos que representen un riesgo en su seguridad debido a su soporte desactualizado.
- La solución debe proporcionar la funcionalidad de monitoreo de Directorio Activo y Políticas de Grupo con un usuario de dominio con privilegios mínimos.
- La solución debe tener la capacidad de visualizar y monitorear los servidores o equipos dentro del alcance del contrato que cuentan con el agente ligero instalado en un dashboard. Cada elemento de este dashboard debe permitir seguir el mapeo relacionado con los servidores o equipos, y profundizar en el análisis de cada uno de ellos, en cuanto a las configuraciones erróneas y cumplimiento, y el seguimiento de las acciones realizadas en dentro de cada equipo.
- Las versiones de sistemas operativos soportados por el agente ligero deberán ser:
    - Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11.

  - Centos 7 y superior, Debian 10 y superior, Red Hat Enterprise Linux (RHEL) y superior, Rocky Linux 9 y superior, SUSE Linux Enterprise Server 12 y superior, Ubuntu 16 y superior.
  - MacOS 10.15 (Catalina) y superior para Intel y Apple Silicon.
- La plataforma de la solución debe desglosar la información por cada equipo, mostrando su información, el estado de las remediaciones de las configuraciones erróneas y el cumplimiento frente a los controles de los estándares de seguridad en los que se basa la plataforma.
- La solución debe tener la capacidad de realizar acciones de manera remota en los agentes ligeros de manera programada. La siguiente lista contiene (mas no limita) las acciones a realizar:
  - Desinstalar el agente ligero.
  - Reiniciar el dispositivo.
  - Extraer los logs del agente ligero.
  - Actualizar políticas de grupo con/sin reinicio del dispositivo.
  - Realizar nuevamente un escaneo desde el agente en busca de configuraciones erróneas.
- La solución debe dar seguimiento a las acciones de remediación de configuraciones erróneas y sus resultados, así como las acciones de gestión operativa de los agentes ligeros. Debe contar con la capacidad de reiniciar, detener o revertir estas acciones, según aplique para cada caso.
- El seguimiento de cada una de las acciones de remediación de configuraciones erróneas o de gestión de agentes ligeros, debe mostrarse detalladamente dentro de un dashboard en la plataforma de la solución del servicio.
- Las actualizaciones de software de los agente ligeros deben de programarse de acuerdo con el criterio de “LOTERÍA”, a través de un proceso por lotes, con base en los grupos generados en conjunto con “LOTERÍA”, para un mayor control de este proceso.

Servicio de autenticación multi factor (MFA)

“EL LICITANTE” como parte de su propuesta técnica y económica debe proporcionar en la modalidad bajo demanda, un mecanismo de autenticación multifactor (MFA) para el control de acceso lógico a las aplicaciones, servicios remotos, mediante la validación de al menos dos factores de autenticación independientes, con el propósito de fortalecer la seguridad de acceso, mitigar riesgos de suplantación de identidad y reducir la superficie de ataque ante amenazas de tipo phishing, robo de credenciales o accesos no autorizados.

La solución ofertada, infraestructura soporte y licenciamiento será responsabilidad de “EL LICITANTE”.

La solución deberá soportar, como mínimo, los siguientes mecanismos de autenticación multifactor, sin requerir dispositivos físicos dedicados (Token):

- Notificaciones de aprobación (“push”) a dispositivos móviles
- Códigos de un solo uso (OTP) basados en tiempo (TOTP)
- Mensajería segura (cuando aplique conforme a políticas de seguridad)
- Integración con autenticación biométrica del dispositivo móvil (huella, reconocimiento facial)
- Capacidad de operar en esquemas passwordless o con segundo factor

La solución debe ser compatible e integrarse de manera nativa o mediante estándares abiertos con:

- Sistemas operativos Windows (login local y remoto)
- Servicios de directorio (Active Directory, LDAP o equivalentes)
- Protocolos de autenticación y federación:

- RADIUS
- SAML 2.0
- OAuth 2.0 / OpenID Connect
- Accesos remotos:
- VPN
- Escritorio remoto (RDP)

- Aplicaciones web y servicios en la nube

La integración debe permitir su implementación sin modificaciones sustanciales a la infraestructura existente.

El servicio deberá permitir la definición de políticas dinámicas de autenticación basadas en contexto, incluyendo:

- Ubicación geográfica del usuario
- Dirección IP
- Tipo de dispositivo
- Horario de acceso
- Nivel de riesgo asociado a la sesión

Deberá permitir aplicar controles diferenciados (permitir, denegar, solicitar factor adicional) conforme a dichas condiciones.

La solución debe contar con una consola de administración centralizada que permita:

- Alta, baja y modificación de usuarios
- Asignación de métodos de autenticación
- Definición de políticas de seguridad
- Gestión de dispositivos asociados a usuarios
- Monitoreo en tiempo real de eventos de autenticación
- Generación de reportes y bitácoras

El servicio debe generar registros detallados de todas las actividades de autenticación, incluyendo:

- Intentos exitosos y fallidos
- Ubicación e IP de origen
- Dispositivo utilizado
- Método de autenticación aplicado

Los registros deberán ser exportables y se deberá integrar con el MDR, tanto para monitoreo como para la respuesta orquestada.

La solución deberá garantizar:

- Proceso de autenticación ágil y de baja fricción
- Compatibilidad con dispositivos móviles comunes (iOS y Android)
- Mecanismos de autoservicio para enrolamiento y recuperación de acceso
- Operación continua con alta disponibilidad

El servicio deberá operar bajo un esquema de alta disponibilidad, con:

- Infraestructura redundante
- Mecanismos de continuidad operativa

- Capacidad de operación en escenarios de degradación controlada

La solución deberá cumplir con las siguientes capacidades de seguridad:

- Protección contra ataques de phishing y “push fatigue”
- Cifrado de comunicaciones extremo a extremo
- Protección de credenciales

EL LICITANTE será responsable de:

- Implementación, configuración e integración del servicio MFA
- Administración continua de la plataforma
- Monitoreo y atención de incidentes relacionados con autenticación
- Actualización y mantenimiento de la solución
- Generación de reportes operativos y de seguridad
- Soporte técnico especializado
- Proveer, instalar y configurar los dispositivos de lectura de huella digital acorde a las licencias a implementar, iniciales y bajo demanda

La solución deberá:

- Integrarse con ecosistemas SIEM y SOAR sin desarrollos propietarios restrictivos
- Permitir automatización mediante APIs documentadas
- Operar bajo un modelo escalable y de alta disponibilidad
- Garantizar trazabilidad completa de eventos
- No depender de dispositivos físicos obligatorios
- Ser interoperable con herramientas de seguridad existentes del SISI

Integración con SIEM (Monitoreo y correlación)

El servicio MFA deberá integrarse con la plataforma SIEM del SISI para el envío y correlación de eventos en tiempo real.

Eventos a integrar

- Intentos de autenticación (exitosos y fallidos)
- Desafíos MFA (aprobados / rechazados)
- Intentos sospechosos (ubicaciones anómalas, accesos simultáneos)
- Cambios en configuración de usuarios
- Enrolamiento o desvinculación de dispositivos

Mecanismos de integración

- Syslog
- API REST
- Conectores nativos o estándares
- Exportación en formatos compatibles (CEF, JSON)

Objetivo

Permitir la correlación de eventos de identidad con:

- Eventos de red (NDR)

- Endpoint (EDR/XDR)
- Aplicaciones
- Perímetro (firewalls, VPN)

El servicio MFA deberá permitir su integración con la plataforma SOAR para la automatización de respuestas ante incidentes de seguridad.

Arquitectura lógica integrada

Flujo de autenticación y control inicial:

- Usuario intenta acceso (aplicación / VPN)
- Servicio MFA valida identidad (push / OTP / biometría)
- Motor de políticas evalúa contexto (Conditional Access)
- Se permite o bloquea el acceso
- Evento se registra y envía al SIEM
- SIEM correlaciona con otros eventos de seguridad
- SOAR ejecuta acciones automatizadas (si aplica)
- SOC monitorea, valida y gestiona el incidente

Este flujo podrá adecuarse a petición de “LOTERÍA” o con base en las propuestas de mejora que realice “EL LICITANTE”

Visibilidad y operación

El servicio deberá proporcionar al MDR:

Acceso a consola de monitoreo (solo lectura y/o administración controlada)

Dashboards de autenticación y riesgo

Reportes de:

- Intentos fallidos
- Accesos por ubicación
- Dispositivos utilizados

Integración con flujos de la mesa de servicio:

- Incidentes
- Problemas
- Cambios

Servicio de Firewall de Siguiente Generación (NGFW)

Los firewalls de siguiente generación (NGFW) protegen datos, activos y usuarios en los entornos híbridos actuales.

Características técnicas

- La solución consistirá en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Nueva Generación (NGFW).
- Deberá ser un equipo de propósito específico.
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.

- La solución deberá ser implementada en alta disponibilidad (Activo/Activo).
- La administración de la solución debe soportar acceso por consola, WEB (HTTPS) y línea de comandos (SSH).
- La administración WEB de la solución, deberá poder configurarse en los idiomas inglés o español.
- Debe permitir activar y desactivar para cada interfaz de la plataforma, los permisos de acceso HTTP, HTTPS, SSH.
- Adicionalmente la plataforma podrá ser gestionada por completo (objetos, redes, políticas, perfiles de seguridad, etc.) por medio de línea de comando (CLI).
- Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
- Debe permitir enviar logs a sistemas de gestión externos mediante syslog.
- Debe soportar la creación de sistemas virtuales en el mismo equipo.
- Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales.
- Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad o LACP.
- Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding.
- Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM).
- Los dispositivos de protección de red deben soportar DHCP Relay, DHCP Server, sFlow, Jumbo Frames, sub-interfaces Ethernet lógicas.
- Debe ser compatible con NAT dinámica (varios-a-1), NAT dinámica (muchos-a-muchos), NAT estática (1-a-1), NAT estático bidireccional 1-a-1, traducción de puertos (PAT), NAT Origen, NAT de destino.
- Debe soportar Dual Stack IPv4/IPv6
- Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66.
- Debe ser compatible con NAT64 y NAT46.
- Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
- Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3).
- Soportar OSPF graceful restart.
- Debe soportar la funcionalidad de SD-WAN de forma nativa y sin la necesidad de licenciamiento adicional.
- Los dispositivos de protección deben tener la capacidad de operar simultáneamente en una única instancia de servidor de seguridad, mediante el uso de sus interfaces físicas en los siguientes modos: modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3).
- Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
- Inspección de tráfico encriptado y que pueda ser controlado mediante políticas de seguridad.
- Debe soportar zonas de seguridad.
- Debe soportar protección contra la suplantación de identidad (anti-spoofing).
- Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de ciertos Países.
- Debe tener integración con LDAP y base de datos local para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios.
- Proporcionar al menos un token (OTP) de forma nativa, lo que permite la autenticación de dos factores, sin la integración de software o hardware de terceros.
- El fabricante que se contemple en la solución deberá contar con una representación debidamente conformada en México, así como un centro de atención técnico (TAC por sus siglas en inglés) para proveer el soporte técnico en español.

- Para el rubro de Hybrid Mesh Firewall (HMF), el fabricante debe aparecer en el cuadrante de líderes, en el cuadrante mágico de Gartner, el más reciente divulgado a la firma del contrato.

Control de Aplicaciones

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.

- Reconocer al menos 500 aplicaciones diferentes.
- Contar con al menos 20 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico.
- Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos.
- Inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo.
- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
- Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor.
- Crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
- Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas.
- Actualización de la base de firmas de la aplicación de forma automática.
- Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante.
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente.
- Debe alertar al usuario cuando sea bloqueada una aplicación.
- Permitir la creación de forma nativa de firmas personalizadas en su propia interfaz gráfica.

Prevención de Amenazas y Antimalware

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- Sistema Prevención Intrusos IPS con capacidades de descifrado.
- Identificar y bloquear la comunicación con redes de bots, con detección de C&C.
- Las características de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante.
- Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos.

- Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo.
- Detectar y bloquear los escaneos de puertos de origen.
- Bloquear ataques realizados por gusanos (worms) conocidos.
- Deber permitir el bloqueo de vulnerabilidades, así como de exploits conocidos.
- Debe ser capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
- Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3.
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS.
- Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante.
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Debe permitir la captura de paquetes por tipo de firma IPS y definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la alerta, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos.

Protocolos Avanzados de VPN

- Soporte VPN de sitio-a-sitio y cliente-a-sitio.
- Soportar VPN IPSec.
- La VPN IPSec debe ser compatible con 3DES.
- La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1.
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 19, Grupo 20, Grupo 21.
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
- La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI.
- La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN.
- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.
- En el caso de conexión VPN el equipo debe tener la capacidad de hacer división de trafico de VPN y tráfico de Internet, esto con el fin de evitar enviar el tráfico de Internet a través del túnel.
- Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting.
- Contar con mínimo una interfaz de conexión que le permita integrarse a un sistema dinámico de control o VPN Broker para actualizaciones de configuraciones y creación de VPNs dinámicas.
- Capacidad de integración con terceros vía túneles de VPN o túneles GRE.

Control de Tráfico

- Todos los requerimientos de seguridad antes mencionados deben funcionar en ambientes simples de interconexión
- Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Upstream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming.
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen.

- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino.
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado.
- En QoS debe permitir la definición de tráfico con máximo ancho de banda.
- Capacidad de integrar conceptos de VPN tradicional o túneles tipo GRE al esquema de SD-WAN
- Contar con mínimo 2 métodos de balanceo, IP Origen, Sesiones, IP Origen-Destino, Volumen.
- Debe soportar QoS (Calidad de Servicio).
- La solución propuesta debe hacer uso de todos los enlaces de manera simultánea y tomar decisiones basadas en políticas, Calidad de enlace (IP SLAs) y tipo de tráfico o aplicaciones.
- Contar con la integración a un sistema de gestión centralizado, el cual cuente con secciones específicas para el concepto de SD-WAN
- Capacidad de realizar Link Aggregation en el caso de contar con múltiples enlaces y que esto no afecte la funcionalidad e integración a un esquema de SD-WAN.
- Capacidad de realizar decisiones de Alta Disponibilidad o Balanceo basado en el desempeño de los enlaces.
- Para el análisis del desempeño considerar como mínimo los siguientes 3 conceptos de forma simultánea: Perdida de paquetes (loss of packets), Latencia (Latency) e Inestabilidad o fluctuación (Jitter).
- Capacidad de realizar ruteo de aplicaciones basado en su payload, lo cual permitirá el envío de cada aplicación de forma independiente a través de la malla de SD-WAN.

Gestión Centralizada

- La gestión de la solución debe soportar acceso por SSH o WEB (HTTPS).
- La administración WEB de la solución, deberá poder configurarse en los idiomas inglés o español.
- Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña de este.
- Debe permitir accesos concurrentes de administradores
- Debe tener interfaz basada en línea de comando para administración de la solución de gestión.
- Debe tener un mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos.
- Bloquear cambios, en el caso de acceso simultaneo de dos o más administradores.
- Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, acceso de lectura, creación de usuarios, cambio de configuraciones.
- Generar alertas automáticas por Email.
- Generar alertas automáticas por SNMP.
- Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horario.
- Debe ser permitido al administrador transferir los backups a un servidor FTP.
- Los cambios realizados en un servidor de gestión deben ser automáticamente replicados al servidor redundante
- Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de cuentas de usuarios LOCALES.
- Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa LDAP.
- Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa RADIUS.

- Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de Certificado Digital X.509 (PKI).
- Debe soportar sincronización de reloj interno por protocolo NTP.
- Debe registrar las acciones efectuadas por cualquier usuario.
- Debe soportar SNMP versión 2 y la versión 3 en los equipos de gestión
- Debe permitir virtualizar la solución de gestión, de manera que cada administrador pueda gerenciar, visualizar y editar solo los dispositivos autorizados y registrados en su ambiente virtualizado.
- La solución de gestión debe permitir crear administradores que tengan acceso a todas las instancias de virtualización.

Solución de Reportes

- Debe soportar acceso vía SSH y WEB (HTTPS) para la gestión de la solución.
- La administración WEB de la solución, deberá poder configurarse en los idiomas inglés o español.
- Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interfaz gráfica (GUI) como vía línea de comandos en consola de gestión.
- Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña de este
- Permitir acceso simultaneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
- Soporte SNMP versión 2 y 3
- Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
- Debe permitir activar y desactivar para cada interfaz de la plataforma, los permisos de acceso HTTP, HTTPS y SSH.
- Autenticación de usuarios de acceso a la plataforma via Radius
- Autenticación de usuarios de acceso a la plataforma via LDAP.
- Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
- Contar con mecanismos de borrado automático de logs antiguos.
- Debe contar con la capacidad de crear informes en formato PDF.
- Debe permitir exportar los logs en formato CSV.
- La solución debe contar con reportes predefinidos
- Permitir especificar el idioma de los reportes creados, incluyendo el idioma español.
- Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
- Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
- Debe permitir descargar de la plataforma los archivos de logs para uso externo.
- Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
- Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
- Debe permitir el uso de filtros en los reportes.
- Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora de este.

- Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
- Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.

Características de los equipos:

Las características de los equipos será de acuerdo al tipo de inmueble que protegen, de acuerdo con el APARTADO A:

Tipo 1

- Rendimiento NGFW: 17 Gbps
- Rendimiento: Protección de Amenazas: 15 Gbps
- Sesiones concurrentes: 12 Millones
- Almacenamiento: 960GB
- Puertos: 2x10 GE SFP+, 8x GE SFP
- Deberán estar implementados en HA

Tipo 2

- Rendimiento NGFW: 800 Mbps
- Rendimiento Protección de Amenazas: 600 Mbps
- Sesiones concurrentes: 700,000
- Interfaces: 3 x 1 GE RJ45

Servicio de Protección a Aplicaciones Móviles

Para solventar las necesidades de protección de las aplicaciones móviles de “LOTERÍA” se requiere de una plataforma bajo demanda que permita blindar los archivos binarios que se publican en tiendas de distribución de Apps Móviles (iOS y Android) sin la necesidad de codificación y de manera automatizada.

La plataforma debe de ser modular, que soporte diferentes funcionalidades como: Protecciones Anti-Fraude, Prevención de Ingeniería Social, bloqueo y prevención de uso de Bots, prevención de fraude por Geolocalización, prevención de Account take over y Deep fakes, entre otros y que puedan ser adquiridos gradualmente conforme se vayan necesitando en el tiempo, con solo adquirir licenciamiento adicional.

Arquitectura

- La solución debe realizar el blindado de los binarios de la aplicación móvil que se publica en tiendas de distribución (Google Play y App Store) sin la necesidad de codificación manual y de manera automatizada.
- La solución debe ser una solución de tipo SaaS (hospedada en la nube), la cual debe contar tanto con una interfaz gráfica de usuario (GUI) como con servicios API.
- La solución debe de poder integrarse con los diferentes servicios de Continuous Integration & Continuous Delivery (CI/CD, plataforma de DevOps), ya sea por medio de APIs o por medio de algún plugin.
- Las Apps protegidas por medio de la solución deben tener la capacidad de desplegarse a las tiendas de distribución de Apps sin depender de código o codificación adicional.

Funcionalidades

- La solución debe ofrecer una cobertura completa de seguridad usando blindaje de aplicaciones, incluyendo: Protección de RASP Completa. Anti-Tampering, Anti-Ingeniería Reversa, Prevención contra Simuladores, Emuladores y Debuggers, Validación de Checksum en Multicapas, Validación de Estructura e Integridad de la App. Debe incluir protección contra fakes, modificaciones (mods), refirma, republicación, seguridad completa de autodefensa (RASP).
- La solución debe ofrecer una cobertura completa de seguridad de código de aplicaciones móviles, lógica de negocio y modelo de interacciones con Ofuscación de Código, incluyendo Ofuscación de Código Nativo y Ofuscación de Código No-Nativo (Flutter, Cordova, Xamarin, React, entre otros). Debe incluir control de reasignación de flujo, revelación de información de debug y control de optimización. Sin necesitar scripts, reglas, símbolos o enriquecimiento de código.
- La solución debe ofrecer una cobertura completa de seguridad de datos de aplicaciones móviles, incluyendo: cifrado AES-256 (todos los estados de los datos) o FIPS 140-2: Datos en Reposo, Datos en Uso, Datos en Tránsito; y Cifrado (todas las partes) de archivos de Sandbox, Preferencias, Resources, String, secrets, XML, archivos DEX, SD card (offline, backups). Debe incluir Control de Cifrado: generación dinámica y segura de llaves (sin acceso a llaves estáticas), sin depender del modelo de datos, formato o base de datos, de las llaves facilitadas por el cliente o proveedor, de la capacidad de optimizar o controlar la cobertura de desempeño y cifrado.
- La solución debe ofrecer una cobertura completa de seguridad del SO (Sistema Operativo) móvil, incluyendo prevención contra Root/Jailbreak, fuentes desconocidas y no confiables.
- La solución debe ofrecer la protección completa contra amenazas en nivel de red (protección contra Man-in-the-Middle, Validación de CA - Certificate Authority, prevención contra certificados falsificados, alterados o falsos, SSL certificate pinning seguro y defensa contra bots con certificados de clientes móviles, shared secret y whitelisting de URLs). Debe incluir prevención contra relleno de credenciales (credential stuffing) y sniffing/extracción de credenciales.
- La solución debe ofrecer un servicio de prevención de manera anticipada y bloquear clones de Android y iOS, aplicaciones falsas y versiones modificadas (mods) de todas las apps móviles, incluyendo reempaquetado, refirma y republicación de aplicaciones en tiendas de aplicaciones no oficiales. Impedir que las aplicaciones móviles sean republicadas como aplicaciones de troyano. Apps de troyano son usados para engañar usuarios de modo a interactuar con aplicaciones, transacciones y call centers falsos, distribuir malware, habilitar acceso remoto a dispositivos y aplicaciones por criminales.
- La solución debe brindar al menos de 3 (tres) modos de configuración básica para la defensa contra amenazas:
    a. La solución detecta, defiende y notifica al usuario (caja de diálogo de SO estándar) utilizando mensajes personalizados.
    b. La solución detecta el ataque o amenaza y le envía el evento a la aplicación, en un formato estándar, para que sea procesado (la aplicación elige cómo y cuándo tomar la acción de bloqueo).
    c. La solución utiliza el modo de "bloqueo" para cualquier ataque o amenaza y le envía el evento a la aplicación, en un formato estándar, para que sea procesado, ganando inteligencia acerca de los ataques y amenazas sin perder cualquier protección.
    d. También debe poseer la opción de "Bloquear la Conexión ~~apenas~~" en casos de ataques de Man-in-the-Middle (MiTM).
- La respuesta customizada de evento de amenazas debe posibilitar diversas configuraciones, incluyendo los modos de detección y defensa "in-app".

- La solución debe brindar un recurso de puntaje (scoring) de riesgos para amenazas, permitiendo la configuración de cada Evento de Amenaza con un Nivel de Riesgos (Score) único para perfeccionar los procesos de Respuesta a Incidentes & Fraudes.
- Debe permitir que el recurso de scoring sea habilitado, pudiendo ser definido un valor específico (por ej. entre 1 y 1,000). Para validar si el recurso de puntaje/scoring está debidamente habilitado, la solución debe evidenciar y dar visibilidad de esa información (recurso habilitado o no habilitado) en el certificado generado para cada build de la aplicación.
- La solución debe brindar la posiblidad, mediante contratación por licenciamiento adicional, de un módulo completo de Dashboards (paneles de visualización) y Telemetría para Inspección de Amenazas, Investigación de Ataques y Centro de Control para Apps Móviles, brindando, como mínimo, visualizaciones detalladas de Amenazas y Ataques en tiempo real, visualizaciones de Threat Intel por Equipos, Apps, Builds, Nombre del Evento de Amenaza, Código del Evento, Score del Evento, además de filtrar los eventos de Inteligencia de Amenazas con base en Llaves de Contexto. Esa visualización de datos debe ser habilitada y configurada en cualquiera de los siguientes escenarios: con o sin implementación in-app (dentro de la aplicación).
- La aplicación debe permitir que sea configurada para informar al Centro MDR o Security Information Event Management (SIEM) de “LOTERÍA” acerca de cada evento de amenaza que ocurra. Así “LOTERÍA” tendrá un mejor entendimiento de la matriz general de amenazas relacionadas a su aplicación y podrá tomar medidas preventivas para bloquear cualquier ataque en sus servidores de aplicación web que se originen por aplicaciones eventualmente comprometidas. De igual modo, se deberá poder exportar la información desde el MDR o SIEM a un dashboard ejecutivo de gestión.
- La solución debe incluir un módulo antibot para dispositivos móviles, compatible con cualquier Web Application Firewall (WAF). La solución debe permitir una comunicación segura y cifrada, utilizando mTLS, entre el dispositivo móvil y el WAF. La implementación de este módulo no debe requerir de integraciones manuales a nivel de código de la misma App móvil de “LOTERÍA”.
- La solución debe incluir un módulo antibot para dispositivos móviles, capaz de defender contra bots en Android y iOS, robo de credenciales, aplicaciones falsas, fraude con tarjetas, apropiación de cuentas (ATO), ataques DDoS y tráfico inválido (IVT). Su implementación no debe requerir cambios manuales en el código de la aplicación móvil de “LOTERÍA”.

Operación, Administración y Gestión de la Tecnología

- La solución debe permitir el uso de mejores prácticas de desarrolladores en el proceso de aplicar recursos de seguridad a las aplicaciones móviles (Mobile OWASP). Controlar las versiones de los releases de seguridad aplicados en las aplicaciones; congelar templates de seguridad tras validación, brindar garantía auditable de que los recursos de seguridad fueron compilados en las aplicaciones Android y iOS para cada y todo build (sin dependencia de terceros). Debe ser capaz de brindar certificados evidenciando la implementación del modelo de seguridad, de modo que sean compartidos con los equipos de seguridad, gestión y desarrollo.
- La solución debe permitir que se agregue toda la telemetría de Eventos de Amenazas en el MDR y en las plataformas de SIEM de “LOTERÍA”. A partir de ello, se podrán exportar y sintetizar esos datos de telemetría en reportes para uso interno.
- La solución debe brindar un recurso para que el equipo de Seguridad pueda crear un template de seguridad aprobado y congele el template, de modo que este equipo se asegure de que el mismo template será aplicado sin cambios.
- La solución debe brindar colaboración estructurada en la plataforma para permitir que los miembros de los equipos de desarrollo puedan asignar diferentes roles y responsabilidades.

Servicio de Soporte del Fabricante

El fabricante de la solución debe brindar acceso online a la base de conocimiento (KB).

- La licencia de suscripción deberá brindar soporte técnico 24x7x365 para incluir soporte vía Chat o Email, además del servicio completo de instalación y configuración.

La solución debe brindar SLAs de Respuesta y Resolución, con SLA de resolución prestado por el fabricante (ej. bugs, errores y tickets de seguridad resueltos por el fabricante, no por el cliente). Sin impacto a la aplicación en nivel de código, sin limitaciones en el desarrollo, facilidad de cambio. Sin impacto de actualizaciones operacionales para updates de SO, updates de versión o disponibilidad de seguridad inmediata (día cero).

El Administrador del Contrato solicitará este servicio mediante correo electrónico, indicando la APP que será protegida e incluyendo el binario correspondiente. El PRESTADOR DEL SERVICIO contará con máximo 30 días naturales para realizar el fortalecimiento de la APP y deberá entregar el reporte técnico de las protecciones aplicadas, junto con el binario debidamente fortalecido.

Centro de detección, análisis y respuesta gestionada (MDR)

Descripción del servicio:

Centro de Detección, Análisis y Respuesta Gestionada (MDR) 24x7x365 (las 24 horas del día, los 7 días de la semana, los 365 días del año, durante la vigencia del contrato). “LOTERÍA” requiere que EL LICITANTE cuente con un Centro de Detección, Análisis y Respuesta Gestionada (MDR).
Este Centro deberá ser propiedad y localizarse físicamente en las instalaciones de EL LICITANTE y que cuente con la certificación en las normas ISO/IEC 27001:2022, ISO/IEC 20000-1:2018, ISO 22301:2019 e ISO 9001:2015, así como con una herramienta de mesa de servicios que tenga por lo menos 12 procesos Certificados en ITIL y/o demostrar que el personal a cargo de la mesa de servicio cuenta con la certificación ITIL v4 Specialist Create, Deliver and Support Certificate o ITIL v4 Practice Manager.
Los 12 procesos solicitados hacen referencia a la herramienta de mesa de servicios que EL LICITANTE deberá presentar.
EL LICITANTE deberá presentar como parte de su propuesta técnica copia de los certificados de las normas ISO/IEC 27001:2022, ISO/IEC 20000-1:2018 e ISO 22301:2019 vigentes y a su nombre y demostrar por lo menos 20 procesos en cada uno, siendo indispensable cumplir con los siguientes procesos similares en las 3 certificaciones:

- Gestión de Incidentes
- Gestión de Cambios
- Gestión de Continuidad de Negocio
- Gestión de Activos
- Monitoreo y Revisiones
- Gestión Requerimientos
- Gestión del Conocimiento
- Respuesta a Incidentes de Seguridad
- Atención y Resolución de Problemas

EL LICITANTE deberá acreditar que cuenta con el certificado ISO 9001:2015 “Sistema de Gestión de Calidad”, presentando copia de la certificación vigente y a su nombre y demostrando por lo menos 20 procesos.
EL LICITANTE deberá acreditar que cuenta con un Sistema de Gestión Antisoborno, presentando como parte de su propuesta técnica copia de la certificación ISO 37001:2016 vigente y a su nombre.
El Centro propuesto por EL LICITANTE deberá llevar a cabo las acciones de Detección, Análisis y Respuesta Gestionada “MDR” para la atención de incidentes de seguridad que pudieran surgir durante la prestación del servicio. El MDR deberá operar como centro operativo único de todos componentes del servicio objeto de este Anexo Técnico, integrándose a

través de consolas y/o logs. Deberá integrar los servicios y equipos de comunicaciones, de seguridad informática y procesamiento de datos que brindan servicio a "LOTERÍA" a través de la integración de sus logs. Deberá incluir dentro de los servicios de SOAR tanto los componentes propuestos por EL LICITANTE, como los servicios y equipos de comunicaciones, de seguridad informática y procesamiento de datos con que cuenta "LOTERÍA".
Como parte de su propuesta técnica EL LICITANTE deberá presentar evidencia fehaciente de sus certificaciones en las normas ISO/IEC 27001:2022, ISO/IEC 20000-1:2018 e ISO 22301:2019 con los procesos anteriormente requeridos, se deberá proporcionar copia de los certificados vigentes y a su nombre, el cual deberá ser emitido por una autoridad certificadora reconocida y avalada para la emisión de certificación en las normas ISO.
Como parte de su propuesta técnica EL LICITANTE deberá presentar evidencia fehaciente de la certificación de la herramienta de mesa de servicio con los procesos certificados solicitados y/o demostrar que el personal a cargo de la mesa de servicio cuenta con la certificación ITIL v4 Specialist Create, Deliver and Support Certificate o ITIL v4 Practice Manager
EL LICITANTE deberá presentar como parte de su propuesta técnica documento comprobatorio en el que se demuestre que es miembro activo del Foro Global de Equipos de Respuesta a Incidentes y Seguridad (FIRST por sus siglas en inglés) con una antigüedad mínima de 5 años a la fecha del acto de presentación y apertura de proposiciones. La omisión de este requisito será motivo para desechar la propuesta.
De igual forma EL LICITANTE deberá presentar evidencia de su acreditación/Certificación ante organismo internacional.
El objetivo de este centro deberá de ser la gestión de la seguridad y responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad propuestas en el presente anexo técnico, que ejecute actividades de detección, análisis, atención y respuesta a incidentes, notificación de alertas y vulnerabilidades. La herramienta de monitoreo de disponibilidad (CPU, memoria RAM, uso de interfaces de Ancho de Banda), deberá ser dedicada a "LOTERÍA", la cual soportará la configuración del poleo de los dispositivos (propuestos por EL LICITANTE) entre 1 y 5 minutos a través del protocolo ICMP, este tiempo será definido y ajustado en las mesas de trabajo con EL LICITANTE.
"LOTERÍA", debe contar con mecanismos que le permitan mantener al día las acciones pertinentes para enfrentar estas amenazas cibernéticas, mecanismos que le permitan conocer con toda certeza, cuáles son sus activos de información críticos, cómo están clasificados, dónde están y con qué tipo de controles de seguridad cuentan y los métodos para hacer frente a los ataques modernos y avanzados de hoy en día y que ésta información sobre los activos de información críticos se actualice al mismo ritmo y medida que los avances tecnológicos para poder tomar acciones informadas para su protección.
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. Este servicio deberá proveerse de forma continua en un esquema 24x7x365 durante la vigencia de "EL CONTRATO", con al menos las siguientes capacidades:
Monitoreo proactivo de la disponibilidad de las tecnologías ofertadas y administradas.

- Monitoreo proactivo de los eventos de seguridad detectados por las tecnologías administradas y su escalamiento para la atención en caso de incidentes de ciberseguridad.
- Administrar y mantener operando la plataforma tecnológica de ciberseguridad que forma parte del servicio, dentro y fuera del horario laboral de "LOTERÍA".
- Prevenir, detectar y apoyar en la mitigación de cualquier incidente de ciberseguridad de "LOTERÍA", que sea identificado y que pueda ser contenido mediante las plataformas tecnológicas que se estarán administrando.
- Brindar la asistencia necesaria para el tratamiento de incidentes que involucran la detección de vulnerabilidades y/o amenazas, ofreciendo información oportuna respecto a las nuevas vulnerabilidades relacionadas a la infraestructura tecnológica ofertada por EL LICITANTE y las acciones correspondientes para mitigarlas.

- Asistencia técnica en sitio y remota

EL LICITANTE considerará en su propuesta los recursos técnicos y humanos necesarios con experiencia de al menos 3 años en servicios similares, el personal presentado en la propuesta técnica será el que garantizará la operación a los servicios requeridos por "LOTERÍA" para la prestación de asistencia en sitio de acuerdo con los niveles de servicio solicitados durante la vigencia del contrato.

- EL LICITANTE integrará como parte de su solución la infraestructura de hardware, software licenciamiento y seguridad que considere convenientes, así como el personal necesario para atención de fallas y soporte remoto y en sitio, en caso de requerirse por parte de "LOTERÍA".
- EL LICITANTE a través de personal en sitio garantizará a "LOTERÍA" la ejecución de los siguientes procesos:
  - Administración y monitoreo continuo de las soluciones de seguridad, operadas por EL LICITANTE para la prevención de fallas.
  - Recuperación del servicio conforme a los niveles de servicio establecidos.
  - Diagnóstico y corrección de raíz en las fallas presentadas.

Contar con una herramienta de correlación de eventos capaz de analizar y correlacionar datos de seguridad de diversas fuentes, permitiendo a "LOTERÍA" detectar amenazas complejas y responder a incidentes de manera más eficiente.
Contar con una herramienta de SOAR de propósito especifico capaz de manejar playbooks complejos y flujos de trabajo avanzado, Integraciones amplias con herramientas de terceros, capacidad de automatizar procesos de principio a fin de forma más granular.

Los playbooks que deberá considerar de manera inicial EL LICITANTE para la herramienta SOAR son:

- Contención en el perímetro: Bloqueo de tráfico malicioso en el perímetro para evitar la propagación y accesos no autorizados.
- Aislamiento de equipos de cómputo: Aislar el dispositivo afectado de la red para un análisis seguro y evitar movimientos laterales.
- Bloqueo de usuario: Suspensión inmediata de la cuenta comprometida en AD.
- Rotación de contraseña en identidad: Forzar el cambio de contraseña en cuentas afectadas ara mitigar el uso de credenciales comprometidas.
- Análisis de IoC propios de la alerta: Revisión y correlación de indicadores de compromiso para determinar el origen de la amenaza.

EL LICITANTE en conjunto con LOTENAL establecerán los playbooks adicionales que consideren necesarios.

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 horas del día, los 7 días de la semana y durante la vigencia del contrato (7x24), esto último conforme la vigencia del contrato.
- Contar con personal en sitio, mínimo uno, para atención del servicio con asistencia física en los inmuebles de la Entidad ubicados en CDMX, el cual se encuentre calificado con base en las credenciales requeridas para la administración y monitoreo de los componentes que integran la solución.
- Administrar, operar y mantener todas las soluciones tecnológicas descritas en el presente anexo técnico.
- Administrar y operar la solución de seguridad Antivirus o EDR a equipos finales con la que cuente "LOTERÍA".
- 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 acciones correctivas y preventivas para asegurar la confidencialidad, integridad y disponibilidad de la información que se maneja en las diferentes soluciones de seguridad.
- Aprovechar las fuentes de red existentes para una mejor detección de ataques avanzados. Las fuentes de red pueden incluir DNS, IPS, VPN, firewall, Directorio Activo/Windows, logs de correo electrónico según lo disponga la Institución.
- Explotación de ACLs mal configuradas o abuso de permisos y privilegios de cuentas del directorio activo
- Ataques de reconocimiento de sistemas internos
- Ataques de acceso a servicios mediante cuentas inusuales
- Ataques de acceso a recursos críticos como las bases de datos, etc.
- 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 (MDR), que permitan establecer mejora en los procesos, procedimientos y controles de seguridad.
- Integrar un Equipo de Atención y Respuesta a Incidentes de Seguridad.
- La herramienta debe soportar la integración de la inteligencia de amenazas legibles por máquina de diferentes fuentes abiertas y comerciales.
- El servicio de requerimientos, cambios, incidentes, entre otros, deberá llevarse a cabo mediante la mesa de servicio propiedad DEL LICITANTE, misma que deberá operar bajo un esquema 7x24 durante la vigencia del contrato, la cual deberá quedar, implementada y habilitada al término del periodo de implementación. La herramienta para operar la mesa de servicio propuesta por EL LICITANTE deberá estar certificada en por lo menos 12 procesos de ITIL, esto se comprobará mediante la presentación de copia de la factura del licenciamiento vigente de la herramienta la cual deberá incluirse como parte de la propuesta o demostrar que el personal a cargo de la mesa de servicio cuenta con la certificación ITIL v4 Specialist Create, Deliver and Support Certificate o ITIL v4 Practice Manager.

Servicio de Correlación de Eventos

“LOTERÍA”, requiere que como parte del MDR, deberá contar con un correlacionador de eventos, también conocido como SIEM (Security Information and Event Management), con la capacidad para analizar y correlacionar datos de seguridad de diversas fuentes, permitiendo a “LOTERÍA” detectar amenazas complejas y responder a incidentes de manera más eficiente.

Se deberá considerar el monitoreo de al menos 1,000 EPS y un tiempo de retención en caliente de 90 días y 12 meses en frío.

Especificaciones técnicas del servicio:

- Interfaz gráfica basada en WEB
- Control de acceso basado en roles enriquecidos para restringir el acceso a la GUI y datos en varios niveles
- Toda la comunicación entre módulos protegida por HTTPS
- Seguimiento completo de auditoría de la actividad del usuario
- Fácil actualización de software con tiempo de inactividad mínimo y pérdida de eventos
- Actualizaciones rápidas a las actualizaciones de la base de conocimiento SIEM (analizadores, reglas, informes)
- Hash de registros en tiempo real para no repudio e integridad verificación

- Autenticación de usuario flexible: local, externa a través de Microsoft AD y OpenLDAP, Cloud SSO / SAML a través de Okta
- Posibilidad de iniciar sesión en un servidor remoto detrás de un recopilador desde SIEM GUI a través del túnel remoto SSH
- Debe estar disponible como Virtual Machine para despliegues en premisa y nube pública/privada en los siguientes hipervisores: Vmware ESX, Microsoft Hiper-V, KVM, Amazon Web Services AMI, Azure
- Debe de estar disponible en múltiples modelos de dispositivos físicos con diferentes niveles de rendimiento para proporcionar una variedad de opciones de implementación
- Debe de escalar la recopilación de datos mediante la implementación de múltiples colectores.
- Los colectores pueden almacenar eventos en el búfer cuando se conecta a SIEM y el Supervisor no está disponible
- Debe de escalar análisis mediante el despliegue de múltiples trabajadores (Workers)
- Debe de poseer una arquitectura de carga equilibrada incorporada para recopilar eventos de sitios remotos a través de coleccionistas
- Para cumplir con los requisitos de alta disponibilidad, el Supervisor puede ser configurado con instancias activas / pasivas
- Debe permitir administrar múltiples grupos de dispositivos y usuarios (organizaciones) con una sola implementación.
- Debe proveer estricta separación lógica entre organizaciones en la capa de aplicación.
- Permite el descubrimiento y categorización de dispositivos de red, servidores, usuarios y aplicaciones en profundidad. Esta información alimenta una base de datos integrada de administración de configuraciones (CMDB), la cual se mantiene actualizada por medio de redescubrimientos programados
- El equipo debe permitir que los registros enviados (como Syslog), y los dispositivos puedan equilibrar la carga de los registros en varios trabajadores o recolectores. Para registros extraídos (como Windows WMI o servicios en la nube a través de REST API), la funcionalidad de extracción se equilibra automáticamente a través de trabajadores y coleccionistas. Los registros se analizan de inmediato en el punto en el que se reciben. Este proceso distribuido acelera la recopilación y el análisis de registros.
- Debe poseer un lenguaje de análisis de registro basado en XML patentado, flexible y computacionalmente eficiente.
- Puede recopilar sin problemas una gran variedad de métricas de rendimiento y disponibilidad para ayudar al investigador a buscar amenazas. También puede alertar cuando las métricas están fuera del perfil normal y puede correlacionar tales violaciones con problemas de seguridad para crear alertas de alta fidelidad.
- Debe proporcionar mecanismos para rastrear y detectar cambios de archivos clave. Debe monitorear la configuración de inicio y ejecución de dispositivos de red a través de SSH. Debe monitorear archivos de configuración en servidores. Debe monitorear eficientemente grandes infraestructuras de servidores. Crear una alerta cuando el archivo cambia de una versión a otra.
- Proporciona soporte llave en mano para una gran cantidad de dispositivos y aplicaciones, los usuarios pueden construir sus
- propio soporte completo de la GUI. Se pueden modificar los analizadores de registro del sistema, los monitores de rendimiento y los detectores de cambio de configuración. Se pueden definir nuevos dispositivos y tipos de aplicaciones y nuevos analizadores de registros; Se pueden definir monitores de rendimiento y detectores de cambio de configuración
- Verifica identidad de usuario y seguimiento de ubicación; al combinar registros de DHCP, registros de VPN, registros de WLAN, eventos de inicio de sesión del controlador de dominio, puede mantener un seguimiento de auditoría para la dirección IP para el usuario y las asignaciones de ubicación geográfica a lo largo del tiempo.

Esta característica permite detectar credenciales robadas, ya que tienden a usarse desde ubicaciones distantes durante un corto período de tiempo.

- La solución tiene un marco flexible para conectarse a una amplia variedad de fuentes de amenazas (tanto gratuitas como de pago), descargar de manera eficiente esta información y encontrar coincidencias en tiempo real en el entorno en el que se está ejecutando. integrando inteligencia de amenazas externas. La solución permite encontrar coincidencias en conjuntos de datos grandes a una tasa de eventos muy alta.
- El motor de reglas con las siguientes características: (a) la capacidad de incluir cualquier dato en una regla, por ejemplo: rendimiento y cambio de métricas junto con registros de seguridad, (b) cálculo distribuido en memoria (pendiente de patente) que involucra nodos Supervisor y Trabajador casi en tiempo real, con altas tasas de eventos, (c) la capacidad para que la regla genere una lista de observación dinámica que puede usarse recursivamente en una nueva regla para crear una jerarquía de reglas anidadas, (d) uso de objetos CMDB en la definición de reglas y (e) lenguaje unificado basado en XML para reglas e informes que facilita la conversión de un informe en una regla y viceversa.
- Debe poseer varios modelos UEBA basados en aprendizaje automático son parte de la biblioteca de reglas incorporadas: (a) detectar inicios de sesión simultáneos de dos países diferentes, (b) detectar inicios de sesión simultáneos de dos ubicaciones geográficas improbables, (c) anomalía de comportamiento de inicio de sesión: inicio sesión en servidores y en momentos en que normalmente no se inicia sesión, etc., (d) detectar tráfico a dominios generados dinámicamente. Debe tener una gran cantidad de reglas de anomalías de comportamiento incorporadas que funcionen de forma inmediata pero que el usuario puede adaptar a su propio entorno. Se proporciona un marco en el que el usuario puede escribir nuevas reglas a través de la GUI, probarlas con eventos reales y luego implementarlas en el sistema.
- Debe permitir la puntuación y riesgo de usuario y dispositivo; al combinar la importancia de los activos, el rol y la importancia del usuario, la gravedad del incidente, la frecuencia de ocurrencia y las vulnerabilidades encontradas. Debe asignar una calificación de riesgo a los usuarios y las máquinas. Este puntaje se muestra en un tablero con capacidades de desglose para identificar los factores subyacentes.
- Debe proporcionar una serie de scripts de mitigación que pueden ejecutar una acción cuando ocurre un incidente. Los scripts pueden invocarse automáticamente cuando ocurre un incidente o pueden invocarse a pedido. También debe poder escribir sus propios scripts de mitigación e implementarlos en un sistema en ejecución
- Debe proporcionar un marco de búsqueda flexible y unificado. El usuario debe poder buscar datos basados en palabras clave o de forma estructurada utilizando atributos analizados. En el modo en tiempo real, mostrar la transmisión de datos coincidentes desde los dispositivos. En el modo histórico, se buscan eventos en la base de datos de eventos. Los nodos Supervisor y Trabajador realizan búsquedas de manera distribuida.
- Debe proporcionar una gran cantidad de informes incorporados (plantillas de búsqueda), según el tipo de dispositivo y la funcionalidad, como disponibilidad, rendimiento, cambio y seguridad. Capacidad de unificación de eventos y las capacidades de profundización o búsqueda de amenazas.
- Debe contener una amplia selección de informes de cumplimiento listos para usar: PCI, COBIT, SOX, ISO, ISO 27001, HIPAA, GLBA, FISMA, NERC, GPG13, SANS Critical Control, NIST800-53, NIST800-171.
- Debe proporcionar una amplia variedad de paneles para que el usuario visualice los datos que recopila y los incidentes que se han desencadenado: paneles de resumen, paneles de widgets, panel de servicios comerciales, panel de incidentes, panel de identidad y ubicación.
- Debe poseer un sistema de tickets incorporado para administrar incidentes a través de tickets. Admitir el ciclo de vida completo del boleto de apertura, escalado, cierre, reapertura y creación de casos con archivos adjuntos para evidencia.

- Debe integrarse con sistemas de tickets de terceros. Cuando se produce un incidente, debe de crear un ticket en el sistema de tickets externo y vincularlo a un dispositivo existente o se puede crear un nuevo dispositivo en el sistema externo. Puede personalizar varios campos de incidentes al campo del sistema de tickets externo. Cuando el boleto se cierra en el sistema de boletaje externo, el boleto debe de cerrarse localmente.
- Debe de ser compatible por defecto con varios sistemas de tickets externos de terceros, por ejemplo, ServiceNow, Salesforce, ConnectWise y Remedy. Se proporciona una API para que se puedan construir otras integraciones.
- Debe poseer un servicio comercial que le permita priorizar incidentes y ver métricas de rendimiento / disponibilidad y desde una perspectiva de servicio comercial. Un servicio comercial se define como un contenedor inteligente de dispositivos y aplicaciones relevantes que cumplen un propósito comercial común. Una vez definido, todo el monitoreo y análisis se presentan desde una perspectiva de servicio comercial.
- Debe permitir definir y mantener fácilmente un servicio comercial. Dado que descubre automáticamente las aplicaciones que se ejecutan en los servidores, así como la conectividad de la red y el flujo de tráfico, puede elegir fácilmente las aplicaciones y los servidores respectivos y recibir una guía inteligente para elegir el resto de los componentes del servicio comercial.

- Deberá soportar la integración de los siguientes orígenes de información para descubrimiento y monitoreo ya sea mediante conectores nativos de la solución o mediante desarrollos de los mismos por EL LICITANTE:
    - Servidores de aplicaciones: Apache, Micosoft ASP.NET, Oracle WebLogic.
    - Bases de datos: Microsoft SQL Server, MySQL Server, Oracle Database Server**.**
    - Servidores de DHCP y DNS: Windows Server (DHCP & DNS).
    - Servidor de directorio: Microsoft Active Directory.
    - Servidor de gestión de documentos: Microsoft SharePoint.
    - Servidor de correo: Microsoft Exchange
    - Herramientas de control de código fuente para la recopilación de registros a través de API: GitHub y GitLab**.**
    - Servidores VoIP: ALCATEL LUCENT.
    - Servidores Web: Apache Web Server, Microsoft IIS for Windows 2022.
    - Aplicaciones Cloud: Google Apps Audit, Microsoft Office 365 Audit, Salesforce CRM Audit.
    - Aplicaciones de antivirus y seguridad de host (HIPS) para descubrimiento y monitoreo: FortiClient, Sophos Central, Sophos Endpoint Security and Control, TrendMicro Vision One.
    - Firewalls: Check Point FireWall-1, SNBT CHECKPOINT 7000, Consola Smart-1 600M, Consola Smart-1 5050, Fortinet FortiGate (1500D, Fortiwifi 40 F y Fortiwifi 60F) Sophos UTM, FWNG instalados en sedes Reforma e Insurgentes.
    - Balanceadores de carga y firewalls de aplicaciones para descubrimiento y monitoreo: FATPIPE, WAF Radware.
    - Routers y Switches: Extreme Networks VSP 8600 SW CORE, SW Acceso ERS 4950.
    - Servidores: Linux Server, Microsoft Windows Server, Sun Solaris Server.
    - Dispositivos de seguridad: DBF Imperva. Defense Pro Radware
    - Detección de amenazas en ThreatConnect: FortiGuard, ThreatConnect. En general cualquier fuente que provea un archivo CSV o que soporte STIC/TAXII standard.
    - Servidores de virtualización: HyperV, Vmware ESX.
    - Dispositivos de Wireless LAN: Extreme Networks Campus Controller, VE6120 Small.

Servicio de Orquestación, Automatización y Respuesta de Seguridad

"LOTERÍA" como parte del MDR requiere una tecnología que ayude a responder de manera más eficiente a los incidentes de seguridad mediante la automatización de tareas y la orquestación de diferentes herramientas y procesos.

La solución propuesta debe crear una oportunidad de ahorro de tiempo en la gestión y respuesta a las alertas, eliminando la fatiga y las tareas repetitivas automatizables, y permitiendo de ese modo que los especialistas en ciberseguridad puedan concentrarse en tareas de más alto valor. La solución debe ofrecer funcionalidades de:

- Gestión de incidentes
- Gestión de amenazas y respuesta a incidentes

Para registros de autoría, se deberán considerar al menos un tiempo de retención en caliente de 90 días y 12 meses en frío.

Especificaciones técnicas del servicio:

- La administración de la solución debe soportar acceso WEB (HTTPS) y mediante CLI
- Debe proporcionar capacidades de respuesta a incidentes en tiempo real, correlacionando múltiples fuentes de datos en un entorno multifabricante
- Capacidad de gestión de acceso RBAC (Role Based Access Control) granular. Los permisos de función se basan en el modelo Crear, Leer, Actualizar y Eliminar (CRUD)
- Debe permitir crear módulos adicionales (contenedores de datos, gráficas, reporting y visualización) así como sus propios playbooks y conectores.
- Debe está disponible como máquina virtual con soporte a VMware ESXi versions 5.5, 6.0, 6.5, 7.0, 8.0 y Redhat KVM
- Virtual appliance debe poder desplegarse en entornos de plataformas de virtualización (VMware) o bien en Cloud (AWS, Azure). Si los requisitos de la plataforma aumentan, es posible crecer vertical y horizontalmente (scale up, scale out).

- Debe proveer capacidades para orquestar y automatizar la gestión de casos de seguridad, incluyendo la gestión de alertas, incidentes, vulnerabilidades y asignación de tareas con trazabilidad total extremo a extremo.
- Debe incluir módulos por defecto disponibles una vez instalada la plataforma, proporcionando una base de datos que almacena los diferentes modelos de datos e incidentes de seguridad.
- Debe ser posible customizar la consola mediante templates, para customizar a nivel de campo todas las pantallas disponibles, insertando gráficas, tablas, y menús adicionales mediante un entorno GUI.
- El módulo de gestión de vulnerabilidades debe permitir integración nativa con múltiples escáneres de vulnerabilidades disponibles comercialmente en el mercado.
- Debe disponer de microservicios que permiten construir plataformas escalables y altamente redundadas en entornos corporativos de misión crítica.
- Debe disponer de múltiples colas y asignar colas a múltiples usuarios. De esta forma se puede tener trazabilidad sobre las alertas, incidentes y tareas controlando los SLAs de investigación y resolución de forma eficiente.
- Debe contar con un módulo de gestión de alertas que permite revisar y asignar las diferentes alertas e incidentes de seguridad recibidas de los SIEM y otras fuentes de datos de los clientes, como por ejemplo e-

mails de alertas de phishing. También es posible crear alertas e incidentes de forma manual mediante el entorno gráfico.

- Las alertas recibidas pueden ser escaladas a Incidentes de seguridad, para posteriormente ser investigados, enriquecidos y remediados mediante la ejecución de acciones y playbooks de forma ágil.
- Debe ser capaz de mapear múltiples registros y agruparlos en función de IOCs que contengan hashes, direcciones IPs, dominios u otros parámetros de forma similar.
- Debe permitir la agrupación por similitudes que permita correlacionar diferentes eventos y alertas simplificando la función de los analistas.
- Debe contar con conectores API y Playbooks que permitan realizar tareas complejas y workflows sobre más de 200 plataformas de ciberseguridad del mercado.
- Debe contar con una plataforma gráfica que permita diseñar playbooks o editar los ya existentes de forma visual y sencilla, sin necesidad de conocimientos de scripting o programación para poder ajustar o crear nuevos playbooks.
- Debe ser posible crear scripts más complejos mediante JINJA, así como crear variables (Dynamic Values) que pueden ser empleados en los scripts JINJA. Permitiendo parsear las salidas y disponer de múltiples variables predefinidas para las tareas más habituales.
- Debe disponer de conectores e integraciones con las principales plataformas de ciberseguridad del mercado, con fabricantes líder en SIEM, Firewall, Servicios de Directorio, Sandbox, Plataformas de Threat Intelligence, Escáneres de vulnerabilidades, plataformas NAC, soluciones de Correo, Servicios Cloud y otros.
- Debe permitir enviar logs a sistemas de gestión externos mediante syslog.
- Los conectores deben estar disponibles en un entorno Market donde sea posible buscar e instalar los diferentes módulos de forma sencilla.
- Se debe tener la capacidad de crear módulos customizados de mediante SDK para recoger datos de fuentes adicionales.
- Debe soportar arquitecturas en alta disponibilidad (HA) y recuperación de desastres en caso de contingencia. Debe disponer de opciones de despliegue de clusters Activo-Pasivo y del empleo de bases de datos internas o externas. En el caso que los datos se almacenen en bases de datos externas, es posible confiar en las soluciones HA de BBDD externas.
- Los cambios realizados deben estar sincronizados en todos los nodos y en caso de fallo del nodo principal, uno de los nodos secundarios toma el control de forma automática.
- La consola de administración debe realizar la gestión de encriptación y backup de las bases de datos de forma automática.
- Debe ser posible realizar backups y snapshots para ser recuperados posteriormente.
- Debe recopilar automáticamente información del centro de inteligencia del fabricante y de cualquier fuente pública para enriquecer las investigaciones, la búsqueda de amenazas y la colaboración.
- Una solución completa para la gestión de casos y la gestión y seguimiento de asignaciones de tareas, colas de trabajo y calendario de turnos.
- Las alertas y los incidentes deben tratarse por separado, cada uno en su propio módulo de interfaz de usuario.
- Los atributos (campos) de cada módulo, como el nombre, la gravedad, etc. del módulo de alerta, deben ser personalizables para que los usuarios puedan añadirlos o eliminarlos; además, los usuarios deben poder crear, modificar y eliminar sus propios atributos personalizados en cualquier módulo del sistema.
- La solución debe disponer de un motor de predicción basado en aprendizaje automático que prediga los valores de los campos basándose en datos históricos. El alcance de la predicción de aprendizaje automático debe abarcar todos los módulos del producto, incluidos los integrados (como alertas, incidencias, indicadores, etc.) y los personalizados.

- La solución debe incluir una capacidad de detección de correo electrónico de suplantación de identidad basada en IA.
- La solución debe contar con un sistema de recomendación de flujos de trabajo basado en IA para ayudar al analista a seleccionar la automatización que debe ejecutar para cada tipo de tickets.

- Debe incluir una sala de guerra (War Room) de gestión de crisis para permitir la colaboración entre equipos durante las crisis; la sala de guerra debe poder crearse manualmente.

- El sistema debe permitir al analista realizar un Análisis de Causas Raíz con un medio de correlación gráfico
- La correlación gráfica debe estar disponible para diferentes tipos de registros, como activos, vulnerabilidades, alertas e incidentes.
- La solución debe integrarse con el marco ATTACK de MITRE para proporcionar enriquecimiento de tácticas, análisis de amenazas, investigación de incidentes y sugerencias de reparación.

- El sistema debe permitir al analista realizar un análisis posterior al incidente mediante indicadores que contengan detalles de todos los datos recopilados de los registros o archivos del sistema, que identifican actividades potencialmente maliciosas en un sistema.

- El sistema debe soportar la asignación de tickets a las fases de cyber kill chain
- La gestión de casos debe permitir adjuntar archivos
- Las notificaciones deben ser flexibles y utilizar múltiples canales como la interfaz de usuario, el correo electrónico y varias integraciones con servicios de conferencia como MS Teams y Slacks. El sistema también debe admitir notificaciones del sistema cuando
- Las colas de entrada, la gestión de turnos y el traspaso deben ser una capacidad integrada. La solución debe ofrecer un sistema de colas en el que los analistas se asignen en función de su disponibilidad (turnos)
- Los Playbooks deben soportar los siguientes disparadores (triggers):
    - Manual: El analista puede ejecutar un playbook manualmente desde la WebUI
    - On record Create/Update/Delete: cuando un registro (Alerta, indicador, incidente...etc) es creado o modificado
    - Via API: cuando SOAR recibe una petición HTTP con parámetros específicos ejecuta un playbook específico
    - Referenced: un playbook debe poder ser ejecutado por otro playbook proporcionando sus parámetros requeridos
- La solución debe tener al menos 590+ conectores de Integración con sistemas de terceros, como soluciones SIEM, servicios de inteligencia de amenazas, cortafuegos...etc.
- El sistema debe disponer de un mecanismo de actualización de contenidos en tiempo real independiente de las actualizaciones del firmware de la solución. Las integraciones con sistemas de terceros deben tener sus propias actualizaciones utilizables sobre cualquier versión soportada del firmware de la solución
- La interfaz de usuario web debe incluir asistentes que ayuden a los usuarios a crear contenidos, ya sean integraciones, extensiones de productos o widgets personalizados.
- La solución debe proporcionar un conector SDK que permita a los clientes desarrollar sus propias integraciones
- La solución debe contar con Rapid Development Kit (RDK) para crear eficientemente integraciones de terceros (conectores) y otros fragmentos de código de utilidad para SOAR
- El sistema debe proporcionar un asistente de ingestión de datos fácil de usar para configurar la ingestión de datos desde sistemas de terceros.

- El sistema debe proporcionar un panel de control de la salud de las integraciones que indique si todas las integraciones con los sistemas de terceros están en buen estado.
- EL LICITANTE debe proporcionar su propio servicio de búsqueda de reputación IoC de inteligencia sobre amenazas que funcione de forma nativa con el SOAR propuesto. El servicio debe incluirse de forma gratuita.
- La solución debe tener una capacidad de gestión de inteligencia sobre amenazas (TIM) que incluya un panel de inteligencia sobre amenazas con estadísticas sobre: Fuentes activas, observables de alta confianza, fuentes de alimentación.
- La solución debe actuar como un servicio de Inteligencia de Amenazas para sistemas de terceros donde colecciones específicas o indicadores pueden ser recuperados de SOAR por SIEMs, EDRs, NGFWs ...etc vía TAXII y CSV sobre HTTP.
- La solución debe permitir realizar copias de seguridad y restaurar tanto la configuración del sistema como los datos

Servicio de Ciberintelligencia

Se requiere un servicio de inteligencia táctica, estratégica y operacional para incrementar la protección y mejorar la postura de seguridad de “LOTERÍA”. Este servicio permitirá identificar y analizar amenazas del entorno, incluyendo sitios, perfiles y/o aplicaciones apócrifas, facilitando la prevención y la respuesta oportuna ante ciberamenazas.
Se requiere una plataforma que permita tener visibilidad de los eventos que acontecen, sin requerir accesos especiales a web obscura y profunda.

La solución de servicios de Ciberinteligencia deberán considerar como mínimo:

- Contar con un motor de descubrimiento autónomo y continuo que identifique todos los activos digitales externos de la organización —dominios, subdominios, rangos IP, recursos en nube y certificados— sin requerir intervención manual, garantizando un inventario actualizado y preciso de la superficie de ataque expuesta.
- Disponer de un centro de alertas centralizado que consolide y priorice todas las notificaciones de seguridad generadas por la plataforma, permitiendo al equipo de seguridad identificar y actuar sobre amenazas activas, cambios en la exposición y variaciones en la postura de riesgo de manera oportuna y sin dispersión operativa.
- Deberá ser capaz de identificar de forma continua vulnerabilidades conocidas (CVEs), configuraciones incorrectas, certificados vencidos, puertos expuestos y superficies de ataque explotables en todos los activos externos descubiertos, asignando puntuaciones de riesgo alineadas a estándares como CVSS e incorporando el impacto contextual al negocio como factor de priorización.
- Deberá detectar las tecnologías, frameworks y bibliotecas de terceros presentes en los activos externos de la organización, y permitir la configuración de listas de monitoreo que generen alertas automáticas cuando se identifiquen nuevas instancias de tecnologías de interés, facilitando la gestión del riesgo asociado a componentes específicos del stack tecnológico.
- Deberá proporcionar monitoreo continuo de la postura de riesgo externo agregada de la organización, incluyendo análisis de tendencias históricas, comparativas de referencia (benchmarking) y dashboards ejecutivos que soporten la comunicación del riesgo cibernético a órganos directivos y comités de gobernanza.
- Deberá detectar proactivamente registros de dominios fraudulentos que imiten la identidad de marca de la organización mediante técnicas de sustitución de caracteres, homoglifos o combinaciones de palabras clave, así como páginas de phishing activas y propiedades web que hagan uso indebido de la marca corporativa, habilitando acciones de remediación tempranas.
- Deberá identificar perfiles no autorizados en redes sociales, aplicaciones móviles fraudulentas publicadas en tiendas de aplicaciones y cuentas de suplantación dirigidas tanto a la identidad de marca de la organización

como a su personal directivo y ejecutivo de alta visibilidad (VIPs), permitiendo la gestión centralizada de solicitudes de eliminación.

- Deberá monitorear de forma continua foros de la dark web, sitios de filtración, bases de datos de brechas y mercados criminales en búsqueda de credenciales corporativas expuestas, generando alertas en tiempo real que permitan al equipo de seguridad iniciar procesos de remediación y prevenir la toma de control de cuentas (ATO) antes de que el adversario las explote.
- Deberá proveer a los analistas de inteligencia acceso a una colección indexada y curada de fuentes de la web abierta, profunda y oscura, a través de un motor de búsqueda integrado en la plataforma, facilitando la investigación ad-hoc de actores de amenaza, campañas activas y activos comprometidos sin requerir herramientas externas.
- Deberá detectar automáticamente la aparición de información sensible de la organización en canales ilícitos, incluyendo datos financieros (PAN/CVV), hilos de correo electrónico internos, código fuente propietario, claves de API e información de identificación personal (PII), mediante casos de uso preconfigurados que no requieran parametrización técnica avanzada para su activación.
- Deberá incluir un feed curado y actualizado en tiempo real de noticias de ciberseguridad global y campañas de ransomware activas, relevantes para el sector e industria de la organización, validadas y enriquecidas por el equipo de investigación de Check Point (CPR), de modo que el equipo de seguridad disponga de contexto situacional actualizado sin depender de múltiples fuentes externas.
- Deberá proveer reportes exclusivos de inteligencia de amenazas producidos por un equipo de investigación, cubriendo amenazas dirigidas a sectores específicos, técnicas de ataque emergentes y tendencias de riesgo cibernético de naturaleza geopolítica, con el nivel de profundidad y especificidad requerido para apoyar decisiones estratégicas de seguridad.
- Deberá permitir la consulta de su base de datos de indicadores de compromiso (IoC) directamente desde la interfaz de la plataforma y mediante una extensión de navegador, retornando puntuaciones de amenaza, datos de atribución e información de campañas relacionadas, con el fin de agilizar el enriquecimiento de contexto durante flujos de investigación activos.
- Se deberá considerar el monitoreo del dominio de “LOTERÍA”.
- Se deberá considerar el poder ejecutar por lo menos 100 takedowns durante la vigencia del contrato.

Servicios de Visibilidad

Para proteger eficazmente la red de “LOTERÍA”, se requiere una solución integrada de visibilidad de la red y que permita comprender el panorama de riesgos de la organización, tomar decisiones informadas y proteger los activos críticos.
Durante la vigencia del contrato, EL LICITANTE deberá brindar acceso a las consolas de administración y reporteo mediante usuarios de solo lectura, con permisos de administrador prevaleciendo los controles de trazabilidad para no repudio, con el fin de que “LOTERÍA” pueda supervisar las siguientes tareas:

- **Identificación de amenazas y vulnerabilidades**. “LOTERÍA” necesita visibilidad sobre todos los sistemas, redes, aplicaciones y datos de la organización para identificar posibles amenazas y vulnerabilidades. Esto incluye visibilidad sobre el hardware, software y los datos en reposo y en tránsito.
  El servicio de gestión de vulnerabilidades debe proporcionar las siguientes funciones de gestión de vulnerabilidades para endpoints de usuario:
    - Detección exhaustiva de vulnerabilidades a través del descubrimiento de los CVE, errores de configuración y exposiciones en el sistema operativo, las aplicaciones y los componentes de la cadena de suministro de IA, para obtener visibilidad total de la superficie de amenazas activa.
    - Reevaluar la severidad de los CVE a través de la inteligencia de riesgos impulsada por IA utilizando la contextualización de las amenazas con análisis impulsados por IA.

- Priorizar las vulnerabilidades en función de la explotabilidad real, la criticidad de los activos y las amenazas activas del entorno específico de “LOTERÍA”.
- Comprobar si el estado actual cumple con las normas de cumplimiento y los marcos de referencia (CIS, NIST, etc.).
- Relacionar el problema detectado con los datos de CVE/CVSS, incluyendo la gravedad y la posibilidad de explotación.
- Clasificar el hallazgo en un nivel de riesgo, de modo que los problemas de alta gravedad se destaquen para su corrección prioritaria.
- Corregir y dar resolución autónoma de exposiciones al aplicar al instante correcciones previamente validadas y controladas por políticas.
- Debe tener la capacidad de aplicar parches para fortalecer y eliminar automáticamente vulnerabilidades críticas en los dispositivos de los usuarios de “LOTERÍA”.
- Revertir de manera segura cada parche y cambio de configuración con el objetivo de causar cero interrupciones. Si una corrección causa un problema, la solución debe ser capaz de desinstalar el parche al instante o restaurar el sistema desde una copia de seguridad para preservar la continuidad del negocio, asegurando una gestión de vulnerabilidades sin disrupciones.

El servicio de gestión de vulnerabilidades debe proporcionar las siguientes funciones de gestión de vulnerabilidades para servidores:

- El servicio tendrá como objetivo:
  - Identificar las brechas de seguridad de los servidores seleccionados para su análisis.
  - Identificar el estado de exposición de la infraestructura sujeta de la evaluación.
  - Proveer una lista de recomendaciones técnicas para el cierre de las brechas y/o vulnerabilidades detectadas en el ejercicio.
- Como parte del servicio, EL LICITANTE, debe proporcionar una solución que cuente con licencia, al momento de llevar a cabo los análisis solicitados, durante la vigencia del contrato o servicio, misma que permita llevar a cabo el escaneo de vulnerabilidades, para la gestión de estas en los servidores que conforman la infraestructura de “LOTERÍA”.
- El análisis deberá ejecutar una evaluación técnica de vulnerabilidades **cada 3 meses** al menos, mediante herramientas confiables, a los servidores que “LOTERÍA” haya seleccionado, del total señalado, y deberá generar una evaluación del riesgo de estos, considerando su impacto en la Confidencialidad, Integridad y Disponibilidad de la información, así como la importancia de dichos servidores dentro de “LOTERÍA”.
- Previo a la evaluación técnica de vulnerabilidades sobre los activos que determine “LOTENAL”. EL LICITANTE, deberá elaborar un Statement of Work (SOW), sujeto a revisión y aprobación de “LOTENAL”, en el que se definan como mínimo el objetivo, alcance, activos autorizados y excluidos, metodología, fechas, horarios, personal participante, herramientas, reglas de compromiso, canales de comunicación y criterios de suspensión. Las evaluaciones deberán realizarse conforme a metodologías y mejores prácticas internacionales reconocidas, tales como NIST, OWASP y SANS/CIS o equivalentes, procurando en todo momento no afectar la disponibilidad ni continuidad de los servicios institucionales. Los resultados deberán documentarse mediante un reporte ejecutivo, reporte técnico y matriz de vulnerabilidades que permita identificar, clasificar, priorizar, remediar y dar seguimiento a los hallazgos; asimismo, deberán realizarse las revalidaciones necesarias para comprobar la atención de las vulnerabilidades corregidas. La evaluación trimestral no sustituirá las actividades continuas de identificación, monitoreo y atención de amenazas y vulnerabilidades establecidas como parte del SISI.

- "EL LICITANTE" deberá mantener, durante toda la vigencia contractual, una solución debidamente licenciada y con capacidad para administrar una base inicial de 159 y hasta un máximo de 200 servidores físicos y/o virtuales. La incorporación de activos dentro de ese límite será notificada por el Administrador del Contrato con al menos cinco días hábiles de anticipación y no generará erogaciones distintas de las contractualmente establecidas.

- Para el escaneo de vulnerabilidades la solución deberá cumplir con al menos las siguientes características:
  - Descubrir los componentes del software instalado en los activos.
  - Ejecución de escaneos ilimitados para cada uno de los activos.
  - Ejecución de escaneos bajo demanda y programados.
  - Ejecución de escaneos autenticados y no autenticados.
- Se acordará previamente entre "LOTERÍA" y EL LICITANTE las fechas y horarios para la ejecución de los ejercicios de los análisis.
- El análisis de vulnerabilidades deberá contar por lo menos con las siguientes fases:
  1. Recolección de información: Inventario, horarios, responsables y tipos de reportes.
  2. Identificación de servicios: Reconocimiento de los activos y validación de alcance a los componentes.
  3. Escaneo de vulnerabilidades.
  4. Análisis de hallazgos.
  5. Informes ejecutivo y técnico.
  6. Recomendaciones y priorización.
- Para la prestación del servicio, EL LICITANTE debe considerar como reglas de compromiso:
  a) No realizar pruebas sobre activos no incluidos expresamente en el SOW.
  b) No ejecutar actividades fuera de las fechas y horarios autorizados.
  c) No realizar acciones de denegación de servicio, degradación intencional, destrucción, modificación o eliminación de información, salvo autorización expresa y por escrito de "LOTENAL".
  d) Evitar técnicas que pudieran generar indisponibilidad o afectaciones a servicios productivos.
  e) No realizar explotación de vulnerabilidades con fines distintos a la validación técnica autorizada.
  f) Detener inmediatamente las pruebas cuando exista riesgo de afectación a un servicio crítico.
  g) Informar de forma inmediata a "LOTERIA" cuando se identifique una vulnerabilidad crítica, exposición activa o indicio de compromiso.
  h) Mantener confidencialidad sobre la información, vulnerabilidades, configuraciones, credenciales y evidencias obtenidas.
  i) Registrar las actividades realizadas para mantener trazabilidad de la evaluación.
  j) Coordinar cualquier actividad que involucre telecomunicaciones, infraestructura de red o componentes operados por terceros conforme al proceso de coordinación establecido para el SISI.

- **Evaluación de riesgos**. La visibilidad permite a "LOTERÍA", evaluar el impacto potencial de las amenazas y vulnerabilidades en la organización, priorizar los riesgos y asignar recursos de manera efectiva.
- **Respuesta a incidentes**. "LOTERÍA" con buena visibilidad puede responder rápidamente a incidentes de seguridad, identificando la causa raíz, conteniendo el daño y recuperándose de manera eficiente.
- **Cumplimiento normativo**. Permitirá a "LOTERÍA" a garantizar el cumplimiento de las regulaciones de seguridad y privacidad de datos relevantes para su industria.

- **Toma de decisiones**. Con una visión clara del panorama de seguridad, "LOTERÍA" puede tomar decisiones informadas sobre inversiones en seguridad, estrategias de mitigación de riesgos y políticas de seguridad.
- **Comunicación efectiva**. La visibilidad permite a "LOTERÍA" comunicar claramente los riesgos y las necesidades de seguridad a la alta dirección y a otras partes interesadas, obteniendo su apoyo y recursos necesarios.
- **Cultura de seguridad**. "LOTERÍA" con visibilidad puede fomentar una cultura de seguridad dentro de la organización, educando a los empleados sobre las mejores prácticas y promoviendo la concienciación sobre la seguridad.
- **Protección de la reputación**. La visibilidad permite a "LOTERÍA" proteger la reputación de la organización al prevenir o mitigar incidentes de seguridad que podrían dañar la confianza del cliente y la imagen pública.

Entregables de cada evaluación trimestral

Al término de cada ejercicio, EL LICITANTE, en un plazo no mayor a 15 días hábiles, una vez concluidas las pruebas, deberá entregar como mínimo:

- Reporte ejecutivo: resumen de la evaluación, nivel de exposición identificado, principales riesgos, comparativo respecto de la evaluación anterior y recomendaciones prioritarias.
- Reporte técnico: deberá identificar los activos evaluados, vulnerabilidades encontradas, severidad, descripción, evidencia, componente afectado, impacto potencial, referencias técnicas, recomendación de remediación y prioridad.
- Matriz de vulnerabilidades: deberá permitir el seguimiento de cada hallazgo y contener como mínimo identificador, activo afectado, vulnerabilidad, severidad, fecha de detección, responsable de atención, recomendación, estado y fecha de cierre.
- Plan de remediación: conjunto de recomendaciones y acciones correctivas propuestas para reducir o eliminar las vulnerabilidades identificadas, sujeto a la aprobación y priorización de "LOTENAL".
- Reporte comparativo: deberá señalar vulnerabilidades nuevas, persistentes, mitigadas, remediadas o reincidentes respecto de la evaluación trimestral anterior.

Coordinación Operativa del "SISI" con el NOC para la Atención de Incidentes de Seguridad en Componentes y Activos de Telecomunicaciones.

Con el objetivo de garantizar la detección, análisis, contención, mitigación, seguimiento y cierre oportuno de eventos e incidentes de ciberseguridad que puedan afectar la infraestructura de telecomunicaciones, servicios críticos, dispositivos de red, enlaces de comunicaciones, plataformas de seguridad perimetral y demás activos tecnológicos de "LOTERÍA", EL LICITANTE deberá operar de manera coordinada, permanente y documentada con el proveedor responsable del Network Operation Center, en adelante NOC.

La coordinación entre EL LICITANTE, LOTERIA, el NOC y demás terceros proveedores involucrados en la seguridad informática de la infraestructura, información y servicios de Lotería, deberá establecerse a más tardar dentro de los 15 días naturales contados posteriores al inicio del servicio, mediante el Proceso de Coordinación Operativa con Terceros que deberá incluir procedimientos operativos documentados, matrices de escalamiento, canales formales de comunicación, criterios de clasificación de incidentes, protocolos de intercambio de información técnica, ventanas de atención, mecanismos de validación cruzada y registro obligatorio de actividades a través de la Mesa de Servicio. El Proceso de Coordinación Operativa con Terceros deberá contener la matriz RACI para dar claridad en los alcances de los actores que intervienen.

EL LICITANTE será responsable de liderar, desde el ámbito de seguridad de la información, la identificación, análisis, correlación, priorización y seguimiento de los eventos e incidentes de ciberseguridad que involucren o puedan involucrar componentes de telecomunicaciones, infraestructura de red, dispositivos perimetrales, enlaces de comunicación, firewalls, switches, routers, access points, balanceadores, concentradores VPN, sistemas de monitoreo, plataformas de

administración, servicios expuestos, segmentos de red, direccionamiento IP, tráfico anómalo, accesos no autorizados o cualquier activo tecnológico relacionado con la conectividad institucional.
Como mínimo, EL LICITANTE deberá realizar las siguientes actividades en coordinación con el NOC:

- Integrar los eventos de seguridad provenientes de las herramientas de telecomunicaciones en el MDR.
- Notificar al proveedor del NOC sobre incidentes de seguridad que puedan tener origen, impacto o relación con la infraestructura de telecomunicaciones, tales como tráfico anómalo, intentos de intrusión, escaneo de puertos, explotación de vulnerabilidades, denegación de servicio, comunicaciones maliciosas, conexiones no autorizadas, movimientos laterales, accesos indebidos, exfiltración de información, uso indebido de servicios, propagación de malware o comportamiento atípico en la red.
- Solicitar al NOC, mediante los canales formales establecidos en el Proceso de Coordinación Operativa con Terceros, la ejecución de actividades de diagnóstico operativo, tales como validación de estado de enlaces, revisión de interfaces, análisis de saturación, verificación de rutas, revisión de tablas de comunicación, validación de conectividad entre segmentos, identificación de caídas, degradaciones, pérdida de paquetes, latencia, errores de interfaz o comportamientos no esperados en dispositivos de red.
- Coordinar con el NOC la aplicación de acciones de contención previamente autorizadas por “LOTERÍA”, incluyendo la ejecución de playbooks que realicen bloqueo de direcciones IP, filtrado de tráfico, cierre temporal de puertos, aislamiento de segmentos, des habilitación de accesos, segmentación de red, aplicación de reglas en dispositivos de seguridad, validación de listas de control de acceso, suspensión de comunicaciones sospechosas o ejecución de cambios emergentes orientados a contener un incidente de seguridad.
- Proporcionar al NOC la información técnica mínima necesaria para la atención coordinada de incidentes, incluyendo identificadores de evento, severidad, fecha y hora de detección, activos involucrados, direcciones IP origen y destino, puertos, protocolos, usuarios asociados, indicadores de compromiso, reglas detonadas, evidencias iniciales, líneas de tiempo, hipótesis de afectación y recomendaciones de contención.
- Mantener comunicación permanente con el NOC y con el personal técnico designado por “LOTERÍA” durante la atención de incidentes críticos, altos o aquellos que puedan afectar la disponibilidad, confidencialidad o integridad de los servicios institucionales.
- Escalar al NOC, de forma inmediata, los incidentes de seguridad que requieran intervención operativa sobre infraestructura de telecomunicaciones, incluyendo fallas asociadas a dispositivos de red, degradación de enlaces, indisponibilidad de servicios críticos, cambios de configuración, afectaciones por reglas de seguridad, bloqueo de comunicaciones legítimas o condiciones que requieran validación física, lógica u operativa.
- Recibir, analizar y correlacionar las alertas técnicas generadas por el NOC que pudieran representar riesgos de seguridad, tales como saturación inusual de enlaces, variaciones anómalas de tráfico, conexiones no reconocidas, degradación de servicios, cambios no autorizados, reinicios inesperados de equipos, pérdida de conectividad, fallas recurrentes, comportamiento irregular en interfaces o eventos operativos que puedan estar asociados a una amenaza cibernética.
- Participar de manera activa en la investigación conjunta de incidentes que involucren infraestructura de telecomunicaciones, realizando análisis de correlación, revisión de eventos, validación de indicadores de compromiso, análisis de comportamiento, identificación de patrones de ataque, determinación de alcance, evaluación de impacto y emisión de recomendaciones técnicas de mitigación.
- Solicitar al NOC la recopilación y entrega de evidencias técnicas necesarias para el análisis de seguridad, incluyendo bitácoras, logs de dispositivos, configuraciones vigentes, respaldos de configuración, métricas de desempeño, trazas de red, capturas de tráfico, reportes de disponibilidad, registros de cambios, eventos de interfaces y cualquier información requerida para la investigación del incidente.
- Coordinar con el NOC la validación posterior a la contención, a fin de confirmar que las acciones aplicadas no afecten servicios legítimos, que la conectividad institucional se mantenga operativa, que los servicios críticos

continúen disponibles y que no existan impactos colaterales derivados de bloqueos, segmentaciones, ajustes de reglas o cambios emergentes.

- Definir, en conjunto con LOTERIA y el NOC , los criterios de recuperación segura de servicios afectados por incidentes de seguridad, asegurando que la restauración operativa no reactive vectores de ataque, comunicaciones maliciosas, accesos no autorizados o condiciones de riesgo previamente identificadas.
- Coordinar a través del "LOTERÍA" y en su caso el NOC, la atención de incidentes que requieran interacción con terceros proveedores de telecomunicaciones, nube, centros de datos, fabricantes, integradores, carriers o proveedores de servicios administrados, cuando se requiera validación externa, aplicación de cambios, revisión de enlaces, escalamiento técnico o soporte especializado.
- Participar en mesas de crisis, sesiones de seguimiento operativo, reuniones técnicas, análisis post-incidente, ejercicios de mejora continua y revisiones extraordinarias convocadas por "LOTERÍA" para la atención de eventos relevantes que involucren seguridad y telecomunicaciones.
- Documentar en la mesa de servicios todas las actividades realizadas durante la gestión de eventos e incidentes, incluyendo fecha y hora de detección, clasificación, severidad, activos afectados, comunicaciones con el NOC, evidencias recibidas, acciones solicitadas, acciones ejecutadas, responsables, tiempos de atención, decisiones tomadas, autorizaciones, resultados obtenidos y cierre del incidente.
- Mantener actualizados, en coordinación con el NOC, los procedimientos de escalamiento, matrices de contacto, directorios operativos, flujos de comunicación, criterios de severidad, tiempos de respuesta, mecanismos de coordinación interproveedor y protocolos de atención conjunta de incidentes.
- Generar reportes técnicos y ejecutivos derivados de los incidentes atendidos en coordinación con el NOC, incluyendo causa raíz, línea de tiempo, impacto operativo, activos involucrados, acciones de contención, acciones de recuperación, evidencias, recomendaciones, controles preventivos, áreas de mejora y compromisos de seguimiento.
- Emitir recomendaciones de mejora a la configuración, arquitectura, segmentación, monitoreo, endurecimiento, visibilidad, reglas de seguridad, controles de acceso, correlación de eventos o procedimientos operativos cuando, derivado del análisis de incidentes, se identifiquen áreas de oportunidad en los componentes o activos de telecomunicaciones.
- Asegurar que toda interacción con el NOC quede registrada mediante mecanismos auditables, trazables y verificables, evitando comunicaciones informales sin respaldo documental cuando se trate de incidentes de seguridad, cambios operativos, acciones de contención, restauración de servicios o decisiones técnicas relevantes.
- En todo momento deberá colaborar de forma activa, diligente, documentada y coordinada para la identificación, contención, mitigación, recuperación y cierre de los incidentes que puedan afectar los servicios tecnológicos de LOTERIA. Deberá mantener una postura de coordinación permanente con el NOC, orientada a asegurar que los eventos operativos relevantes sean analizados desde una perspectiva de seguridad, y que los incidentes de seguridad sean atendidos considerando su impacto operativo en la infraestructura de telecomunicaciones.

Matriz de Escalamiento Operativo

Como parte de la coordinación entre EL LICITANTE y el NOC deberá establecerse en el Proceso de Coordinación Operativa con Terceros la matriz de escalamiento operativo que deberá contener como mínimo: Tipo de incidente, Severidad, Responsable "SISI", Responsable SOC, Tiempo de atención, Tiempo de escalamiento, Medio de comunicación, Responsable de validación.

Severidad	Tiempo de Escalamiento	Responsable NOC	Responsable "SISI"	Notificación
Crítico	≤15 minutos	Líder NOC		Teléfono + Teams + Mesa de Servicio
Alto	≤30 minutos	Ingeniero N2		Teams + Mesa de Servicio
Medio	≤1 hora	Operador NOC		Mesa de Servicio
Bajo	≤4 horas	Mesa de Ayuda		Mesa de Servicio

Los tiempos de escalamiento podrán actualizarse en conjunto con LOTERIA de acuerdo con la operación y los resultados de la misma.

Reporte mensual

El reporte mensual considerará anexos con la siguiente información:

- Análisis de las brechas de seguridad públicas más relevantes que afectaron al sector.
- Resumen de sitios de phishing, aplicaciones móviles apócrifas y perfiles de redes sociales que ya se hayan dado de baja en relación con lo reportado mensualmente.

  a) Colección: La colección deberá de realizarse de manera interna aprovechando las tecnologías propuestas y actuales, y de manera externa apoyándose del análisis de redes sociales, plataformas para el análisis de feeds de inteligencia, e información provista por su ciber ecosistema de ciberseguridad el cual deberá de incluir aliados tanto en México como en el extranjero, está colección tendrá que ser planeada con base en los requerimientos de inteligencia de "LOTERÍA".
  b) Análisis: El análisis deberá ser plasmado en los productos de inteligencia finales, el cual deberán ser realizado por los especialistas DEL LICITANTE, siguiendo técnicas avanzadas de análisis que le permitan evitar sesgos cognitivos y falacias lógicas, además de adaptar dentro de su ciclo de análisis el ciclo OODA "Observe Orient, Decide, Act" y F3EAD "Find, Fix, Finish, Exploit, Analyze and Disseminate".

- Diseminación: Los análisis generados deberán de ser orientados a entregar inteligencia estratégica, táctica y operativa según los requerimientos de inteligencia de "LOTERÍA".
- Se deberá considerar por EL LICITANTE los sitios con los que cuenta "LOTERÍA" para el servicio:

INMUEBLE	UBICACIÓN
Insurgentes	Av. Insurgentes Sur No. 1397, Col. Insurgentes Mixcoac, Demarcación Benito Juárez, C.P. 03920. CDMX
Edison	Edison No. 15, Col. Tabacalera, Demarcación Cuauhtémoc, C.P. 06037, CDMX
Jalisco	Av. De las Repúblicas No. 117, Col. Tabacalera, Demarcación Cuauhtémoc, C.P. 06037 CDMX
Rosales	Rosales No. 15, Col. Tabacalera, Demarcación Cuauhtémoc, C.P. 06037 CDMX
Basilio Badillo	Basilio Badillo No. 39 Col. Centro, Demarcación Cuauhtémoc, C.P. 06037 CDMX
Hidalgo	Hidalgo No. 130, Col. Centro, Demarcación Cuauhtémoc, C.P. 06037 CDMX
Contreras	Av. San Francisco No. 156, Colonia Magdalena Contreras, Demarcación Magdalena Contreras C.P. 10500, Ciudad de México.
Subdirección Occidente	Av. Ignacio L Vallarta 1540 Int. 204, Esq. Marsella, Col. Americana, Guadalajara Jalisco, C.P. 44160
Subdirección Pacifico	Hernando de Soto No. 2 Altos, esquina Domingo Olivares, Colonia Los Arcos, Hermosillo, Sonora C.P. 85250

INMUEBLE	UBICACIÓN
Subdirección Sureste	Calle 7 No. 457, entre calle 48 y calle 50, Colonia Residencial Pensiones, Mérida, Yucatán, C.P. 97217
Subdirección Noreste	Gral. Jerónimo Treviño 409 Despacho 520, Edificio BISA, Col. Centro, Monterrey, Nuevo León, C.P. 64000
Subdirección Norte	Antonio de Montes No. 2112-1, Col. San Felipe, Chihuahua, Chihuahua C.P. 51240
Subdirección Sur	Av. Martin Alonso Pinzón No. 757, Fraccionamiento Reforma, Veracruz, Veracruz C.P. 91919

Con la finalidad de que EL LICITANTE pueda demostrar su capacidad para el servicio deberá proporcionar la documentación que evidencie que cuenta con una metodología para la ejecución de este servicio. Las metodologías pueden ser diseñadas e implementadas según las propuestas DEL LICITANTE para los servicios de Ciber patrullaje. Como pueden ser:

a) Metodología de implementación basada en cinco fases (Prevención, Atención, Reacción, Investigación y Gestión) utilizado para el modelo homologado de las unidades de Policía Cibernética.
b) La metodología utilizada por Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología – DICAT

Mesa de servicio

- EL LICITANTE deberá incluir en su oferta una Mesa de Servicio atendida por Técnicos de Servicio con la finalidad de dar seguimiento a las solicitudes e incidentes que se presenten en la operación del servicio solicitado.
- La Mesa de Servicio deberá permitir el registro y seguimiento para la atención a fallas, incidentes, problemas, realización de diagnósticos a los distintos dispositivos de la plataforma del objeto de los servicios, que EL LICITANTE gestione a favor de “LOTERÍA”.
- Para recibir y dar seguimiento a solicitudes de servicio e incidentes que interrumpan o degraden el servicio o atender actualizaciones, EL LICITANTE deberá atender las siguientes prácticas:
- Ser un punto de contacto para reportar incidencias, contar con personal de primer nivel para proveer soporte, atención y la solución de solicitudes, incidentes y atención de requerimientos relacionados con el servicio.
- Será responsabilidad DEL LICITANTE la gestión, adquisición y mantenimiento de las herramientas y el hardware necesario con la cual opere el área de atención.
- Deberá proporcionar la atención para el levantamiento de reportes de servicio en un horario de 24 horas del día los 7 días de la semana (24x7).
- Con la herramienta de mesa de servicio se llevará a cabo 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 800 directo o número específico en las instalaciones del (MDR).
    - Correo Electrónico
    - Portal Web
    - Contar con mecanismos de comunicación alternativa tales como: mensajería instantánea, WhatsApp o mensajes SMS.
- EL LICITANTE debe proporcionar asistencia técnica telefónica desde sus instalaciones, con personal capacitado y sin ningún costo adicional para “LOTERÍA”.

- Contar con un aplicativo para la gestión de las solicitudes y proporcionar un acceso a esta herramienta para el personal técnico de "LOTERÍA". Toda la información relativa a cualquier solicitud debe estar disponible a través del aplicativo.
- En caso de que la falla sea atribuible al Licitante, éste le dará una atención hasta la solución y en su caso se aplicará la deducción-penalización correspondiente de acuerdo con los niveles de servicio.
- Un reporte será considerado como cerrado satisfactoriamente cuando se haya concluido exitosamente, regresando a la normalidad todos los conceptos o elementos involucrados, dentro de la ventana de tiempo especificada.
- Una vez concluida la atención y soporte de las solicitudes, conforme al nivel de soporte determinado para la atención del servicio deberá notificar que se dio por concluida la atención, comunicando la causa de la falla y la acción de solución, así como la hora en que el servicio se restablece.
- Los niveles de servicio deberán enfocarse al tiempo de solución y considerar sólo como referencia el tiempo de atención, de tal manera que EL LICITANTE oriente sus acciones a esa métrica.
- Como parte de las tareas del personal técnico DEL LICITANTE que opere la Mesa de Servicio, deberá registrar en su aplicativo las solicitudes o llamadas, dar seguimiento a casos abiertos, así como brindar asesoría y/o consulta de los requerimientos relacionados al servicio.
- Escalar incidentes o problemas a los técnicos de soporte en sitio, para su solución.
- Coordinar y supervisar la atención oportuna de los incidentes escalados al personal de soporte técnico en sitio.
- Coadyuvar en el proceso de altas, bajas y cambios del equipamiento utilizado, para prestar el servicio.
- Monitoreo del estatus que guarda el equipamiento suministrado para la prestación del servicio, siempre que la conectividad de red de datos de "LOTERÍA" se lo permita y que este no sea demandante de un gran ancho de banda.
- En caso de identificar telefónicamente o mediante el monitoreo alguna incidencia o potencial falla, despachar, de forma proactiva, a los recursos humanos y técnicos necesarios, para atender y solucionar la incidencia. Levantando el debido reporte dentro de la herramienta de la Mesa de Servicio.

EL LICITANTE deberá garantizar la actualización constante de cada servicio y herramienta descritos en este Anexo Técnico, asegurando la aplicación de parches de seguridad, mejoras de funcionalidad y compatibilidad con nuevas versiones.
Asimismo, el prestador de servicio será responsable de realizar las actualizaciones de manera oportuna y sin afectar la continuidad del servicio. En caso de que se materialicen ataques o vulnerabilidades debido al uso de versiones obsoletas, se determinarán las responsabilidades correspondientes y se aplicarán las penas establecidas en el contrato.
Dado que el servicio de MDR es responsable de la actualización y el mantenimiento de seguridad, en caso de incumplimiento en la actualización de herramientas y servicios críticos, se aplicarán sanciones tanto al servicio afectado como al Centro de Detección, Análisis y Respuesta Gestionada (MDR).

Transferencia de conocimiento

"EL LICITANTE" deberá incluir en su propuesta la transferencia de conocimiento técnica necesaria al personal designado por el Administrador del Contrato, mediante escrito o correo electrónico, a fin de que esté en condiciones de realizar la correcta administración y supervisión del proyecto sobre los bienes y/o servicios suministrados, dicha transferencia de conocimiento será para mínimo cinco (5) personas y máximo quince (15), por cada una de las tecnologías suministradas. Esta transferencia tecnológica deberá hacerse sobre las versiones que se instalarán dentro de los primeros 60 (sesenta días naturales) contados a partir de la notificación del fallo.
Cuando se tengan nuevas versiones de cualquiera de las herramientas utilizadas para la provisión del servicio dentro de la vigencia del contrato, EL LICITANTE deberá brindar la actualización de la transferencia de conocimiento al personal

designado por el Administrador del Contrato, mediante escrito o correo electrónico y deberá considerar mínimo cinco (5) personas y máximo quince (15).
La transferencia de conocimiento no deberá generar un cargo ni costo adicional para la Entidad.

Personal requerido

EL LICITANTE, como parte de su propuesta técnica, deberá presentar las certificaciones vigentes por cada perfil establecido en este inciso y en caso de que durante la vigencia del contrato el certificado expire, EL LICITANTE deberá presentar al administrador del contrato la recertificación o renovación de dicho documento y/o poder reemplazar el personal asignado en el perfil, en un plazo máximo de 3 días naturales a partir de la fecha de vencimiento del certificado. Asimismo, deberá presentar copia de la identificación oficial vigente.
En caso de que el certificado no tenga fecha de vencimiento, se deberá manifestar a través de carta firma por el representante legal DEL LICITANTE, que el certificado que presenta es la última versión y que permanecerá vigente hasta que salga una nueva versión disponible.
Para la identificación oficial, se considerarán válidas la credencial para votar emitida por el Instituto Nacional Electoral (ambos lados), el pasaporte (donde se encuentre la foto y firma), cédula profesional con fotografía, cartilla liberada y en el caso de personas extranjeras, las tarjetas de residencia temporal o permanente emitidas por el Instituto Nacional de Migración (INM). Las identificaciones deberán encontrarse vigentes a la fecha del acto de presentación y apertura de proposiciones de esta licitación pública y ser legibles.
A continuación, se establece los perfiles requeridos:

PERFIL	CERTIFICACIONES VIGENTES PARA DEMOSTRAR	EXPERIENCIA POR DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Administrador del Centro de Detección, Análisis y Respuesta Gestionada (MDR)	EL LICITANTE deberá presentar la siguiente certificación vigente: CISSP (Certified Information Systems Security Professional) ITIL V4 Foundation Certificate in IT Service Management	Tres años de experiencia en participación de proyectos de seguridad de la información, deberá presentar copia simple del título o cédula de grado mínimo de Licenciatura / Ingeniería relacionada con: Tecnologías de la Información, Comunicaciones, Electrónica, Telemática y Sistemas Computacionales	Responsable de la administración, monitoreo, operación de los servicios proporcionados por el (MDR), así como del soporte, atención a fallas e incidentes de seguridad.	Al menos 1 recurso

Administración y Operación de soluciones y herramientas tecnológicas	EL LICITANTE deberá presentar la siguiente certificación vigente: Certificado del fabricante de las soluciones propuestas para al menos: • Protección de Información en Correo Electrónico • Visibilidad y Monitoreo de los Usuarios • Segmentación zero trust • Protección de Endpoint de siguiente generación (EDR). Protección para Servidores • Protección de Endpoint de siguiente generación en Equipos de Cómputo personales • Entorno de ataque cambiante (EAC) • Servicio de Firewall de Siguiente Generación (NGFW) • Servicio de Protección a Aplicaciones Móviles	Tres años de experiencia en participación de proyectos de seguridad de la información, deberá presentar copia simple del título o cédula de grado mínimo de Licenciatura / Ingeniería relacionada con: Tecnologías de la Información, Comunicaciones, Electrónica, Telemática y Sistemas Computacionales	Operar administrar y monitorear las soluciones de seguridad propuestas.	Al menos 2 recursos

PERFIL	CERTIFICACIONES VIGENTES PARA DEMOSTRAR	EXPERIENCIA POR DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
	• Servicio de Correlación de Eventos • Servicio de Orquestación, Automatización y Respuesta de Seguridad • Servicio de Diagnóstico y Reparación de Configuraciones Erróneas.			

PERFIL	CERTIFICACIONES VIGENTES PARA DEMOSTRAR	EXPERIENCIA POR DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Coordinador (MDR)	EL LICITANTE deberá presentar la siguiente certificación vigente: - EC-Council Certified Incident Handler - EC-Council CEH (Certified Ethical Hacker)	Tres años de experiencia en participación de proyectos de seguridad de la información, deberá presentar copia simple del título o cédula de grado mínimo de Licenciatura / Ingeniería relacionada con: Tecnologías de la Información, Comunicaciones, Electrónica, Telemática y Sistemas Computacionales	Responsable de la coordinación del soporte a fallas e incidentes de seguridad.	Al menos 1 recurso
Analista del Centro de Detección, Análisis y Respuesta Gestionada (MDR)	EL LICITANTE deberá presentar la siguiente certificación vigente: ITIL V4 Foundation Certificate	Tres años de experiencia en participación de proyectos de seguridad de la información, deberá presentar copia simple del título o cédula de grado mínimo de Licenciatura / Ingeniería relacionada con: Tecnologías de la Información, Comunicaciones, Electrónica, Telemática y Sistemas Computacionales	Operar administrar y monitorear las soluciones de seguridad propuestas y de los servicios proporcionados por el (MDR).	Al menos 4 recursos para garantizar el servicio 7x24 (las 24 horas del día, los 7 días de la semana) durante la vigencia del contrato

PERFIL	CERTIFICACIONES VIGENTES PARA DEMOSTRAR	EXPERIENCIA POR DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Líder de proyecto	EL LICITANTE deberá presentar la siguiente certificación vigente: PMP (Project Management Professional), PMI - CRISC (Certified in Risk and Information Systems Control) - ITIL 4 Master	Cinco años de experiencia en participación de proyectos de seguridad de la información, deberá presentar copia simple del título o cédula de grado mínimo de Licenciatura / Ingeniería relacionada con: Tecnologías de la Información, Comunicaciones, Electrónica, Telemática y Sistemas Computacionales	Es la persona encargada de administrar y coordinar el proyecto.	Al menos 1 recurso.
Consultor especializado en protección de datos	EL LICITANTE deberá presentar la siguiente certificación vigente: CISM Certified Information Security Manager - CISSP (Certified Information Systems Security Professional) - CRISC (Certified in Risk and Information Systems Control)	Cinco años de experiencia en participación de proyectos de seguridad de la información, deberá presentar copia simple del título o cédula de grado mínimo de Licenciatura de las áreas Físico Matemáticas e Ingeniería, relacionada con: Tecnologías de la Información, Comunicaciones, Electrónica, Telemática y Sistemas Computacionales	Analizar y diseñar los planes de protección y seguridad de datos que serán configurados en las soluciones.	Al menos 1 recurso

PERFIL	CERTIFICACIONES VIGENTES PARA DEMOSTRAR	EXPERIENCIA POR DEMOSTRAR	FUNCIÓN	NÚMERO DE RECURSOS
Consultor especializado en continuidad operativa y seguridad de la información	EL LICITANTE deberá presentar una de las siguientes certificaciones vigentes: • Certified ISO/IEC 27001 Information Security Associate. o • Certificado ISO/IEC 27001:2022 Lead Auditor o • Certificado ISO 22301:2019 Lead Auditor	Tres años de experiencia en participación de proyectos de seguridad de la información, deberá presentar copia simple del título o cédula de grado mínimo de Licenciatura / Ingeniería relacionada con: Tecnologías de la Información, Comunicaciones, Electrónica, Telemática y Sistemas Computacionales	Encargado de realizar el análisis y gestión de la continuidad operativa y seguridad de la información.	Al menos 1 recursos
Consultor especializado en la herramienta ITSM	EL LICITANTE deberá presentar una de las siguientes certificaciones vigentes: Certificado del fabricante de la solución propuesta de la herramienta de ITSM O Certificado Auditor Líder 22301:2019.	Tres años de experiencia en participación de proyectos de seguridad de la información, deberá presentar copia simple del título o cédula de grado mínimo de Licenciatura / Ingeniería relacionada con: Tecnologías de la Información, Comunicaciones, Electrónica, Telemática y Sistemas Computacionales	Encargado de realizar el análisis y gestión de la continuidad operativa de la herramienta de mesa de servicio.	Al menos 1 recurso

EL LICITANTE deberá asignar los perfiles requeridos conforme a lo solicitado en el presente anexo técnico, a fin de garantizar el nivel de especialización de los servicios.
Los siguientes servicios serán bajo demanda por parte de “LOTERÍA”, EL LICITANTE deberá iniciar su atención dentro de los 5 días hábiles posterior a la solicitud que realice el Servidor Público Administrador del Servicio al Proveedor del Servicio mediante oficio o correo electrónico.

EL LICITANTE deberá presentar el Plan de Trabajo Detallado para dar atención a la totalidad de requerimientos del presente Anexo Técnico dentro de los 10 días naturales posteriores al fallo. “LOTERÍA” analizará y en su caso autorizará la ejecución de dicho plan en un plazo máximo de 5 días. En caso de que “LOTERÍA” tenga observaciones, EL LICITANTE tendrá un plazo máximo de 3 días naturales a partir de la recepción de las observaciones para subsanarlas en su totalidad.
La duración de las actividades contempladas en el Plan de Trabajo Detallado no deberá exceder 120 días naturales posteriores al fallo y deberá considerar las pruebas operativas previas para su implementación.

DESGLOSE DE LOS COMPONENTES DE SERVICIOS PERMANENTES. ETAPA INICIAL.
(Máximo hasta 120 días naturales contados a partir del día hábil siguiente a la fecha de la notificación del fallo)

CONCEPTO	VIGENCIA
SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA	
Centro de Detección, Análisis y Respuesta Gestionada (MDR)	La vigencia del servicio será a partir del día hábil siguiente a la fecha de la notificación del fallo y hasta máximo 120 días naturales contados a partir de la notificación del fallo.

DESGLOSE DE LOS COMPONENTES BAJO DEMANDA. ETAPA INICIAL.
(Máximo hasta 120 días naturales contados a partir del día hábil siguiente a la fecha de la notificación del fallo)

CONCEPTO	UNIDAD DE MEDIDA	CANTIDAD MÍNIMA	CANTIDAD MAXIMA
SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA			
Protección de Información en Correo Electrónico	Usuarios	520	1300
Visibilidad y Monitoreo de los Usuarios	Usuarios	520	1300
Segmentación Zero Trust	Equipos	12	30
Protección de Endpoint De Siguiente Generación (EDR)	Equipos	520	1300
Entorno de ataque cambiante (EAC)	Equipos	520	1300
Servicio de Firewall de Siguiente Generación	Equipos	5	12

DESGLOSE DE LOS COMPONENTES DE SERVICIOS PERMANENTES. ETAPA OPERATIVA
A partir de día natural 121, contado a partir del día hábil siguiente a l de la notificación del fallo y hasta el término contractual del servicio

CONCEPTO	VIGENCIA
SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA	
Centro de Detección, Análisis y Respuesta Gestionada (MDR)	La vigencia del servicio será a partir de la conclusión de la ETAPA

	INICIAL (120 días naturales) y hasta el término contractual del servicio, es decir a partir del día natural 121 contado a partir del día hábil siguiente a la fecha de notificación del fallo

DESGLOSE DE LOS COMPONENTES BAJO DEMANDA. ETAPA OPERATIVA **A partir de día natural 121, contado a partir del día hábil siguiente a l de la notificación del fallo y hasta el término contractual del servicio**			
CONCEPTO	**UNIDAD DE MEDIDA**	**CANTIDAD MÍNIMA**	**CANTIDAD MAXIMA**
SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA			
Protección de Información en Correo Electrónico	Usuarios	520	1300
Visibilidad y Monitoreo de los Usuarios	Usuarios	520	1300
Segmentación Zero Trust	Equipos	30	1000
Protección de Endpoint De Siguiente Generación (EDR)	Equipos	520	1300
Entorno de ataque cambiante (EAC)	Equipos	520	1300
Diagnóstico y reparación de configuraciones erróneas	Equipos	520	1300
Autenticación Multifactor (MFA)	Usuarios	520	1300
Servicio de Firewall de Siguiente Generación Tipo 1	Equipos	5	12
Servicio de Firewall de Siguiente Generación Tipo 2	Equipos	5	12
Servicio de Protección a Aplicaciones Móviles	Servicios	3	6

Para garantizar la integración, eficiencia y calidad en la prestación del servicio, todos los componentes del servicio bajo demanda deberán estar integrados al Centro de Detección, Análisis y Respuesta Gestionada (MDR).
Esta disposición tiene como finalidad fomentar la libre participación y la competencia de precios en el mercado, sin exentar el cumplimiento de los requerimientos técnicos establecidos en el anexo técnico.
La cantidad mínima y máxima mensual de cada servicio se refiere al número de usuarios o dispositivos protegidos, según corresponda:
Descripción de las unidades de medida de las Unidades de Servicio

- Protección de Información en Correo Electrónico: Cantidad de usuarios cuyos correos electrónicos están protegidos contra amenazas como phishing, malware y accesos no autorizados.
- Visibilidad y Monitoreo de los Usuarios: Número de usuarios cuyo comportamiento y actividades dentro de la red son supervisados para detectar posibles riesgos de seguridad.
- Segmentación Zero Trust: Cantidad de usuarios asociados a un equipo de cómputo a los que se les aplica un modelo de acceso restringido basado en principios de confianza cero, minimizando la exposición a amenazas.
- Protección de Endpoint de Siguiente Generación (EDR): Número de dispositivos de cómputo (endpoints) protegidos.
- Entorno de Ataque Cambiante (EAC): Número de usuarios cuya infraestructura de trabajo (endpoints) se encuentra protegida mediante la aplicación dinámica de medidas de seguridad que dificultan la explotación de vulnerabilidades.
- Servicio de Firewall de Siguiente Generación. Equipos para la protección perimetral.

- Servicio de Protección a Aplicaciones Móviles. Servicios unitarios de protección a aplicaciones móviles. Cada servicio se considera concluido una vez que se recibe la App debidamente protegida y lista para ser enviado a las tiendas Apple y Android.

Las unidades de medida de cada herramienta o servicio han sido establecidas conforme a los parámetros operativos y de seguridad definidos en el alcance del proyecto. En el caso de servicios bajo demanda, estos valores se determinan en función de las necesidades específicas y las condiciones establecidas para su prestación.

Licenciamiento como parte del Servicio

El licenciamiento necesario para la operación de los servicios indicados en el presente Anexo Técnico se debe incluir dentro de la contratación del servicio, por lo que EL LICITANTE deberá garantizar su provisión, administración y actualización durante toda la vigencia del contrato; así mismo el licenciamiento debe estar suscrito a nombre de "LOTERÍA" por lo que se debe entregar el certificado o constancia del fabricante de la solución ofertada en la que sé que acredite que el licenciamiento este a nombre de la Entidad, m´áximo 10 días hábiles después de finalizada la implementación de la etapa inicial al servidor público administrador del contrato.
EL LICITANTE será responsable de:

- Garantizar la disponibilidad y operatividad de las licencias necesarias para cada uno de los servicios contratados.
- Asegurar la compatibilidad e integración de las soluciones dentro del entorno tecnológico del contratante.
- Proporcionar actualizaciones y mantenimiento de las licencias sin costos adicionales, siempre que sean requeridas para la continuidad del servicio.
- Cumplir con las mejores prácticas y normatividad vigente en materia de ciberseguridad y gestión de licenciamiento.

Entregables

Entregables generales

Durante la habilitación, transición y operación de los servicios de seguridad, "LOTERÍA" 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 LICITANTE efectuará bajo la supervisión del Funcionario Público Administrador del Contrato y se recibirán todos los entregables que deberán remitirse a la misma ubicada en, Insurgente Sur 1397, Col. Insurgentes Mixcoac, C.P. 03920, Benito Juárez, CDMX, en días hábiles, en las fechas que dicha "LOTERÍA" designa a continuación:

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto de acuerdo con las fases de la metodología del PMI, Scrum o Lean	Única Vez	10 días naturales posteriores al inicio del servicio
	Documento Compromiso de suscripción de OLAs	Única Vez	15 días naturales posteriores al inicio del servicio

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Matriz de Escalación	Única Vez	15 días naturales posteriores al inicio del servicio
	Escrito por parte DEL LICITANTE, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	Única Vez	15 días naturales posteriores al inicio del servicio
Servicios de Seguridad – Continuidad Operativa	Documento con el diseño de las Soluciones de Seguridad a implementar	Única Vez	15 días naturales posteriores al inicio del servicio
	Memorias Técnicas de las Soluciones de Seguridad Implementadas	Única Vez	15 días naturales posteriores al inicio del servicio todos los componentes.
Centro de Detección, Análisis y Respuesta Gestionada (MDR)	Documento con el diseño detallado de las Soluciones de Seguridad a implementar.	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes y servicios
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requirieron integrar activos de infraestructura para su habilitación	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes.
	Procesos de operación implementados: Cambios Configuraciones Incidentes Problemas Disponibilidad	Única Vez	15 días naturales posteriores al inicio del servicio

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posteriores al inicio del servicio
	Expedientes Curriculares del personal del (MDR)	Única Vez	15 días naturales posteriores al inicio del servicio
	Proceso de Coordinación Operativa con Terceros	Única Vez	15 días naturales contados posteriores al inicio del servicio
Entorno de ataque cambiante (EAC)	Plan de Implementación y Despliegue: -Documento detallado que incluya los pasos necesarios para la implementación del servicio EAC en la infraestructura objetivo, cronograma de actividades, roles y responsabilidades de los equipos involucrados, y las dependencias técnicas y logísticas	Única Vez	Hasta 20 días hábiles posteriores a la solicitud generada por parte de “LOTERÍA”
	Arquitectura de la Solución: - Diseño detallado de la arquitectura del EAC, incluyendo diagramas de flujo de datos, integración con sistemas existentes (NGAV, EPP, EDR/XDR), y descripción de componentes principales.	Única Vez	Hasta 20 días hábiles posteriores a la solicitud generada por parte de “LOTERÍA”

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Documentación de Integración: - Guía técnica para la integración del EAC con las plataformas y sistemas de gestión de incidentes existentes, como SIEM (Security Information and Event Management).	Única Vez	Hasta 20 días hábiles posteriores a la solicitud generada por parte de "LOTERÍA"
	Informe de Estado del Proyecto: - Resumen del estado del proyecto al término de la fase inicial, incluyendo hitos alcanzados, desafíos encontrados y próximos pasos.	Única Vez	Hasta 20 días hábiles posteriores a la solicitud generada por parte de "LOTERÍA"

Entregables por Evento o a petición extraordinaria por "LOTERÍA"

EL LICITANTE, 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
Servicio de Protección de Información en Correo Electrónico	Reporte Técnico de los eventos de actividad sospechosa presentados, que hayan sido identificados, bloqueados o puestos en suspensión por el servicio de Protección de Información en Correo Electrónico	Evento	5 días hábiles posteriores a la solicitud generada por parte de "LOTERÍA"
Servicio de Visibilidad y Monitoreo de los Usuarios	Reporte Técnico de los eventos de actividad sospechosa presentados, que hayan sido identificados por el servicio de Visibilidad y Monitoreo de los Usuarios	Evento	5 días hábiles posteriores a la solicitud generada por parte de "LOTERÍA"

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicio de Segmentación Zero Trust	Reporte Técnico de los eventos de actividad sospechosa presentados, que hayan sido identificados por el servicio de Segmentación Zero Trust	Evento	5 días hábiles posteriores a la solicitud generada por parte de “LOTERÍA”
Servicio de Protección de Endpoint de siguiente generación (EDR)	Reporte Técnico de los eventos de actividad sospechosa presentados, que hayan sido identificados por el servicio de Protección de Endpoint de siguiente generación (EDR)	Evento	5 días hábiles posteriores a la solicitud generada por parte de “LOTERÍA”
Servicios del Centro de Detección, Análisis y Respuesta Gestionada (MDR)	Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad	Evento	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por “LOTERÍA”
	Actualización de la matriz de escalación	Evento	5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del SOC
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad	Evento	5 días hábiles posteriores a la ejecución de la ventana mantenimiento
	Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad	Evento	5 días hábiles posteriores a la solicitud generada por parte de “LOTERÍA”
	Reporte Técnico de las configuraciones de las soluciones de seguridad	Evento	5 días hábiles posteriores a la solicitud generada por parte de “LOTERÍA”
	Diagramas de Arquitectura de las soluciones de seguridad	Evento	5 días hábiles posteriores a la solicitud generada por parte de “LOTERÍA”

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicio de Protección a Aplicaciones Móviles	Reporte Técnico de la protección implementada en la APP protegida	Evento	30 días naturales posteriores a la solicitud generada por “LOTERÍA”.

Entregables de cada evaluación trimestral de vulnerabilidades	Reporte ejecutivo: resumen de la evaluación, nivel de exposición identificado, principales riesgos, comparativo respecto de la evaluación anterior y recomendaciones prioritarias. Reporte técnico: deberá identificar los activos evaluados, vulnerabilidades encontradas, severidad, descripción, evidencia, componente afectado, impacto potencial, referencias técnicas, recomendación de remediación y prioridad. Matriz de vulnerabilidades: deberá permitir el seguimiento de cada hallazgo y contener como mínimo identificador, activo afectado, vulnerabilidad, severidad, fecha de detección, responsable de atención, recomendación, estado y fecha de cierre. Plan de remediación: conjunto de recomendaciones y acciones correctivas propuestas para reducir o eliminar las vulnerabilidades identificadas, sujeto a la aprobación y priorización de “LOTENAL”. Reporte comparativo: deberá señalar vulnerabilidades nuevas, persistentes, mitigadas, remediadas o reincidentes	Cada tres meses	15 días hábiles, una vez concluidas las pruebas,

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	respecto de la evaluación trimestral anterior.		

Entregables periódicos

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

FASE INICIAL. Hasta por 120 días naturales posteriores a la notificación del fallo

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de la infraestructura y servicios de "LOTERÍA": Protección de Información en Correo Electrónico Visibilidad y Monitoreo de los Usuarios Segmentación Zero Trust Protección de Endpoint de Siguiente Generación (EDR) Que contenga al menos lo siguiente: Incidentes/Fallas Actividad Sospechosa Estadísticas de uso de los servicios	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
Servicios del Centro de Detección, Análisis y Respuesta Gestionada (MDR)	Reporte Técnico de los incidentes de ciberseguridad presentados, que hayan sido identificados por el Centro de Detección, Análisis y Respuesta Gestionada (MDR) de la infraestructura y servicios de "LOTERÍA".	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados, que hayan sido identificados de la infraestructura y servicios de "LOTERÍA".	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido

	Reporte de las estadísticas de uso y desempeño de los servicios de seguridad en la infraestructura y servicios de “LOTERÍA”..	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
Entorno de ataque cambiante (EAC)	Informe de Actividades Mensuales: - Detalle de las actividades realizadas durante el mes, incluyendo despliegues, actualizaciones, mantenimiento y mejoras en el servicio en la infraestructura y servicios de “LOTERÍA”.	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
	Análisis de Alertas y Eventos: - Informe detallado de todas las alertas generadas, su clasificación, análisis forense realizado, y las medidas de respuesta adoptadas para cada incidente en la infraestructura y servicios de “LOTERÍA”.	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido

ETAPA OPERATIVA

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de las soluciones implementadas: Protección de Información en Correo Electrónico Visibilidad y Monitoreo de los Usuarios Segmentación Zero Trust Protección de Endpoint de Siguiente Generación (EDR) Que contenga al menos lo siguiente: Incidentes/Fallas Actividad Sospechosa Estadísticas de uso de los servicios	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido

Servicios del Centro de Detección, Análisis y Respuesta Gestionada (MDR)	Reporte Técnico de los incidentes de ciberseguridad presentados, que hayan sido identificados por el Centro de Detección, Análisis y Respuesta Gestionada (MDR)	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados, que hayan sido identificados	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
	Reporte de las estadísticas de uso y desempeño de los servicios de seguridad implementados.	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
Entorno de ataque cambiante (EAC)	Informe de Actividades Mensuales: - Detalle de las actividades realizadas durante el mes, incluyendo despliegues, actualizaciones, mantenimiento y mejoras en el servicio.	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
	Análisis de Alertas y Eventos: - Informe detallado de todas las alertas generadas, su clasificación, análisis forense realizado, y las medidas de respuesta adoptadas para cada incidente.	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
Gestión de Vulnerabilidades	Reporte de Vulnerabilidades y Prioridades de Parches: - Informe mensual con el inventario de vulnerabilidades detectadas y su priorización según el nivel de riesgo, recomendaciones para la aplicación de parches y mitigaciones implementadas.	Mensual	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido

Los entregables correspondientes a las etapas anteriormente descritas, deberán ser entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados.

De igual manera, EL LICITANTE 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 "LOTERÍA" definirá en las mesas de trabajo, los permisos de acceso correspondientes para el administrador del contrato, y personal que se conforme para este propósito u otros funcionarios que sean designados por el primero mencionado.

Convenio de confidencialidad

EL LICITANTE 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 de "LOTERÍA":
Se deberán establecer controles de acceso y privilegios restringidos al personal EL LICITANTE, a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones de "LOTERÍA".
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 EL LICITANTE y las de "LOTERÍA".
Los empleados DEL LICITANTE de "SISI", con acceso a la información sensible de "LOTERÍA", deberán firmar acuerdos de confidencialidad con este último y entregarlos a "LOTERÍA".
El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por EL LICITANTE, observando los requisitos de seguridad y resguardo de la información.
EL LICITANTE deberá permitir el acceso a información relacionada con el servicio prestado a "LOTERÍA" para la realización de auditorías.
EL LICITANTE 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.

El prestador de servicios será enteramente responsable de resolver los conflictos que pudiesen surgir entre él y su personal o de este último entre sí, y también será responsable de los accidentes que se originen aun cuando estos ocurran en las instalaciones de "LOTERÍA", por lo que libera de toda responsabilidad por reclamaciones que sus trabajadores le presenten a la Entidad por tal concepto. En consecuencia, el prestador de servicios exime expresamente a "LOTERÍA" de cualquier responsabilidad civil, penal, de seguridad social o de cualquier otra especie que en su caso pudiera llegar a generarse. Independientemente de lo antes señalado EL LICITANTE se compromete a sacar en paz y a salvo a "LOTERÍA" en caso de que el personal de este intente alguna reclamación en contra de "LOTERÍA", así como a pagar cualquier gasto o costa judicial que "LOTERÍA" haya tenido que rogar por concepto de las reclamaciones intentadas en su contra.
Para garantizar claridad y trazabilidad de la información, EL LICITANTE deberá incluir en su propuesta técnica lo siguiente:
1. Listado detallado de herramientas y servicios

- Nombre de cada herramienta o servicio.
- Versión y fecha de última actualización.
- Proveedor o desarrollador.

2. Información recopilada

- - Tipo de datos recolectados por cada herramienta o servicio.
- - Propósito de la recopilación de datos.

- - Mecanismos de almacenamiento y protección de la información.

3. Procedimientos de descarga y acceso

- - Requisitos y pasos para acceder o descargar la información.
- - Restricciones o controles de acceso aplicables.

4. Responsabilidades del prestador de servicio

- - Garantías de disponibilidad y seguridad de los datos.
- - Frecuencia y método de actualización de la información recopilada.

5. Normativas aplicables

- - LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

Normatividad aplicable

EL LICITANTE deberá sujetarse a las políticas internas vigentes de "LOTERÍA" 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:

- Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.
- ISO / IEC 27001:2022
- Lineamientos, manuales, guías técnicas, procedimientos de "LOTERÍA".
- Políticas de seguridad con base en el Sistema de Gestión de Seguridad de la Información (SGSI) de "LOTERÍA".
- Normatividad interna aplicable a "LOTERÍA".
- Reglas y políticas de administración y operación en los inmuebles.
- Reglamentos internos de conducta.

- EL LICITANTE deberá acreditar en su propuesta técnica con una solución para la Protección de Endpoint de Siguiente Generación (EDR) reconocida en el Cuadrante Mágico de Gartner en la categoría de Endpoint Protection Platforms (EPP).

- EL LICITANTE deberá contar con una solución de seguridad que haya participado en las evaluaciones de MITRE ATT&CK, demostrando capacidades avanzadas de detección y respuesta ante amenazas. La solución deberá alinearse con los principios de Zero Trust, garantizando visibilidad, monitoreo continuo y control de acceso basado en riesgo.

Este requisito garantiza que EL LICITANTE cumpla con estándares de calidad y reconocimiento en el mercado.

A. Cumplimiento de políticas

EL LICITANTE deberá respetar todas las políticas de seguridad vigentes en "LOTERÍA" y en ninguna circunstancia deberá permitir que se viole ninguno de las normatividades y lineamientos vigentes. Si alguno de los lineamientos de Seguridad

implantados en “LOTERÍA” llegase a cambiar en el transcurso del contrato establecido con EL LICITANTE, 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 EL LICITANTE 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 LICITANTE decida necesario para la correcta operación de su personal, así como de la adquisición, instalación, mantenimiento y licenciamiento de estos, el costo será absorbido por EL LICITANTE.

B. Consideraciones en la conclusión de la vigencia del contrato

Al concluir la vigencia contractual, durante el periodo de transición o cuando se determine la terminación anticipada, “EL PROVEEDOR” debe ejecutar un procedimiento formal de desvinculación o plan de desvinculación integrado al plan de transición, previamente aprobado por “LOTENAL”. Este comprenderá la identificación, restricción, revocación y baja de todos los accesos físicos y lógicos otorgados a su personal; la devolución de credenciales, dispositivos y bienes asignados; la transferencia de la información y documentación institucional; y la eliminación segura de las copias que permanezcan bajo su posesión o control.
Durante el periodo de transición únicamente permanecerán habilitados los accesos nominales, temporales y de mínimo privilegio indispensables para las actividades autorizadas. Estos deberán mantenerse monitoreados y revocarse cuando desaparezca la necesidad operativa o, a más tardar, al concluir la transición.
“EL PROVEEDOR” debe integrar y entregar un Expediente de Desvinculación con los inventarios, registros de revocación, constancias de devolución, actas de transferencia, certificados de eliminación segura, relación de excepciones y demás evidencias que permitan acreditar el cierre. El procedimiento finalizará con la validación de “LOTENAL” y la formalización del Acta de Cierre de Desvinculación, sin perjuicio de las obligaciones de confidencialidad y seguridad que subsistan después de la terminación contractual.
La totalidad de la infraestructura y licenciamiento dentro del periodo de alcance del servicio quedarán en propiedad y a nombre de “LOTERÍA” al finalizar el contrato, sin que ello genere erogaciones adicionales para LOTERÍA, por lo cual, se deberán coordinar ambas partes LOTERÍA y El Proveedor, para que jurídicamente se establezca la transferencia de propiedad, obligándose a proveer la documentación que corresponda para la elaboración del acuerdo de sesión o el documento que jurídicamente corresponda.
Lo anterior será realizado de manera independiente a la coordinación con la entrega del nuevo contrato o de la solución que dará continuidad a la operación de “LOTERÍA” referente a los servicios del servicio “SISI”, observando los acuerdos operativos de migración de un contrato a otro, y que consideren aspectos como la migración de la información de usuario en la plataforma de cómputo actual hacia la nueva.
EL PROVEEDOR debe entregar a “LOTERÍA”, a más tardar un mes antes de la conclusión de la vigencia del Contrato, un plan de trabajo detallado, de ser posible en colaboración con el nuevo prestador de servicio asignado por “LOTERÍA” o en su caso, directamente a “LOTERÏA”, para lograr una transición efectiva, en el que se incluyan todos los hitos y plazos necesarios para efectuarlo. Dicho plan deberá permitir una correcta transición de los servicios, incluyendo la conformación y actualización de la documentación necesaria del proyecto.

La documentación debe 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,

operativos e infraestructura auxiliar que "LOTERÍA" solicite se mantengan para la transición de un nuevo contrato de servicios, procurando afectar de forma mínima la operación.
Asimismo, al término del contrato o en la terminación anticipada, el proveedor debe garantizar la operación acorde a los Niveles de Servicio en las mismas condiciones contractualmente pactados, durante el período de transferencia, que será mínimo de 60 días hábiles, contados al término del contrato o a la conclusión del servicio, esto durante el proceso de entrega a un nuevo Proveedor o directamente a Lotería.
Dicho período de transición tendrá un plazo de 60 días hábiles a partir de la conclusión de la vigencia del contrato o servicio, y estará sujeto al Plan de Trabajo que EL PROVEEDOR haya presentado previamente, y que "LOTERÍA" hubiera aprobado. No obstante, durante dicho periodo, EL PROVEEDOR debe proporcionar orientación tecnológica adecuada al personal de "LOTERÍA" para garantizar la continuidad de los servicios a su personal o a quien "LOTERÍA" designe para dicho propósito.

Perfil DEL LICITANTE

EL LICITANTE 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, conforme a las características y especificaciones mencionadas en el presente Anexo Técnico.
"EL LICITANTE" deberá acreditar mediante copia simple de contratos celebrados con Dependencias y/o Entidades Públicas o Sector Privado, una experiencia mínima de 3 años en la prestación de servicios similares a los requeridos en el Anexo Técnico. Cada contrato deberá estar debidamente formalizado y completo incluyendo sus anexos (podrán testarse las partes confidenciales y que no afecten la identificación del objeto del contrato y alcance de los servicios prestados).
Se podrán presentar contratos vigentes y/o concluidos.
Los contratos no deberán tener una antigüedad mayor de 10 años de haber sido celebrados previo a la fecha del acto de presentación y apertura de proposiciones.
El cómputo del tiempo de experiencia se realizará considerando solamente el tiempo calendario efectivamente prestado (todos los traslapes se contabilizarán solo una vez)
Cada contrato deberá tener servicios similares a los requeridos en el Anexo Técnico y tener una vigencia mínima de 6 meses.
Se aceptará la presentación de contratos plurianuales.
"EL LICITANTE" que presente contratos con empresas del mismo grupo de interés económico, deberá presentar copia simple de las facturas timbradas que avalen la efectiva prestación de los servicios durante el plazo de los contratos respectivos.
"EL LICITANTE" deberá acreditar una experiencia de 3 y 5 años del personal propuesto respectivamente de conformidad con lo solicitado en el punto "PERFIL REQUERIDO" del Anexo Técnico, para garantizar el cumplimiento de los servicios objeto de la presente licitación.

Requisitos y/o documentos que deberá presentar junto con su propuesta

Propuesta Técnica en hoja membretada firmada por el Representante Legal en el que se describa ampliamente los (bienes y/o servicios) que ofrece, en concordancia con lo señalado en el presente Anexo Técnico, dando cumplimiento a todas y cada una de las especificaciones técnicas establecidas
Propuesta Económica en hoja membretada rubricada cada hoja y firma al final por el Representante Legal. (Anexo A)
Escrito en hoja membretada firmado por el Representante Legal, en el cual manifieste que cuentan con capacidad de respuesta inmediata, así como con los recursos técnicos, financieros y demás que sean necesarios, y cuyas actividades comerciales o profesionales estén relacionadas con la prestación del servicio, entrega de los bienes o arrendamiento. (ANEXO B).

Escrito de no existencia de conflicto de interés: los licitantes deberán entregar dentro de su propuesta técnica escrito firmado por el representante legal manifestando la no existencia de conflicto de interés al no prestar o desarrollar servicios o bien de estar relacionado con una empresa o filial que actualmente preste o desarrolle servicios de operación y seguridad en las TIC's de "LOTERÍA".
EL LICITANTE deberá presentar las siguientes cartas firmadas por el representante legal del fabricante de los productos que actualmente tiene Lotería Nacional, lo anterior, en apego a los artículos 54 y 55 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, toda vez que el área requirente verificó que estos requerimientos guardan relación directa con el objeto de la contratación y no limitan la libre participación, concurrencia o competencia económica. Derivado de la verificación efectuada por el área requirente, se determina que, por la naturaleza técnica, operativa y sensible de los servicios requeridos, resultan necesarias estos requisitos para que EL LICITANTE acredite contar con los conocimientos, habilidades y controles suficientes para garantizar la correcta prestación del servicio, la calidad en su ejecución y la protección de la información que sea tratada, procesada, almacenada o administrada con motivo del contrato. que oferte, donde cumpla con lo siguiente:

- Nivel mínimo Expert para las licencias de Trend Micro propiedad de Lotería.
- Nivel mínimo Advanced para los equipos Firewall Fortinet propiedad de Lotería.

Aunado a lo anterior, deberá presentar:

- Carta del representante legal del Fabricante, que es Socio de Negocio de las tecnologías ofertadas para dar cumplimiento a los servicios a ser implementados y que mientras se tenga licenciamiento y soporte vigente contarán con apoyo técnico del mismo en caso de ser requerido para los siguientes servicios:
    - Protección de Información en Correo Electrónico
    - Visibilidad y Monitoreo de los Usuarios
    - Segmentación Zero Trust
    - Protección de Endpoint de siguiente generación (EDR)
    - Entorno de ataque cambiante (EAC)
    - Servicio de Diagnóstico y Reparación de Configuraciones Erróneas
    - Servicio de Firewall de Siguiente Generación (NGFW)
    - Servicio de Protección a Aplicaciones Móviles
    - Servicio de Correlación de Eventos
    - Servicio de Orquestación, Automatización y Respuesta de Seguridad
    - Servicio de Ciberinteligencia
    - Gestión de vulnerabilidades para endpoints y servidores
- Carta firmada por el representante legal del fabricante del producto ofertado indicando que cuentan con al menos el segundo nivel más alto de partner para los siguiente servicios:
    - Protección de Información en Correo Electrónico
    - Visibilidad y Monitoreo de los Usuarios
    - Segmentación Zero Trust
    - Protección de Endpoint de siguiente generación (EDR)
    - Entorno de ataque cambiante (EAC)
    - Servicio de Diagnóstico y Reparación de Configuraciones Erróneas
    - Servicio de Firewall de Siguiente Generación (NGFW)
    - Servicio de Protección a Aplicaciones Móviles
    - Servicio de Correlación de Eventos
    - Servicio de Orquestación, Automatización y Respuesta de Seguridad
    - Servicio de Ciberinteligencia

Copia de los certificados vigentes a nombre DEL LICITANTE, los cuales deberán ser emitidos por una autoridad certificadora reconocida y avalada para la emisión de certificaciones en las normas ISO ISO/IEC 27001:2022, ISO/IEC 20000-1:2018, ISO 22301:2019, ISO 9001:2015 e ISO 37001:2016.
EL LICITANTE deberá presentar una carta, en papel membretado y firmada por su representante legal donde especifique lo siguiente:

- Que cualquier software, marca y/o patente de algún sistema, aplicativo o programa que sea utilizado para la prestación del servicio objeto de la presente licitación, ha sido adquirido y/o se encuentra licenciado debidamente, cumpliendo con todas las disposiciones legales pertinentes en México.
- Que, en caso de infracción o reclamación relacionada con derechos de autor, marcas, patentes o cualquier otro derecho de propiedad intelectual vinculado con el software, sistemas, aplicativos o programas utilizados para la prestación del servicio, [Nombre de la Empresa o Licitante] se compromete a:

  c) Defender, indemnizar y mantener indemne a "LOTERÍA", contra cualquier reclamación, demanda, acción legal, daño, pérdida, costo o gasto, incluyendo honorarios legales, derivados de dicha infracción o reclamación.

  d) Tomar las medidas necesarias para garantizar la continuidad de la prestación del servicio a "LOTERÍA", sin que ello implique un costo adicional para la misma.

Documentación que EL LICITANTE deberá presentar por cada uno de sus recursos humanos enlistados para el cumplimiento del subrubro "PERFIL REQUERIDO" del Anexo Técnico es la siguiente:

2) Currículum vitae que cumpla con el perfil y certificaciones solicitadas, el cual debe de incluir:
   - Nombre completo.
   - Escolaridad.
   - Años de experiencia.
   - Teléfono.
   - Correo electrónico.

Descripción de certificado(s) requerido (s) en el ANEXO TÉCNICO.

3) Acreditar la relación laboral con "EL LICITANTE" presentando copia simple del último pago ante el IMSS y/o documento afiliatorio ante el IMSS, pudiendo testar información sensible.
4) Presentar copia simple de la identificación oficial vigente del personal propuesto.

Currículo Empresarial donde se describen las actividades y los clientes de la empresa.
"EL LICITANTE" deberá presentar al menos 3 contratos en copia simple, celebrados con Dependencias y/o Entidades Públicas o Sector Privado, demostrando experiencia mínima de 3 años en la prestación de servicios similares a los requeridos en el Anexo Técnico.

En su caso, método que se utilizará para realizar las pruebas que permitan verificar el cumplimiento de las especificaciones de los bienes a adquirir o arrendar o servicios a contratar, la institución pública o privada que las realizará y el momento para efectuarlas, así como la unidad de medida con la cual se determinará el resultado mínimo que deberá obtenerse en las pruebas señaladas.	No aplica
Normas que deben de cumplirse o Registros Sanitarios o Permisos Especiales, en su caso:	• *Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.* • *CISSP (Certified Information Systems Security Professional), acreditado por (ISC)2* • *ITIL V4 Foundation Certificate* • *Certified Incident Handler por EC-Council* • *PMP (Project Management Professional), acreditado por el PMI* • *CISM Certified Information Security Manager* • *ISO / IEC 27001: 2022 (Monitoreo y Revisiones, Respuesta a incidentes de Seguridad, Gestión de Cambios y Gestión de Incidentes)* • *Certificado Lead Auditor ISO 22301:2019* • *ISO-9001:2015* • *ISO/IEC 20000-1:2018* • *ISO 22301:2019* • *ISO 37001:2016*
Origen del servicio:	Nacional
Instalación:	Conforme a lo establecido en el presente anexo técnico en los sitios que determine Lotería Nacional.
Capacitación	Para todas las soluciones tecnológicas ofertadas tales como appliances y soluciones de software de seguridad informática por parte del fabricante mínimo para 10 personas.
Puesta en marcha:	A partir del día hábil siguiente a la fecha de la notificación del fallo.

CONDICIONES DE CONTRATACIÓN	
Modalidad del contrato:	La contratación del servicio será bajo la modalidad abierto por monto de conformidad al artículo 68 de la LAASSP.
Plazo de entrega o del servicio:	La vigencia del servicio será a partir del día hábil siguiente al de la fecha de notificación del fallo y hasta 24 meses posteriores. El plazo de entrega será conforme a los plazos suscritos en el Anexo técnico.

CONDICIONES DE CONTRATACIÓN	
Forma de pago:	El pago correspondiente se realizará en moneda nacional (MXN) por mes vencido durante la vigencia del contrato por la prestación del servicio dentro de los 17 días hábiles contados a partir de la entrega y verificación de la factura (Comprobante Fiscal Digital por Internet - CFDI- enviado a la cuenta de correo electrónico facturas@loterianacional.gob.mx), de conformidad con el servicio que se haya devengado en el mes objeto de pago, previa validación del servicio a entera satisfacción del Administrador del contrato en términos del presente anexo técnico de conformidad con el artículo 73, de la LAASSP en caso de que la prestación del servicio no sea por el mes completo que se trate, únicamente se pagará los días que efectivamente se recibió el servicio a satisfacción para estos casos los meses se entenderán siempre de 30 días. EL LICITANTE deberá entregar en la Subgerencia de Seguridad Informática adscrita a la Dirección de Tecnologías de la Información y Telecomunicaciones, en el primer piso de Insurgentes Sur 1397, Colonia Insurgentes Mixcoac, C.P. 03920, Demarcación Benito Juárez. México, D.F., en días y horas hábiles, los siguientes documentos: Factura que expida EL LICITANTE y que la misma reúna los requisitos fiscales, indicando 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 "LOTERÍA" (Acta Entrega-Recepción de los Servicios) para el administrador del contrato. En caso de que EL LICITANTE presente sus facturas con errores o deficiencias, estos se le harán saber máximo 5 días naturales posteriores a su entrega por parte de "LOTERÍA" y el plazo de pago se ajustará en proporción a los días que demoren las correcciones, debiendo presentar nuevamente toda la documentación mencionada anteriormente (en original y/o copia, según corresponda). Los pagos preferentemente se realizarán mediante el sistema de pago electrónico interbancario SPEI o mediante transferencia vía electrónica, a la cuenta bancaria que Licitante proporcione al administrador del contrato.

CONDICIONES DE CONTRATACIÓN	
Lugar de entrega:	

Insurgentes	Av. Insurgentes Sur No. 1397, Col. Insurgentes Mixcoac, Demarcación Benito Juárez, C.P. 03920. CDMX
Edison	Edison No. 15, Col. Tabacalera, Demarcación Cuauhtémoc, C.P. 06037, CDMX
Jalisco	Av. De las Repúblicas No. 117, Col. Tabacalera, Demarcación Cuauhtémoc, C.P. 06037 CDMX
Rosales	Rosales No. 15, Col. Tabacalera, Demarcación Cuauhtémoc, C.P. 06037 CDMX
Basilio Badillo	Basilio Badillo No. 39 Col. Centro, Demarcación Cuauhtémoc, C.P. 06037 CDMX
Hidalgo	Hidalgo No. 130, Col. Centro, Demarcación Cuauhtémoc, C.P. 06037 CDMX
Contreras	Av. San Francisco No. 156, Colonia Magdalena Contreras, Demarcación Magdalena Contreras C.P. 10500, Ciudad de México.
Subdirección Occidente	Av. Ignacio L Vallarta 1540 Int. 204, Esq. Marsella, Col. Americana, Guadalajara Jalisco, C.P. 44160
Subdirección Pacifico	Hernando de Soto No. 2 Altos, esquina Domingo Olivares, Colonia Los Arcos, Hermosillo, Sonora C.P. 85250
Subdirección Sureste	Calle 7 No. 457, entre calle 48 y calle 50, Colonia Residencial Pensiones, Mérida, Yucatán, C.P. 97217
Subdirección Noreste	Gral. Jerónimo Treviño 409 Despacho 520, Edificio BISA, Col. Centro, Monterrey, Nuevo León, C.P. 64000
Subdirección Norte	Antonio de Montes No. 2112-1, Col. San Felipe, Chihuahua, Chihuahua C.P. 51240
Subdirección Sur	Av. Martin Alonso Pinzón No. 757, Fraccionamiento Reforma, Veracruz, Veracruz C.P. 91919

Anticipo:	No aplica
Garantía de cumplimiento:	Para garantizar el cumplimiento de todas y cada una de las obligaciones, el **Licitante del Servicio** deberá entregar a la Gerencia de Adquisiciones en las oficinas de **Lotería Nacional**, Av. Insurgentes Sur 1397 sexto piso, Col. Insurgentes Mixcoac, Demarcación Benito Juárez, Ciudad de México, CP. 03920, dentro de los 10 (diez) días naturales posteriores a la firma del contrato, fianza expedida por la afianzadora debidamente constituida en términos de la Ley de Instituciones de Seguros y de Fianzas, cheque certificado o de caja, por un importe equivalente al 10% (diez por ciento) del monto máximo del contrato, sin considerar el Impuesto al Valor Agregado y a favor de **Lotería Nacional,** la cual debe ser valida durante toda la vigencia del contrato . Las obligaciones cuyo cumplimiento se garantiza, son divisibles, en consecuencia, en caso de incumplimiento imputable al **Licitante del Servicio**, así como cuando se determine la rescisión, la garantía se hará efectiva por el monto total de las obligaciones incumplidas, del servicio afectado

CONDICIONES DE CONTRATACIÓN	
Convenio de confidencialidad	El representante legal del "LICITANTE" deberá firmar al día hábil siguiente de la notificación del fallo una carta de confidencialidad en donde se comprometa a no utilizar ni divulgar información resultado del uso de su infraestructura; asimismo será responsable de custodiar y cuidar la información a la que tenga acceso por razón de la operación. Por lo que, se deberá impedir o evitar su uso, sustracción, destrucción ocultamiento o inutilización indebidas. Con excepción de aquella información que de conformidad con la Ley General de Transparencia y Acceso a la Información Pública se deba poner a disposición del público. En consecuencia, si el personal del "LICITANTE" viola este principio de confidencialidad será responsable de los daños y perjuicios ocasionados a "LOTERÍA".
Garantía de Responsabilidad Civil	El **Licitante del Servicio** adjudicado deberá entregar a la Gerencia de Adquisiciones en las oficinas de **Lotería Nacional**, Av. Insurgentes Sur 1397 sexto piso, Col. Insurgentes Mixcoac, Demarcación Benito Juárez, Ciudad de México, CP. 03920 dentro de los 10 (diez) días naturales posteriores a la firma del contrato, Póliza de Responsabilidad Civil a favor de **Lotería Nacional** por el 10% del monto máximo del contrato antes de IVA, por daños y perjuicios a terceros en su integridad física y en sus bienes. A efecto de garantizar los días para presentar la Póliza de Responsabilidad Civil, el Licitante del Servicio adjudicado deberá presentar a la Gerencia de Adquisiciones en las oficinas de Lotería Nacional, Av. Insurgentes Sur 1397 sexto piso, Col. Insurgentes Mixcoac, Demarcación Benito Juárez, Ciudad de México, CP. 03920, Carta Responsiva, al día hábil posterior a la notificación del fallo en la que manifieste que la póliza de responsabilidad civil será entregada conforme a lo solicitado. garantizando el monto máximo del contrato durante toda su vigencia. En caso de no cumplir con la entrega en tiempo y forma de la Póliza de Responsabilidad Civil, la Gerencia de Adquisiciones dará aviso al Área Requirente para iniciar el procedimiento de rescisión del contrato.

Penas convencionales:

De conformidad con lo estipulado en el Artículo 75 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 96 de su Reglamento el Administrador del contrato aplicará al Licitante una pena convencional por atraso en el cumplimiento de las fechas pactadas de entrega o de la prestación del servicio que se derivan o relacionan con el presente documento "Anexo Técnico" conforme al siguiente criterio:
"LOTERÍA" impondrá penas convencionales del 1% del monto mensual antes de IVA de la factura correspondiente a cargo DEL LICITANTE por cada día natural de atraso en el cumplimiento de las fechas pactadas de entrega de la prestación de los servicios, dichas penas no excederán del monto de la garantía de cumplimiento del contrato y serán determinadas por el **administrador del contrato** en función de los servicios no entregados o prestados oportunamente.
Para el pago de las penas convencionales, el Servidor Público Administrador del Contrato de Lotería Nacional notificará por escrito al Licitante, el cálculo de la o las penas a las que se hizo acreedor, indicando la base para su cálculo y el monto.
El Licitante se encargará de cubrirlas con notas de crédito, el original deberá ser entregado al Servidor Público Administrador del Contrato; una vez realizado esto podrá solicitar el pago de los servicios prestados.
El cálculo de las penalizaciones se realizará sobre el importe antes del Impuesto al Valor Agregado (IVA).
La suma de las penas convencionales no deberá exceder del importe de la garantía de cumplimiento del contrato, por lo que se procederá a la rescisión del contrato; en el entendido de que si el contrato es rescindido no procederá el cobro de dichas penas ni la contabilización de estas al hacer efectiva la garantía de cumplimiento.

Inicio de la Etapa Inicial	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	1 día hábil posterior a la fecha de notificación del fallo y hasta por 120 días naturales contados a partir de esta fecha
Inicio de la Etapa de Operación	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	A partir de la conclusión de la ETAPA INICIAL (120 días naturales) y hasta el término contractual del servicio, es decir a partir del día natural 121 contado a partir del día hábil siguiente a la fecha de notificación del fallo)"
Convenio de confidencialidad	Convenio de confidencialidad	El representante legal del "LICITANTE" deberá firmar al día hábil siguiente de la

			notificación del fallo una carta de confidencialidad en donde se comprometa a no utilizar ni divulgar información resultado del uso de su infraestructura; asimismo será responsable de custodiar y cuidar la información a la que tenga acceso por razón de la operación.	

Entregables Generales (Única vez)

Servicio	Entregable	Deductiva	Entrega
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto de acuerdo con las fases de la metodología del PMI, Scrum o Lean	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	10 días naturales posterior al inicio del servicio
	Documento Compromiso de suscripción de OLAs	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	15 días naturales posterior al inicio del servicio
	Matriz de Escalación	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	15 días naturales posterior al inicio del servicio
	Escrito por parte DEL LICITANTE, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	15 días naturales posterior al inicio del servicio
Servicios de Seguridad – Continuidad Operativa	Documento con el diseño de las Soluciones de Seguridad a implementar	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	15 días naturales posterior al inicio del servicio
	Memorias Técnicas de las Soluciones de	1% del costo mensual antes de IVA del	15 días naturales posterior al

	Seguridad Implementadas	total del servicio por cada día natural de atraso.	inicio del servicio
Centro de Detección, Análisis y Respuesta Gestionada (MDR)	Documento con el diseño detallado de las Soluciones de Seguridad a implementar	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	15 días hábiles posteriores al término de la habilitación de todos los componentes y servicios
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requirieron integrar activos de infraestructura para su habilitación	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	15 días hábiles posteriores al término de la habilitación de todos los componentes
	Procesos de operación implementados: Cambios; Configuraciones; Incidentes; Problemas; Disponibilidad	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	15 días naturales posterior al inicio del servicio
	Matriz de Escalación Técnica y Organizacional	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	15 días naturales posterior al inicio del servicio
	Expedientes Curriculares del personal del (MDR)	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	15 días naturales posterior al inicio del servicio

	Proceso de Coordinación Operativa con Terceros	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	15 días naturales contados posteriores al inicio del servicio
Entorno de ataque cambiante (EAC)	Plan de Implementación y Despliegue: documento detallado con pasos, cronograma, roles, responsabilidades y dependencias	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	Hasta 20 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"
	Arquitectura de la Solución: diseño detallado, diagramas de flujo de datos, integración con NGAV/EPP/EDR-XDR y descripción de componentes	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	Hasta 15 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"
	Documentación de Integración: guía técnica para la integración del EAC con SIEM y plataformas de gestión de incidentes existentes	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	Hasta 20 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"
	Informe de Estado del Proyecto: resumen de hitos alcanzados, desafíos y próximos pasos al término de la fase inicial	1% del costo mensual antes de IVA del total del servicio por cada día natural de atraso.	Hasta 20 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"

Entregables por Evento (a petición)

Servicio	Entregable	Deductiva	Entrega

Servicio de Protección de Información en Correo Electrónico	Reporte Técnico de los eventos de actividad sospechosa presentados, identificados, bloqueados o suspendidos	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"
Servicio de Visibilidad y Monitoreo de los Usuarios	Reporte Técnico de los eventos de actividad sospechosa presentados, identificados	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"
Servicio de Segmentación Zero Trust	Reporte Técnico de los eventos de actividad sospechosa presentados, identificados	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"
Servicio de Protección de Endpoint de siguiente generación (EDR)	Reporte Técnico de los eventos de actividad sospechosa presentados, identificados	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"
Servicios del Centro de Detección, Análisis y Respuesta Gestionada (MDR)	Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior al término de la implementación de cualquier solución de seguridad o conforme a la solicitud

	Actualización de la matriz de escalación	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la incorporación o sustitución de nuevo personal del SOC
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la ejecución de la ventana de mantenimiento
	Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la solicitud generada por parte de “LOTERÍA”
	Reporte Técnico de las configuraciones de las soluciones de seguridad	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la solicitud generada por parte de “LOTERÍA”
	Diagramas de Arquitectura de las soluciones de seguridad	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la solicitud generada por parte de “LOTERÍA”
Entregables de cada evaluación trimestral de vulnerabilidades	Reporte ejecutivo: resumen de la evaluación, nivel de exposición identificado, principales riesgos,	1% del costo mensual antes de IVA del servicio por cada día	15 días hábiles, una vez concluidas las pruebas.

	comparativo respecto de la evaluación anterior y recomendaciones prioritarias. Reporte técnico: deberá identificar los activos evaluados, vulnerabilidades encontradas, severidad, descripción, evidencia, componente afectado, impacto potencial, referencias técnicas, recomendación de remediación y prioridad. Matriz de vulnerabilidades: deberá permitir el seguimiento de cada hallazgo y contener como mínimo identificador, activo afectado, vulnerabilidad, severidad, fecha de detección, responsable de atención, recomendación, estado y fecha de cierre. Plan de remediación: conjunto de recomendaciones y	natural de atraso. 1% del costo mensual antes de IVA del servicio por cada día natural de atraso. 1% del costo mensual antes de IVA del servicio por cada día natural de atraso. 1% del costo mensual antes de IVA del servicio por cada día natural de atraso.		

	acciones correctivas propuestas para reducir o eliminar las vulnerabilidades identificadas, sujeto a la aprobación y priorización de "LOTENAL". Reporte comparativo: deberá señalar vulnerabilidades nuevas, persistentes, mitigadas, remediadas o reincidentes respecto de la evaluación trimestral anterior.	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	

Entregables periódicos

FASE INICIAL. Hasta por 120 días naturales posteriores al día natural siguiente a la fecha de notificación del fallo

SERVICIO	ENTREGABLE	DEDUCTIVA	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de la infraestructura y servicios de "LOTERÍA": Protección de Información en Correo Electrónico Visibilidad y Monitoreo de los Usuarios Segmentación Zero Trust Protección de Endpoint de Siguiente Generación (EDR)	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido

	Que contenga al menos lo siguiente: Incidentes/Fallas Actividad Sospechosa Estadísticas de uso de los servicios		
Servicios del Centro de Detección, Análisis y Respuesta Gestionada (MDR)	Reporte Técnico de los incidentes de ciberseguridad presentados, que hayan sido identificados por el Centro de Detección, Análisis y Respuesta Gestionada (MDR) de la infraestructura y servicios de "LOTERÍA".	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados, que hayan sido identificados de la infraestructura y servicios de "LOTERÍA".	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
	Reporte de las estadísticas de uso y desempeño de los servicios de seguridad en la infraestructura y servicios de "LOTERÍA"..	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
Entorno de ataque cambiante (EAC)	Informe de Actividades Mensuales: - Detalle de las actividades realizadas durante el mes, incluyendo	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido

	despliegues, actualizaciones, mantenimiento y mejoras en el servicio en la infraestructura y servicios de "LOTERÍA".		
	Análisis de Alertas y Eventos: - Informe detallado de todas las alertas generadas, su clasificación, análisis forense realizado, y las medidas de respuesta adoptadas para cada incidente en la infraestructura y servicios de "LOTERÍA".	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido

ETAPA OPERATIVA

SERVICIO	ENTREGABLE	DEDUCTIVA	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de las soluciones implementadas: Protección de Información en Correo Electrónico Visibilidad y Monitoreo de los Usuarios Segmentación Zero Trust Protección de Endpoint de Siguiente Generación (EDR) Que contenga al menos lo siguiente:	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido

	Incidentes/Fallas Actividad Sospechosa Estadísticas de uso de los servicios		
Servicios del Centro de Detección, Análisis y Respuesta Gestionada (MDR)	Reporte Técnico de los incidentes de ciberseguridad presentados, que hayan sido identificados por el Centro de Detección, Análisis y Respuesta Gestionada (MDR)	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados, que hayan sido identificados	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
	Reporte de las estadísticas de uso y desempeño de los servicios de seguridad implementados.	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
Entorno de ataque cambiante (EAC)	Informe de Actividades Mensuales: - Detalle de las actividades realizadas durante el mes, incluyendo despliegues, actualizaciones, mantenimiento y mejoras en el servicio.	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido
	Análisis de Alertas y Eventos: - Informe detallado de todas las alertas generadas, su	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido

	clasificación, análisis forense realizado, y las medidas de respuesta adoptadas para cada incidente.		
Gestión de Vulnerabilidades	Reporte de Vulnerabilidades y Prioridades de Parches: - Informe mensual con el inventario de vulnerabilidades detectadas y su priorización según el nivel de riesgo, recomendaciones para la aplicación de parches y mitigaciones implementadas.	1% del costo mensual antes de IVA del servicio por cada día natural de atraso	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido

Para todos aquellos entregables descritos en el Anexo técnico, no citados en las tablas antes expuestas, la deductiva será de 1% del costo mensual antes de IVA del servicio, según corresponda, por cada día natural de atraso.

Deducciones

NIVELES DE SERVICIOS
El objetivo de los Niveles de Servicio consiste en proporcionar a "LOTERÍA" un mecanismo que permita:
Medir de forma efectiva el desempeño de los servicios proporcionados por EL LICITANTE.
Procurar que los servicios de sean proporcionados con la calidad prevista.

SERVICIO	PORCENTAJE DE DISPONIBILIDAD MENSUAL	UNIDAD PARA EL CÁLCULO DE DEDUCTIVAS	DEDUCTIVA
Protección de información en correo electrónico	99.9%	El cálculo se hará por servicio y será acumulable durante el período evaluado.	3% por cada décima porcentual por debajo del nivel comprometido, del costo mensual antes de IVA del servicio que corresponda prestado de forma deficiente.
Visibilidad y monitoreo de usuarios	99.9%	El cálculo se hará por servicio y será acumulable durante el período evaluado.	3% por cada décima porcentual por debajo del nivel comprometido, del costo mensual antes de IVA del servicio que corresponda prestado de forma deficiente.
Segmentación Zero Trust	99.9%	El cálculo se hará por servicio y será acumulable durante el período evaluado.	2% por cada décima porcentual por debajo del nivel comprometido, del costo mensual antes de IVA del servicio que corresponda prestado de forma deficiente.
Protección de endpoint de siguiente generación (EDR) • Protección de para Servidores	99.9%	El cálculo se hará por servicio y será acumulable durante el período evaluado.	5% por cada décima porcentual por debajo del nivel comprometido, del costo mensual antes de IVA del servicio que corresponda prestado de forma deficiente.
Protección de endpoint de siguiente generación (EDR) • Protección de Equipos de Cómputo personal	99.9%	El cálculo se hará por servicio y será acumulable durante el período evaluado.	5% por cada décima porcentual por debajo del nivel comprometido, del costo mensual antes de IVA del servicio que corresponda prestado de forma deficiente.

Entorno de ataque cambiante (EAC)	99.9%	El cálculo se hará por servicio y será acumulable durante el período evaluado.	3% por cada décima porcentual por debajo del nivel comprometido, del costo mensual antes de IVA del servicio que corresponda prestado de forma deficiente.
Servicio de firewall de siguiente generación (NGFW)	99.9%	El cálculo se hará por servicio y será acumulable durante el período evaluado.	5% por cada décima porcentual por debajo del nivel comprometido, del costo mensual antes de IVA del servicio prestado de forma deficiente.
Servicio de protección a aplicaciones móviles	99.9%	El cálculo se hará por servicio y será acumulable durante el período evaluado	3% por cada décima porcentual por debajo del nivel comprometido, del costo mensual antes de IVA del servicio que corresponda prestado de forma deficiente.
Servicio de diagnóstico y reparación de configuraciones erróneas	99.9%	El cálculo se hará por servicio y será acumulable durante el período evaluado	2% por cada décima porcentual por debajo del nivel comprometido, del costo mensual antes de IVA del servicio prestado de forma deficiente.
Servicio de autenticación multi factor (MFA)	99.9%	El cálculo se hará por servicio y será acumulable durante el período evaluado	3% por cada décima porcentual por debajo del nivel comprometido, del costo mensual antes de IVA del servicio que corresponda prestado de forma deficiente.
Centro de operaciones de la seguridad y respuesta gestionada (MDR)	99.9%	El cálculo se hará por servicio y será acumulable durante el período evaluado	5% por cada décima porcentual por debajo del nivel comprometido, del costo mensual antes de IVA del servicio prestado de forma deficiente.
Mesa de Servicio	99.9%	El cálculo se hará por servicio y será	3% por cada décima porcentual por debajo del nivel comprometido, del

		acumulable durante el período evaluado	costo mensual antes de IVA del servicio que corresponda prestado de forma deficiente.

Se aplicarán deducciones al pago por incumplimiento en niveles de servicio por parte DEL LICITANTE adjudicado, del 1% (uno por ciento) del costo mensual antes de IVA del servicio, de acuerdo a la siguiente fórmula:

Monto de la deductiva Deductiva= Monto mensual del servicio afectado antes de IVA * 0.01

Para cada uno de los servicios afectados.

Servicio	Servicio Afectado
Servicios del Centro de Detección, Análisis y Respuesta Gestionada (MDR) (PARA LA ETAPA INICIAL Y ETAPA OPERATIVA)	Incidentes de ciberseguridad presentados – 100% Reportados VS atendidos
	Eventos de actividad sospechosa presentados - 100% Reportados VS atendidos
Entorno de ataque cambiante (EAC) (PARA LA ETAPA INICIAL Y ETAPA OPERATIVA)	Despliegues, actualizaciones, mantenimiento y mejoras – 95%
	Vulnerabilidades originadas por falta de Parches: inventario de vulnerabilidades, priorización, recomendaciones y mitigaciones – 100% Reportados VS atendidos
	Alertas y Eventos: clasificación de alertas, análisis forense y medidas de respuesta - 100% Reportados VS Atendidos

Con fundamento en lo dispuesto en el artículo 76 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 96 de su Reglamento, el Funcionario Público Administrador del Contrato aplicará al Licitante deductivas por el incumplimiento parcial o deficiente de los servicios, de conformidad con lo siguiente:

Para entregables periódicos o mensuales, las deductivas a aplicar serán confirme a lo siguiente:

Entregables Periódicos, mensuales

Servicio	Entregable	Deductiva	Entrega
Servicios de Seguridad – Continuidad Operativa (PARA LA ETAPA INICIAL Y ETAPA OPERATIVA)	Reportes Técnicos de las soluciones implementadas: Protección de Información en Correo Electrónico Visibilidad y Monitoreo de los Usuarios	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	Dentro de los 10 días hábiles posteriores al cumplimiento del mes vencido

		Segmentación Zero Trust Protección de Endpoint de Siguiente Generación (EDR) Que contenga al menos lo siguiente: Incidentes/Fallas Actividad Sospechosa Estadísticas de uso de los servicios		
	Servicios del Centro de Detección, Análisis y Respuesta Gestionada (MDR) (PARA LA ETAPA INICIAL Y ETAPA OPERATIVA)	Reporte Técnico de los incidentes de ciberseguridad presentados, que hayan sido identificados por el Centro de Detección, Análisis y Respuesta Gestionada (MDR)	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"
		Reporte Técnico de los eventos de actividad sospechosa presentados, que hayan sido identificados	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"
		Reporte de las estadísticas de uso y desempeño de los servicios de seguridad implementados.	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"
	Entorno de ataque cambiante (EAC) (PARA LA ETAPA INICIAL Y ETAPA OPERATIVA)	Informe de Actividades Mensuales: - Detalle de las actividades realizadas durante el mes, incluyendo despliegues, actualizaciones, mantenimiento y mejoras en el servicio.	1% del costo mensual antes de IVA del servicio por cada día natural de atraso.	5 días hábiles posterior a la solicitud generada por parte de "LOTERÍA"

<table>
<tr><td></td><td colspan="4"><table>
<tr><td></td><td>Reporte de Vulnerabilidades y Prioridades de Parches:
- Informe mensual con el inventario de vulnerabilidades detectadas y su priorización según el nivel de riesgo, recomendaciones para la aplicación de parches y mitigaciones implementadas.</td><td>1% del costo mensual antes de IVA del servicio por cada día natural de atraso.</td><td>5 días hábiles posterior a la solicitud generada por parte de “LOTERÍA”</td></tr>
<tr><td></td><td>Análisis de Alertas y Eventos:
- Informe detallado de todas las alertas generadas, su clasificación, análisis forense realizado, y las medidas de respuesta adoptadas para cada incidente.</td><td>1% del costo mensual antes de IVA del servicio por cada día natural de atraso.</td><td>5 días hábiles posterior a la solicitud generada por parte de “LOTERÍA”</td></tr>
<tr><td>Servicio de Protección a Aplicaciones Móviles</td><td>Reporte Técnico de la protección implementada en la APP protegida</td><td>1% del costo del servicio antes de IVA por cada día natural de atraso.</td><td>30 días naturales posteriores a la solicitud generada por “LOTERÍA”.</td></tr>
</table>
Si el incumplimiento resulta en una brecha de seguridad con impacto operacional, el prestador de servicio será responsable de los costos de mitigación y recuperación. Aunado a lo anterior, deductiva adicional del 30% del monto mensual del total de la factura, antes de IVA.</td></tr>
<tr><td>Reposición de los servicios y/o entrega de los bienes:</td><td colspan="4">No aplica.</td></tr>
</table>

Forma y términos en que se realizará la verificación de las especificaciones y la aceptación de los bienes o servicios:	La recepción, verificación y aceptación de los bienes y/o servicios objeto de la contratación se llevará a cabo de conformidad con las características, especificaciones técnicas, condiciones, alcances, niveles de servicio, entregables y demás requisitos establecidos en el Anexo Técnico, así como en los términos y condiciones previstos en el instrumento contractual correspondiente. La verificación del cumplimiento de las obligaciones técnicas y de los entregables estará a cargo de la persona titular de la Subgerencia de Seguridad Informática, actualmente el Ing. Daniel Alejandro Toledo Aldaraca, o de quien legalmente la sustituya en el cargo, en el ámbito de sus atribuciones y responsabilidades. Para tal efecto, se realizará la revisión y validación de los bienes suministrados y/o servicios prestados, a fin de constatar que cumplen con las especificaciones, características, condiciones y demás requerimientos establecidos en el Anexo Técnico. La recepción y aceptación se formalizarán mediante la suscripción de un acta de entrega-recepción, constancia de aceptación, informe de cumplimiento o cualquier otro documento que resulte aplicable, en el que se deje evidencia documental de los bienes y/o servicios recibidos, los entregables presentados, las verificaciones realizadas y el cumplimiento de las obligaciones contractuales correspondientes. La aceptación de los bienes y/o servicios quedará sujeta a la verificación de su cumplimiento satisfactorio, sin que la simple entrega física de los bienes o la presentación de los entregables implique, por sí misma, su aceptación definitiva.

FUNDAR Y MOTIVAR LA CONTRATACIÓN DE LOS SERVICIOS Y/O ADQUISICIÓN DE LOS BIENES	
Justificación Técnica:	“LOTERÍA”, requiere del “SERVICIO INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN PARA LOTERÍA NACIONAL(SISI)”, que le permita contar con las herramientas tecnológicas en materia de seguridad informática necesarias, para mantener la integridad, confidencialidad y disponibilidad de la información y/o datos de la Entidad El objetivo principal de esta contratación es mejorar el control sobre la infraestructura tecnológica, de oficina y empresarial de servidores, instalados y operando en las instalaciones de “LOTERÍA” y Centro de datos, así como obtener métricas y estadísticas apropiadas de riesgos para establecer contramedidas adecuadas para mitigar o contener los mismos. Para “LOTERÍA” la seguridad de la información es sumamente importante y esencial, y el objetivo de esta consiste en preservar la confidencialidad de la información, así como su integridad y disponibilidad. Esto incluye a los sistemas implicados en el tratamiento de la información dentro de la Entidad considerando que la información es un activo fundamental con un rol vital para “LOTERÍA”. En consecuencia, la seguridad informática es de vital importancia ya que radica en la prevención, puesto que se debe evitar el robo de información en las distintas áreas de “LOTERÍA”. Además, ayuda a identificar cuando existen amenazas de virus y riesgos en los sistemas de información internos.

Justificación Económica:	"LOTERÍA", al contar con la protección de los servicios de Servicios de Seguridad - Continuidad Operativa, Centro de Detección, Análisis y Respuesta Gestionada (MDR) y demás servicios asociados, evita afectaciones en la infraestructura tecnológica de cómputo por actividades maliciosas, que pudiesen poner en riesgo la operación de la Entidad la cual afectaría los servicios de tesorería, expendedora, cobro, acceso a bancos y celebración de sorteos, procesos vitales en la recaudación de recursos económicos para la Entidad El "SERVICIO INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN PARA LOTERÍA NACIONAL(SISI)" es importante para el resguardo y seguridad de la información que la Entidad maneja en sus operaciones diarias, también es importante la modificación de esta por lo que con la contratación en comento se garantizará que la información sea modificada por las personas con los permisos que otorgue "LOTERÍA". La seguridad de la información parte de la premisa de que los datos son el gran valor de la nueva era de Lotería Nacional, ya que los malos manejos que se puedan hacer con ella pueden ser catastróficos y con ello se vería afectado el desarrollo de las actividades de las áreas sustantivas de la Entidad, pudiendo ocasionar con ello el incumplimiento en el logro de los objetivos y metas encaminados a maximizar la generación de recursos económicos.

AVISO

De conformidad con numeral 6, del Anexo Primero del Acuerdo por el que se modifica el diverso que expide el Protocolo de Actuación en Materia de Contrataciones Públicas, Otorgamiento y Prórroga de Licencias, Permisos, Autorizaciones y Concesiones, publicado en el Diario Oficial de la Federación el día 28 de febrero de 2017, se hace del conocimiento lo siguiente:
Los servidores públicos en el contacto con particulares deben observar el presente Protocolo y éste puede ser consultado en la sección de la Antes Secretaría de la Función Pública Ahora Secretaría Anticorrupción y Buen Gobierno, que se encuentra en el portal de la Ventanilla Única Nacional (gob.mx), a través de la liga https://www.gob.mx/buengobierno.

A fin de promover las mejores prácticas en materia de combate a la corrupción y prevención de conflictos de interés, en los procedimientos que a continuación se enuncian las reuniones, visitas y actos públicos serán videograbados:

i. Contrataciones públicas sujetas a la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, cuyo monto rebase el equivalente a cinco millones de Unidades de Medida y Actualización;

ii. Contrataciones públicas sujetas a la Ley de Obras Públicas y Servicios Relacionados con las Mismas, cuyo monto rebase el equivalente a diez millones de Unidades de Medida y Actualización;

iii. Contrataciones públicas sujetas a la Ley de Asociaciones Público-Privadas, cuyo monto rebase el equivalente a cuatrocientos millones de Unidades de Inversión, y

iv. Otorgamiento y prórroga de concesiones.

Las videograbaciones de las reuniones, visitas y actos públicos podrán ponerse a disposición de las autoridades encargadas de verificar la legalidad de dichos procedimientos y podrán ser utilizadas como elemento de prueba. A efecto de lo anterior, dichas videograbaciones deberán conservarse en los archivos de la unidad administrativa que las haya generado.

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

Tienen derecho a presentar queja o denuncia por el incumplimiento de obligaciones que adviertan en el contacto con los servidores públicos, ante el Órgano Interno de Control correspondiente, o bien, a través del Sistema Integral de Quejas y Denuncias Ciudadanas, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 9 de diciembre de 2015.

Del mismo modo, para dar cumplimiento a la fracción II del artículo Primero del Acuerdo por el que se modifica el diverso que expide el Protocolo de Actuación en Materia de Contrataciones Públicas, Otorgamiento y Prórroga de Licencias, Permisos, Autorizaciones y Concesiones, por el que se expide el protocolo de actuación en materia de contrataciones púbicas, otorgamiento y prórroga de licencia, permisos, autorizaciones y concesiones publicado en el Diario Oficial de la Federación el día 28 de febrero de 2017 y de conformidad con el Anexo Segundo “MANIFIESTO QUE PODRÁN FORMULAR LOS PARTICULARES EN LOS PROCEDIMIENTOS DE CONTRATACIONES PÚBLICAS, DE OTORGAMIENTO Y PRÓRROGA DE LICENCIAS, PERMISOS, AUTORIZACIONES Y CONCESIONES”; a través del vínculo https://manifiesto.buengobierno.gob.mx/SMP-web/loginPage.jsf , en el cual podrán encontrar la directriz para

formular un manifiesto en el que afirmen o nieguen los vínculos o relaciones de negocios, laborales, profesionales, personales o de parentesco por consanguinidad o afinidad hasta el cuarto grado tenga la (s) persona (s), con el o los servidores públicos, por lo que se le invita a realizar dicho manifiesto.

_____

ÁREA REQUIRENTE Y ÁREA TÉCNICA
LIC. ARMANDO CARDENAS REYES
GERENTE DE TELECOMUNICACIONES Y SEGURIDAD INFORMÁTICA

P.A. Armando Cardens Reyes

_____

ADMINISTRADOR DEL CONTRATO
ING. DANIEL ALEJANDRO TOLEDO ALDARACA
SUBGERENTE DE SEGURIDAD INFORMÁTICA

ANEXO II
ACREDITAMIENTO DE PERSONALIDAD JURÍDICA PERSONA FÍSICA

(Lugar y fecha) _____ a ___de _____de 2026

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

(Nombre de la Persona Física), manifiesto bajo protesta de decir verdad, que los datos aquí asentados son ciertos y han sido debidamente verificados, así como que cuento con facultades suficientes para suscribir la proposición en la presente la Licitación, a nombre y representación de (**Persona Física**).

No. de la Licitación Pública:

Registro Federal de Contribuyentes:	CURP:
Domicilio fiscal:	
Calle y número:	
Colonia:	Demarcación Territorial o municipio:
Código Postal:	Entidad federativa:
Teléfonos:	
Correo electrónico:	
Descripción de la actividad empresarial	
Nombre del representante:	

Manifiesto que acepto todos y cada uno de los términos y condiciones establecidos en la presente convocatoria y su Anexo Técnico y que cuento con la capacidad legal, técnica y financiera para prestar el servicio objeto del presente procedimiento de contratación.

Asimismo, manifiesto que el domicilio señalado es el lugar donde recibiré toda clase de notificaciones que resulten de los contratos y convenios que celebren, 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, deberán ser comunicados, dentro de los cinco días hábiles siguientes a la fecha en que se generen. Adicionalmente acepto que las notificaciones se realizarán de acuerdo a las establecidas en los artículos 35 y 36 de la Ley Federal de Procedimiento Administrativo.

(Lugar y Fecha)
Protesto lo necesario
Nombre de la persona física, y Firma

Nota: Este escrito deberá ser presentado, preferentemente, en papel membretado de la o el licitante

ANEXO III
ACREDITAMIENTO DE PERSONALIDAD JURÍDICA PERSONA MORAL

(Lugar y fecha) _____ a ___de _____de 2026

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

_____(Nombre de la/el Representante Legal)_____, manifiesto **Bajo Protesta a Decir Verdad**, que los datos aquí asentados son ciertos y han sido verificados; así como que cuento con facultades suficientes para **comprometerme** en la presente Licitación Pública, a nombre y representación de:_____(Nombre de la persona moral)_____.

No. de la Licitación Pública: _____.

Del licitante	Registro Federal de Contribuyentes: Domicilio: (calle y número) Colonia: Demarcación Territorial o Municipio: Código postal: Entidad Federativa: Teléfono: Correo electrónico: No. de la escritura pública en la que consta su acta constitutiva: Fecha: Descripción del objeto social: Reformas al acta constitutiva: Fecha y datos de inscripción en el Registro Público correspondiente.
De los socios	Nombres / R.F.C. Nota: Deberá agregar los datos de todos los Socios.
Del Representante	Nombre: R.F.C. Domicilio: Datos del documento mediante el cual acredita su personalidad y facultades: Escritura pública número: Fecha:

Manifiesto que acepto todos y cada uno de los términos y condiciones establecidos en la presente convocatoria y su Anexo Técnico y que cuento con la capacidad legal, técnica y financiera para prestar el servicio objeto del presente procedimiento de contratación.

Asimismo, manifiesto que el domicilio señalado es el lugar donde recibiré toda clase de notificaciones que resulten de los contratos y convenios que celebren, 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, deberán ser comunicados, dentro de los cinco días hábiles siguientes a la fecha en que se generen. Adicionalmente acepto que las notificaciones se realizarán de acuerdo a las establecidas en los artículos 35 y 36 de la Ley Federal de Procedimiento Administrativo.

(Nombre y firma de la o el Representante Legal)

Nota: Este escrito deberá ser presentado, preferentemente, en papel membretado de la o el licitante

ANEXO IV
ESCRITO DE LOS SUPUESTOS ESTABLECIDOS EN LOS ARTÍCULOS 71 Y 90 DE LA LEY

(Lugar y fecha) _____, a _____ de _____ del 2026.

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

(EN CASO DE SER PERSONA FÍSICA)
(Nombre de la persona física) , declaro **Bajo Protesta de Decir Verdad** lo siguiente:

Que el suscrito, no se encuentran en alguno de los supuestos señalados en los artículos 71 y 90 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).

(EN CASO DE SER PERSONA MORAL)
(Nombre de la o el Representante Legal)) , con las facultades que la empresa denominada _____(Nombre de la empresa que representa)__ me otorga, declaro **Bajo Protesta de Decir Verdad** lo siguiente:

Que el suscrito, mi representada legal y las personas que forman parte de la sociedad, no se encuentran en alguno de los supuestos señalados en los artículos 71 y 90 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).

(**PÁRRAFO TANTO PARA PERSONA FÍSICA COMO PERSONA MORAL**)

En el entendido que de no manifestarme con veracidad, acepto que ello sea causa de desechamiento de la proposición o rescisión administrativa del contrato celebrado.

(Nombre y firma de la/el Representante Legal o persona física)

Nota: Este escrito deberá ser presentado, preferentemente, en papel membretado de la o el licitante

ANEXO V
ESCRITO DE DECLARACIÓN DE INTEGRIDAD

(Lugar y fecha)_____, _____de_____de 2026

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

_____(Nombre de la o el Representante Legal o persona física)_____, en mi carácter de _____, de la ___(Persona Moral o física)___, en cumplimiento a lo ordenado por el artículo 40 fracción X de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, fracción VI, inciso f y antepenúltimo párrafo del 83 de su Reglamento; y para efectos de presentar proposición y en su caso poder celebrar el contrato respectivo con esta LN en relación a la Licitación Pública Nacional (Nombre y número de procedimiento): _____.

(EN CASO DE SER PERSONA FÍSICA)
Me permito manifestar BAJO PROTESTA DE DECIR VERDAD que me abstendré por sí mismo o a través de interpósita persona, de adoptar conductas para que las o los servidores públicos, induzcan o alteren las evaluaciones de las proposiciones, el resultado del procedimiento, u otros aspectos que le otorguen condiciones más ventajosas con relación a las o los demás participantes; así como de incorporar durante la vigencia de los contratos a personas que se encuentren inhabilitadas. ***EN CASO DE NO SER PERSONA MORAL, ELIMINAR ESTE PÁRRAFO.***

(EN CASO DE SER PERSONA MORAL)
Me permito manifestar BAJO PROTESTA DE DECIR VERDAD que la empresa que represento se abstendrá por sí misma o a través de interpósita persona, de adoptar conductas para que las o los servidores públicos, induzcan o alteren las evaluaciones de las proposiciones, el resultado del procedimiento, u otros aspectos que le otorguen condiciones más ventajosas con relación a las o los demás participantes; así como de incorporar durante la vigencia de los contratos a personas que se encuentren inhabilitadas. ***EN CASO DE NO SER PERSONA FÍSICA, ELIMINAR ESTE PÁRRAFO.***

(Nombre y firma de la/el Representante Legal o persona física)

Nota: Este escrito deberá ser presentado, preferentemente, en papel membretado de la o el licitante

ANEXO VI
ESCRITO DE NACIONALIDAD

(Lugar y fecha)_____de _____ de 2026.

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

(EN CASO DE SER PERSONA FÍSICA)
Conforme a lo señalado en el artículo 39 fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 58 de su Reglamento, manifiesto **bajo protesta de decir verdad** que **soy de Nacionalidad Mexicana.**

(EN CASO DE SER PERSONA MORAL)
Conforme a lo señalado en el artículo 39 fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 58 de su Reglamento, manifiesto **bajo protesta de decir verdad** que **mi Representada es de Nacionalidad Mexicana.**

Nombre y Firma de la/el Representante Legal o persona física

Nota: Este escrito deberá ser presentado, preferentemente, en papel membretado de la o el licitante.

ANEXO VII
ACEPTACIÓN DE CONDICIONES DE LA PLATAFORMA

(Lugar y fecha)_____de _____ de 2026

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

_____(Nombre de la o el Representante Legal o persona física)_____, en mi carácter de _____, de la ___(Persona Moral o física)___, manifiesto mi aceptación de que se tendrán como no presentadas mis proposiciones y, en su caso, la documentación requerida, cuando el archivo electrónico en el que se contengan la proposición y/o demás información no pueda abrirse por tener algún virus informático o por cualquier otra causa ajena a la LN, en términos de lo dispuesto por el numeral 29 del Acuerdo.

Este escrito no exime a mi representada de la entrega de cualquier otro documento solicitado.

_____
Nombre y Firma de la/el Representante Legal o persona física

Nota: Este escrito deberá ser presentado, preferentemente, en papel membretado de la o el licitante

ANEXO VIII
MANIFESTACIÓN DE VÍNCULOS

_____de _____ de 2026.

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

SIN VINCULOS

(Nombre del que suscribe el presente escrito) *en mi carácter de* ***(Representante o Apoderado Legal de la Persona moral)/(Persona Física)***, manifiesto bajo protesta de decir verdad que ***(ni mi representada)*** **ni el que suscribe tenemos** vínculo alguno de negocios, laborales, profesionales, personales o de parentesco por consanguinidad o afinidad hasta el cuarto grado con las personas servidoras públicas que intervienen, participan o tienen injerencia en el procedimiento de contratación de los **"_____"**, conforme a lo establecido en el Protocolo de Actuación.

Así mismo, me comprometo a informar de manera inmediata y por escrito si durante el desarrollo del procedimiento llegase a surgir o conocerse algún vínculo de esta naturaleza.

CON VINCULOS

(Nombre del que suscribe el presente escrito) *en mi carácter de* ***(Representante o Apoderado Legal de la Persona moral)/(Persona Física)***, manifiesto bajo protesta de decir verdad que de conformidad con lo establecido en el Protocolo de Actuación, **sí existe vínculo** de **(especificar tipo: negocios, laboral, profesional, personal o parentesco)** con la persona servidora pública **(nombre completo del servidor público)**, quien **(describir brevemente su intervención en el procedimiento).**

Lo anterior se hace del conocimiento del ente contratante para los efectos legales a que haya lugar, y me comprometo a colaborar plenamente con cualquier aclaración o medida que proceda conforme a la normatividad aplicable.

A t e n t a m e n t e

_____
Nombre, Cargo y Firma del Representante Legal

ANEXO IX
MANIFESTACIÓN DE BENEFICIOS O VENTAJAS

_____de _____ de 2026.

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

(Nombre del que suscribe el presente escrito) *en mi carácter de* ***(Representante o Apoderado Legal de la Persona moral)/(Persona Física)***, manifiesto bajo protesta de decir verdad que no realizo ni ejecuto, con ningún otro licitante, actos o acciones que tengan por objeto o efecto obtener un beneficio o ventaja indebida en el presente procedimiento de contratación.

A t e n t a m e n t e

_____
Nombre, Cargo y Firma del Representante Legal

ANEXO X
MANIFESTACIÓN DE SUBCONTRATACIÓN

_____de _____ de 2026.

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

(Nombre del que suscribe el presente escrito) *en mi carácter de* ***(Representante o Apoderado Legal de la Persona moral)/(Persona Física)***, manifiesto bajo protesta de decir verdad que, en caso de resultar adjudicado, no subcontrataré a ningún otro licitante que haya presentado proposición en el presente procedimiento.

A t e n t a m e n t e

_____
Nombre, Cargo y Firma del Representante Legal

ANEXO XI
ESTRATIFICACIÓN DE LAS MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS

_____ de _____ de 2026 (**1**)

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

Me refiero al procedimiento de _____(**2**)_____ No. _____(**3**) _____ en el que mi representada, la empresa_____(**4**)_____, participa a través de la presente proposición.

Al respecto y de conformidad con lo dispuesto por el artículo 57 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 _____(**5**)_____, 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 _____(**6**)_____, con base en lo cual se estratifica como una empresa _____(**7**)_____.

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 el artículo 4 fracción II, 69, 70 y 81 de la Ley General de Responsabilidades Administrativas, y demás disposiciones aplicables.

_____(**8**)_____

Nota: Este escrito deberá ser presentado, preferentemente, en papel membretado de la o el licitante

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. Precisar el procedimiento de contratación de que se trate (licitación pública o invitación a cuando menos tres personas).
3. Indicar el número de procedimiento de contratación.
4. Anotar el nombre, razón social o denominación de la o el licitante.
5. Indicar el Registro Federal de Contribuyentes de la o el licitante.
6. Señalar el número que resulte de la aplicación de la expresión: Tope Máximo Combinado = (Trabajadores) x10% + (Ventas anuales en millones de pesos) x 90%. Para tales efectos puede utilizar la calculadora MIPYME disponible en la página http://www.comprasdegobierno.gob.mx/calculadora
   Para el concepto "Trabajadores", utilizar el total de los trabajadores con los que cuenta la empresa a la fecha de la emisión de la manifestación.
   Para el concepto "ventas anuales", utilizar los datos conforme al reporte de su ejercicio fiscal correspondiente a la última declaración anual de impuestos federales, expresados en millones de pesos.
7. Señalar el tamaño de la empresa (Micro, Pequeña o Mediana), conforme al resultado de la operación señalada en el numeral anterior.
8. Anotar el nombre y firma del apoderado o representante legal de la o el licitante.

ANEXO XII
FORMATO DE INFORMACIÓN RESERVADA Y CONFIDENCIAL

_____, a _____ de _____de 2026.

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

___(Nombre de la/el Representante Legal o persona física)_____, en mi carácter de _____, de la ___(Persona Moral o física)___, manifiesto por medio de la presente que los documentos contenidos en mi propuesta y remitida a la convocante para la Licitación Pública Nacional _____ contiene información de carácter Confidencial y Comercial Reservada, de conformidad con lo siguiente:

No.	Documento (1)	Información a clasificar (2)	Fundamentación (3)	Motivación (4)

(1) Señalar el documento de la proposición que contiene información clasificada.
(2) Precisar que rubro o información del documento es sujeto de clasificación por contener información reservada o confidencial.
(3) Indicar en qué artículos de la LGTAIP o demás disposiciones reglamentarias aplicables, fundamenta la clasificación de la información, ya sea reservada o confidencial.
(4) Indicar los motivos y/o razones por los cuales la información señalada debe ser considerada en alguno de los supuestos de clasificación.

(La o el licitante deberá de fundamentar y motivar cada uno los numerales de su propuesta administrativa-legal y/o técnica que considere información reservada y/o confidencial. Cabe señalar que de no clasificarse la información por parte de la o el licitante en los términos antes señalados, la información presentada como parte de su proposición administrativa – técnica – legal – económica tendrá tratamiento de información de carácter público, de conformidad con artículo 115 de la Ley General de Transparencia y Acceso a la Información Pública en vigor.

Nombre y Firma de la/el Representante Legal o persona física

Nota: Este escrito deberá ser presentado, preferentemente, en papel membretado de la o el licitante

ANEXO XIII
NOTA OCDE

Nota informativa para participantes de países miembros de la Organización para la Cooperación y el Desarrollo Económico (OCDE)

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

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

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

- La compatibilidad de nuestro marco jurídico con las disposiciones de la Convención.

- El conocimiento que tengan los sectores público y privado de las recomendaciones de la Convención.

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

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

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

Las **responsabilidades** del sector privado contemplan:

- **Las empresas**: adoptar esquemas preventivos como el establecimiento de códigos de conducta, de mejores prácticas corporativas (controles internos, monitoreo, información financiera pública, auditorías externas) y de mecanismos que prevengan el ofrecimiento y otorgamiento de recursos o bienes a servidores públicos, para obtener beneficios particulares o para la empresa.

- **Los contadores públicos**: realizar auditorías: no encubrir actividades ilícitas (doble contabilidad y transacciones indebidas, como asientos contables falsificados, informes financieros fraudulentos, transferencias sin autorización, acceso a los activos sin consentimiento de la gerencia); utilizar registros contables precisos; informar a los directivos sobre conductas ilegales.

- **Los abogados**: promover el cumplimiento y revisión de la Convención (imprimir el carácter vinculatorio entre ésta y la legislación nacional); impulsar los esquemas preventivos que deben adoptar las empresas.

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

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

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

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

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

"Artículo 222. Cometen el delito de cohecho:

I.- El servidor público que, por sí, o por interpósita persona solicite o reciba ilícitamente para sí o para otro, dinero o cualquier beneficio, o acepte una promesa, para hacer o dejar de realizar un acto propio de sus funciones inherentes a su empleo, cargo o comisión;

II.- El que dé, prometa o entregue cualquier beneficio a alguna de las personas que se mencionan en el artículo 212 de este Código, para que haga u omita un acto relacionado con sus funciones, a su empleo, cargo o comisión, y

III.- El legislador federal que, en el ejercicio de sus funciones o atribuciones, y en el marco del proceso de aprobación del presupuesto de egresos respectivo, gestione o solicite:

a) La asignación de recursos a favor de un ente público, exigiendo u obteniendo, para sí o para un tercero, una comisión, dádiva o contraprestación, en dinero o en especie, distinta a la que le corresponde por el ejercicio de su encargo;

b) El otorgamiento de contratos de obra pública o de servicios a favor de determinadas personas físicas o morales.

Se aplicará la misma pena a cualquier persona que gestione, solicite a nombre o en representación del legislador federal las asignaciones de recursos u otorgamiento de contratos a que se refieren los incisos a) y b) de este artículo.

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

Cuando la cantidad o el valor de la dádiva, de los bienes o la promesa no exceda del equivalente de quinientas veces el valor diario de la Unidad de Medida y Actualización en el momento de cometerse el delito, o no sea valuable, se impondrán de tres meses a dos años de prisión y de treinta a cien días multa.

Cuando la cantidad o el valor de la dádiva, los bienes, promesa o prestación exceda de quinientas veces el valor diario de la Unidad de Medida y Actualización en el momento de cometerse el delito, se impondrán de dos a catorce años de prisión y de cien a ciento cincuenta días multa.

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

"Capítulo XI

Cohecho a servidores públicos extranjeros

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

I. A un servidor público extranjero, en su beneficio o el de un tercero, para que dicho servidor público gestione o se abstenga de gestionar la tramitación o resolución de asuntos relacionados con las funciones inherentes a su empleo, cargo o comisión;

II. A un servidor público extranjero, en su beneficio o el de un tercero, para que dicho servidor público gestione la tramitación o resolución de cualquier asunto que se encuentre fuera del ámbito de las funciones inherentes a su empleo, cargo o comisión, o

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

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

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

ANEXO XIV
PROPUESTA ECONÓMICA

LOTERÍA NACIONAL
AVENIDA INSURGENTES SUR No. 1397,
COLONIA INSURGENTES MIXCOAC,
DEMARCACIÓN BENITO JUÁREZ,
C.P. 03920, CIUDAD DE MÉXICO
P R E S E N T E

PROPUESTA DE COTIZACIÓN

COMPONENTES DE SERVICIO DE FASE INICIAL (120 DÍAS NATURALES MÁXIMO A PARTIR DE LA NOTIFICACIÓN DEL FALLO)			
CONCEPTO	CANTIDAD EN MESES	COSTO MENSUAL	COSTO TOTAL
i. Centro de Detección, Análisis y Respuesta Gestionada (MDR) **. Fase Inicial**	4		
		SUBTOTAL	
		IVA	
		COSTO TOTAL (FASE INICIAL)	

COMPONENTES DE SERVICIO DE FASE INICIAL (120 DÍAS NATURALES MÁXIMO A PARTIR DE LA NOTIFICACIÓN DEL FALLO)									
CONCEPTO	UNIDAD DE MEDIDA	CANTIDAD MINIMA MENSUAL	CANTIDAD MAXIMA MENSUAL	COSTO UNITARIO MENSUAL	COSTO MÍNIMO MENSUAL	COSTO MÁXIMO MENSUAL	CANTIDAD EN MESES	SUBTOTAL MÍNIMO	SUBTOTAL MÁXIMO
ii. Protección de Información en Correo Electrónico. **Fase Inicial**	Buzones	520	1300				4		
iii. Visibilidad y Monitoreo de los Usuarios. **Fase Inicial**	Usuarios	520	1300				4		
iv. Segmentación Zero Trust. **Fase Inicial**	Equipos	12	30				4		
v. Protección de Endpoint	Equipos	520	1300				4		

de siguiente generación (EDR). **Fase Inicial**									
vi. Entorno de ataque cambiante (EAC). **Fase Inicial**	Equipos	520	1300				4		
vii. Servicio de Firewall de Siguiente Generación. **Fase Inicial**	Equipos	5	12				4		
				SUBTOTAL					
				IVA					
				TOTAL					

COMPONENTES DE SERVICIOS PERMANENTES. FASE OPERATIVA			
CONCEPTO	**CANTIDAD EN MESES**	**COSTO MENSUAL**	**SUBTOTAL**
SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA			
viii. Centro de Detección, Análisis y Respuesta Gestionada (MDR). **Fase Operativa**	20		
		SUBTOTAL	
		IVA	
		COSTO TOTAL (VIGENCIA DEL CONTRATO)	

COMPONENTES DE SERVICIOS BAJO DEMANDA. FASE OPERATIVA									
CONCEPTO	UNIDAD DE MEDIDA	CANTIDAD MINIMA MENSUAL	CANTIDAD MAXIMA MENSUAL	COSTO UNITARIO MENSUAL	COSTO MÍNIMO MENSUAL	COSTO MÁXIMO MENSUAL	CANTIDAD EN MESES	SUBTOTAL MÍNIMO	SUBTOTAL MÁXIMO
ix. Protección de Información en Correo Electrónico. **Fase Operativa**	Buzones	200	1300				20		
x. Visibilidad y Monitoreo de los Usuarios. **Fase Operativa**	Usuarios	200	1300				20		
xi. Segmentación Zero Trust. **Fase Operativa**	Equipos	10	1000				20		
xii. Protección de Endpoint de siguiente generación (EDR). **Fase Operativa**	Equipos	200	1300				20		
xiii. Entorno de ataque cambiante (EAC). **Fase Operativa**	Equipos	200	1300				20		
xiv. Servicio de Diagnóstico y reparación de configuraciones erróneas. **Fase Operativa**	Equipos	200	1300				20		
xv. Servicio de autenticación multifactor (MFA). **Fase Operativa**	Usuarios	200	1300				20		
xvi. Servicio de Firewall de Siguiente Generación. **TIPO 1** Fase Operativa	Equipos	4	12				20		
xvii. Servicio de Firewall de Siguiente Generación. **TIPO 2.** Fase Operativa	Equipos	5	12				20		
				SUBTOTAL					
				IVA					
				TOTAL					

	COMPONENTES DE SERVICIO BAJO DEMANDA. FASE OPERATIVA					
CONCEPTO	**UNIDAD DE MEDIDA**	**CANTIDAD MINIMA**	**CANTIDAD MAXIMA**	**COSTO UNITARIO**	**SUBTOTAL MÍNIMO**	**SUBTOTAL MÁXIMO**
i. Servicio de Protección a Aplicaciones Móviles*	Apps	1	25			
				SUBTOTAL		
				IVA		
				COSTO TOTAL (VIGENCIA DEL CONTRATO)		

*Este servicio se pagará por evento, una vez concluido cada uno de los servicios de protección a aplicaciones móviles.

CUADRO RESUMEN
Anotar en el siguiente recuadro los montos mínimos y máximos totales durante la vigencia del contrato

CONCEPTO	SUBTOTAL MÍNIMO	SUBTOTAL MÁXIMO
i. Centro de Detección, Análisis y Respuesta Gestionada (MDR) **. Fase Inicial**		
ii. Protección de Información en Correo Electrónico. **Fase Inicial**		
iii. Visibilidad y Monitoreo de los Usuarios. **Fase Inicial**		
iv. Segmentación Zero Trust. **Fase Inicial**		
v. Protección de Endpoint de siguiente generación (EDR). **Fase Inicial**		
vi. Entorno de ataque cambiante (EAC). **Fase Inicial**		
vii. Servicio de Firewall de Siguiente Generación. **Fase Inicial**		
viii. Centro de Detección, Análisis y Respuesta Gestionada (MDR). **Fase Operativa**		
ix. Protección de Información en Correo Electrónico. **Fase Operativa**		
x. Visibilidad y Monitoreo de los Usuarios. **Fase Operativa**		
xi. Segmentación Zero Trust. **Fase Operativa**		
xii. Protección de Endpoint de siguiente generación (EDR). **Fase Operativa**		
xiii. Entorno de ataque cambiante (EAC). **Fase Operativa**		
xiv. Servicio de Diagnóstico y reparación de configuraciones erróneas. **Fase Operativa**		
xv. Servicio de autenticación multifactor (MFA). **Fase Operativa**		
xvi. Servicio de Firewall de Siguiente Generación. **TIPO 1. Fase Operativa**		
vii. Servicio de Firewall de Siguiente Generación. **TIPO 2. Fase Operativa**		
viii. Servicio de Protección a Aplicaciones Móviles		
SUBTOTAL		
IVA		
TOTAL		

Para garantizar la integración, eficiencia y calidad en la prestación del servicio, todos los componentes del servicio bajo demanda deberán estar integrados al Centro de Detección, Análisis y Respuesta Gestionada (MDR). "LOTERÍA" pagará únicamente la cantidad de licencias/agentes efectivamente desplegados y reportados en la consola central durante el mes devengado.

La propuesta económica deberá cumplir con lo siguiente:

A. Señalar el número del presente procedimiento.

B. Fecha de emisión de la propuesta económica, misma que deberá ser entre el periodo comprendido entre la fecha de la conclusión de la última Junta de Aclaraciones y la fecha del Acta de Presentación y Apertura de Proposiciones.

C. Se deberá cotizar en moneda nacional y a dos decimales.

D. Deberá cotizar el precio unitario de cada uno de los conceptos indicados del servicio objeto de la presente Licitación, sin IVA, establecer el importe, subtotal, IVA y total; así mismo deberá de requisitar el cuadro resumen, para lo cual podrá utilizar el **Anexo XIV**.

E. La vigencia de la cotización será de 60 (sesenta) días naturales; Los precios serán fijos durante la vigencia del contrato, así como su conformidad a las condiciones de pago establecidas en el Anexo Técnico, aceptando que en caso de que la Secretaría Anticorrupción y Buen Gobierno, derivado de una inconformidad, decrete la suspensión del procedimiento, la proposición enviada permanecerá vigente.

F. Deberá Indicar que los precios serán fijos durante la vigencia del contrato.

G. Manifestar su conformidad con las condiciones de pago establecidas en esta convocatoria.

H. Folio en la propuesta económica.

Lugar y fecha
Representante Legal DEL LICITANTE

_____
Nombre y Firma

APARTADO A

"COMPONENTES DE SEGURIDAD CON LOS QUE CUENTA "LOTERÍA""

Soluciones Licenciadas y componentes con los que cuenta Lotería Nacional.

DESCRIPCIÓN	CANTIDAD	TIPO O MARCA
Licenciamiento de la solución de protección de correo electrónico, Trend Micro Email Security	1080	**SaaS**
TrendAI - Cyber Risk Exposure Management (CREM) - Essentials	1	**SaaS**
TrendAI - Zero Trust Secure Access - Private Access	100	**SaaS**
TrendAI - Endpoint Security (Pro)	300	**SaaS**
TrendAI - Endpoint Security (Essentials)	1100	**SaaS**
TrendAI - XDR for Endpoints (EDR),	1800	**SaaS**
Entorno de ataque cambiante (EAC)	1296	**SaaS**
Gateway Insurgentes	1	**Pc | Dell modelo optiplex 9020**
Gateway Reforma	1	**Pc | Dell modelo optiplex 9020**
Proxy, Centro de datos Triara, Apodaca N.L.	1	**Server | virtualizado**
Unidad de almacenamiento, 40 TB	1	**DellEMC storage SCv2020**
Unidad de procesamiento, Server	1	**DellEMC Power Edge R450 | Tag GSDYPR3**
Servidor PRTG	1	**HP Proliat DL380 G6 | TAG HPF0G24**

Los servicios, están en modalidad **SaaS**, no obstante Lotería cuenta con equipos habilitados como Gateway para la integración de servicios a las plataformas de monitoreo, uno por cada sede, reforma e insurgentes y un equipo más como proxy para eficientar los tiempos de respuesta y no saturación de anchos de banda para la conexión con las plataformas **SaaS** de monitoreo de servidores (TrendAI - Endpoint Security (Pro)).

Para el caso de los equipos DellEMC, y en caso de considerar el uso de esta infraestructura, la misma deberá habilitarse considerando cableado de comunicación entre los activos involucrados y la configuración de dichos activos.

Firewalls

OFICINA	TIPO	MODELO	SERIE
SUBDIRECCIÓN SURESTE, Mérida	2	Fortinet FortiWiFi 40F	FWF40FTK22005583
SUBDIRECCIÓN PACIFICO, Hermosillo	2	Fortinet FortiWiFi 40F	FWF40FTK22005650
SUBDIRECCIÓN NORESTE, Monterrey	2	Fortinet FortiWiFi 40F	FWF40FTK22006325
SUBDIRECCIÓN OCCIDENTE, Guadalajara	2	Fortinet FortiWiFi 40F	FWF40FTK22005692
SUBDIRECCIÓN NORTE, Chihuahua	2	Fortinet FortiWiFi 40F	FWF40FTK22006079
SUBDIRECCIÓN SUR, Veracruz	2	Fortinet FortiWiFi 40F	FWF40FTK22005807
EDIFICIO CONTRERAS	2	*Fortinet FortiWiFi 60	FWF60FTK23003080
EDIFICIO EDISON, OFICINAS CENTRALES	1	FortiGate 1500D	FG1K5DT918801433
	1		FE1K5DT918801544
EDIFICIO INSURGENTES, OFICINAS CENTRALES	1	FortiGate 1500D	FG1K5DT918801545
	1		FG1K5DT918801426
EDIFICIO JALISCO, OFICINAS CENTRALES	2	*N/A	N/A

ANEXO XV
ACUSE DE RECEPCIÓN DE LA DOCUMENTACIÓN CONFORME A LOS NUMERALES 4.1, 4.2 Y 4.3 DE LA CONVOCATORIA

Partidas para las que participa:	
Licitación Pública:	
Razón Social del (los) Licitante(s):	
Fecha:	

NUMERAL 4.1. DOCUMENTACIÓN LEGAL-ADMINISTRATIVA

Inciso	Descripción	Presenta	No presenta	FOLIO
a)	Acreditamiento de Personalidad Jurídica. y datos de notificación. ANEXO II o III.			
b)	Acta constitutiva			
c)	Identificación Oficial.			
d)	Escrito de los supuestos establecidos en los artículos 71 y 90 cuarto párrafo de la Ley. Anexo IV			
e)	Escrito de Declaración de Integridad. Anexo V			
f)	Escrito de Nacionalidad. Anexo VI			
g)	Modelo de Convenio de Participación Conjunta.			
h)	Escrito de Aceptación de condiciones de la Plataforma. Anexo VII			
i)	Manifestación de vínculos. Anexo VIII			
j)	Manifestación de beneficios o ventajas. Anexo IX			
k)	Manifestación de subcontratación. Anexo X			
l)	Manifestación de Correo Electrónico			
m)	Escrito de estratificación de las micro, pequeñas y medianas empresas. Anexo XI			
n)	Información reservada y confidencial. Anexo XII			

NUMERAL 4.2. DOCUMENTACIÓN TÉCNICA

Inciso	Descripción	Presenta	No presenta	Folio
A	Propuesta Técnica en hoja membretada firmada por el Representante Legal en el que se describa ampliamente los (bienes y/o servicios) que ofrece, en concordancia con lo señalado en el presente Anexo Técnico, dando cumplimiento a todas y cada una de las especificaciones técnicas establecidas.			

Inciso	Descripción	Presenta	No presenta	Folio
B	Escrito en hoja membretada firmado por el Representante Legal, en el cual manifieste que cuentan con capacidad de respuesta inmediata, así como con los recursos técnicos, financieros y demás que sean necesarios, y cuyas actividades comerciales o profesionales estén relacionadas con la prestación del servicio, entrega de los bienes o arrendamiento. (ANEXO B).			
C	Escrito de no existencia de conflicto de interés: los licitantes deberán entregar dentro de su propuesta técnica escrito firmado por el representante legal manifestando la no existencia de conflicto de interés al no prestar o desarrollar servicios o bien de estar relacionado con una empresa o filial que actualmente preste o desarrolle servicios de operación y seguridad en las TIC's de "LOTERÍA"			
D	EL LICITANTE deberá presentar las siguientes cartas firmadas por el representante legal del fabricante de los productos que actualmente tiene Lotería Nacional, lo anterior, en apego a los artículos 54 y 55 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, toda vez que el área requirente verificó que estos requerimientos guardan relación directa con el objeto de la contratación y no limitan la libre participación, concurrencia o competencia económica. Derivado de la verificación efectuada por el área requirente, se determina que, por la naturaleza técnica, operativa y sensible de los servicios requeridos, resultan necesarias estos requisitos para que EL LICITANTE acredite contar con los conocimientos, habilidades y controles suficientes para garantizar la correcta prestación del servicio, la calidad en su ejecución y la protección de la información que sea tratada, procesada, almacenada o administrada con motivo del contrato. que oferte, donde cumpla con lo siguiente: • Nivel mínimo Expert para las licencias de Trend Micro propiedad de Lotería. • Nivel mínimo Advanced para los equipos Firewall Fortinet propiedad de Lotería. Aunado a lo anterior, deberá presentar: • Carta del representante legal del Fabricante, que es Socio de Negocio de las tecnologías ofertadas para dar cumplimiento a los servicios a ser implementados y que mientras se tenga licenciamiento y soporte vigente contarán con apoyo técnico del mismo en caso de ser requerido para los siguientes servicios: o Protección de Información en Correo Electrónico o Visibilidad y Monitoreo de los Usuarios o Segmentación Zero Trust o Protección de Endpoint de siguiente generación (EDR) o Entorno de ataque cambiante (EAC) o Servicio de Diagnóstico y Reparación de Configuraciones Erróneas o Servicio de Firewall de Siguiente Generación (NGFW) o Servicio de Protección a Aplicaciones Móviles o Servicio de Correlación de Eventos o Servicio de Orquestación, Automatización y Respuesta de Seguridad o Servicio de Ciberinteligencia			

Inciso	Descripción	Presenta	No presenta	Folio
	○ Gestión de vulnerabilidades para endpoints y servidores • Carta firmada por el representante legal del fabricante del producto ofertado indicando que cuentan con al menos el segundo nivel más alto de partner para los siguiente servicios: ○ Protección de Información en Correo Electrónico ○ Visibilidad y Monitoreo de los Usuarios ○ Segmentación Zero Trust ○ Protección de Endpoint de siguiente generación (EDR) ○ Entorno de ataque cambiante (EAC) ○ Servicio de Diagnóstico y Reparación de Configuraciones Erróneas ○ Servicio de Firewall de Siguiente Generación (NGFW) ○ Servicio de Protección a Aplicaciones Móviles ○ Servicio de Correlación de Eventos ○ Servicio de Orquestación, Automatización y Respuesta de Seguridad ○ Servicio de Ciberinteligencia			
E	Copia de los certificados vigentes a nombre DEL LICITANTE, los cuales deberán ser emitidos por una autoridad certificadora reconocida y avalada para la emisión de certificaciones en las normas ISO ISO/IEC 27001:2022, ISO/IEC 20000-1:2018, ISO 22301:2019, ISO 9001:2015 e ISO 37001:2016			
F	EL LICITANTE deberá presentar una carta, en papel membretado y firmada por su representante legal donde especifique lo siguiente: ➢ Que cualquier software, marca y/o patente de algún sistema, aplicativo o programa que sea utilizado para la prestación del servicio objeto de la presente licitación, ha sido adquirido y/o se encuentra licenciado debidamente, cumpliendo con todas las disposiciones legales pertinentes en México. ➢ Que, en caso de infracción o reclamación relacionada con derechos de autor, marcas, patentes o cualquier otro derecho de propiedad intelectual vinculado con el software, sistemas, aplicativos o programas utilizados para la prestación del servicio, [Nombre de la Empresa o Licitante] se compromete a: a) Defender, indemnizar y mantener indemne a "LOTERÍA", contra cualquier reclamación, demanda, acción legal, daño, pérdida, costo o gasto, incluyendo honorarios legales, derivados de dicha infracción o reclamación. b) Tomar las medidas necesarias para garantizar la continuidad de la prestación del servicio a "LOTERÍA", sin que ello implique un costo adicional para la misma			
G.	Documentación que EL LICITANTE deberá presentar por cada uno de sus recursos humanos enlistados para el cumplimiento del subrubro "PERFIL REQUERIDO" del Anexo Técnico es la siguiente:			

Inciso	Descripción	Presenta	No presenta	Folio
	1) Currículum vitae que cumpla con el perfil y certificaciones solicitadas, el cual debe de incluir: • Nombre completo. • Escolaridad. • Años de experiencia. • Teléfono. • Correo electrónico. Descripción de certificado(s) requerido (s) en el ANEXO TÉCNICO. 1) Acreditar la relación laboral con "EL LICITANTE" presentando copia simple del último pago ante el IMSS y/o documento afiliatorio ante el IMSS, pudiendo testar información sensible. 2) Presentar copia simple de la identificación oficial vigente del personal propuesto			
H.	Currículo Empresarial donde se describen las actividades y los clientes de la empresa			
I.	"EL LICITANTE" deberá presentar al menos 3 contratos en copia simple, celebrados con Dependencias y/o Entidades Públicas o Sector Privado, demostrando experiencia mínima de 3 años en la prestación de servicios similares a los requeridos en el Anexo Técnico			

NUMERAL 4.3. DOCUMENTACIÓN ECONÓMICA

Inciso	Descripción	Presenta	No presenta	Folio
NUMERAL 4.3	**Propuesta económica**			

ANEXO XVI
ESCRITO DE MANIFIESTACIÓN 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.

(Lugar y fecha)_____, a _____ de _____de 2026.

Lotería Nacional
Subdirección General de Administración y Finanzas
Dirección de Recursos Materiales y Servicios Generales
Gerencia de Adquisiciones
Presente.

PROCEDIMIENTO No. _____

(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.

(PARA PERSONAS MORALES)

_____(Nombre de la/el Representante Legal)_____, 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.

_____

Nombre y Firma de la/el Representante Legal o persona física

ANEXO XVII
MODELO DE CONTRATO

MODELO DE CONTRATO PARA LA PRESTACIÓN DE SERVICIOS, LAASSP.

CONTRATO **(ABIERTO O CERRADO)** PARA LA PRESTACIÓN DE SERVICIOS DE **(DESCRIPCIÓN),** CON CARÁCTER **(NACIONAL / INTERNACIONAL BAJO COBERTURA DE LOS TRATADOS / INTERNACIONAL ABIERTA)** QUE CELEBRAN, POR UNA PARTE, EL EJECUTIVO FEDERAL POR CONDUCTO DE LA (NOMBRE DE LA DEPENDENCIA O ENTIDAD), EN LO SUCESIVO **"LA DEPENDENCIA O ENTIDAD",** REPRESENTADA POR **(NOMBRE DEL REPRESENTANTE DE LA DEPENDENCIA O ENTIDAD)**, EN SU CARÁCTER DE **(SEÑALAR CARGO DEL REPRESENTANTE)**, Y POR LA OTRA, (**NOMBRE DE LA PERSONA FÍSICA O RAZÓN SOCIAL DE LA PERSONA MORAL), (SI ES CONJUNTA MENCIONAR EL NOMBRE DE CADA UNO DE ELLOS)** EN LO SUCESIVO **"EL PRESTADOR DE SERVICIOS"**, (**SÓLO SI EL "EL PRESTADOR DE SERVICIOS" ES PERSONA MORAL MOSTRAR EL SIGUIENTE TEXTO):** REPRESENTADA POR (NOMBRE DEL REPRESENTANTE DE LA PERSONA FÍSICA O MORAL), EN SU CARÁCTER DE **(SEÑALAR EN SU CASO EL CARÁCTER DEL REPRESENTANTE:** APODERADO, REPRESENTANTE LEGAL, ADMINISTRADOR ÚNICO O PRESIDENTE DEL CONSEJO DE ADMINISTRACIÓN), (MENCIONAR CADA UNO DE LOS REPRESENTANTES DE LAS PERSONAS QUE DE MANERA CONJUNTA FORMALIZAN EL CONTRATO) A QUIENES DE MANERA CONJUNTA SE LES DENOMINARÁ **"LAS PARTES"**, AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

DECLARACIONES

1. **"LA DEPENDENCIA O ENTIDAD"** declara que:

I.1 Es una **"LA DEPENDENCIA O ENTIDAD"**, de conformidad con **(ORDENAMIENTO JURÍDICO EN LOS QUE SE REGULE SU EXISTENCIA),** cuya competencia y atribuciones se señalan en ___ **(NUMERAL Y ORDENAMIENTOS JURÍDICOS EN LOS QUE SE REGULEN SUS ATRIBUCIONES Y COMPETENCIAS)**.

I.2 Conforme a lo dispuesto por **(NUMERAL Y ORDENAMIENTO JURÍDICO EN EL QUE SE REGULEN SUS FACULTADES O INSTRUMENTO NOTARIAL EN EL QUE SE LE OTORGA LAS FACULTADES),** el C. (**NOMBRE Y CARGO DEL O LA REPRESENTANTE DE LA DEPENDENCIA O ENTIDAD**), es el servidor público que cuenta con facultades legales para celebrar el presente contrato, quien podrá ser sustituido en cualquier momento en su cargo o funciones, sin que, por ello, sea necesario celebrar un convenio modificatorio.

I.3 De conformidad con **(ORDENAMIENTO JURÍDICO EN EL QUE SE REGULEN SUS FACULTADES)** __ suscribe el presente instrumento el C.**(NOMBRE DEL ADMINISTRADOR DEL CONTRATO)**, (**SEÑALAR CARGO DEL ADMINISTRADOR DEL CONTRATO**), con R.F.C. **(INCORPORAR RFC)**, designado para dar seguimiento y verificar el cumplimiento de las obligaciones que deriven del objeto del presente contrato, quien podrá ser sustituido en cualquier momento, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, informando a **"EL PRESTADOR DE SERVICIOS"** para los efectos del presente contrato.

INSTRUCCIÓN: EN CASO DE REQUERIR QUE EL INSTRUMENTO JURÍDICO SEA FIRMADO POR MÁS SERVIDORES PÚBLICOS, SE DEBERÁ AGREGAR LA SIGUIENTE DECLARACIÓN TANTAS VECES FIRMANTES SEAN AÑADIDOS Y RECORRER LOS NUMERALES SUBSECUENTES.

I.4 De conformidad con **(ORDENAMIENTO JURÍDICO EN LOS QUE SE REGULEN SUS FACULTADES)** suscribe el presente instrumento el C. **(NOMBRE DEL FIRMANTE X)**, **(SEÑALAR CARGO DEL FIRMANTE X)**, R.F.C. **(INCORPORAR RFC DEL FIRMANTE X)**, facultado para **(INCORPORAR FACULTADES Y PARTICIPACIÓN EN EL CONTRATO).**

I.5 La adjudicación del presente contrato se realizó mediante el procedimiento de (**TIPO DE PROCEDIMIENTO**) de carácter **(INCORPORAR EL CARÁCTER DEL PROCEDIMIENTO)**, al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; **(CITAR LOS NUMERALES)** de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"LAASSP"**, y **(CITAR LOS NUMERALES)** de su Reglamento.

I.6 **"LA DEPENDENCIA O ENTIDAD"** cuenta con suficiencia presupuestaria otorgada mediante **(NÚMERO Y FECHA DE OFICIO),** emitido por la **_____**.

INSTRUCCIÓN: EN CASO DE QUE SE TRATE DE UN CONTRATO PLURIANUAL, SE DEBERÁ CONSIGNAR EL OFICIO DE AUTORIZACIÓN DE LA SHCP EN TÉRMINOS DEL ARTÍCULO 50 DE LA LEY FEDERAL DE PRESUPUESTO Y RESPONSABILIDAD HACENDARIA Y SU REGLAMENTO, COMO SIGUE:

La Secretaría de Hacienda y Crédito Público **(O EN SU CASO EL TITULAR DE LA ENTIDAD)** autorizó la plurianualidad mediante el oficio **(NÚMERO Y FECHA DE OFICIO)**.

INSTRUCCIÓN: SI LA CONTRATACIÓN ES PREVIA A LA AUTORIZACIÓN DE SU PRESUPUESTO, CONFORME AL ARTÍCULO 33, PÁRRAFO SEGUNDO DE LA LAASSP (ANTICIPADA) MOSTRAR EL SIGUIENTE TEXTO:

En caso de que se trate de una contratación cuya vigencia inicie en el ejercicio fiscal siguiente de aquél en que se formalice, se deberá consignar el oficio de autorización de la Secretaría de Hacienda y Crédito Público en términos de los artículos 35 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria y 146 de su Reglamento.

I.7 Cuenta con el Registro Federal de Contribuyentes **N° (RFC DEPENDENCIA O ENTIDAD)**.

I.8 Tiene establecido su domicilio en _____ mismo que señala para los fines y efectos legales del presente contrato.

INSTRUCCIÓN: EN CASO DE QUE SE APLIQUE REDUCCIÓN DE GARANTÍA DE CUMPLIMIENTO INCORPORAR LA SIGUIENTE DECLARACIÓN:

I.9 De la revisión al historial de cumplimiento en materia de contrataciones en el Registro Único de Participantes, se advierte que **"EL PRESTADOR DE SERVICIOS"** cuenta con un grado de cumplimiento **(INDICAR EL RANGO),** por lo que **"LA DEPENDENCIA O ENTIDAD"** determina procedente efectuar la reducción del monto de la garantía por un porcentaje de ___.

INSTRUCCIÓN: CUANDO LA PROPOSICIÓN GANADORA HAYA SIDO PRESENTADA EN FORMA CONJUNTA POR VARIAS PERSONAS, LAS DECLARACIONES SE DEBERÁN FORMULAR POR CADA UNO DE ELLOS, EN TÉRMINOS DEL ARTÍCULO 88 DEL REGLAMENTO DE LA LAASSP.

II. "EL PRESTADOR DE SERVICIOS" declara que **(TRATÁNDOSE DE PERSONA FÍSICA)**:

II. "EL PRESTADOR DE SERVICIOS" por conducto de su representante declara que **(TRATÁNDOSE DE PERSONA MORAL)**:

INSTRUCCIÓN: EN CASO DE PROPUESTAS CONJUNTAS, INCORPORAR A CADA UNO DE LOS PRESTADORES DE SERVICIO QUE LA INTEGRAN, EN TÉRMINOS DE LO SEÑALADO EN LOS NUMERALES II A III.1

INSTRUCCIÓN: SI ES PERSONA FÍSICA INCORPORAR LAS DECLARACIONES DE LOS NUMERALES II. Y II.1

II.1 Es una persona **física,** de nacionalidad _____lo que acredita con _____ **(EN EL CASO DE PERSONAS EXTRANJERAS DESCRIBIR EL DOCUMENTO)** _____, expedida por _____.

INSTRUCCIÓN: SI ES PERSONA MORAL, ATENDER A LAS DECLARACIONES DE LOS NUMERALES II2 A II.2

II.2 Es una persona **moral** legalmente constituida mediante **_____ (DESCRIBIR EL INSTRUMENTO PÚBLICO QUE LE DAN ORIGEN Y EN SU CASO LAS MODIFICACIONES QUE SE HUBIERAN REALIZADO),** denominada **(NOMBRE O RAZÓN SOCIAL)**, cuyo objeto social es **_____**, entre otros, **(OBJETO SOCIAL)**, inscrita en el Registro Público de la Propiedad de **_____** con el folio **_____** de fecha **_____**.

II.2 La o el C. **(NOMBRE DEL REPRESENTANTE LEGAL)**, en su carácter de **_____**, cuenta con facultades suficientes para suscribir el presente contrato y obligar a su representada, como lo acredita con **(INSTRUMENTO NOTARIAL DE CONSTITUCIÓN O PODER OTORGADO AL REPRESENTANTE LEGAL)**, mismo que bajo protesta de decir verdad manifiesta no le ha sido limitado ni revocado en forma alguna.

INSTRUCCIÓN: EN EL CASO DE PERSONAS DE NACIONALIDAD EXTRANJERA, DEBERÁN PRESENTAR LA DOCUMENTACIÓN CORRESPONDIENTE DEBIDAMENTE APOSTILLADA.

II.3 Reúne las condiciones técnicas, jurídicas y económicas, y cuenta con la organización y elementos necesarios para su cumplimiento.

II.4 Cuenta con su Registro Federal de Contribuyentes **(RFC DEL PRESTADOR DE SERVICIOS).**

II.5 Acredita el cumplimiento de sus obligaciones fiscales en términos de lo dispuesto en el artículo 32-D del Código Fiscal de la Federación vigente, incluyendo las de Aportaciones Patronales y Entero de Descuentos, ante el Instituto del Fondo Nacional de la Vivienda para los Trabajadores y las de Seguridad Social ante el Instituto Mexicano del Seguro Social, conforme a las Opiniones de Cumplimiento de Obligaciones Fiscales emitidas por el SAT, INFONAVIT e IMSS, respectivamente.

II.6 Tiene establecido su domicilio en _____ mismo que señala para los fines y efectos legales del presente contrato.

III. De "LAS PARTES":

III.1 Que es su voluntad celebrar el presente contrato y sujetarse a sus términos y condiciones, por lo que de común acuerdo se obligan de conformidad con las siguientes:

CLÁUSULAS

PRIMERA. OBJETO DEL CONTRATO.

"EL PRESTADOR DE SERVICIOS" acepta y se obliga a proporcionar a **"LA DEPENDENCIA O ENTIDAD"** la prestación del servicio de **(DESCRIPCIÓN PORMENORIZADA)**, en los términos y condiciones establecidos en la **(CONVOCATORIA, INVITACIÓN O SOLICITUD DE COTIZACIÓN, SEGÚN EL PROCEDIMIENTO DE CONTRATACIÓN)**, este contrato y sus anexos **(NUMERAR Y DESCRIBIR LOS ANEXOS)** que forman parte integrante del mismo.

SEGUNDA. MONTO DEL CONTRATO.

INSTRUCCIÓN: TRATÁNDOSE DE CONTRATO CERRADO Y ANUAL, MOSTRAR EL SIGUIENTE PÁRRAFO:

"LA DEPENDENCIA O ENTIDAD" pagará a **"EL PRESTADOR DE SERVICIOS"** como contraprestación por los servicios objeto de este contrato, la cantidad de $ **(MONTO TOTAL DEL CONTRATO SIN IMPUESTOS)** más impuestos que asciende a $ **(IMPUESTOS),** que hace un total de **(MONTO TOTAL CON IMPUESTOS).**

INSTRUCCIÓN: EN CASO DE SER CERRADO Y PLURIANUAL, MOSTRAR LA TABLA Y LOS DOS PÁRRAFOS SIGUIENTES:

"LA DEPENDENCIA O ENTIDAD" conviene con **"EL PRESTADOR DE SERVICIOS"** que el monto total de los servicios es por la cantidad de **$ (MONTO TOTAL DEL CONTRATO SIN IMPUESTOS)** más impuestos que asciende a $ **(IMPUESTOS),** lo que hace un total de **(MONTO TOTAL CON IMPUESTOS)** importe que se cubrirá en cada uno de los ejercicios fiscales, de acuerdo a lo siguiente:

Ejercicio Fiscal	Monto sin impuestos	Monto con impuestos
(INCORPORAR EJERCICIO FISCAL)	(MONTO SIN IMPUESTOS DEL EJERCICIO)	(MONTO CON IMPUESTOS DEL EJERCICIO)
Se agregarán tantos se hayan programado		
TOTAL:	$(MONTO TOTAL SIN IMPUESTOS)	(MONTO TOTAL CON IMPUESTOS)

Las partes convienen expresamente que las obligaciones de este contrato, cuyo cumplimiento se encuentra previsto realizar durante los ejercicios fiscales de **(CONCATENAR EJERCICIOS FISCALES QUE INVOLUCRAN LA PLURIANUALIDAD)** quedarán sujetas para fines de su ejecución y pago a la disponibilidad presupuestaria, con que cuente **"LA DEPENDENCIA O ENTIDAD"**, conforme al Presupuesto de Egresos de la Federación que para el ejercicio fiscal correspondiente apruebe la Cámara de Diputados del H. Congreso de la Unión, sin que la no realización de la referida condición suspensiva origine responsabilidad para alguna de las partes.

INSTRUCCIÓN: LOS MONTOS Y PRECIOS SE PODRÁN INDICAR EN MONEDA EXTRANJERA, CUANDO ASÍ SE HAYA DETERMINADO EN LA CONVOCATORIA, INVITACIÓN, O SOLICITUD DE COTIZACIÓN, DE CONFORMIDAD CON EL ARTÍCULO 66, FRACCIÓN XIII DE LA LAASSP.

El(los) precio(s) unitario(s) del presente contrato, expresado(s) en moneda nacional es(son):

Partida	**Descripción ***	**Unidad***	**Cantidad ***	**Precio unitario ***	**Precio total antes de imp. ***	**Precio total después de imp. ***

INSTRUCCIÓN: INDICAR EL ANEXO CORRESPONDIENTE

El precio unitario es considerado fijo y en (**TIPO DE MONEDA**) hasta que concluya la relación contractual que se formaliza, incluyendo todos los conceptos y costos involucrados en la prestación del servicio de **(DESCRIPCIÓN),** por lo que **"EL PRESTADOR DE SERVICIOS"** no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

INSTRUCCIÓN: EN CASO DE QUE SE HAYA PREVISTO VARIACIÓN DE PRECIOS, Y SE CUENTE CON UNA FÓRMULA O MECANISMO DE AJUSTE SE CONSIDERARÁ LA SIGUIENTE REDACCIÓN:

El precio unitario será considerado en moneda nacional, y podrá ser modificado conforme a la siguiente: **(ESTABLECER LA FÓRMULA O MECANISMO DE AJUSTE PUBLICADA EN LA CONVOCATORIA, INVITACIÓN O SOLICITUD DE COTIZACIÓN).**

INSTRUCCIÓN: EN CASO DE SER ABIERTO Y ANUAL INCORPORAR EL SIGUIENTE PÁRRAFO:

"LA DEPENDENCIA O ENTIDAD" pagará a **"EL PRESTADOR DE SERVICIOS"** como contraprestación por los servicios objeto de este contrato, la cantidad mínima de **(MONTO MÍNIMO TOTAL DEL CONTRATO)** más impuestos por $_____ **(INDICAR LA CANTIDAD EN LETRA)** y un monto máximo de **(MONTO MÁXIMO TOTAL DEL CONTRATO),** más impuestos que asciende a $_____ **(INDICAR LA CANTIDAD EN LETRA).**

INSTRUCCIÓN: EN CASO DE SER PLURIANUAL ABIERTO, MOSTRAR LA TABLA Y LOS TRES PÁRRAFOS SIGUIENTES:

"LA DEPENDENCIA O ENTIDAD" conviene con **"EL PRESTADOR DE SERVICIOS"** que el **monto mínimo** de la prestación de servicios objeto del presente contrato para los ejercicios fiscales de **(CONCATENAR EJERCICIOS FISCALES QUE INVOLUCRAN LA PLURIANUALIDAD)** es por la cantidad de **(MONTO MÍNIMO TOTAL)** más impuestos que asciende a $_____ **(INDICAR LA CANTIDAD EN LETRA).**

Asimismo, que el **monto máximo** de los servicios para los ejercicios fiscales de **(CONCATENAR EJERCICIOS FISCALES QUE INVOLUCRAN LA PLURIANUALIDAD)** es por la cantidad de un monto máximo de **(MONTO MÁXIMO TOTAL DEL CONTRATO)**, más impuestos que asciende a $_____ **(INDICAR LA CANTIDAD EN LETRA)**.

Importes mínimos y máximos a pagar en cada ejercicio fiscal de acuerdo a lo siguiente:

Ejercicio Fiscal	Monto mínimo	Monto máximo

(INCORPORAR EJERCICIO FISCAL)	(MONTO MÍNIMO ANUAL SIN IMPUESTOS)	(MONTO MÁXIMO ANUAL SIN IMPUESTOS)
Se agregarán tantos se hayan programado		
TOTAL SIN IMPUESTOS:	(MONTO MÍNIMO TOTAL)	(MONTO MÁXIMO TOTAL DEL CONTRATO)

Las partes convienen expresamente que las obligaciones de este contrato, cuyo cumplimiento se encuentra previsto realizar durante los ejercicios fiscales de **(CONCATENAR EJERCICIOS FISCALES QUE INVOLUCRAN LA PLURIANUALIDAD)** quedarán sujetas para fines de su ejecución y pago a la disponibilidad presupuestaria, con que cuente **"LA DEPENDENCIA O ENTIDAD"**, conforme al Presupuesto de Egresos de la Federación que para el ejercicio fiscal correspondiente apruebe la Cámara de Diputados del H. Congreso de la Unión, sin que la no realización de la referida condición suspensiva origine responsabilidad para alguna de las partes.

INSTRUCCIÓN: LOS MONTOS Y PRECIOS SE PODRÁN INDICAR EN MONEDA EXTRANJERA, CUANDO ASÍ SE HAYA DETERMINADO EN LA CONVOCATORIA, INVITACIÓN, O SOLICITUD DE COTIZACIÓN, DE CONFORMIDAD CON EL ARTÍCULO 66, FRACCIÓN XIII DE LA LAASSP.

INSTRUCCIÓN: INDICAR EL(LOS) PRECIO(S) UNITARIO(S):

El(los) precio(s) unitario(s) del presente contrato, expresado(s) en **(TIPO DE MONEDA)** es (son):

Partida	Descripción *	Unidad *	Precio unitario *	Cantidad Mínima *	Cantidad Máxima *	Precio Total Mínimo *	Precio Total Máximo *

INSTRUCCIÓN: INDICAR EL ANEXO CORRESPONDIENTE

El precio unitario es considerado fijo y en **(TIPO DE MONEDA)** hasta que concluya la relación contractual que se formaliza, incluyendo todos los conceptos y costos involucrados en la prestación del servicio de **(DESCRIPCIÓN PORMENORIZADA DE LOS SERVICIOS A PRESTAR)**, por lo que **"EL PRESTADOR DE SERVICIOS"** no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

INSTRUCCIÓN: EN CASO QUE SE HAYA PREVISTO VARIACIÓN DE PRECIOS, Y SE CUENTE CON UNA FÓRMULA O MECANISMO DE AJUSTE SE CONSIDERARÁ LA SIGUIENTE REDACCIÓN Y SE ELIMINARÁ EL PÁRRAFO ANTERIOR:

El precio unitario será considerado en **(TIPO DE MONEDA)**, y podrá ser modificado conforme a la siguiente: **(ESTABLECER LA FÓRMULA O MECANISMO DE AJUSTE PUBLICADA EN LA CONVOCATORIA, INVITACIÓN O SOLICITUD DE COTIZACIÓN).**

INSTRUCCIÓN: EN EL CASO DE QUE LA PRESTACIÓN DEL SERVICIO REQUIERA DEL USO INTENSIVO DE MANO DE OBRA QUE IMPLIQUE UN COSTO SUPERIOR AL TREINTA POR CIENTO DEL MONTO TOTAL DEL CONTRATO, SE DEBERÁ INCLUIR ALGUNO DE LOS SIGUIENTES PÁRRAFOS:

"LA DEPENDENCIA O ENTIDAD" conviene con **"EL PRESTADOR DE SERVICIOS",** que se aplicará la siguiente fórmula **(ESTABLECER LA FÓRMULA PUBLICADA EN LA CONVOCATORIA, INVITACIÓN O SOLICITUD DE COTIZACIÓN),** cuando la prestación del servicio requiera de un uso intensivo de mano de obra que implique un costo superior al 30% (treinta por ciento) del monto total del contrato.

O BIEN

"LA DEPENDENCIA O ENTIDAD" conviene con **"EL PRESTADOR DE SERVICIOS",** que se aplicará el mecanismo de ajuste que reconozca el incremento a los salarios mínimos, cuando la prestación del servicio requiera de un uso intensivo de mano de obra que implique un costo superior al 30% (treinta por ciento) del monto total del contrato.

TERCERA. ANTICIPO.

INSTRUCCIÓN: SÓLO EN CASO DE QUE NO SE OTORGUE ANTICIPO, MOSTRAR EL SIGUIENTE TEXTO):

Para el presente contrato **"LA DEPENDENCIA O ENTIDAD"** no otorgará anticipo a **"EL PRESTADOR DE SERVICIOS".**

INSTRUCCIÓN: SÓLO EN CASO DE QUE SE OTORGUE ANTICIPO, MOSTRAR LO SIGUIENTE):

Se otorgará a **"EL PRESTADOR DE SERVICIOS",** un anticipo del _____ por ciento sobre el monto total del contrato equivalente a $**_____ (INDICAR LA CANTIDAD EN LETRA)** el cual se entregará en la siguiente fecha: _____.

Asimismo, la amortización del anticipo se llevará a cabo proporcionalmente en cada uno de los pagos conforme (**SEÑALAR LA FORMA EN QUE SE LLEVARÁ A CABO SU AMORTIZACIÓN**).

"EL PRESTADOR DE SERVICIOS" deberá amortizar el total del anticipo otorgado.

CUARTA. FORMA Y LUGAR DE PAGO.

"LA DEPENDENCIA O ENTIDAD" efectuará el pago a través de transferencia electrónica en pesos de los Estados Unidos Mexicanos, a mes vencido (otra temporalidad o calendario establecido) o porcentaje de avance (pagos progresivos), conforme a los servicios efectivamente prestados y a entera satisfacción del administrador del contrato y de acuerdo con lo establecido en el **"ANEXO _____"** que forma parte integrante de este contrato.

"LA DEPENDENCIA O ENTIDAD" realizará el pago en un plazo máximo de 17 (diecisiete) días hábiles siguientes, contados a partir del envío y verificación del Comprobante Fiscal Digital por Internet (CFDI) o factura electrónica a través de la Plataforma, y con la aceptación del Administrador del presente contrato, previa entrega de los bienes.

INSTRUCCIÓN: TRATÁNDOSE DE PRESTADORES DE SERVICIOS EXTRANJEROS, PRESENTAR LA FACTURA QUE SE EMITA CONFORME A LAS REGLAS DEL PAÍS DE ORIGEN.

El cómputo del plazo para realizar el pago se contabilizará a partir del día hábil siguiente de la aceptación del CFDI o factura electrónica, y ésta reúna los requisitos fiscales que establece la legislación en la materia, el desglose de los servicios prestados, los precios unitarios, se verifique su autenticidad, no existan aclaraciones al importe y vaya acompañada con la documentación soporte de la prestación de los servicios facturados.

De conformidad con el artículo 135, del Reglamento de la **"LAASSP"**, en caso de que el CFDI o factura electrónica entregado presente errores, el Administrador del presente contrato o a quien éste designe por escrito, dentro de los 3 (tres) días hábiles siguientes de su recepción, indicará a **"EL PRESTADOR DE SERVICIOS"** las deficiencias que deberá corregir; por lo que, el procedimiento de pago reiniciará en el momento en que **"EL PRESTADOR DE SERVICIOS"** presente el CFDI y/o documentos soporte corregidos y sean aceptados.

El tiempo que **"EL PRESTADOR DE SERVICIOS"** utilice para la corrección del CFDI y/o documentación soporte entregada, no se computará para efectos de pago, de acuerdo con lo establecido en el artículo 73 de la **"LAASSP"**.

El CFDI o factura electrónica deberá ser presentada a través de la Plataforma.

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

"EL PRESTADOR DE SERVICIOS" manifiesta su conformidad que, hasta en tanto no se cumpla con la verificación, supervisión y aceptación de la prestación de los servicios, no se tendrán como recibidos o aceptados por el Administrador del presente contrato.

Para efectos de trámite de pago, **"EL PRESTADOR DE SERVICIOS"** deberá ser titular de una cuenta bancaria, en la que se efectuará la transferencia electrónica de pago, respecto de la cual deberá proporcionar toda la información y documentación que le sea requerida por **"LA DEPENDENCIA O ENTIDAD"**.

"EL PRESTADOR DE SERVICIOS" deberá presentar la información y documentación **que "LA DEPENDENCIA O ENTIDAD"** le solicite para el trámite de pago, atendiendo a las disposiciones legales e internas de **"LA DEPENDENCIA O ENTIDAD"**.

El pago de la prestación de los servicios recibidos, quedará condicionado al pago que **"EL PRESTADOR DE SERVICIOS"** deba efectuar por concepto de penas convencionales y, en su caso, deductivas.

INSTRUCCIÓN: EN CASO DE PAGO EN MONEDA EXTRANJERA, INDICAR LA FUENTE OFICIAL QUE SE TOMARÁ PARA LLEVAR A CABO LA CONVERSIÓN Y LA TASA DE CAMBIO O LA FECHA A CONSIDERAR PARA HACERLO:

La fuente oficial para la conversión de la moneda extranjera será el Banco de México y la fecha a considerar será _____.

Para el caso que se presenten pagos en exceso, se estará a lo dispuesto por el artículo 73, párrafo tercero, de la **"LAASSP"**.

INSTRUCCIÓN: EN EL CASO DE QUE AÚN NO SEA POSIBLE ENVIAR LA FACTURA ELECTRÓNICA POR LA PLATAFORMA, LA DEPENDENCIA O ENTIDAD DEBERÁ SEÑALAR LA FORMA DE ENTREGA DE LA MISMA.

INSTRUCCIÓN: EN EL CASO DE QUE SE UTILICE EL PROGRAMA DE CADENAS PRODUCTIVAS, DEBERÁ SEÑALAR LO SIGUIENTE.

En virtud de que **"LA DEPENDENCIA O ENTIDAD"** está incorporada al programa de cadenas productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo, **"EL PRESTADOR DE SERVICIOS"** podrá transferir sus derechos de cobro a favor de un intermediario financiero que esté incorporado a la cadena productiva de **"LA DEPENDENCIA O ENTIDAD"** mediante operaciones de factoraje o descuento electrónico.

En caso de que **"EL PRESTADOR DE SERVICIOS"** decida utilizar el programa de cadenas productivas, el pago se realizará conforme a los procedimientos establecidos en las Disposiciones Generales a las que deberán sujetarse las dependencias y entidades de la Administración Pública Federal para su incorporación al programa de cadenas productivas de Nacional Financiera, S.N.C, Institución de Banca de Desarrollo.

QUINTA. LUGAR, PLAZOS Y CONDICIONES DE LA PRESTACIÓN DE LOS SERVICIOS.

La prestación de los servicios, se realizará conforme a los plazos, condiciones y entregables establecidos por **"LA DEPENDENCIA O ENTIDAD"** en el **(ESTABLECER EL DOCUMENTO O ANEXO DONDE SE ENCUENTRAN DICHOS PLAZOS, CONDICIONES Y ENTREGABLES O EN SU DEFECTO REDACTARLOS, LOS CUALES FORMAN PARTE DEL PRESENTE CONTRATO).**

Los servicios serán prestados en los domicilios señalados en el **(ESTABLECER EL DOCUMENTO O ANEXO DONDE SE ENCUENTRAN LOS DOMICILIOS, O EN SU DEFECTO REDACTARLOS)** y fechas establecidas en el mismo;

En los casos que derivado de la verificación se detecten defectos o discrepancias en la prestación del servicio o incumplimiento en las especificaciones técnicas, **"EL PRESTADOR DE SERVICIOS"** contará con un plazo de_____ para la reposición o corrección, contados a partir del momento de la notificación por correo electrónico y/o escrito, sin costo adicional para **"LA DEPENDENCIA O ENTIDAD"**.

SEXTA. VIGENCIA.

"LAS PARTES" convienen en que la vigencia del presente contrato será del **(INCORPORAR FECHA DE INICIO)** al (**INCORPORAR FECHA DE TÉRMINO DEL CONTRATO)**.

SÉPTIMA. MODIFICACIONES DEL CONTRATO.

"LAS PARTES" están de acuerdo que **"LA DEPENDENCIA O ENTIDAD"** por razones fundadas y explícitas podrá ampliar el monto o la cantidad de los servicios, de conformidad con el artículo 74 de la "LAASSP", siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) de los establecidos originalmente, el precio unitario sea igual al originalmente pactado y el contrato esté vigente. La modificación se formalizará mediante la celebración de un Convenio Modificatorio.

"LA DEPENDENCIA O ENTIDAD", podrá ampliar la vigencia del presente instrumento, siempre y cuando, no implique incremento del monto contratado o de la cantidad de los servicios solicitados, siendo necesario que se obtenga el previo consentimiento de **"EL PRESTADOR DE SERVICIOS".**

De presentarse caso fortuito o fuerza mayor, o por causas atribuibles a **"LA DEPENDENCIA O ENTIDAD"**, se podrá modificar el plazo del presente instrumento jurídico, debiendo acreditar dichos supuestos con las constancias respectivas. La modificación del plazo por caso fortuito o fuerza mayor podrá ser solicitada por cualquiera de **"LAS PARTES".**

En los supuestos previstos en el párrafo anterior, no procederá la aplicación de penas convencionales por atraso.

Cualquier modificación al presente contrato deberá formalizarse a través de la Plataforma, por el servidor público de **"LA DEPENDENCIA O ENTIDAD"** que lo haya hecho, o quien lo sustituya o esté facultado para ello, para lo cual **"EL PRESTADOR DE SERVICIOS"** realizará el ajuste respectivo de la garantía de cumplimiento, en términos del artículo 136, último párrafo del Reglamento de la **"LAASSP"**, salvo que por disposición legal se encuentre exceptuado de presentar garantía de cumplimiento.

"LA DEPENDENCIA O ENTIDAD" se abstendrá de hacer modificaciones que se refieran a precios, anticipos, pagos progresivos, especificaciones y, en general, cualquier cambio que implique otorgar condiciones más ventajosas a un prestador de servicios comparadas con las establecidas originalmente.

OCTAVA. GARANTÍA DE LOS SERVICIOS.

INSTRUCCIÓN: EN CASO DE QUE NO SE REQUIERA GARANTÍA SOBRE LA CALIDAD DEL SERVICIO, AÑADIR LO SIGUIENTE:

Para la prestación de los servicios materia del presente contrato, no se requiere que **"EL PRESTADOR DE SERVICIOS"** presente una garantía por la calidad de los servicios contratados.

INSTRUCCIÓN: EN CASO DE QUE SÍ SE REQUIERA GARANTÍA SOBRE LA CALIDAD DE LOS SERVICIOS, AÑADIR LO SIGUIENTE:

"EL PRESTADOR DE SERVICIOS" se obliga con **"LA DEPENDENCIA O ENTIDAD"** a entregar al inicio de la prestación del servicio, una garantía por la calidad de los servicios prestados, por **(INCORPORAR NUMERO DE MESES)** meses, la cual se constituirá **(INDICAR LA FORMA DE GARANTIZARLA)**, pudiendo ser mediante la póliza de garantía, en términos de los artículos 77 y 78 de la Ley Federal de Protección al Consumidor.

NOVENA. GARANTÍA(S).

INSTRUCCIÓN: EN CASO DE OTORGAR ANTICIPO, AÑADIR LO SIGUIENTE:

A) GARANTÍA DE ANTICIPO

"EL PRESTADOR DE SERVICIOS" entregará a **"LA DEPENDENCIA O ENTIDAD"**, previamente a la entrega del anticipo una garantía constituida por la totalidad del monto del(os) anticipo(s) recibido(s).

El otorgamiento de anticipo, deberá garantizarse en los términos de los artículos 69, de la **"LAASSP";** 126, fracción V, de su Reglamento.

Si las disposiciones jurídicas aplicables lo permiten, la entrega de la garantía de anticipo podrá realizarse de manera electrónica.

Una vez amortizado el cien por ciento del anticipo, el servidor público facultado por **"LA DEPENDENCIA O ENTIDAD"** procederá inmediatamente a extender la constancia de cumplimiento de dicha obligación contractual y dará inicio a los trámites para la cancelación de la garantía, lo que comunicará a **"EL PRESTADOR DE SERVICIOS".**

INSTRUCCIÓN: EN CASO DE QUE PROCEDA LA CONSTITUCIÓN DE LA GARANTÍA DE CUMPLIMIENTO DEL CONTRATO INCORPORAR LO SIGUIENTE:

B) CUMPLIMIENTO DEL CONTRATO.

Conforme a los artículos 69, párrafo primero, fracción II, 70, fracción (**SEÑALAR LA FRACCIÓN I EN EL CASO DE DEPENDENCIAS O II EN EL CASO DE ENTIDADES)**, de la **"LAASSP";** 130, párrafo tercero, fracción III, y 151 de su Reglamento **"EL PRESTADOR DE SERVICIOS"** se obliga a constituir una garantía **(EN CASO DE SER INDIVISIBLE) indivisible** por el cumplimiento fiel y exacto de todas las obligaciones derivadas de este contrato; **(EN CASO DE SER DIVISIBLE) divisible** y en este caso se hará efectiva en proporción al incumplimiento de la obligación principal, mediante fianza expedida por compañía afianzadora mexicana autorizada por la Comisión Nacional de Seguros y Fianzas, a favor de la **_(TESORERÍA DE LA FEDERACIÓN O DE LA ENTIDAD),** por un importe equivalente al **(INCORPORAR EL PORCENTAJE DE LA GARANTÍA DE CUMPLIMIENTO)** del monto total del contrato, sin incluir el IVA.

Dicha fianza deberá ser entregada a **"LA DEPENDENCIA O ENTIDAD"**, a más tardar dentro de los 10 días naturales posteriores a la firma del presente contrato.

Si las disposiciones jurídicas aplicables lo permiten, la entrega de la garantía de cumplimiento se podrá realizar de manera electrónica.

En caso de que **"EL PRESTADOR DE SERVICIOS"** incumpla con la entrega de la garantía en el plazo establecido, **"LA DEPENDENCIA O ENTIDAD"** podrá rescindir el contrato y dará vista al Órgano Interno de Control para que proceda en el ámbito de sus facultades.

La garantía de cumplimiento no será considerada como una limitante de responsabilidad de **"EL PRESTADOR DE SERVICIOS",** derivada de sus obligaciones y garantías estipuladas en el presente instrumento jurídico, y no impedirá que **"LA DEPENDENCIA O ENTIDAD"** reclame la indemnización por cualquier incumplimiento que pueda exceder el valor de la garantía de cumplimiento.

En caso de incremento al monto del presente instrumento jurídico o modificación al plazo, **"EL PRESTADOR DE SERVICIOS"** se obliga a entregar a **"LA DEPENDENCIA O ENTIDAD",** dentro de los 10 (diez días) naturales siguientes a la formalización del mismo, de conformidad con el último párrafo del artículo 136, del Reglamento de la **"LAASSP"**, los documentos modificatorios o endosos correspondientes, debiendo contener en el documento la estipulación de que se otorga de manera conjunta, solidaria e inseparable de la garantía otorgada inicialmente.

Cuando la contratación abarque más de un ejercicio fiscal, la garantía de cumplimiento del contrato, podrá ser por el porcentaje que corresponda del monto total por erogar en el ejercicio fiscal de que se trate, y deberá ser renovada por **"EL PRESTADOR DE SERVICIOS"** cada ejercicio fiscal por el monto que se ejercerá en el mismo, la cual deberá presentarse a **"LA DEPENDENCIA O ENTIDAD"** a más tardar dentro de los primeros diez días naturales del ejercicio fiscal que corresponda.

Una vez cumplidas las obligaciones a satisfacción, el Administrador del contrato, procederá inmediatamente a extender la constancia de cumplimiento de las obligaciones contractuales y dará inicio a los trámites para la cancelación de la garantía cumplimiento del contrato, lo que comunicará a **"EL PRESTADOR DE SERVICIOS".**

INSTRUCCIÓN: PARA EL CASO DE EXCEPTUAR LA GARANTÍA DE CUMPLIMIENTO POR TRATARSE DE SERVICIOS DE ASEGURAMIENTO, MOSTRAR EL PÁRRAFO SIGUIENTE:

Con fundamento en los artículos 15 y 294, fracción VI de la Ley de Instituciones de Seguros y Fianzas, **"EL PRESTADOR DE SERVICIOS"** se encuentra exceptuado de la presentación de la garantía de cumplimiento, ya que las aseguradoras no se encuentran obligadas a presentar una póliza de fianza que garantice el cumplimiento de sus contratos.

INSTRUCCIÓN: PARA EL CASO DE EXCEPTUAR LA GARANTÍA DE CUMPLIMIENTO CUANDO SE PRESTEN LOS SERVICIOS DENTRO DE LOS PRIMEROS 10 DÍAS NATURALES A LA FIRMA DEL CONTRATO, MOSTRAR EL PÁRRAFO SIGUIENTE:

Cuando la prestación de los servicios, se realice en un plazo menor a diez días naturales, **"EL PRESTADOR DE SERVICIOS"** quedará exceptuado de la presentación de la garantía de cumplimiento, de conformidad con lo establecido en el artículo 69 último párrafo de la **"LAASSP".**

La constancia de recepción de los servicios que ampare, que los mismos se prestaron dentro del plazo a que se refiere el párrafo anterior, se integrará en el expediente de contratación de la **"LA DEPENDENCIA O ENTIDAD"**.

En términos de lo establecido en el artículo 69, segundo párrafo de la **"LAASSP"** se exceptúa a **"EL PRESTADOR DE SERVICIOS"** de la presentación de la garantía de cumplimiento, ya que la contratación se fundamenta en **(UTILIZAR EL FUNDAMENTO REQUERIDO EN EL ARTÍCULO 54, FRACCIÓN _____O 55 DE LA "LAASSP")** y a la petición de exceptuar a **"EL PRESTADOR DE SERVICIOS"** de presentar la garantía del cumplimiento del contrato, formulada por el titular del área requirente de los servicios, en términos de las políticas bases y lineamientos de la dependencia o entidad**.**

INSTRUCCIÓN: EN EL CASO DE QUE, POR LA NATURALEZA DE LOS SERVICIOS, SE REQUIERA LA GARANTÍA PARA RESPONDER POR VICIOS OCULTOS, AÑADIR LO SIGUIENTE:

C) GARANTÍA PARA RESPONDER POR VICIOS OCULTOS.

"EL PRESTADOR DE SERVICIOS" deberá responder por los defectos, vicios ocultos y por la calidad de los servicios prestados, así como de cualquier otra responsabilidad en que hubiere incurrido, en los términos señalados en este contrato, convenios modificatorios respectivos y en la legislación aplicable, de conformidad con los artículos 75, párrafo segundo de la **"LAASSP"** y 142, párrafo tercero de su Reglamento.

"EL PRESTADOR DE SERVICIOS", quedará liberado de su obligación, una vez transcurridos **(INCORPORAR NUMERO DE MESES)**, contados a partir de la fecha en que conste por escrito la recepción física de los servicios prestados, siempre y cuando **"LA DEPENDENCIA O ENTIDAD"** no haya identificado defectos o vicios ocultos en la calidad de los servicios prestados, así como cualquier otra responsabilidad en los términos de este contrato y convenios modificatorios respectivos.

INSTRUCCIÓN: CUANDO LA GARANTÍA DE ANTICIPO, CUMPLIMIENTO O VICIOS OCULTOS SE PRESENTE A TRAVÉS DE UNA FIANZA, SE DEBERÁN OBSERVAR LOS MODELOS DE PÓLIZA DE FIANZAS CONSTITUIDAS COMO GARANTÍA EN LAS CONTRATACIONES PÚBLICAS REALIZADAS AL AMPARO DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO Y LA LEY DE OBRAS PÚBLICAS Y SERVICIOS RELACIONADOS CON LAS MISMAS, APROBADOS EN LAS DISPOSICIONES DE CARÁCTER GENERAL PUBLICADOS EN EL DIARIO OFICIAL DE LA FEDERACIÓN, EL 15 DE ABRIL DE 2022, QUE SE ENCUENTRA DISPONIBLE EN LA PLATAFORMA DIGITAL DE CONTRATACIONES PÚBLICAS DENOMINADA COMPRAS MX.

DÉCIMA. OBLIGACIONES DE "EL PRESTADOR DE SERVICIOS".

"EL PRESTADOR DE SERVICIOS", se obliga a:

- **a)** Prestar los servicios en las fechas o plazos y lugares establecidos conforme a lo pactado en el presente contrato y anexos respectivos.
- **b)** Cumplir con las especificaciones técnicas, de calidad y demás condiciones establecidas en el presente contrato y sus respectivos anexos.
- **c)** Asumir la responsabilidad de cualquier daño que llegue a ocasionar a **"LA DEPENDENCIA O ENTIDAD"** o a terceros con motivo de la ejecución y cumplimiento del presente contrato.
- **d)** Proporcionar la información que le sea requerida por la Secretaría Anticorrupción y Buen Gobierno y el Órgano Interno de Control, de conformidad con el artículo 156 del Reglamento de la **"LAASSP"**.
- **e)** Mantener al corriente sus obligaciones fiscales durante la vigencia del presente contrato INSTRUCCIÓN: EL SIGUIENTE INCISO, SERÁ OBLIGATORIO PARA EFECTOS DEL ARTÍCULO 125, PÁRRAFO CUARTO DEL REGLAMENTO DE LA **"LAASSP"**.
- **f)** Entregar bimestralmente, las constancias de cumplimiento de la inscripción y pago de cuotas al Instituto Mexicano del Seguro Social del personal que utilice para la prestación de los servicios.

INSTRUCCIÓN: EN CASO DE ESTIPULAR OBLIGACIONES ADICIONALES, AGREGAR LOS INCISOS QUE SE REQUIERAN

DÉCIMA PRIMERA. OBLIGACIONES DE "LA DEPENDENCIA O ENTIDAD".

"LA DEPENDENCIA O ENTIDAD", se obliga a:

- **a)** Otorgar las facilidades necesarias, a efecto de que **"EL PRESTADOR DE SERVICIOS"** lleve a cabo en los términos convenidos la prestación de los servicios objeto del contrato.

- **b)** Realizar el pago correspondiente en tiempo y forma.

INSTRUCCIÓN: EL SIGUIENTE PÁRRAFO APARECERÁ SIEMPRE QUE HAYA EXISTIDO GARANTÍA DE CUMPLIMIENTO.

c) Extender a **"EL PRESTADOR DE SERVICIOS"** por conducto del servidor público facultado, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa de dicho servidor público para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.

INSTRUCCIÓN: EN CASO DE ESTIPULAR OBLIGACIONES ADICIONALES, AGREGAR LOS INCISOS QUE SE REQUIERAN

DÉCIMA SEGUNDA. ADMINISTRACIÓN, VERIFICACIÓN, SUPERVISIÓN Y ACEPTACIÓN DE LOS SERVICIOS.

"LA DEPENDENCIA O ENTIDAD" designa como Administrador(es) del presente contrato a **(INCORPORAR NOMBRE DE LA, EL O LOS ADMINISTRADORES DEL CONTRATO), con RFC (INCORPORAR RFC), (INCORPORAR CARGO DEL ADMINISTRADOR DEL CONTRATO),** quien dará seguimiento y verificará el cumplimiento de los derechos y obligaciones establecidos en este instrumento.

Los servicios se tendrán por recibidos previa revisión del Administrador del presente contrato, la cual consistirá en la verificación del cumplimiento de las especificaciones establecidas y en su caso en los anexos respectivos, así como las contenidas en la propuesta técnica.

"LA DEPENDENCIA O ENTIDAD", a través del Administrador del contrato, rechazará los servicios, que no cumplan las especificaciones establecidas en este contrato y en sus Anexos, obligándose **"EL PRESTADOR DE SERVICIOS"** en este supuesto a realizarlos nuevamente bajo su responsabilidad y sin costo adicional para **"LA DEPENDENCIA O ENTIDAD",** sin perjuicio de la aplicación de las penas convencionales o deducciones al cobro correspondiente.

"LA DEPENDENCIA O ENTIDAD", a través del Administrador del contrato, podrá aceptar los servicios que incumplan de manera parcial o deficiente las especificaciones establecidas en este contrato y en los anexos respectivos, sin perjuicio de la aplicación de las deducciones al pago que procedan, y reposición del servicio, cuando la naturaleza propia de éstos lo permita.

DÉCIMA TERCERA. DEDUCCIONES.

"LA DEPENDENCIA O ENTIDAD" aplicará deducciones al pago por el incumplimiento parcial o deficiente, en que incurra **"EL PRESTADOR DE SERVICIOS"** conforme a lo estipulado en las cláusulas del presente contrato y sus anexos respectivos, las cuales se calcularán por un **(EN CASO DE EXISTIR SÓLO UN PORCENTAJE, SEÑALAR PORCENTAJE DE DEDUCTIVA)** % sobre el monto de los servicios, **(EN CASO DE ESTABLECER POR DIVERSOS CONCEPTOS DEDUCTIVAS REMITIR AL ANEXO CORRESPONDIENTE),** proporcionados en forma parcial o deficiente. Las cantidades a deducir se aplicarán en el CFDI o factura electrónica que **"EL PRESTADOR DE SERVICIOS"** presente para su cobro, en el pago que se encuentre en trámite o bien en el siguiente pago.

De no existir pagos pendientes, se requerirá a **"EL PRESTADOR DE SERVICIOS"** que realice el pago de la deductiva a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA´s), a favor de la Tesorería de la Federación, o de la Entidad. En caso de negativa se procederá a hacer efectiva la garantía de cumplimiento del contrato.

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

El cálculo de las deducciones correspondientes las realizará el Administrador del contrato de **"LA DEPENDENCIA O ENTIDAD",** cuyá notificación se realizará por escrito o vía correo electrónico, dentro de los **(DÍAS)** posteriores al incumplimiento parcial o deficiente.

DÉCIMA CUARTA. PENAS CONVENCIONALES.

En caso que **"EL PRESTADOR DE SERVICIOS"** incurra en atraso en el cumplimiento conforme a lo pactado para la prestación de los servicios, objeto del presente contrato, conforme a lo establecido en el Anexo (No.___) parte integral del presente contrato, **"LA DEPENDENCIA O ENTIDAD"** por conducto del Administrador del contrato aplicará la pena convencional equivalente al **(INCORPORAR PORCENTAJE DE PENA CONVENCIONAL)%, (EN CASO DE EXISTIR SÓLO UN PORCENTAJE O ESTABLECER DIVERSOS PORCENTAJES REMITIR AL ANEXO CORRESPONDIENTE)** por cada **(CALCULAR PERIODICIDAD DE PENA)** de atraso sobre la parte de los servicios no prestados, de conformidad con este instrumento legal y sus respectivos anexos.

El Administrador del contrato determinará el cálculo de la pena convencional, cuya notificación se realizará por escrito o vía correo electrónico, dentro de los **(DÍAS)** posteriores al atraso en el cumplimiento de la obligación de que se trate.

El pago de los servicios quedará condicionado, proporcionalmente, al pago que **"EL PRESTADOR DE SERVICIOS"** deba efectuar por concepto de penas convencionales por atraso; en el supuesto que el contrato sea rescindido en términos de lo previsto en la **CLÁUSULA VIGÉSIMA CUARTA DE RESCISIÓN**, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento del contrato.

El pago de la pena podrá efectuarse a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA´s), a favor de la Tesorería de la Federación, o la Entidad; o bien, a través de un comprobante de egreso (CFDI de Egreso) conocido comúnmente como Nota de Crédito, en el momento en el que emita el comprobante de Ingreso (Factura o CFDI de Ingreso) por concepto de los servicios, en términos de las disposiciones jurídicas aplicables.

El importe de la pena convencional, no podrá exceder el equivalente al monto total de la garantía de cumplimiento del contrato, y en el caso de no haberse requerido esta garantía, no deberá exceder del 20% (veinte por ciento) del monto total del contrato.

Cuando **"EL PRESTADOR DE SERVICIOS"** quede exceptuado de la presentación de la garantía de cumplimiento, en los supuestos previsto en la **"LAASSP"**, el monto máximo de las penas convencionales por atraso que se puede aplicar, será del 20% (veinte por ciento) del monto de los servicios prestados fuera de la fecha convenida, de conformidad con lo establecido en el artículo 142, cuarto párrafo del Reglamento de la **"LAASSP"**.

INSTRUCCIÓN: PARA EL CASO DE CONTRATACIONES CON CAMPESINOS O GRUPOS URBANOS MARGINADOS, COMO PERSONAS FÍSICAS O MORALES, COOPERATIVAS U ORGANISMOS DEL SECTOR SOCIAL DE LA ECONOMÍA CERTIFICADOS POR EL INSTITUTO NACIONAL DE LA ECONOMÍA SOCIAL, INCLUYENDO AQUELLOS CUYO OBJETO SEA LA INCLUSIÓN LABORAL DE MUJERES Y PERSONAS VULNERABLES, ASÍ COMO ALGUNA ORGANIZACIÓN CONSTITUIDA O CONFORMADA POR GRUPOS DE ATENCIÓN PRIORITARIA, AL AMPARO DEL ARTÍCULO 54, FRACCIÓN XI, DE LA LAASSP, EL ÁREA CONTRATANTE DEBERÁ CONSIDERAR QUE EL MONTO MÁXIMO DE LAS PENAS CONVENCIONALES POR ATRASO SERÁ DEL 10% (DIEZ POR CIENTO), CONFORME LO ESTABLECIDO EN EL ARTÍCULO 142, PÁRRAFO CUARTO DEL REGLAMENTO DE LA **"LAASSP".**

DÉCIMA QUINTA. LICENCIAS, AUTORIZACIONES Y PERMISOS.

"EL PRESTADOR DE SERVICIOS" se obliga a observar y mantener vigentes las licencias, autorizaciones, permisos o registros requeridos para el cumplimiento de sus obligaciones.

DÉCIMA SEXTA. PÓLIZA DE RESPONSABILIDAD CIVIL.

INSTRUCCIÓN: CUANDO NO SE REQUIERA LA CONTRATACIÓN DE SEGURO INCORPORAR EL SIGUIENTE PÁRRAFO:

Para la prestación de los servicios materia del presente contrato, no se requiere que **"EL PRESTADOR DE SERVICIOS"** contrate una póliza de seguro por responsabilidad civil.

INSTRUCCIÓN: CUANDO SE REQUIERA LA CONTRATACIÓN DE SEGURO INCORPORAR LOS SIGUIENTES DOS PÁRRAFOS:

"EL PRESTADOR DE SERVICIOS" se obliga a contratar una póliza de seguro por su cuenta y a su costa, expedida por una Institución Nacional de Seguros, debidamente autorizada, en la cual se incluya la cobertura de responsabilidad civil, que ampare los daños y perjuicios y que ocasione a los bienes y personal de **"LA DEPENDENCIA O ENTIDAD"**, así como, los que cause a terceros en sus bienes o personas, con motivo de la prestación del servicio materia del presente contrato.

La póliza deberá contener las siguientes coberturas:

INSTRUCCIÓN: DESCRIBIR LAS COBERTURAS, ATENDIENDO A LAS NECESIDADES, TIPO Y CARACTERÍSTICAS DEL SERVICIO

DÉCIMA SÉPTIMA. TRANSPORTE.

"EL PRESTADOR DE SERVICIOS" se obliga bajo su costa y riesgo, a trasportar los bienes e insumos necesarios para la prestación del servicio objeto de este contrato, desde su lugar de origen, hasta las

instalaciones señaladas en el **(ESTABLECER EL DOCUMENTO O ANEXO DONDE SE ENCUENTRAN LOS DOMICILIOS, O EN SU DEFECTO REDACTARLOS)** del presente contrato.

DÉCIMA OCTAVA. IMPUESTOS Y DERECHOS.

Los impuestos, derechos y gastos que procedan con motivo de la prestación de los servicios, objeto del presente contrato, serán pagados por **"EL PRESTADOR DE SERVICIOS"** mismos que no serán repercutidos a **"LA DEPENDENCIA O ENTIDAD"**.

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

DÉCIMA NOVENA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES.

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

Se exceptúa de lo anterior en el caso de fusión, escisión, o transformación de sociedades, siempre que la nueva sociedad que resulte cuente con la solvencia técnica, jurídica y económica exigidas al adjudicarse el contrato, cumpla con lo dispuesto en el Reglamento de la **"LAASSP"** y no se encuentre en los supuestos de impedimento previstos en la **"LAASSP"**.

VIGÉSIMA. DERECHOS DE AUTOR, PATENTES Y/O MARCAS.

"EL PRESTADOR DE SERVICIOS" será responsable en caso de infringir patentes, marcas o viole otros registros de derechos de propiedad industrial a nivel nacional e internacional, con motivo del cumplimiento de las obligaciones del presente contrato, por lo que se obliga a responder personal e ilimitadamente de los daños y perjuicios que pudiera causar a **"LA DEPENDENCIA O ENTIDAD"** o a terceros.

De presentarse alguna reclamación en contra de **"LA DEPENDENCIA O ENTIDAD"**, por cualquiera de las causas antes mencionadas, **"EL PRESTADOR DE SERVICIOS"** se obliga a salvaguardar los derechos e intereses de **"LA DEPENDENCIA O ENTIDAD"** de cualquier controversia, liberándola de toda responsabilidad de carácter civil, penal, mercantil, fiscal o de cualquier otra índole, sacándola en paz y a salvo.

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

VIGÉSIMA PRIMERA. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES.

"LAS PARTES" acuerdan que la información que se intercambie de conformidad con las disposiciones del presente instrumento, se tratarán de manera confidencial, siendo de uso exclusivo para la consecución del objeto del presente contrato y no podrá difundirse a terceros de conformidad con lo

establecido en las disposiciones vigentes en materia de transparencia y acceso a la información pública y de protección de datos personales.

Para el tratamiento de los datos personales que **"LAS PARTES"** recaben con motivo de la celebración del presente contrato, deberá de realizarse con base en lo previsto en los Avisos de Privacidad respectivos.

Por tal motivo, **"EL PRESTADOR DE SERVICIOS"** asume cualquier responsabilidad que se derive del incumplimiento de su parte, o de sus empleados, a las obligaciones de confidencialidad descritas en el presente contrato.

Asimismo **"EL PRESTADOR DE SERVICIOS"** deberá observar lo establecido en el Anexo aplicable a la Confidencialidad de la información del presente contrato.

VIGÉSIMA SEGUNDA. SUSPENSIÓN TEMPORAL DE LA PRESTACIÓN DE LOS SERVICIOS.

Con fundamento en el artículo 80 de la **"LAASSP"** y 150, fracción II, de su Reglamento, **"LA DEPENDENCIA O ENTIDAD"** en el supuesto de caso fortuito o de fuerza mayor o por causas que le resulten imputables, podrá suspender la prestación de los servicios, de manera temporal, quedando obligado a pagar a **"EL PRESTADOR DE SERVICIOS"** aquellos servicios que hubiesen sido efectivamente prestados, y en su caso, se reintegrarán los anticipos no amortizados, así como, al pago de gastos no recuperables previa solicitud y acreditamiento.

Una vez que hayan desaparecido las causas que motivaron la suspensión, el contrato podrá continuar produciendo todos sus efectos legales, si **"LA DEPENDENCIA O ENTIDAD"** así lo determina; y en caso que subsistan los supuestos que dieron origen a la suspensión, se podrá iniciar la terminación anticipada del contrato, conforme lo dispuesto en la cláusula siguiente.

VIGÉSIMA TERCERA. TERMINACIÓN ANTICIPADA DEL CONTRATO.

"LA DEPENDENCIA O ENTIDAD" cuando concurran razones de interés general, de común acuerdo o bien, cuando por causas justificadas se extinga la necesidad de requerir los servicios originalmente contratados y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas, se ocasionaría algún daño o perjuicio a **"LA DEPENDENCIA O ENTIDAD"**, o se determine la nulidad de los actos que dieron origen al presente contrato, con motivo de la resolución de una inconformidad o intervención de oficio, emitida por la Secretaría Anticorrupción y Buen Gobierno, podrá dar por terminado anticipadamente el presente contrato sin responsabilidad alguna para **"LA DEPENDENCIA O ENTIDAD"**, ello con independencia de lo establecido en la cláusula que antecede.

Cuando **"LA DEPENDENCIA O ENTIDAD"** determine dar por terminado anticipadamente el contrato, lo notificará a **"EL PRESTADOR DE SERVICIOS"** hasta con 30 (treinta) días naturales anteriores al hecho, debiendo sustentarlo en un dictamen que precise las razones o las causas justificadas que le dieron origen a la misma, una vez notificada la terminación anticipada, se extinguirá el contrato, lo que dará lugar a formalizar el finiquito entre las partes.

En el finiquito se harán constar los pagos que, en su caso, deba efectuar **"LA DEPENDENCIA O ENTIDAD"** por concepto de los servicios prestados hasta el momento de la terminación anticipada, además, en su caso, pactará en el mismo el reembolso al prestador de servicios

de los gastos no recuperables en que haya incurrido, siempre que estos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato.

VIGÉSIMA CUARTA. RESCISIÓN.

"LA DEPENDENCIA O ENTIDAD" podrá iniciar en cualquier momento el procedimiento de rescisión, cuando **"EL PRESTADOR DE SERVICIOS"** incurra en alguna de las siguientes causales:

a) Contravenir los términos pactados para la prestación de los servicios, establecidos en el presente contrato;
b) Transferir en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual;
c) Ceder los derechos de cobro derivados del contrato, sin contar con la conformidad previa y por escrito de **"LA DEPENDENCIA O ENTIDAD"**;
d) Suspender total o parcialmente y sin causa justificada la prestación de los servicios del presente contrato;
e) No realizar la prestación de los servicios en tiempo y forma conforme a lo establecido en el presente contrato y sus respectivos anexos;
f) No proporcionar a los Órganos de Fiscalización, la información que le sea requerida con motivo de las auditorías, visitas e inspecciones que realicen;
g) Ser declarado en concurso mercantil, o por cualquier otra causa distinta o análoga que afecte su patrimonio;
h) En caso de que compruebe la falsedad de alguna manifestación, información o documentación proporcionada para efecto del presente contrato;
i) No entregar dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato, la garantía de cumplimiento del mismo;
j) Cuando la suma de las penas convencionales exceda el monto total de la garantía de cumplimiento del contrato;
INSTRUCCIÓN: EL SIGUIENTE INCISO, SERÁ OBLIGATORIO PARA EFECTOS DEL ARTÍCULO 125, PÁRRAFO CUARTO DEL REGLAMENTO DE LA **"LAASSP"**.
k) No presentar bimestralmente, las constancias de la inscripción y pago de cuotas al Instituto Mexicano del Seguro Social del personal que utilice para la prestación de los servicios;

INSTRUCCIÓN: CUANDO NO SE HAYA REQUERIDO LA GARANTÍA DE CUMPLIMIENTO, SE UTILIZARÁ EL SIGUIENTE TEXTO: "En caso de que la suma de las penas convencionales exceda el 20% del monto total del contrato."

l) Cuando la suma de las deducciones al pago, excedan el límite máximo establecido para las deducciones;
m) Divulgar, transferir o utilizar la información que conozca en el desarrollo del cumplimiento del objeto del presente contrato, sin contar con la autorización de **"LA DEPENDENCIA O ENTIDAD"** en los términos de lo dispuesto en la **CLÁUSULA VIGÉSIMA PRIMERA DE CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES** del presente instrumento jurídico;
n) Impedir el desempeño normal de labores de **"LA DEPENDENCIA O ENTIDAD";**
o) Cambiar su nacionalidad por otra e invocar la protección de su gobierno contra reclamaciones y órdenes de **"LA DEPENDENCIA O ENTIDAD"**, cuando sea extranjero, y
p) No presentar la opinión favorable de sus obligaciones fiscales, cada **(ESTABLECER PERIODICIDAD)** durante la vigencia del presente contrato.
q) Incumplir cualquier obligación distinta de las anteriores y derivadas del presente contrato.

Para el caso de optar por la rescisión del contrato, **"LA DEPENDENCIA O ENTIDAD"** comunicará por escrito a **"EL PRESTADOR DE SERVICIOS"** el incumplimiento en que haya incurrido, para que en un término de 5 (cinco) días hábiles contados a partir del día siguiente de la notificación, exponga lo que a su derecho convenga y aporte en su caso las pruebas que estime pertinentes.

Transcurrido dicho término **"LA DEPENDENCIA O ENTIDAD"**, en un plazo de 10 (diez) días hábiles siguientes, tomando en consideración los argumentos y pruebas que hubiere hecho valer **"EL PRESTADOR DE SERVICIOS",** determinará de manera fundada y motivada dar o no por rescindido el contrato, y comunicará a **"EL PRESTADOR DE SERVICIOS"** dicha determinación dentro del citado plazo.

Cuando se rescinda el contrato, se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar **"LA DEPENDENCIA O ENTIDAD"** por concepto del contrato hasta el momento de rescisión, o los que resulten a cargo de **"EL PRESTADOR DE SERVICIOS".**

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

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

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

De no rescindirse el contrato, **"LA DEPENDENCIA O ENTIDAD"** establecerá con **"EL PRESTADOR DE SERVICIOS",** otro plazo, que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento, aplicando las sanciones correspondientes. El convenio modificatorio que al efecto se celebre deberá atender a las condiciones previstas por el artículo 74, párrafos cuarto y quinto de la **"LAASSP"**.

No obstante, de que se hubiere firmado el convenio modificatorio a que se refiere el párrafo anterior, si se presenta de nueva cuenta el incumplimiento, **"LA DEPENDENCIA O ENTIDAD"** quedará expresamente facultada para optar por exigir el cumplimiento del contrato, o rescindirlo, aplicando las sanciones que procedan.

Si se llevara a cabo la rescisión del contrato, y en el caso de que a **"EL PRESTADOR DE SERVICIOS"** se le hubieran entregado pagos en exceso, éste deberá de reintegrarlos más los intereses correspondientes, conforme a lo indicado en el artículo 73, párrafo cuarto, de la **"LAASSP"**.

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

VIGÉSIMA QUINTA. RELACIÓN Y EXCLUSIÓN LABORAL.

"EL PRESTADOR DE SERVICIOS" reconoce y acepta ser el único patrón de todos y cada uno de los trabajadores que intervienen en la prestación del servicio, deslindando de toda responsabilidad a **"LA DEPENDENCIA O ENTIDAD"** respecto de cualquier reclamo que en su caso puedan efectuar sus trabajadores, sea de índole laboral, fiscal o de seguridad social y en ningún caso se le podrá considerar patrón sustituto, patrón solidario, beneficiario o intermediario.

"EL PRESTADOR DE SERVICIOS" asume en forma total y exclusiva las obligaciones propias de patrón respecto de cualquier relación laboral, que el mismo contraiga con el personal que labore bajo sus órdenes o intervenga o contrate para la atención de los asuntos encomendados por **"LA DEPENDENCIA O ENTIDAD"**, así como en la ejecución de los servicios.

Para cualquier caso no previsto, **"EL PRESTADOR DE SERVICIOS"** exime expresamente a **"LA DEPENDENCIA O ENTIDAD"** de cualquier responsabilidad laboral, civil o penal o de cualquier otra especie que en su caso pudiera llegar a generarse, relacionado con el presente contrato.

Para el caso que, con posterioridad a la conclusión del presente contrato, **"LA DEPENDENCIA O ENTIDAD"** reciba una demanda laboral por parte de trabajadores de **"EL PRESTADOR DE SERVICIOS"** en la que se demande la solidaridad y/o sustitución patronal a **"LA DEPENDENCIA O ENTIDAD"**, **"EL PRESTADOR DE SERVICIOS"** queda obligado a dar cumplimiento a lo establecido en la presente cláusula.

VIGÉSIMA SEXTA. DISCREPANCIAS.

"LAS PARTES" convienen que, las estipulaciones que se establezcan en este contrato no deberán modificar las condiciones previstas en la convocatoria a la licitación, invitación o solicitud de cotización, y sus juntas de aclaraciones; en caso de discrepancia, prevalecerá lo estipulado en éstas, conforme a lo previsto en el artículo 66, párrafo segundo de la **"LAASSP"**.

VIGÉSIMA SÉPTIMA. CONCILIACIÓN.

"LAS PARTES" acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente contrato podrán someterse al procedimiento de conciliación establecido en los artículos 109, 111 y 112 de la **"LAASSP"**, y 186 al 196 de su Reglamento.

VIGÉSIMA OCTAVA. DOMICILIOS.

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

VIGÉSIMA NOVENA. LEGISLACIÓN APLICABLE.

"LAS PARTES" se obligan a sujetarse estrictamente para la prestación de los servicios objeto del presente contrato a todas y cada una de sus cláusulas, sus anexos que forman parte integral del mismo, a la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento; Código Civil Federal; Ley Federal de Procedimiento Administrativo, Código Federal de Procedimientos Civiles; Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento.

TRIGÉSIMA. JURISDICCIÓN.

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

"LAS PARTES" manifiestan estar conformes y enterados de las consecuencias, valor y alcance legal de todas y cada una de las estipulaciones que el presente instrumento jurídico contiene, por lo que lo ratifican y firman en las fechas especificadas.

POR:
"LA DEPENDENCIA O ENTIDAD"

NOMBRE	CARGO	R.F.C.
(NOMBRE DEL REPRESENTANTE DE LA DEPENDENCIA O ENTIDAD	(CARGO DEL REPRESENTANTE DE LA DEPENDENCIA O ENTIDAD	(R.F.C. DEL REPRESENTANTE DE LA DEPENDENCIA O ENTIDAD
(NOMBRE DEL ADMINISTRADOR DEL CONTRATO)	(CARGO DEL ADMINISTRADOR DEL CONTRATO)	(R.F.C. DEL ADMINISTRADOR DEL CONTRATO)
(NOMBRE DEL FIRMANTE X)	(CARGO DEL FIRMANTE X)	(R.F.C. FIRMANTE X)

POR:
"EL PRESTADOR DE SERVICIOS"

NOMBRE	R.F.C.
(RAZÓN SOCIAL DE LA PERSONA FÍSICA O MORAL)	(R.F.C. DE LA PERSONA FÍSICA O MORAL)

ANEXO XVIII
FORMA DE REDACCIÓN DE LA PÓLIZA QUE GARANTICE EL CUMPLIMIENTO DEL CONTRATO

("Afianzadora" o "Aseguradora")
Denominación social: _____. en lo sucesivo (la Afianzadora o la Aseguradora)
Domicilio: _____.
Autorización del Gobierno Federal para operar: _____(Número de oficio y fecha)

"Beneficiaria":
Lotería Nacional, en lo sucesivo la **"Beneficiaria".**
Domicilio: **Avenida Insurgentes Sur número 1397, Colonia Insurgentes Mixcoac, Demarcación Benito Juárez, Ciudad de México, Código Postal 03920.**

El medio electrónico, por el cual se pueda enviar la fianza a la Contratante" y a la "Beneficiaria": carlos.gama@loterianacional.gob.mx y leopoldo.trejoPE@loterianacional.gob.mx

Fiado (s): (En caso de proposición conjunta, el nombre y datos de cada uno de ellos)
Nombre o denominación social: _____.
RFC: _____.
Domicilio: _____. (El mismo que aparezca en el contrato principal)

Datos de la póliza:
Número: _____. (Número asignado por la "Afianzadora" o la "Aseguradora")

Monto Afianzado: _____. (número y letra), sin incluir el Impuesto al Valor Agregado.

Moneda: _____.

Fecha de expedición: _____.

Vigencia: _____.

Obligación garantizada: El cumplimiento de las obligaciones estipuladas en el contrato en los términos de la Cláusula PRIMERA de la presente póliza de fianza.

Naturaleza de las Obligaciones: ____ (**Divisible o Indivisible**), de conformidad con lo estipulado en el contrato.

Si es **Divisible** aplicará el siguiente texto: La obligación garantizada será **divisible**, por lo que, en caso de presentarse algún incumplimiento, se hará efectiva solo en la proporción correspondiente al incumplimiento de la obligación principal.

Si es **Indivisible** aplicará el siguiente texto: La obligación garantizada será **indivisible** y en caso de presentarse algún incumplimiento se hará efectiva por el monto total de las obligaciones garantizadas.

Datos del contrato simplificado o contrato, en lo sucesivo el **"Contrato":**

Número asignado por **"la Contratante": _____.**

Objeto: _____.

Monto del Contrato: _____(letra y numero), sin el Impuesto al Valor Agregado.

Moneda: _____.

Fecha de suscripción: _____.

Tipo: (Adquisiciones, Arrendamientos, Servicios, Obra Pública o servicios relacionados con la misma).

Obligación contractual para la garantía de cumplimiento: (**Divisible o Indivisible**), de conformidad con lo estipulado en el contrato.

Procedimiento al que se sujetará la presente póliza de fianza para hacerla efectiva: El previsto en el artículo 279 de la Ley de Instituciones de Seguros y de Fianzas.

Competencia y Jurisdicción: Para todo lo relacionado con la presente póliza, el fiado, el fiador y cualesquier otro obligado, así como la **"Beneficiaria"**, se someterán a la jurisdicción y competencia de los tribunales federales de la **Ciudad de México**, renunciando al fuero que pudiera corresponderle en razón de su domicilio o por cualquier otra causa.

La presente fianza se expide de conformidad con lo dispuesto por los artículos 69, fracción II y último párrafo, y artículo 70, fracción II, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 151 de su Reglamento.

Validación de la fianza en el portal de internet, dirección electrónica www.amig.org.mx

Nombre del representante de la (Afianzadora o Aseguradora):_____

CLÁUSULAS GENERALES A QUE SE SUJETARÁ LA PRESENTE PÓLIZA DE FIANZA PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO EN MATERIA DE ADQUISICIONES, ARRENDAMIENTOS, SERVICIO, OBRA PÚBLICA O SERVICIOS RELACIONADOS CON LA MISMA.

PRIMERA. - OBLIGACIÓN GARANTIZADA.

Esta póliza de fianza garantiza el cumplimiento de las obligaciones estipuladas en el "Contrato" a que se refiere esta póliza y en sus convenios modificatorios que se hayan realizado o a los anexos del mismo, cuando no rebasen el porcentaje de ampliación indicado en la cláusula siguiente, aún y cuando parte de las obligaciones se subcontraten.

SEGUNDA. - MONTO AFIANZADO.

(Nombre de La "Afianzadora" o la "Aseguradora"), se compromete a pagar a la **"Beneficiaria"**, hasta el monto de esta póliza, que es (con número y letra sin incluir el Impuesto al Valor Agregado) que representa el **10 %** (diez por ciento) del valor del "Contrato".

(Nombre La "Afianzadora" o la "Aseguradora") reconoce que el monto garantizado por la fianza de cumplimiento se puede modificar en el caso de que se formalice uno o varios convenios modificatorios de ampliación del monto del "Contrato" indicado en la carátula de esta póliza, siempre y cuando no se rebase el **20%** (veinte por ciento) de dicho monto. Previa notificación del fiado y cumplimiento de los requisitos legales, (Nombre de la "Afianzadora" o la "Aseguradora") emitirá el documento modificatorio correspondiente o endoso para el solo efecto de hacer constar la referida ampliación, sin que se entienda que la obligación sea novada.

En el supuesto de que el porcentaje de aumento al "Contrato" en monto fuera superior a los indicados, (Nombre de la "Afianzadora" o la "Aseguradora") se reserva el derecho de emitir los endosos subsecuentes, por la diferencia entre ambos montos, sin embargo, previa solicitud del fiado, (Nombre de la "Afianzadora" o la "Aseguradora") podrá garantizar dicha diferencia y emitirá el documento modificatorio correspondiente.

(Nombre La "Afianzadora" o la "Aseguradora") acepta expresamente que, en caso de requerimiento, se compromete a pagar el monto total afianzado, siempre y cuando en el "Contrato" se haya estipulado que la obligación garantizada es indivisible; de estipularse que es divisible, (Nombre de la "Afianzadora" o la "Aseguradora") pagará de forma proporcional el monto de la o las obligaciones incumplidas.

TERCERA. - INDEMNIZACIÓN POR MORA.

(Nombre de la "Afianzadora" o la "Aseguradora"), se obliga a pagar la indemnización por mora que en su caso proceda de conformidad con el artículo 283 de la Ley de Instituciones de Seguros y de Fianzas.

CUARTA. - VIGENCIA.

La fianza permanecerá vigente hasta que se dé cumplimiento a la o las obligaciones que garantice en los términos del "Contrato" y continuará vigente en caso de que "la Contratante" otorgue prórroga o espera al cumplimiento del "Contrato", en los términos de la siguiente cláusula.

Asimismo, esta fianza permanecerá vigente durante la substanciación de todos los recursos legales, arbitrajes o juicios que se interpongan con origen en la obligación garantizada hasta que se pronuncie resolución definitiva de autoridad o tribunal competente que haya causado ejecutoria.

De esta forma la vigencia de la fianza no podrá acotarse en razón del plazo establecido para cumplir la o las obligaciones contractuales.

QUINTA. - PRÓRROGAS, ESPERAS O AMPLIACIÓN AL PLAZO DEL CONTRATO.

En caso de que se prorrogue el plazo originalmente señalado o conceder esperas o convenios de ampliación de plazo para el cumplimiento del contrato garantizado y sus anexos, el fiado dará aviso a (Nombre de la "Afianzadora" o la "Aseguradora"), la cual deberá emitir los documentos modificatorios o endosos correspondientes.

(Nombre de la "Afianzadora" o la "Aseguradora") acepta expresamente garantizar la obligación a que esta póliza se refiere, aún en el caso de que se otorgue prórroga, espera o ampliación al fiado por parte de la "Contratante" para el cumplimiento total de las obligaciones que se garantizan, por lo que no se actualiza el supuesto de extinción de fianza previsto en el artículo 179 de la Ley de Instituciones de Seguros y de Fianzas, sin que se entienda novada la obligación.

SEXTA. - SUPUESTOS DE SUSPENSIÓN.

Para garantizar el cumplimiento del "Contrato", cuando concurran los supuestos de suspensión en los términos de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y demás disposiciones aplicables, "la Contratante" deberá emitir el o las actas circunstanciadas y, en su caso, las constancias a que haya lugar. En estos supuestos, a petición del fiado, (Nombre de la "Afianzadora" o la "Aseguradora") otorgará el o los endosos conducentes, conforme a lo estatuido en el artículo 166 de la Ley de Instituciones de Seguros y de Fianzas, para lo cual bastará que el fiado exhiba a (Nombre de la "Afianzadora" o la "Aseguradora") dichos documentos expedidos por "la Contratante".

El aplazamiento derivado de la interposición de recursos administrativos y medios de defensa legales, no modifica o altera el plazo de ejecución inicialmente pactado, por lo que subsistirán inalterados los términos y condiciones originalmente previstos, entendiendo que los endosos que emita (Nombre de la "Afianzadora" o la "Aseguradora") por cualquiera de los supuestos referidos, formarán parte en su conjunto, solidaria e inseparable de la póliza inicial.

SÉPTIMA. - SUBJUDICIDAD.

(Nombre de la "Afianzadora" o la "Aseguradora") realizará el pago de la cantidad reclamada, bajo los términos estipulados en esta póliza de fianza, y, en su caso, la indemnización por mora de acuerdo a lo establecido en el artículo 283 de la Ley de Instituciones de Seguros y de Fianzas, aun cuando la obligación se encuentre subjúdice, en virtud de procedimiento ante autoridad judicial, administrativa o tribunal arbitral, salvo que el fiado obtenga la suspensión de su ejecución, ante dichas instancias.

(Nombre de la "Afianzadora" o la "Aseguradora") deberá comunicar a "la "Beneficiaria" de la garantía, el otorgamiento de la suspensión al fiado, acompañándole las constancias respectivas que así lo acrediten, a fin de que se encuentre en la posibilidad de abstenerse del cobro de la fianza hasta en tanto se dicte sentencia firme.

OCTAVA. - COAFIANZAMIENTO O YUXTAPOSICIÓN DE GARANTÍAS.

El coafianzamiento o yuxtaposición de garantías, no implicará novación de las obligaciones asumidas por (Nombre de la "Afianzadora" o la "Aseguradora") por lo que subsistirá su responsabilidad exclusivamente en la medida y condiciones en que la asumió en la presente póliza de fianza y en sus documentos modificatorios.

NOVENA. - CANCELACIÓN DE LA FIANZA.

(Nombre de la "Afianzadora" o la "Aseguradora") quedará liberada de su obligación fiadora siempre y cuando "la Contratante" le comunique por escrito, por conducto del servidor público facultado para ello, su conformidad para cancelar la presente garantía.

El fiado podrá solicitar la cancelación de la fianza para lo cual deberá presentar a (Nombre de la "Afianzadora" o la "Aseguradora") la constancia de cumplimiento total de las obligaciones contractuales. Cuando el fiado solicite dicha cancelación derivado del pago realizado por saldos a su cargo o por el incumplimiento de obligaciones, deberá presentar el recibo de pago correspondiente.

Esta fianza se cancelará cuando habiéndose cumplido la totalidad de las obligaciones estipuladas en el "Contrato", "la Contratante" haya calificado o revisado y aceptado la garantía exhibida por el fiado para responder por los defectos, vicios ocultos de los bienes entregados y por el correcto funcionamiento de los mismos o por la calidad de los servicios prestados por el fiado, respecto del "Contrato" especificado en la carátula de la presente póliza y sus respectivos convenios modificatorios.

DÉCIMA. - PROCEDIMIENTOS.

(Nombre de la "Afianzadora" o la "Aseguradora") acepta expresamente someterse al procedimiento previsto en el artículo 279 de la Ley de Instituciones de Seguros y de Fianzas para hacer efectiva la fianza.

DÉCIMA PRIMERA. -RECLAMACIÓN

La "Beneficiaria" podrá presentar la reclamación a que se refiere el artículo 279, de la Ley de Instituciones de Seguros y de Fianzas en cualquier oficina, o sucursal de la Institución y ante cualquier apoderado o representante de la misma.

DÉCIMA SEGUNDA. - DISPOSICIONES APLICABLES.

Será aplicable a esta póliza, en lo no previsto por la Ley de Instituciones de Seguros y de Fianzas la legislación mercantil y a falta de disposición expresa el Código Civil Federal.

Fecha de inicio de la fianza: (Debe ser la fecha de inicio de prestación de los servicios señalada en la cláusula de vigencia del contrato y que es distinta a la fecha de formalización del mismo).

=Fin de Texto=