2024 — 2027

SECRETARÍA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL
DIRECCIÓN DE ADQUISICIONES
Coordinación de Licitaciones, Concursos y Excepciones

BASES PARA LA LICITACIÓN PÚBLICA NACIONAL PRESENCIAL NÚMERO SAIA-DA-CL-43/2025

SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS

I. PRESENTACIÓN.

El Municipio de San Pedro Garza García, Nuevo León, a través de la Secretaría de Administración e Inteligencia Artificial y de la Dirección de Adquisiciones, en cumplimiento con lo establecido en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos; artículos 1, 5 frac. III, 11, 21, 25 fracción I, 43 inciso a) del Reglamento Orgánico de la Administración Pública Municipal de San Pedro Garza García, Nuevo León; los relativos al procedimiento de Licitación Pública en los artículos 1 fracción V, 2, 14, 16 fracción II y III, 25 fracción I, 27 tercer párrafo fracción II, 29 fracción I, 31 al 35, 37, 39, 40, 46, 48 y 50 de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León; en adelante la Ley; artículos 1, 57, 58, 59 al 62, 65, 66, 67, 69, 72 al 75, 78, 79, 87, 88, 90, 99 y 106 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León; y artículo 36, fracciones VII, XII, XVIII, XXI y XXX, 123 fracción I del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León, en debida concordancia con el artículo 77 de la Ley de Egresos del Estado de Nuevo León para el ejercicio fiscal 2025 y demás relativos y aplicables de las leyes antes citadas, CONVOCA a las personas físicas y morales a participar en el procedimiento de **LICITACIÓN PÚBLICA NACIONAL PRESENCIAL** número **SAIA-DA-CL-43/2025**, relativa al "**SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS .**"

B A S E S

II. INFORMACIÓN GENERAL DEL DESARROLLO DE LA LICITACIÓN PÚBLICA NACIONAL, COSTO Y PAGO DE BASES.

ACTO	PERÍODO O DÍA	HORA	LUGAR
PUBLICACIÓN DE LA CONVOCATORIA	25 de julio de 2025		Periódico Oficial del Estado de Nuevo León, Portal de la **CONVOCANTE** y en uno de los diarios de mayor circulación en la Entidad.
CONSULTA DE BASES	A partir del 25 de julio de 2025		https://sanpedro.gob.mx/concursos-y-licitaciones
VENTA DE BASES Y REGISTRO PARA PARTICIPAR EN LA LICITACIÓN PÚBLICA NACIONAL	Del 25 de julio al 08 de agosto de 2025	9:00 a 16:00 hrs.	El pago deberá ser efectuado en la Dirección de Ingresos de la Secretaría de Finanzas y Tesorería Municipal, sito en PB 09, Planta Baja, Av. Alfonso Reyes 901, Zona Valle Poniente (Plaza Nativa) y/o Libertad #101, Centro de San Pedro Garza García, Nuevo León, y el pago

			será mediante efectivo o cheque a favor del Municipio de San Pedro Garza García, N.L. y para la entrega de las mismas en la Dirección de Adquisiciones calle Independencia Nº 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León.
JUNTA DE ACLARACIONES	04 de agosto de 2025	11:30 hrs.	En la Sala de Juntas de la Dirección de Adquisiciones, ubicada en calle Independencia Nº 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León.
PRESENTACIÓN DE PROPUESTA TÉCNICA Y ECONÓMICA Y APERTURA DE PROPUESTA TÉCNICA	12 de agosto de 2025	10:30 hrs.	En la Sala de Juntas de la Dirección de Adquisiciones, ubicada en calle Independencia Nº 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León.
RESULTADO DE LA EVALUACIÓN TÉCNICA Y APERTURA DE PROPUESTA ECONÓMICA	14 de agosto de 2025	15:00 hrs.	En la Sala de Juntas de la Dirección de Adquisiciones, ubicada en calle Independencia Nº 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León.
FALLO DEFINITIVO Y ADJUDICACIÓN	18 de agosto de 2025	11:00 hrs.	En la Sala de Juntas de la Dirección de Adquisiciones, ubicada en calle Independencia Nº 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León.

ORIGEN DE LOS RECURSOS.- El financiamiento del servicio o suministro o arrendamiento, será con recursos propios disponibles de **LA CONVOCANTE**, según consta en la solicitud de contratación núm. **SC-909** que contiene la suficiencia presupuestal autorizada, por tal motivo esta Licitación se ajustará a lo indicado por el artículo 77 de la Ley de Egresos del Estado de Nuevo León para el ejercicio fiscal 2025 y siguiendo el procedimiento marcado en la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León y su Reglamento, así como

el Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León. El presupuesto se ejercerá en 3-tres ejercicios fiscales.

1. CONSULTA, COSTO Y PAGO DE LAS BASES.

Las bases se encuentran disponibles sólo para su consulta en el portal de **LA CONVOCANTE**: www.sanpedro.gob.mx

El costo de estas bases será de **$2,750.00 (DOS MIL SETECIENTOS CINCUENTA PESOS 00/100 M.N.) Incluyendo el Impuesto al Valor Agregado**.

Los interesados deberán presentar cheque certificado o de caja expedido a favor de Municipio de San Pedro Garza García N.L., o bien efectuar el pago en efectivo, en la Dirección de Ingresos de la Secretaría de Finanzas y Tesorería Municipal, sito en PB 09, Planta Baja, Av. Alfonso Reyes No. 901, Zona Valle Poniente (Plaza Nativa) y/o Libertad No. 101, Centro de San Pedro Garza García, Nuevo León, **de Lunes a Viernes de 8:00 a 16:00 horas**, teniendo como fecha y hora límite el día **08 de agosto de 2025 a las 10:30 horas (sólo en días hábiles).**

2. PARA LA INSCRIPCIÓN Y PARTICIPACIÓN DEBEN CUMPLIR CON LOS SIGUIENTES REQUISITOS:

2.1. Los interesados en obtener las bases de la Licitación Pública Nacional, deberán acudir a solicitar su inscripción en la oficina de la Coordinación de Licitaciones, Concursos y Excepciones adscrita a la Dirección de Adquisiciones de **LA CONVOCANTE** ubicada en calle Independencia No. 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León, a partir de la fecha de publicación de la Convocatoria y hasta la fecha límite de inscripción, de Lunes a Viernes de 9:00 a 16:00 horas, debiendo presentar los siguientes requisitos:

2.2. Los interesados en concursar en la presente licitación deberán acudir para obtener su derecho a participar en el proceso a las oficinas de la Dirección de Adquisiciones, a más tardar el día **08 de agosto de 2025 a las 10:30 horas**, acompañando en papel membretado del **PARTICIPANTE** escrito, firmado en original por la persona física o por el representante legal de la persona moral licitante, los documentos siguientes:

I.- Es requisito indispensable para participar en la Licitación de referencia adquirir las bases mediante el pago de las mismas, para lo cual deberá **previamente** a éste, adquirir una solicitud de inscripción en la Coordinación de Licitaciones, Concursos y Excepciones adscrita a la Dirección de Adquisiciones de **LA CONVOCANTE** ubicada en la calle Independencia No. 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León, dicha solicitud se emitirá al cumplir con los siguientes requisitos:

a) Escrito en el que su firmante manifieste “Bajo protesta de decir verdad”, que cuenta con facultades suficientes para comprometerse por sí o su representada, según lo establecido en el segundo párrafo del artículo 31, fracción IX de la Ley; mismo que deberá contener los datos siguientes:

- Acreditación de existencia legal: Documento denominado **FORMATO I,** debidamente requisitado en papel membretado, anexando así mismo, copia simple de la Constancia de Situación Fiscal (aplicable tanto para personas físicas como personas morales), copia simple del Registro vigente en el Padrón de Proveedores del Municipio; en caso de no presentar este requisito, sus proposiciones estarán condicionadas al Registro en el Padrón a más tardar a la fecha del Fallo Definitivo y Adjudicación. (El formato antes referido lo podrá obtener en el siguiente link: https://transparencia.sanpedro.gob.mx/documentosTransparenciaLinks/5303/300anexo_50634_FORMATO%20%20I.docx o solicitar al siguiente correo electrónico fernanda.barron@sanpedro.gob.mx).
- Con la solicitud antes citada deberá presentarse a realizar el pago en las cajas de la Dirección de Ingresos de la Secretaría de Finanzas y Tesorería Municipal, sito en PB 09, Planta Baja, Av. Alfonso Reyes No. 901, Zona Valle Poniente (Plaza Nativa) y/o Libertad No. 101, Centro de San Pedro Garza García, Nuevo León.

Una vez realizado lo anterior, deberá presentar en la Coordinación de Licitaciones, Concursos y Excepciones adscrita a la Dirección de Adquisiciones, el pago de bases efectuado en tiempo y forma con el fin de que le sean proporcionadas las bases correspondientes; dándose en ese momento por formalizada su inscripción. De no formalizar su inscripción ante **LA CONVOCANTE,** antes de la fecha y hora estipulada **LOS PARTICIPANTES NO PODRÁN PARTICIPAR, NI PRESENTAR SUS PROPUESTAS TÉCNICA Y ECONÓMICA.**

3. REGLAS DE LA LICITACIÓN PÚBLICA NACIONAL PRESENCIAL.

MEDIOS A UTILIZAR Y CELEBRACIÓN DE ACTOS.- La Junta de Aclaraciones, Acto de Presentación de Propuesta Técnica y Económica y Apertura de Propuesta Técnica, Resultado de Evaluación Técnica y Apertura Económica y el Fallo Definitivo y Adjudicación, se llevarán a cabo en forma presencial en la sala de juntas de la Dirección de Adquisiciones de la Secretaría de Administración e Inteligencia Artificial del Municipio de San Pedro Garza García, Nuevo León, ubicado en el domicilio calle Independencia No. 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León.

CONDICIONES Y REQUISITOS.- Ninguna de las condiciones establecidas en la convocatoria y requisitos contenidos en las presentes bases, podrán ser negociadas.

COSTOS PROPUESTOS.- Los costos propuestos deberán contemplar el precio unitario, incluyendo todos los impuestos que se generen, la remuneración por el servicio, suministro o arrendamiento, los transportes, seguros y maniobras de transportación, incluyendo la carga y descarga, serán por cuenta y riesgo del **PARTICIPANTE** hasta el destino de nuestras instalaciones.

IDIOMA.- La Propuesta Técnica que prepare el **PARTICIPANTE**, así como toda la correspondencia y documentos relativos, deberán redactarse en el idioma español; en todo caso cualquier material impreso que proporcione el **PARTICIPANTE** a **LA CONVOCANTE** podrá estar en otro idioma a condición de que venga acompañado de su correspondiente traducción al español, la cual prevalecerá para los efectos de interpretación de las propuestas.

PROPUESTAS CONJUNTAS.- No se aceptarán propuestas conjuntas.

MEDIOS REMOTOS.- Para el presente procedimiento **NO** se aceptarán propuestas que sean enviadas por medios remotos de comunicación (electrónicos), servicio postal o mensajería.

SUBCONTRATACIÓN.- En la presente Licitación Pública Nacional Presencial los **PARTICIPANTES**, no podrán subcontratar lo solicitado.

FORMA DE COTIZAR.- La presente Licitación Pública Nacional se conforma de 1 partida la cual esta integrada por sub-partidas, por lo que el **PARTICIPANTE** deberá cotizar la partida de forma completa. Asimismo, se hace de su conocimiento que la **CONVOCANTE** realizará la adjudicación por partida completa considerando la oferta económica más conveniente.

4. VISITAS Y VERIFICACIONES.

LA CONVOCANTE, podrá en cualquier momento a partir de la inscripción del **PARTICIPANTE**, a través de la Secretaría de la Contraloría y Transparencia o quien se designe, realizar las visitas necesarias a las instalaciones del **PARTICIPANTE** con el propósito de verificar su capacidad técnica y administrativa, la cual se hará constar en acta circunstanciada, misma que será firmada por quien haya hecho la visita y verificación, así como el **PARTICIPANTE** y el responsable del Área Requirente de **LA CONVOCANTE**, la falta de firma del **PARTICIPANTE** no invalidará dicha acta circunstanciada. Los medios de conducción para la práctica de las mismas correrán a cargo del **PARTICIPANTE** previo aviso, en caso de ubicarse sus instalaciones y/o maquinaria fuera del Área Metropolitana de Nuevo León.

LA CONVOCANTE podrá validar a través de la Secretaría de la Contraloría y Transparencia, con

cualquier Dependencia Pública Municipal, Estatal o Federal y/o con cualquier empresa privada toda la información presentada por el **PARTICIPANTE**.

5. DESCRIPCIÓN DEL SERVICIO, SUMINISTRO O ARRENDAMIENTO A LICITAR.

El **SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS** debe apegarse a la descripción que se establece en las **Especificaciones Técnicas citadas en el ANEXO 1 "Especificaciones Técnicas"** de las presentes bases.

6. **VIGENCIA, PLAZO Y LUGAR DE ENTREGA DEL SERVICIO.**

VIGENCIA DEL CONTRATO: La vigencia del contrato será por un plazo de 2 años contados a partir del día hábil siguiente a la emisión del fallo.

PLAZO DE PRESTACIÓN DEL SERVICIO: La adjudicataria deberá de entregar lo solicitado en el Anexo 1 "Especificaciones Técnicas", a más tardar a los 30 días naturales contados a partir de la fecha de la notificación del fallo de adjudicación.

LUGAR: El servicio se entregará en la Dirección General de Tecnologías, con la Lic. Claudia Esther Cervantes Alanís, ubicada en calle Corregidora No. 507, Centro, C.P. 66200, en San Pedro Garza García, N.L., teléfono 81-8400-45-95.

Las solicitudes de cambios, devolución o reposición, se efectuarán a través del Área Requirente de **LA CONVOCANTE**, en días y horas hábiles dentro de los primeros 10 días calendario y el **PARTICIPANTE** deberá hacer las entregas programadas y/o solicitadas en el término establecido por dicha Área en la solicitud de cambio, y así mismo deberá proporcionar a dicha área el nombre, correo electrónico, teléfono y fax de las personas autorizadas para recibir dichas solicitudes.

7. PROCEDIMIENTO A SEGUIR EN LA JUNTA DE ACLARACIONES.

7.1. De conformidad con el artículo 34 de la Ley, se realizará la Junta de Aclaraciones, el día **04 de agosto de 2025 a las 11:30 horas,** en la Sala de Juntas del domicilio de la Unidad Convocante. La asistencia a la Junta de Aclaraciones es optativa para los licitantes, de acuerdo a lo establecido en el artículo 164 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León, por lo cual la inasistencia a la misma, no será causa de descalificación.

Los interesados en participar en la Junta de Aclaraciones de la presente Licitación Pública Nacional de conformidad a lo establecido por artículo 157 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García,

Nuevo León, deberán presentar a más tardar el día **01 de agosto de 2025 a las 11:30 horas en la Dirección de Adquisiciones** lo siguiente:

1. Carta de interés en participar.

Pliego de preguntas, mismas que deberán presentarse de manera presencial por escrito, firmadas de manera autógrafa en papel membretado del participante, indicando el numeral o punto específico con el cual se relaciona, en la Dirección de Adquisiciones ubicada en calle Independencia No. 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León. Dicho formato se podrá descargar a través del siguiente link: https://transparencia.sanpedro.gob.mx/documentosTransparenciaLinks/5303/300anexo_55775_FORMATO%20JUNTA%20ACLARACIONES.docx

2. Se hace del conocimiento de los **PARTICIPANTES** que las preguntas que formulen en la Junta de Aclaraciones, deberán realizarse de una en una, en forma clara y precisa, y estar relacionadas con el objeto de la Licitación, en caso contrario **LA CONVOCANTE** las **desechará** y no propalará respuesta alguna.

3. Dispositivo **USB** que contenga el pliego de preguntas en formato editable en Word (sin utilizar imágenes, ni establecer contraseñas).

La recepción de la documentación será en el domicilio de la Unidad Convocante de lunes a viernes de 8:00 am y hasta la fecha y horario establecido en el segundo párrafo del **punto 7.1.**

7.2 Las preguntas se contestarán el día establecido para la Junta de Aclaraciones.

7.3 Los licitantes podrán designar a una persona distinta al representante legal, la cual solamente podrá acudir en su representación a los diversos actos del proceso de licitación y entregar las propuestas, para ello deberá entregar un poder simple, debiendo, invariablemente, incluir copia simple de las identificaciones oficiales vigentes de las personas que suscriban el citado documento. No será motivo de descalificación la falta de identificación o de la representación de la persona que acuda a los actos, pero sólo podrá participar con el carácter de observador.

7.4 La asistencia a la Junta de Aclaraciones puede ser presencial o podrán seguirla en línea a través de la página de internet en el siguiente enlace: www.sanpedro.gob.mx no es indispensable acudir, sin embargo; se recomienda estar pendientes de los cambios suscitados en la misma.

7.5 En la realización de la o las juntas de aclaraciones se deberá considerar lo siguiente:

a. El servidor público, designado por la Unidad Convocante para presidir la Junta de Aclaraciones será asistido por un Representante del Área Técnica o Usuaria de los bienes, arrendamientos o servicios objeto de la contratación, a fin de que resuelvan en forma clara y precisa las dudas y planteamientos de los licitantes relacionados con los aspectos contenidos en la convocatoria.

b. La Unidad Convocante levantará el acta correspondiente en la que se harán constar las dudas y cuestionamientos realizados en dicho evento. Cualquier modificación a las bases y sus anexos, derivada del resultado de la Junta de Aclaraciones será considerada como parte integrante de las propias bases y por ende obligatorio para los **PARTICIPANTES** de conformidad a lo establecido en el artículo 33, segundo párrafo de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León y 150 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el municipio de San Pedro Garza García, Nuevo León.

Los participantes podrán recoger copia del acta que se derive de la Junta de Aclaraciones en el domicilio de la Unidad Convocante de lunes a viernes de 9:00 a 16:00 horas, o podrá descargarla en formato electrónico a través de portal del Municipio. Siendo de la exclusiva responsabilidad de los licitantes enterarse de su contenido y obtener copia de la misma. Lo anterior sustituirá a la notificación personal.

8. PROCEDIMIENTO A SEGUIR EN LOS ACTOS DE APERTURA TÉCNICA Y APERTURA DE PROPUESTAS ECONÓMICAS.

De conformidad con lo dispuesto por el artículo 122 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León, la presente Licitación Pública Nacional se realizará de la siguiente forma:

8.1 APERTURA TÉCNICA.

De conformidad con lo dispuesto por el artículo 180, fracción II del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León, **el Acto de Presentación y Apertura de Propuestas Técnicas se llevará a cabo de la siguiente manera**:

8.1.1 Presidirá el Acto de Presentación de Propuesta Técnica y Económica y Apertura de Propuestas Técnica, el representante de **LA CONVOCANTE**, con la asistencia de los participantes, funcionarios e invitados.

8.1.2 El Acto de Presentación y Apertura de Propuestas Técnicas será público, pero solo participarán quienes hayan realizado el pago, adquirido las bases de la Licitación Pública Nacional

en tiempo y forma y formalizado su registro ante **LA CONVOCANTE**, dentro de la fecha y hora límite estipulada.

8.1.3 Se procederá a firmar una lista de asistencia de los participantes, funcionarios e invitados presentes.

8.1.4 Se procederá a la recepción de los **sobres cerrados** que contienen las Propuestas Técnicas y Económicas, una vez recibidos se procederá a la Apertura de la Propuesta Técnica y se verificará que los documentos solicitados en el contenido de las presentes bases estén completos y se desecharán las que hubieren omitido alguno de los requisitos exigidos en las mismas ya que todos serán considerados indispensables para la evaluación y en su caso la adjudicación del contrato respectivo, quedando en resguardo de la **CONVOCANTE** el sobre cerrado de la propuesta económica previamente rubricado por los asistentes al acto de referencia.

El **LICITANTE** podrá presentar a su elección, dentro o fuera del sobre, la documentación **distinta** a la que conforma la Propuesta Técnica, considerando que desde el momento de su presentación esta pasará a formar parte de su proposición, no eximiéndolo de cumplir inicialmente con lo solicitado en las presentes bases.

8.1.5 Los **PARTICIPANTES** que hayan asistido, en forma conjunta con el Representante del Área Requirente de **LA CONVOCANTE**, rubricarán las partes de las Propuestas Técnicas presentadas, consistentes en: las especificaciones técnicas del suministro y/o servicio y/o arrendamiento que se presenten dentro del sobre, mismas que se le entregarán al representante de área técnica para que emita el resultado de su evaluación técnica, las que para estos efectos constatarán documentalmente.

8.1.6 Se levantará el acta correspondiente al Acto de Presentación de Propuesta Técnica y Económica y Apertura de Propuesta Técnica, en la que se hará constar las Propuestas Técnicas aceptadas para su análisis, así como las que hubieren sido desechadas y las causas que lo motivaron, el acta será firmada por los asistentes, sin embargo la falta de firma de algún **PARTICIPANTE** no invalidará su contenido y efectos, poniéndose a partir de esa fecha a disposición de los que no hubieren asistido para efectos de notificación a través del portal de **LA CONVOCANTE**. Aquellas propuestas que por haberse desechado al no cumplir con los requisitos exigidos o que no fueron aceptadas, deberán conservarse quedando en resguardo de **LA CONVOCANTE**.

8.1.7 Una vez conocido el Resultado de la Evaluación Técnica, se llevará a cabo en día y hora señalada para el evento de Apertura de la Propuesta Económica de los **PARTICIPANTES** cuyas Propuestas Técnicas no fueron desechadas, en fecha y hora señalada para tal evento en las presentes bases.

8.2. RESULTADO DE LA EVALUACIÓN TÉCNICA Y APERTURA DE PROPUESTA ECONÓMICA.

El acto de fallo técnico y apertura de los sobres que contienen las propuestas económicas, se celebrará el día **14 de agosto de 2025 a las 15:00 horas,** en la Sala de Juntas del domicilio de **LA CONVOCANTE**, debiendo considerar lo siguiente:

a. Se declarará iniciado el acto puntualmente en la fecha, lugar y hora señalados, el cual será presidido por el titular de **LA CONVOCANTE** o por el servidor público que este mismo designe, quien será el único facultado para tomar todas las decisiones durante la realización del acto en los términos de la multicitada Ley y Reglamentos respectivos.

b. Se procederá a pasar lista de asistencia a los licitantes y demás funcionarios presentes.

c. Se procederá al Fallo Técnico, informando el resultado de la revisiones cuantitativa y cualitativa de la documentación técnica, mencionándose a cada una de los licitantes y manifestando si acreditan o no la etapa técnica.

d. En caso de que, como resultado de la revisión cualitativa de la propuesta técnica, se descalifique a un licitante, se precisarán las causas del desechamiento y no se le dará lectura a la propuesta económica. Acto seguido, se procederá a la apertura de los sobres que contengan las propuestas económicas, verificando que se encuentran inviolados y que contengan todos los documentos solicitados y que éstos satisfagan los requisitos y especificaciones establecidos en las bases de licitación.

e. El funcionario que presida el acto, leerá en voz alta, cuando menos, los montos totales de cada propuesta admitida, los cuales deberán ser firmados por todos los participantes del evento para constancia de la legalidad de la licitación.

f. Se levantará el acta correspondiente al Acto de Fallo Técnico y Apertura de Propuestas Económicas en la que se harán constar las propuestas recibidas, los montos ofrecidos, así como las que hubieren sido desechadas o descalificadas y las omisiones de documentación por las que se desecharon o descalificaron. Así mismo, se señalará el lugar, fecha y hora en que se dará a conocer el fallo de la licitación, así como las manifestaciones que en su caso emitan los licitantes en relación al mismo.

g. El acta será firmada por todos los participantes y se entregará a cada uno de ellos una copia de la misma. En caso de que alguno de los concursantes se negara a firmar, así se hará constar en el acta. La omisión de firma de algunos de los concursantes no invalidará el contenido, efectos del acta de referencia.

h. El concursante que retire sus propuestas una vez iniciado el Acto de Apertura, perderá su garantía de seriedad de la propuesta.

Los participantes que no hayan asistido al acto, podrán recoger copia del acta en la Dirección de Adquisiciones, en el Domicilio de la Unidad Convocante de lunes a viernes de 9:00 a 16:00 horas, o podrá descargarla en formato electrónico a través de portal del Municipio. Siendo de la exclusiva responsabilidad de los participantes enterarse de su contenido y obtener copia de la misma. Lo anterior sustituirá a la notificación personal.

9. DOCUMENTOS QUE DEBE CONTENER EL SOBRE DE LA PROPUESTA TÉCNICA (DEBIENDO INCLUIR LA DOCUMENTACIÓN ORIGINAL QUE SE REQUIERA PARA COTEJO SEGÚN EL INCISO).

Los **PARTICIPANTES** deberán presentar todos los documentos solicitados en las presentes bases para la integración de su Propuesta Técnica (**INCLUYENDO LA DOCUMENTACIÓN ORIGINAL QUE SE REQUIERA PARA COTEJO SEGÚN EL INCISO)**, dentro de un sobre cerrado debiendo describir fuera del mismo: El nombre de la Persona Física o Moral **PARTICIPANTE**, domicilio, la descripción del suministro y/o servicio y/o arrendamiento, y el número de Licitación. Los documentos que integran su Propuesta Técnica deberán estar debidamente firmados por el Representante Legal, foliados y sellados en cada una de sus hojas, a excepción de la documentación original solicitada, misma que será devuelta a los participantes una vez cotejada en el mismo acto de Apertura Técnica. Así mismo, los documentos que sean elaborados por el **PARTICIPANTE** deberán además estar debidamente identificados con el nombre y número de la Licitación respectiva.

Los **PARTICIPANTES** deberán agregar dentro del sobre de su Propuesta Técnica una **USB** con su propuesta escaneada. Los archivos deberán contener la misma información que presentarán en el sobre de su propuesta, en formato PDF, elaborando un archivo **por cada** documento requerido en el inciso respectivo. Estos archivos electrónicos no sustituyen por ningún motivo los documentos físicos que se entreguen en el Acto de Presentación de Propuesta Técnica y Económica y Apertura de Propuesta Técnica, por lo que en caso de no haberse presentado los documentos físicos no podrá argumentarse que fueron entregados de manera electrónica para subsanar la omisión.

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

a) Para intervenir en el Acto de Presentación de Propuesta Técnica y Económica y Apertura de Propuesta Técnica en representación de los **LICITANTES** bastará que se presente un escrito en el que su firmante manifieste, bajo protesta de decir verdad, que cuenta con facultades suficientes para comprometerse por sí o su representada, conforme a lo establecido en los

artículos 31 fracción IX de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León y 74 fracción IV de su Reglamento. Anexando copia simple de la identificación vigente del compareciente al acto**.**

b) Copia y original para su cotejo del recibo de pago de las bases efectuado en tiempo y forma.

c) Copia simple y original para su cotejo del registro vigente en el Padrón de Proveedores del Municipio y/o la copia simple de la solicitud de inscripción.

d) Escrito en el que el **LICITANTE** manifieste bajo protesta de decir verdad, que es de nacionalidad mexicana.

e) Escrito bajo protesta de decir verdad en el cual manifieste que los bienes que oferta y entregará, serán producidos en México y que contarán con el porcentaje de contenido nacional correspondiente. En caso de ser prestación de servicios el presente requisito no aplica, debiendo manifestarlo por escrito.

f) Escrito bajo protesta de decir verdad en el cual manifieste que en caso de que **LA CONVOCANTE** lo solicite, le proporcionará la información y demás documentales expedidos por la autoridad competente que permita verificar que los bienes ofertados son de producción nacional y cumplen con el porcentaje de contenido nacional requerido. En caso de ser prestación de servicios el presente requisito no aplica, debiendo manifestarlo por escrito.

g) PERSONALIDAD DEL **PARTICIPANTE** Y DE SU REPRESENTANTE.- Para acreditar la personalidad del **PARTICIPANTE** y la de su Representante Legal, deberá de presentar en original el **FORMATO I** en el que el firmante manifieste bajo protesta de decir verdad, que cuenta con las facultades suficientes para comprometerse por sí o su representada, así como para suscribir a nombre de su representada la propuesta y formalizar en su caso el contrato correspondiente, adicionando a esté la siguiente documentación según le corresponda:

PERSONA MORAL

- Copia simple del Acta Constitutiva y original o copia certificada para su cotejo, adjuntando Boleta de Inscripción del Registro Público de la Propiedad y de Comercio.
- Copia simple de la última modificación al Acta Constitutiva y original o copia certificada para su cotejo (en caso de que no existan modificaciones deberá de manifestarlo por escrito).
- Copia simple del Acta con la cual compruebe que el objeto social del **PARTICIPANTE** está relacionado con la presente licitación y original o copia certificada para su cotejo.
- Copia simple del Poder del Representante Legal y original o copia certificada para su cotejo.
- Copia simple de la Identificación Oficial vigente de la persona que firme la proposición y original o copia certificada para su cotejo.

- Copia simple del documento que emite actualmente el SAT, el cual contiene los conceptos relativos a Cédula de Identificación Fiscal y Constancia de Situación Fiscal (ambos en el mismo formato), la cual debe ser generada de fecha actual (no mayor a 30 días naturales).
- Copia simple de las Opiniones de Cumplimiento de Obligaciones Fiscales en sentido positivo de: SAT, INFONAVIT e IMSS, no mayor a 30 días naturales.
- Copia simple de la Opinión de Cumplimiento de Obligaciones Fiscales en sentido positivo emitida por la Secretaría de Finanzas y Tesorería General del Estado (no mayor a 30 días naturales).
- Copia simple del comprobante de domicilio a nombre del **PARTICIPANTE** y original o copia certificada para su cotejo.

PERSONA FÍSICA

- Copia simple de la Identificación Oficial vigente de la persona que firme la proposición y original o copia certificada para su cotejo.
- Copia simple del documento que emite actualmente el SAT, el cual contiene los conceptos relativos a Cédula de Identificación Fiscal y Constancia de Situación Fiscal (ambos en el mismo formato), la cual debe ser generada en fecha actual (no mayor a 30 días naturales) con el cual deberá comprobar dentro de su Actividad Económica que está relacionada con el objeto de la presente licitación.
- Copia simple de las Opiniones de Cumplimiento de Obligaciones Fiscales en sentido positivo de: SAT, INFONAVIT e IMSS, no mayor a 30 días naturales.
- Copia simple de la Opinión de Cumplimiento de Obligaciones Fiscales en sentido positivo emitida por la Secretaría de Finanzas y Tesorería General del Estado (no mayor a 30 días naturales).
- Copia simple del comprobante de domicilio a nombre del **PARTICIPANTE** y original o copia certificada para su cotejo.

h) Copia simple y original para su cotejo de la documentación que compruebe estar al corriente en el pago del Impuesto Sobre Nóminas, Impuesto Sobre Tenencia o Uso de Vehículos y los Derechos de Control Vehicular y el último pago de Impuesto Predial, de conformidad con lo establecido en el artículo 33-BIS del Código Fiscal del Estado de Nuevo León.

i) Deberá proporcionar por escrito un correo electrónico y un domicilio dentro del Estado de Nuevo León, para efectos de notificación.

j) Carta Compromiso del **PARTICIPANTE** (**FORMATO II**).

k) Copia del acuse de recibo de la carta de aceptación de la convocatoria, bases, contenido de la Junta de Aclaraciones y validez de propuesta (**FORMATO III**). **Dicho acuse del formato, podrá sellarse hasta un día antes del evento de Presentación de Propuesta Técnica y Económica y Apertura de Propuesta Técnica en la Coordinación de Licitaciones, Concursos y**

excepciones adscrita a la Dirección de Adquisiciones, debiendo el PARTICIPANTE anexarlo dentro de su sobre técnico.

l) Carta de no impedimento legal para contratar **(FORMATO IV)**.

m) Declaración de Integridad **(FORMATO V)**.

n) Política de Integridad (**FORMATO VI)**.

o) Certificado de determinación independiente **(FORMATO VII)**.

p) Origen extranjero de los bienes que oferten. En caso de ser prestación de servicios el presente formato no aplica, debiendo manifestarlo por escrito. **(FORMATO VIII)**.

q) Origen nacional de los bienes o servicios que oferten **(FORMATO IX)**.

r) Manifestación sobre la estratificación en caso de encontrarse en las consideradas MIPYMES **(FORMATO X)**, en caso contrario deberá manifestarlo por escrito.

s) Documentación anexada por el **LICITANTE (FORMATO XI)**.

t) Manifiesto del Artículo 49 fracción IX de la Ley de Responsabilidades Administrativas del Estado de Nuevo León. **(FORMATO XII)**.

u) Manifiesto del Artículo 69-B del Código Fiscal de la Federación (**FORMATO XIII**)

v) Infraestructura.- El **LICITANTE** para acreditar su experiencia técnica deberá presentar el Currículum de la empresa, además de la documentación solicitada, de cualquiera de las viñetas que a continuación se detallan, en el entendido que la viñeta que se va a considerar deberá cumplir con el punto completo:

- Una relación de las principales operaciones de ventas o prestación de servicios de los últimos doce meses, que incluya un informe técnico de los mismos, adjuntando las constancias de cumplimiento expedidas por los clientes del licitante;
- Una descripción de las instalaciones, maquinaria, equipos y demás elementos técnicos necesarios para el objeto de la licitación, de los que dispone el licitante;
- La indicación de los títulos de estudios y profesionales de los responsables de la producción de los bienes o de la prestación de los servicios;
- La entrega de muestras, fotografías o descripciones de bienes o servicios, sujetos a comprobación.

w) Acreditar a través de 3-tres facturas, emitidas en un plazo no mayor a 12-doce meses previos, que cuenta con experiencia relacionada con el objeto de la presente licitación.

x) El **PARTICIPANTE** deberá anexar copia de las **Especificaciones Técnicas del ANEXO 1 "Especificaciones Técnicas"** firmado, con lo cual acepta lo estipulado, anexando al mismo los requisitos que en dicho anexo se solicitan.

y) El **PARTICIPANTE** deberán presentar su inscripción en el Registro de Prestadores de Servicios Especializados u Obras Especializadas (REPSE) vigente, lo anterior de acuerdo al artículo 15 de la Ley Federal del Trabajo vigente y en caso de no estar obligado presentar un escrito en el que justifique el motivo de su excepción.

z) El **PARTICIPANTE** deberá manifestar bajo protesta de decir verdad y por escrito, que si resulta participante ganador se compromete a que su Representante Legal, tomará el Curso de Prevención y Concientización sobre Faltas Administrativas y Hechos de Corrupción.

aa) El **PARTICIPANTE** deberán manifestar bajo protesta de decir verdad y por escrito que sufragarán todos los costos relacionados con la preparación y presentación de su propuesta, liberando de cualquier responsabilidad a **LA CONVOCANTE** por dicho concepto, por lo que no resultará procedente la devolución de importe alguno, cualquiera que sea el resultado de la presente Licitación Pública Nacional.

bb) Carta bajo protesta de decir verdad que garantice satisfactoriamente el cumplimiento del servicio objeto de la presente Licitación Pública Nacional.

cc) El **PARTICIPANTE** deberá presentar carta donde garantice que cuenta con la infraestructura necesaria, el personal capacitado y con los técnicos especializados para el tipo de servicio solicitado.

dd) Escrito bajo protesta de decir verdad en el cual manifieste, que es el único responsable de la relación laboral generada con motivo de la prestación del servicio, deslindando en todo momento a la Unidad Convocante y/o al Municipio de cualquier responsabilidad.

ee) Currículos del personal con el que brindará el servicio con los cuales acredite que cuentan con las certificaciones y acreditar las mismas con copias simples y número de folio de las siguientes certificaciones:

- OffSec Exploit Developer (OSED)
- OffSec Experienced Penetration Tester (OSEP)
- OffSec Web Expert (OSWE)
- OffSec Certified Expert 3 (OSCE3)

- Offensive Security Certified Professional (OSCP)
- Web Application Penetration Tester eXtreme (eWPTX v2.0)
- Certified Penetration Tester eXtreme v2 (eCPTX)
- Certified Secure Web Application Engineer (SWAE)

ff) Carta bajo protesta de decir verdad que garantizará la atención ininterrumpida 24X7X365 (24 horas al día, 7 días a la semana, 365 días al año) de incidentes graves o críticos, en estricta observancia de los Acuerdos de Nivel de Servicio (SLAs) detallados en el ANEXO TÉCNICO.

gg) Carta bajo protesta de decir verdad que garantizará que en caso de que se produzca cualquier incidente de ciberseguridad que impacte la prestación de los servicios o la integridad de los equipos suministrados, el proveedor se compromete a activar de inmediato su plan de respuesta ante incidentes en un término que no podrá variar de 1 a 3 horas como máximo, debiendo notificar al personal de la Dirección de Tecnologías en un plazo máximo de 1 hora en que se registre el incidente y proporcionando informes periódicos hasta la completa resolución del incidente.

hh) Carta bajo protesta de decir verdad que garantizará realizar la ejecución de todas las acciones correctivas y preventivas necesarias para mitigar y erradicar el incidente, restaurando la normalidad en las operaciones sin costo adicional para la convocante. Así como, asumir la obligación de indemnizar a la convocante por cualquier daño, perjuicio o pérdida económica directa o indirecta ocasionada por el monto del 100%, en la medida en que se determine que dichos perjuicios surgieron a consecuencia del incumplimiento de las medidas de ciberseguridad contratadas.

ii) Carta bajo protesta de decir verdad que garantizará que, ante una falla en el servicio y la consecuente rescisión del contrato, la empresa se compromete a facilitar la migración del servicio durante un período de **dos (2) meses**, brindando el soporte, servicio y servidores necesarios para que el **CONVOCANTE** pueda adaptarse sin contratiempos a una nueva plataforma o proveedor.

jj) Carta con firma original emitida por el fabricante donde lo respalde en la solución que está ofertando, debiendo asentar en la misma los datos del **Ingeniero de Respaldo del Fabricante Remoto Dedicado** por un período de 12 meses para apoyo en la implementación, migración, operación y adopción de nuevas tecnologías para los servicios 1.1, 1.2, 1.3, 1.4, 3.1, 3.2, 3.3, 3.4, 3.5, 5.1, 7.1, 7.2, 7.3, 9.1 de la FICHA TÉCNICA.

10. DOCUMENTOS QUE DEBE CONTENER EL SOBRE DE LA PROPUESTA ECONÓMICA.

I. Documento elaborado en papel membretado, firmado de manera autógrafa por la persona física o por el representante legal de la empresa concursante, que contenga su propuesta

económica en pesos mexicanos, debidamente llenado cada campo solicitado y preparado en base al **Anexo 2. "Propuesta Económica"**. De igual manera, esta información deberá presentarla en archivo.xls. electrónico en formato editable en un USB. No serán aceptadas ofertas económicas del mismo valor. En caso de existir igualdad de condiciones, se considerará además lo establecido en el Artículo 192 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León. Debiendo anexar el desglose de precios unitarios de los insumos, trabajos o servicios propuestos como referencia.

II. Garantía de seriedad de sostenimiento de propuesta, en cheque o fianza a favor de Municipio de San Pedro Garza García, N.L**., por un monto no menor al 5% del total de su propuesta**, incluyendo el Impuesto al Valor Agregado, en el caso que su propuesta genere dicho impuesto y el cálculo deberá ser sobre el monto total de su propuesta. Tratándose de cheque este podrá ser simple, cruzado, certificado o de caja de cuenta de banco nacional, identificado con la razón social de la empresa o persona física participante y deberá cumplir con lo estipulado en los artículos 199, 200 y demás relativos y aplicables de la Ley General de Títulos y Operaciones de Crédito vigente; en caso de presentar Fianza, deberá acompañarla con la copia del recibo de pago de la misma. La garantía antes citada le será devuelto el día que se dé el Fallo Definitivo y Adjudicación al **PARTICIPANTE** que no haya resultado ganador, el cual se podrá solicitar en la Coordinación de Licitaciones, Concursos y Excepciones, de **LA CONVOCANTE** y al **PARTICIPANTE** adjudicado le será devuelto el día que presente la fianza de garantía de buen cumplimiento del contrato.

III. CAPACIDAD FINANCIERA.- Comprobación de ingresos los cuales sean por lo menos equivalentes al 20% del monto total de su oferta, mediante la declaración fiscal anual 2024, ante el Sistema de Administración Tributaria (SAT), e incluir acuse de recibo de la declaración y su comprobante de pago bancario y la última declaración fiscal provisional del impuesto sobre la renta presentada en el mes inmediato anterior que le corresponda, a la fecha del Acto de presentación y apertura de propuestas técnicas (incluir acuse de recibo de la declaración y su comprobante de pago bancario). Así mismo, deberá incluir Estado de Resultado y Balance General del mes anterior, debidamente firmado por Contador Público, anexando copia de su cédula profesional.

Cada uno de los documentos que integren la Propuesta Técnica y Económica y aquellos distintos a esta, deberán estar antefirmados, foliados en todas y cada una de las hojas que los integren, además deberán estar firmados por la persona que cuente con el poder para actos de administración y/o dominio con firma autógrafa en la última página de cada documento, de conformidad con el artículo 180, fracción XV del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León.

Todos los documentos solicitados en las propuestas son esenciales, la omisión de cualquiera de ellos no podrá subsanarse y será motivo de desechamiento de la propuesta.

11. JUNTA DE ACLARACIONES.

Se llevará a cabo el día **04 de agosto de 2025 a las 11:30 horas** en la Sala de Juntas de la Dirección de Adquisiciones de **LA CONVOCANTE** ubicada en calle Independencia No. 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León.

12. ACTO DE PRESENTACIÓN DE PROPUESTA TÉCNICA Y ECONÓMICA Y APERTURA DE PROPUESTAS TÉCNICA.

Las Propuestas Técnicas se entregarán el día **12 de agosto de 2025 a las 10:30 horas**, el evento se llevará a cabo en la Sala de Juntas de la Dirección de Adquisiciones de **LA CONVOCANTE** ubicada en calle Independencia No. 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León, después de la hora indicada ya no se recibirán propuestas.

En esta etapa los **PARTICIPANTES** deberán de presentar en **dos sobres cerrados** uno que contenga la propuesta técnica y otro con la propuesta económica debidamente referenciados, los requisitos señalados en las presentes bases. Las propuestas que no cumplan dichos requisitos se desecharán, asentándose en el acta correspondiente.

13. RESULTADO DE LA EVALUACIÓN TÉCNICA Y APERTURA DE PROPUESTA ECONÓMICA

El evento se llevará a cabo el día **14 de agosto de 2025 a las 15:00 horas** en la Sala de Juntas de la Dirección de Adquisiciones de **LA CONVOCANTE** ubicada en calle Independencia No. 316 esquina con Corregidora, 4° piso, en el centro del Municipio de San Pedro Garza García, Nuevo León, después de la hora indicada ya no se recibirán propuestas.

Los **PARTICIPANTES** deberán considerar en su oferta económica las cantidades totales del **SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS.**

14. CRITERIOS.

14.1 CRITERIOS ESPECÍFICOS DE EVALUACIÓN.

De conformidad a lo establecido en el artículo 116 del Reglamento de Adquisiciones,

Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León, una vez recibidas las propuestas, las cuales deben contar con toda la documentación vigente, serán analizadas y evaluadas por el Área Requirente verificando que cumplan con todos los requisitos solicitados en las presentes bases, con el propósito de que emita el resultado de su evaluación técnica, asimismo, se corroborará que hayan cumplido con los requisitos legales.

14.2 CRITERIOS DE ADJUDICACIÓN.

LA CONVOCANTE adjudicará la Licitación Pública Nacional al **PARTICIPANTE** que haya ofertado la propuesta más conveniente en cuanto a precio y que previamente haya cumplido con los requisitos legales y técnicos solicitados en las presentes bases.

15. FALLO DEFINITIVO Y ADJUDICACIÓN.

De conformidad con lo establecido por el artículo 195 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León **LA CONVOCANTE** emitirá el Fallo Definitivo y Adjudicación el día **18 de agosto de 2025 a las 11:00 horas.**

16. CAUSAS DE DESECHAMIENTO.

LA CONVOCANTE podrá desechar la propuesta presentada por alguno de los **PARTICIPANTES** en los siguientes casos:

a) Si el pago de las bases no se realizó en tiempo y forma conforme a los requisitos de la Licitación Pública Nacional.
b) Si el **PARTICIPANTE** no se presenta con puntualidad el día señalado para el Acto de Presentación de Propuesta Técnica y Económica y Apertura de Propuesta Técnica.
c) Si se comprueba que el **PARTICIPANTE** se encuentra en los supuestos de los artículos 37 y 95 de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León, y 38 de su Reglamento.
d) Por no cumplir con la presentación de los sobres tal y como se establece en los puntos 9 y 10 de las presentes bases y estos no están a nombre del **PARTICIPANTE**.
e) Cuando la última hoja de cada uno de los documentos carezca de firma autógrafa.
f) Si se comprueba que algún LICITANTE ha acordado con otro u otros elevar el costo de los bienes, arrendamientos o servicios, o cualquier otro acuerdo que tenga como fin obtener una ventaja sobre los demás LICITANTES.
g) Cuando la documentación presentada por el PARTICIPANTE en la Licitación Pública Nacional esté incompleta, es decir que, si faltara CUALQUIER documento o requisito de los señalados en las bases, o en las aclaraciones que se llegasen a ver en la Junta de Aclaraciones.
h) Si al revisar la información presentada por el PARTICIPANTE se encuentran diferencias o incongruencias que pongan en duda la veracidad de dicha información o falsedad en la misma.

i) Cuando se modifiquen los conceptos o las cantidades a cotizar.
j) Cuando en las propuestas propongan alternativas que modifiquen las condiciones y/o especificaciones establecidas.
k) Si el cheque o la fianza de garantía no cubre por lo menos el 5% del precio total de su propuesta económica, incluyendo I.V.A. en caso de que se genere dicho impuesto.
l) Cuando en caso de que en la visita de inspección que en su caso realice LA CONVOCANTE determine que el PARTICIPANTE no demuestre tener la Capacidad Técnica para garantizar satisfactoriamente el cumplimiento del contrato.
m) Si no cumple con la infraestructura señalada en el punto 9.
n) Si del Resultado de la Evaluación Técnica y/o Económica en su caso emitido por el Área Requirente resulta que no cumple con las Especificaciones.
o) Si del Resultado de la Evaluación cualitativa de la propuesta Técnica y/o Económica en su caso resulta que no cumple con alguno de los requisitos.
p) Cuando las Propuestas Económicas recibidas, estén muy por debajo de los precios obtenidos del Estudio de Mercado Realizado, y se consideren precios no aceptables o se encuentren por encima del techo presupuestal.
q) Si al realizar la verificación de precios, cálculo y sumatoria de los mismos, se compruebe que existe error en los montos asentados.
r) Cuando presenten propuestas en idioma diferente al español.
s) Cuando presenten documentos alterados o apócrifos.
t) Si no presenta las USB solicitadas en el sobre técnico y económico respectivamente.
u) Así como cualquier incumplimiento en las presentes bases de Licitación Pública Nacional.

17. LICITACIÓN DESIERTA.

La Licitación Pública Nacional será declarada desierta en los siguientes supuestos:

a) Cuando no se inscriba **PARTICIPANTE** alguno.
b) Cuando después de revisar las Propuestas Técnicas, recibidas determine que ninguna de ellas es conveniente para los intereses de **LA CONVOCANTE**.
c) Si no se recibe propuesta alguna o todas las presentadas fueren desechadas, se declara desierta la Licitación Pública Nacional, levantándose el acta correspondiente conviniendo expresamente el **PARTICIPANTE** de liberar de toda responsabilidad y no se reserva reclamación presente o futura, civil, administrativa o de cualquier otra naturaleza en contra de **LA CONVOCANTE**.
d) Cuando por caso fortuito o fuerza mayor, sea imposible realizarse dicho procedimiento tales como (falta de energía eléctrica, terremoto, derrumbe, huracán, etc.).
e) Cuando las propuestas económicas, rebasen el monto autorizado para la adquisición de los productos y/o servicios objeto de la presente licitación.
f) Cuando la mejor propuesta sea presentada por una empresa que tenga antecedentes documentados de incumplimiento con el municipio.

18. SUSPENSIÓN Y/O CANCELACIÓN TOTAL O PARCIAL DEL PROCESO DE LA LICITACIÓN.

LA CONVOCANTE a su juicio, sin existir causa alguna, sin necesidad de declaración judicial y/o administrativa, tendrá el derecho de suprimir o cancelar total o parcialmente la Licitación en cualquier etapa de dicho proceso, sin que tengan derecho los **PARTICIPANTES** a exigir indemnización o reclamación económica alguna, el cumplimiento del procedimiento de Licitación y/o cualquier otro concepto. El **PARTICIPANTE** sólo tendrá derecho a la devolución del pago de las bases, siempre y cuando se haya realizado el pago en las cajas de cobro de **LA CONVOCANTE**, para tal efecto deberá entregar el original del recibo que acredite dicho pago.

Así mismo, **LA CONVOCANTE** estará facultada para determinar la cancelación de un procedimiento de Licitación Pública Nacional por razones de programación, restricción o reducción presupuestal o por haberse presentado una disminución en la disponibilidad de recursos para financiar el proyecto respectivo.

19. DERECHOS DE LA CONVOCANTE.

19.1 COMPROBACIÓN POR PARTE DE LA CONVOCANTE.

LA CONVOCANTE se reserva el derecho de verificar toda la información proporcionada por el **PARTICIPANTE** en cualquier momento de la Licitación Pública Nacional o posterior a ella y para el caso de que la misma no cumpla con la Ley o lo establecido dentro de las presentes bases se procederá a rechazar la propuesta, toda vez que la omisión o incumplimiento de cualquiera de los requisitos y documentos solicitados, faculta de pleno derecho a **LA CONVOCANTE** a desechar cualquier propuesta.

19.2 FACULTADES POR PARTE DE LA CONVOCANTE.

LA CONVOCANTE tiene la facultad en todo tiempo para suspender, suprimir, cancelar o modificar cualquier suministro y/o servicio y/o arrendamiento contratado, sin que exista causa que lo justifique y sin que por ello el **PARTICIPANTE** tenga derecho a exigir reclamación o indemnización alguna, bastando para ello, la simple notificación por oficio de **LA CONVOCANTE** al **PARTICIPANTE**.

19.3 INSPECCIONES.

LA CONVOCANTE tiene el derecho de visitar las instalaciones de los **PARTICIPANTES** durante el desarrollo de la Licitación Pública Nacional para verificar la información presentada por ellos, asimismo, podrá realizar durante la vigencia del contrato, evaluaciones analíticas y de atributos del servicio, para verificar que cumplan con las especificaciones y requisitos de calidad requeridos en las presentes bases, otorgando el **PARTICIPANTE** ganador las facilidades necesarias al personal

que **LA CONVOCANTE** designe para tal efecto.

Así mismo, **LA CONVOCANTE** sin perjuicio de las atribuciones correspondientes a la Secretaría de la Contraloría y Transparencia del Municipio, podrá verificar la calidad de los bienes o servicios requeridos mediante las personas que **LA CONVOCANTE** designe para ello y así lo notifique al proveedor adjudicado. El resultado de las comprobaciones se hará constar en un dictamen que será firmado por quien haya hecho la comprobación, así como por el proveedor y un representante de **LA CONVOCANTE**, de los bienes o servicios. La falta de firma del **PROVEEDOR** no invalidará el dictamen, lo anterior de conformidad con lo dispuesto por el artículo 32 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León.

20. ASPECTOS ECONÓMICOS.

20.1 DEL PRECIO.

El contrato se celebrará bajo condición de precio fijo.

20.2 FORMA DE PAGO.

La forma de pago será mensual contra entrega de reportes y de acuerdo a lo siguiente:

El **PARTICIPANTE** recibirá de **LA CONVOCANTE** como pago por el suministro y/o servicio y/o arrendamiento objeto de la presente Licitación y a satisfacción de este último por los trabajos contratados, a través de transferencia electrónica dentro de los 10 días hábiles contados a partir de la presentación de la(s) factura(s) ante la Dirección de Egresos de la Secretaría de Finanzas y Tesorería Municipal, sujeto a que la documentación soporte este completa y correcta. Los días de pago serán los miércoles de cada semana. De acuerdo al apartado VII. Políticas Generales, en Específicas, inciso A) Pago a Proveedores (pág.16) punto 21, así como el inciso B) Pago Directo (pág. 19) punto 35 al Manual de Políticas y Procedimientos Generales Administrativos de la Dirección de Egresos. Este plazo está sujeto a que la documentación soporte esté completa y correcta. Queda convenido que la forma de pago se efectuará en Moneda Nacional.

Las facturas que sean presentadas para trámite de pago deberán ser a favor del Municipio de San Pedro Garza García NL, con Registro Federal de Contribuyentes MSP8212143G3, con domicilio en la calle Libertad No. 101, colonia Centro, C.P. 66200, en original, documento que debe reunir los requisitos fiscales establecidos en los artículos 29 y 29-A del Código Fiscal de la Federación. Así mismo, la facturación será por precios unitarios, unidades completas y/o servicios prestados, haciendo mención de las características particulares de la prestación del servicio, arrendamiento o suministro entregado, anotándose además el número y fecha del contrato, así como el nombre del **PARTICIPANTE**.

21. DEL CONTRATO.

La contratación abarcará 3–tres ejercicios fiscales.

Una vez adjudicada la Licitación Pública Nacional el **PARTICIPANTE** ganador deberá firmar el contrato correspondiente en la fecha, hora y lugar que se establezca en el acta de Fallo Definitivo y Adjudicación, en caso de no formalizarse el contrato por causas imputables al **PARTICIPANTE**, se hará efectiva la garantía de seriedad de su propuesta solicitada en las presentes bases, por el simple retardo en su cumplimiento y la presente adjudicación dejará de surtir efectos, asimismo, **LA CONVOCANTE** sin necesidad de un nuevo procedimiento podrá asignar el contrato al **PARTICIPANTE** que haya obtenido el segundo o ulteriores lugares, siempre que la diferencia en precio con respecto a la propuesta inicialmente adjudicada no sea superior a un margen del diez por ciento.

En caso de que el **PARTICIPANTE** ganador no firme el contrato correspondiente, será sancionado en los términos del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León.

22.1 CARACTERÍSTICAS DEL CONTRATO.

El servicio, arrendamiento o suministro establecido en el contrato podrá variar hasta un +/- 20% según las necesidades de **LA CONVOCANTE**, sin que por esto se modifiquen las condiciones que se asienten en el contrato correspondiente.

22. GARANTÍAS.

a. **GARANTÍA DE ANTICIPO.-** No se otorgará anticipo.

b. **GARANTÍA DE BUEN CUMPLIMIENTO DEL CONTRATO**.- El **PARTICIPANTE** ganador presentará a **LA CONVOCANTE**, dentro de los 10-diez días hábiles contados a partir de la fecha en que se suscriba el contrato, una fianza de garantía equivalente al 10% del valor total del contrato incluyendo I.V.A., a fin de garantizar y asegurar el fiel y oportuno cumplimiento del mismo y de los defectos, vicios ocultos u otras responsabilidades en que pudieran incurrir de conformidad con la legislación aplicable y el contrato respectivo, la cual deberá estar vigente hasta seis meses posteriores a la entrega.

Así mismo, continuará vigente hasta la substanciación de todos los recursos legales o juicios que se interpongan hasta en tanto se dicte resolución definitiva por autoridad competente, incluyendo el juicio de amparo en caso de conflicto legal entre **LA CONVOCANTE** y el **PARTICIPANTE** ganador, ante cualquier autoridad judicial o administrativa.

23. PENA CONVENCIONAL, MULTAS Y SANCIONES.

PENA CONVENCIONAL.- El **PARTICIPANTE** asignado se hará acreedor a una pena convencional por el atraso en la entrega de los bienes, arrendamientos o servicios, así como por el incumplimiento de sus obligaciones, de conformidad con lo que establece el artículo 46 fracción XIX de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León. La penalización se calculará con un porcentaje del 1% por cada día hábil de retraso contra lo no entregado, en la entrega de los bienes, arrendamientos o servicios sobre el monto unitario de cada uno de los bienes solicitados y que el proveedor no entregue en los tiempos establecidos, y de manera proporcional al importe de la garantía de buen cumplimiento del contrato. La penalización, iniciará al día siguiente del plazo de vencimiento para la entrega de los bienes, arrendamientos o prestación del servicio, lo anterior previa notificación de atraso emitida por el Área Requirente.

MULTAS Y SANCIONES.- De conformidad con lo establecido en el artículo 251, fracción I, inciso b), del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León, **LA CONVOCANTE** podrá hacer efectivas las multas y demás sanciones que se apliquen al **PARTICIPANTE** adjudicado con cargo a la garantía que se entregue. La pena por incumplimiento en el servicio, no podrá exceder del monto de la garantía de buen cumplimiento del contrato.

24. RECURSO.

El domicilio para presentar el recurso de reconsideración será el ubicado en la calle Independencia No. 316, Colonia Centro en San Pedro Garza García, Nuevo León, C.P. 66200.

25. SUPLETORIEDAD.

En cuanto a lo no previsto por el Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León, supletoriamente le serán aplicables, la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León, así como el Reglamento de dicha Ley, el Código Civil del Estado, el Código de Procedimientos Civiles del Estado, la Ley de Egresos del Estado de Nuevo León para el ejercicio fiscal 2025 y las demás disposiciones jurídicas aplicables.

Las condiciones establecidas en la convocatoria para la Licitación Pública Nacional no podrán ser negociadas, de conformidad con el artículo 131, fracción I, inciso h), del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro garza García, Nuevo León, ni lo establecido en las presentes bases.

ANEXO 1
ESPECIFICACIONES TÉCNICAS

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS

DESCRIPCIÓN DEL SERVICIO: Suministro de licencias, suscripciones de seguridad informática, soporte de infraestructura instalada, equipamiento en sitio necesario y servicios administrados; así como proveer los servicios administrados de dicha infraestructura para reducir riesgos asociados a la seguridad en la red, navegación en internet, portales web, equipos de cómputo y bases de datos de sistemas municipales.

ALCANCE DEL OBJETO:
Proveer de seguridad informática al municipio de San Pedro Garza García en su infraestructura Manteniendo licencias y suscripciones vigentes, así como personal dedicado para Proveer los servicios administrados con el fin de mantener las actualizaciones de nuevas firmas de seguridad de forma constante; es decir las actualizaciones que vayan surgiendo para proteger de nuevas formas de ataques y de vulnerabilidades que puedan darse en la operación diaria de los diversos usuarios del Municipio. Los servicios deberán ser administrados y supervisados por personal de la compañía. La compañía deberá trabajar en conjunto y bajo supervisión de la Dirección de Tecnologías del Municipio.

Se adjuntan (anexos) documento técnico donde especifica cantidades y descripciones detalladas, así como tareas básicas de los servicios administrados esperados sin dejar de tomar en cuenta las generalidades descritas en el presente documento.

RESUMEN FORMAL DE SERVICIOS DE INGENIERÍA ESTRATÉGICA PARA LA PROTECCIÓN CONTRA AMENAZAS CIBERNÉTICAS

El presente documento detalla los servicios de ingeniería estratégica diseñados para salvaguardar los sistemas y redes del municipio ante una diversidad de amenazas cibernéticas. Se describen a continuación las áreas clave de protección:

- **Prevención de intrusiones no autorizadas** al portal oficial y páginas públicas del municipio, con el objetivo de evitar la modificación o daño de dichos recursos.
- **Defensa contra ataques** originados en archivos consultados o descargados de internet que puedan contener código malicioso.

- **Protección contra amenazas** vehiculizadas a través de archivos descargados desde correos electrónicos, tanto oficiales como no oficiales.
- **Impedimento de acceso no autorizado** a la red interna con la intención de dañar aplicaciones y/o servidores.
- **Salvaguarda de bases de datos** contra accesos no autorizados que busquen afectar, dañar o sustraer información confidencial y sensible.
- **Mitigación de ataques** a la infraestructura de red mediante la saturación de accesos (ataques de denegación de servicio).
- **Protección integral** contra daños causados por nuevos virus, versiones o variantes de malware.
- **Prevención del secuestro de información** (ransomware) en los equipos de cómputo del municipio.
- **Resguardo contra ataques** que puedan comprometer los sistemas operativos y aplicaciones fundamentales para la operación municipal.
- **Detección y eliminación de código malicioso** (malware) en los equipos de cómputo que puedan afectar la operatividad diaria.
- **Protección contra malware** diseñado para infiltrarse en los dispositivos municipales con el fin de robar información confidencial, identidades o credenciales de acceso.

Este enfoque integral tiene como objetivo asegurar que el municipio pueda operar de manera segura y eficiente, minimizando el riesgo de interrupciones causadas por amenazas cibernéticas.

DETALLE CARACTERÍSTICAS Y ESPECIFICACIONES TÉCNICAS DEL BIEN Y/O SERVICIO:

Anexos adjuntos

SERVICIOS DE GESTIÓN DE HERRAMIENTAS DE SEGURIDAD.

La empresa deberá proveer servicios de gestión de las herramientas de seguridad implementadas bajo un esquema 5x8 y deberá incluir al menos una junta semanal informativa de hechos, así como juntas de emergencias en caso de eventos extraordinarios.

El servicio contratado deberá comprender, como mínimo, las siguientes actividades esenciales dentro de su alcance:

- **Supervisión integral del estado operativo de las herramientas gestionadas**, incluyendo la verificación del correcto funcionamiento de los servicios y la adecuada generación de registros (logs) en las consolas correspondientes.
- **Ejecución de pruebas de funcionalidad**, diseñadas para asegurar, de manera expedita y eficiente, el óptimo desempeño de las herramientas.
- **Revisión y análisis diario de alertas**, con especial atención a aquellas que señalen potenciales amenazas o desviaciones que requieran intervención inmediata.
- **Ajuste y optimización de la configuración de las herramientas**, garantizando su rendimiento y eficiencia.
- **Implementación de configuraciones en las herramientas**, en respuesta a acciones proactivas, preventivas o reactivas, con el objetivo primordial de evitar cualquier interrupción en el servicio. Estas actividades se llevarán a cabo en estrecha coordinación con el Municipio, asegurando una comunicación fluida y efectiva.
- **Establecimiento y seguimiento de Indicadores Clave de Rendimiento (KPIs)**, con el fin de garantizar la robustez y salud de las herramientas. Estos indicadores permitirán la mitigación de riesgos, mediante el aumento de la cobertura y la optimización de las herramientas.
- **Propuesta de mejoras a las herramientas o infraestructura**, basadas en la supervisión continua del servicio administrado. Se deberán recomendar cambios y mejoras necesarias para disminuir riesgos y fortalecer la seguridad, incluyendo, pero no limitándose a, mejoras en la arquitectura, configuraciones, políticas, versiones de software o hardware, mejores prácticas y la corrección de desviaciones en los procesos.
- **Implementación de actualizaciones**, siempre y cuando estas no impliquen cambios mayores de versión.

Se garantizará la atención ininterrumpida (24 horas al día, 7 días a la semana, 365 días al año) de incidentes graves o críticos, en estricta observancia de los Acuerdos de Nivel de Servicio (SLAs) detallados en el presente documento.

La empresa proveedora deberá facilitar al menos tres medios de contacto distintos, debidamente alineados con los niveles de criticidad correspondientes a cada uno.

La empresa deberá proporcionar al menos 3 medios de contacto distintos, alineados con los niveles de criticidad correspondientes para cada uno.

La empresa deberá proveer sus servicios de gestión de herramientas bajo un esquema jerárquico de atención a solicitudes L1 y L2, que minimice la necesidad de escalaciones de soporte técnico al fabricante.

Cada participante debe presentar la carta de fabricante donde lo respalde en la solución que está ofertando.

La empresa deberá incluir en la entrega de sus servicios de gestión, al menos los siguientes roles:

- **Respaldo del Ingeniero del Fabricante Remoto Dedicado**. Durante 12 meses para apoyo en la implementación, migración, operación y adopción de nuevas tecnologías para los servicios 1.1, 1.2, 1.3, 1.4, 3.1, 3.2, 3.3, 3.4, 3.5, 5.1, 7.1, 7.2, 7.3, 9.1.
- **Ingeniero Analista L1.** Encargado de atender las solicitudes de soporte básico del cliente y realizar la primera línea de diagnóstico y resolución de problemas. Monitorea los sistemas y realiza la primera intervención en caso de incidencias, escalando los problemas no resueltos al nivel correspondiente de soporte. Se asegura de registrar y documentar adecuadamente todas las interacciones con el cliente y las soluciones implementadas.
- **Ingeniero Analista L2.** Encargado de atender las solicitudes de soporte del cliente de nivel 2, proporcionando soluciones avanzadas y resolviendo problemas complejos para el Analista L1.
- **Ingeniero de Operaciones.** Líder de los analistas, responsable de coordinar las actividades de soporte y ser el contacto principal para presentar avances dentro de las sesiones de seguimiento. Experiencia en liderazgo de equipos técnicos, capacidad para gestionar proyectos, habilidades de presentación y comunicación, estas funciones serán realizadas de manera híbrida, remoto o en sitio.
- **Gerente de Servicios Administrados:** Responsable de supervisar y coordinar todos los aspectos relacionados con los servicios administrados ofrecidos a los clientes. Se encarga de establecer estrategias, gestionar equipos y garantizar la entrega exitosa de los servicios de acuerdo con los requisitos y expectativas del cliente, estas funciones serán realizadas 100% de manera Remota.
- **Ingeniero de Soporte.** Responsable de la resolución de problemas y responder consultas complejas, relacionadas con las herramientas gestionadas. Tendrá la responsabilidad de escalar al fabricante, cuando sea necesario.
- **Customer Advisor:** Responsable de guiar, con carácter técnico, la materialización de los niveles de servicio e indicadores de desempeño definidos

buscando crecimiento y evolución del servicio en pro de mayor robustez de la seguridad de la información en las cuentas asignadas, estas funciones serán realizadas 100% de manera remota.

Se deberá proveer al menos un ingeniero en sitio, de lunes a viernes, en horario de 8 am a 4 pm

La Empresa será responsable de estar al pendiente de las actualizaciones de firmas que surjan y aplicarlas en coordinación con la Dirección de Tecnologías.

La Empresa deberá proporcionar un número de contacto para atención del Municipio, en el que se canalizará la llamada de forma inmediata con un ingeniero certificado. Deberá proporcionarse una forma de contacto para eventos de emergencia en horas no hábiles.

Como parte de los alcances del servicio de gestión, se deberán entregar, al menos los siguientes reportes:

- **Mensual de cobertura de métricas.** Que permita dar seguimiento a la efectividad de los controles de seguridad implementados, así como recomendaciones de mejora en operación o detección de incidentes.
- **Mensual de operación de herramientas.** Que permita evaluar el uso y desempeño de los sistemas implementados y la efectividad del servicio

SERVICIOS DE MONITOREO DE SEGURIDAD.

Se deberá proveer un servicio de monitoreo de eventos de seguridad en un esquema 5x8, que esté alineado con buenas prácticas de ciberseguridad, de acuerdo con el marco NIST CSF v2.0 e ISO/IEC 27001. El servicio deberá incluir la disponibilidad de un SOC ubicado en Monterrey o su zona metropolitana.

La empresa deberá incluir como parte de sus servicios una herramienta de tipo XDR, para la ejecución de sus actividades de monitoreo.

El proceso de monitoreo de eventos de ciberseguridad deberá cumplir con las siguientes etapas:

- Integración con fuentes de información dentro del entorno de seguridad del municipio.
- Calificación de los distintos tipos de eventos identificados, investigando a profundidad o descartándolos conforme al contexto de seguridad y experiencia de los analistas de ciberseguridad.

El servicio deberá incluir el monitoreo de eventos de ciberseguridad y la elaboración y entrega de reportes que permitan conocer el contexto de las detecciones y las recomendaciones que puedan ayudar a mitigarlo o contenerlo.

Gestión de respuesta a incidentes

Un incidente es considerado un evento confirmado que afecta a la disponibilidad, integridad y/o confidencialidad de la información y la infraestructura del Municipio.

Como parte de los alcances del servicio, se deberá incluir la capacidad de responder al menos a un evento de criticidad alta o dos eventos de criticidad media, para su gestión bajo demanda.

La empresa deberá cumplir con al menos las siguientes características en la entrega de sus servicios:

- **Investigación y Análisis de Incidentes:** Investigación exhaustiva de los incidentes detectados para comprender su alcance, impacto y método de entrada, recolección de evidencia y determinación de la causa raíz.
- **Comunicación y Notificación:** Comunicación clara y oportuna con las partes interesadas internas y externas, incluidos los equipos de liderazgo y los empleados, según sea necesario.
- **Bitácora del incidente gestionado:** Registro detallado y documentación de todos los incidentes reportados, incluidos los pasos tomados durante la respuesta.
- **Lecciones aprendidas y recomendaciones:** Documentación y entrega de lecciones aprendidas para mejorar la preparación futura, evaluación de la eficacia de la respuesta al incidente después de que este se haya resuelto, identificando áreas de mejora y desarrollando planes de acción para fortalecer la postura de seguridad de la organización.

El servicio deberá cubrir al menos las siguientes actividades:

- Coordinar la ejecución de las tareas del proceso de respuesta a incidentes y asignación de tareas a las partes involucradas.
- Comunicar del proceso y las tareas a ejecutar durante la respuesta al incidente a las partes involucradas.
- Asegurar que exista sintonía y comunicación entre todas las partes involucradas y que se siga el flujo del proceso de respuesta a incidentes.
- Identificar acciones vs los hallazgos del incidente de seguridad.

- Reportar el estatus durante la duración del incidente y hasta el cierre de este.
- Brindar asesoría en la ejecución de tareas de remediación y contención al personal del Municipio sobre las herramientas no administradas por la empresa.
- Dar seguimiento a la implementación de recomendaciones para aplicar por parte del Municipio a través del envío de un plan de Medidas de Contención y Mitigación del incidente. Este plan integrará un reporte detallado de las actividades a realizar o realizadas durante el incidente, sus fuentes y sus objetivos, así como la documentación técnica basada en MITRE ATT&CK sobre la táctica invasiva. Este reporte no deberá ser una dependencia para la ejecución de los servicios de gestión de respuesta.
- Documentar acciones realizadas y lecciones aprendidas.

La empresa deberá llevar a cabo un levantamiento inicial del entorno de seguridad del Municipio, de modo que pueda gestionar de manera rápida y eficaz a los eventos que puedan presentarse.

LUGAR DE PRESTACIÓN DEL SERVICIO O ENTREGA DE BIENES: El servicio se entregará en la Dirección de Tecnologías, con el Lic. Claudia Esther Cervantes Alanis en Corregidora 507 Centro, C.P. 66200 San Pedro Garza García, N.L. teléfono 81-8400-45-95.

ENTREGABLES ADICIONALES EN CASO DE APLICAR:

Los entregables son:

Servicios administrados de seguridad informática.

- Reporte mensual vía correo electrónico de los acontecimientos suscitados durante el mes.
- Reporte semanal de indicadores de calidad operativa, vía correo electrónico que incluya:
  - Ataques bloqueados por red
  - Cantidad de malware detectado y eliminado en computadoras
  - Intentos de intrusión bloqueados
  - Intentos de acceso a internet con riesgo de seguridad
  - Incidentes de seguridad

Nivel de Servicio Esperado (SLA)

El proveedor deberá contar para los servicios contratados con una mesa de servicios que se encargará del registro, atención, solución y cierre de incidentes y requerimientos de soporte generados por parte del MUNICIPIO DE SAN PEDRO.

Dicha mesa operará resolviendo los temas que pueden atenderse de manera inmediata y que son concernientes a la implementación específica del MUNICIPIO DE SAN PEDRO y realizando las escalaciones necesarias para aquellas situaciones que requieran atención del especialista indicado.

De esta manera, el proveedor deberá garantizar al MUNICIPIO DE SAN PEDRO tener un canal de comunicación abierto con atención personalizada.

Las actividades que el proveedor deberá realizar en el servicio administrado sobre servicios contratados son:

- Soporte técnico para incidentes graves sobre todos los servicios contratados en esquema de 7x24 365 días del año.
- Servicio de monitoreo automatizado con detección y resolución de fallas, así como optimización de desempeño.
- Tiempos de respuesta de acuerdo con el tipo de incidente (descripciones de estos más abajo).
- Planificación y recomendaciones para la optimización de arquitectura.
- Monitoreo continuo de servicios de seguridad y accesos.

Modelo de Operación

Una vez concluido el periodo de implementación de los Servicios Contratados, el equipo de soporte del proveedor comenzará con la administración de los controles de seguridad con base en tiempos de atención y solución predefinidos (niveles de servicio).

La información de contacto para realizar el levantamiento de cualquier solicitud deberá ser basada en la siguiente tabla (agregar contactos de ser necesario):

Contacto	Correo	Teléfono
Ingeniero de soporte		
Ingeniero de escalación		

Al realizar el reporte, éste será turnado a los especialistas del proveedor, los cuales darán seguimiento a las solicitudes.

Atención de Incidentes operativos

El equipo de servicios administrados atenderá los incidentes operativos reportados por MUNICIPIO DE SAN PEDRO y escalará a soporte técnico conforme al siguiente proceso:

A cada incidente, la Mesa de Servicio asignará una prioridad para cumplir con los requerimientos y expectativas del usuario, respetando los criterios de impacto y urgencia. Esta prioridad facilitará la atención de incidentes y escalará la atención a los mismos, de acuerdo con la magnitud de cada incidente y las cargas de trabajo existentes en el proceso.

Las prioridades que serán asignadas a los incidentes se obtendrán al aplicarles la siguiente matriz:

Matriz de cálculo de prioridades

IMPACTO				
URGENCIA	Extenso/ Generalizado	Significativo/ Amplio	Moderado/ Limitado	Menor/ Localizado
Crítica	A	A	B	B
Alta	A	B	B	C
Media	B	C	C	C
Baja	D	D	D	D

Donde:

Impacto: determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados.

Urgencia: Depende del tiempo máximo de demora que sea factible soportar para las operaciones de municipio.

Dentro de la atención se dará prioridad a los incidentes que se generen como críticos. (Considerando que un incidente es un evento que ocurre de forma inesperada y que está ocasionando un impacto grave en la operación o el servicio).

Tipos de prioridades

A-Crítico

El incidente estará asociado con la afectación total de uno o más productos que no están disponibles. Existe un impacto severo en la operación. Este tipo de incidentes requieren resolución inmediata por parte del proveedor y podrían ser necesarias escalaciones jerárquicas, y ayuda de diferentes áreas de especialidad para su atención.

B- Alto

El producto se puede utilizar, pero de una forma alterada, se tiene un impacto moderado en el municipio y puede ser tratado durante el horario normal. Un único usuario de MUNICIPIO DE SAN PEDRO, o producto están parcialmente afectados. Este tipo de incidentes también requieren resolución inmediata, podrán necesitar ayuda de diferentes áreas de especialidad para su atención y escalaciones jerárquicas de ser necesario.

C- Medio

La falla tiene un impacto organizacional mínimo, no hay impacto del producto o la productividad para MUNICIPIO DE SAN PEDRO. Un solo usuario está experimentando interrupción, por lo que la atención del incidente no requiere de atención inmediata, sin embargo, no puede ser diferida en un lapso de tiempo considerable.

D- Bajo

Falla en la que su atención y solución puede ser calendarizada. El incidente afecta a uno o pocos usuarios de un servicio, cuando éste se encuentra disponible pero su capacidad operativa se ve reducida. La atención de estas incidencias puede esperar un tiempo adecuado para su solución.

Tiempos de atención y niveles de servicio.

El proveedor deberá considerar los niveles de servicio que se estipulan a continuación:

Tiempo de Atención: Tiempo que transcurre desde la creación del ticket hasta su documentación por parte del ingeniero indicando que ya está trabajando en su solución. Es

decir, el momento en el que pasa de estado “Nuevo” a “En curso” en la herramienta de seguimiento.

Tiempo de Solución: Tiempo que transcurre desde la creación del ticket hasta su solución. Es decir, desde el momento en que pasa de estado “En curso” a “Resuelto”.

Niveles de servicios para el manejo de incidentes.

El proveedor ofrecerá un esquema de niveles de servicio como se indica a continuación para la atención de incidentes

Nivel de Severidad	Tiempo de Monitoreo del Requerimiento	Tiempo de Atención	Tiempo de Solución
A-Crítico	Cada hora	10min	< 3 hrs
B- Alta	Cada 2 hrs	15min	< 4 hrs
C- Medio	Cada día hábil	30min	< 48 hrs
D- Bajo	Cada dos días hábiles	60min	< 72 hrs

Para requerimientos nuevos, los tiempos de atención que deberá brindar El proveedor serán los siguientes:

Nivel de Severidad	Tiempo de Monitoreo del Requerimiento	Tiempo de atención	Tiempo de Solución
C- Medio	Cada día hábil	4 hrs	< 48 hrs
D- Bajo	Cada dos días hábiles	8 hrs	< 72 hrs

Gestión de Cambios

El proceso de cambios se encontrará directamente relacionado con las modificaciones que se realizarán en la infraestructura, por lo tanto, el proceso con el que deberá cumplir el proveedor se ha definido de la siguiente manera:

Los cambios que se atenderán dentro de la operación son:

- CAMBIOS NORMALES: Son aquellos cambios que están planeados y siguen el proceso completo

- CAMBIOS EMERGENTES: Son aquellos cambios que realizan para reparar un error en un servicio derivado de un incidente, lo cual provoca un impacto negativo en el municipio
- CAMBIOS ESTÁNDAR: Son aquellos cambios que se hacen de manera rutinaria y que se encuentran pre-aprobados.

Nivel de cambio	Tiempo de atención	Tiempo de Solución
Cambios Normales	2 hrs	< 48 hrs
Cambios Emergentes	15 min	< 4 hrs
Cambios Estándar	2 hrs	<48 hrs

ANEXO A. REQUERIMIENTOS DE PRODUCTOS

En esta sección se señalan los productos y sus capacidades generales, así como las cantidades requeridas.

Las soluciones de software propuestas deberán contar con soporte técnico directamente del fabricante, con disponibilidad 24/7 y Acuerdos de Nivel de Servicio (SLA) definidos y garantizados. Este soporte técnico deberá incluir actualizaciones de software, parches de seguridad y asistencia para la resolución de problemas

Las capacidades y/o características específicas detalladas de los mismos se encuentran en el anexo E.

Vale la pena señalar que las capacidades y/o características requeridas son consideradas como mínimas y que deben cumplirse en su totalidad e incluyendo las descritas en este apartado y el anexo E.

Las consideraciones para el aprovisionamiento de los productos son:

- Que los controles/herramientas tengan el menor número de consolas con el objetivo de reducir el esfuerzo de administración
- Que los componentes incluyan su propia plataforma de hardware, si así se requiere.

REFERENCIA PARA ANEXOS	DESCRIPCIÓN GENERAL DE LAS CAPACIDADES DE LA TECNOLOGÍA	
1	**PLATAFORMA DE SEGURIDAD PARA LA NAVEGACIÓN, LAS APLICACIONES SAAS Y EL ACCESO SEGURO A LA RED.** **Que sea una plataforma unificada, administrada desde la nube, con capacidades para "Cloud Access Security Broker" (CASB), control de acceso basado en Zero Trust (mínimo privilegio) y protección integral de la navegación web.**	**CANTIDAD**
1.1	**Control en la navegación y seguridad web** Que cuente con un Secure Web Gateway (SWG) en la nube para filtrar contenido basándose en categorías web, niveles de riesgo o detección de "Shadow IT". Debe ofrecer al menos una modalidad de "Remote Browser Isolation" para sitios sospechosos o maliciosos, así como control de acceso a los "tenants" corporativos, limitando el acceso a instancias personales. Además, debe contemplar políticas de prevención de fuga de información (DLP básico) en el canal web. La protección debe instalarse o configurarse en PCs, Mac, iOS y Android—ya sea mediante un agente/cliente o un modo proxy—para inspeccionar y asegurar la navegación, tanto dentro como fuera de la red corporativa.	1,500
1.2	**"Cloud Access Security Broker"** Que el CASB pueda integrarse mediante API con las aplicaciones SaaS o como un reverse proxy/agente, permitiendo visibilidad de la actividad de usuarios y de la información manejada en servicios en la nube (Google Workspace, Office 365, etc.). Debe contar con análisis de comportamiento que, en caso de detectar amenazas o acciones indebidas, pueda controlar y bloquear accesos. Es esencial que permita acotar la actividad en herramientas de colaboración como Google Drive y Gmail, manejando restricciones de lectura, descarga o compartición, según las políticas definidas. Asimismo, se espera que soporte integraciones SSO/IdP para autenticar y aplicar controles de acceso según el contexto de usuario y dispositivo.	

1.3	**Control de acceso a la red con el mínimo privilegio** Que sea parte de la misma plataforma (enfoque Zero Trust), con la capacidad de proveer acceso seguro a cualquier protocolo que use puertos TCP/UDP, segmentando de forma lógica el acceso a recursos internos. Debe incluir autenticación multifactor (MFA), validando además la "postura" del dispositivo (por ejemplo, la presencia de antivirus activo) previo a conceder el acceso. Idealmente, requerirá un gateway en la nube que no obligue a publicar el recurso en el firewall de forma tradicional, sino que utilice túneles salientes o un conector en la red, evitando la exposición de IPs públicas. Esto permite un control granular para autorizar únicamente a usuarios, horarios o dispositivos específicos.	
2	**PLATAFORMA ANTI MALWARE** Que sea una plataforma que se tenga la opción para instalarse en la nube Y en una consola en sitio, para administrar controles específicos o solventar cualquier requerimiento normativo	**CANTIDAD**
2.1	**Anticipación de campañas de malware** Que cuente con un módulo para identificar de manera anticipada campañas de malware y la afectación de las mismas en el mundo y en el ambiente del municipio y que este módulo identifique si hay indicadores de compromiso que señalan la presencia de malware en el ambiente y que señale los mecanismos de afectación basados en el marco de Mitre	1,500
2.2	**Antimalware con anti ransomware y parcheo virtual** Que cuente con un módulo específico anti ransomware que permita "regresar" a su estado inicial a una computadora si esta llega a ser cifrada y que tenga diferentes mecanismos para solventar la infección de cualquier malware como pueden ser controles de reputación, controles basados en algoritmos de machine learning, sandbox, controles basados en firmas o vacunas, así como que permita acotar el impacto de las amenazas relacionadas a parches de tal forma que pueda evitar su explotación y que soporte los sistemas operativos Windows, Linux Ubuntu y Debian	
2.3	**Control de dispositivos periféricos en las computadoras**	

	Que cuente con el control de dispositivos periféricos en los sistemas operativos Windows y Mac, de tal modo que les detecte todas sus capacidades y que pueda acotar su acceso de manera general o específica, utilizando algún criterio como pudiera ser el número de serie, fabricante o modelo, etc. Los medios que debe poder controlar son USB, Bluetooth, dispositivos multimedia, smartphones, Smartphones	
2.4	**Control de cambios para servers**	
	Que cuente con un mecanismo para evitar los cambios no permitidos de cualquier índole en los servidores de los sistemas operativos Windows y Linux Ubuntu, Debian, Fedora	
2.5	**Control de aplicaciones para computadoras**	
	Que cuente con un mecanismo de control de aplicaciones que, basado en un inventario obtenido de todo el ambiente del municipio de San Pedro, evite la instalación y/o ejecución de la misma, así como que permita la ejecución específica de aplicaciones basado en un inventario que señale las aplicaciones que sí se puedan instalar o ejecutar. Que cuente con los siguientes mecanismos de operación: permitir señalar usuarios de confianza que pueda instalar cualquier aplicación, que permita señalar directorios compartidos en la red como de confianza, que pueda permitir si así se señala a cualquier usuario justificar la instalación de una aplicación para su posterior validación	
2.6	**Firewall para las computadoras**	
	Que cuente con un módulo que permita, desde la perspectiva de las computadoras bloquear el tráfico de la red sobre puertos y aplicaciones específicas, desde un punto central y uniforme	
2.7	**EDR para Servidores**	
	Que cuente con un EDR que soporte sistemas operativos Windows y Linux, que además cuenta con la capacidad de ofrecer investigaciones guiadas. Que retenga la información para su análisis al menos por 30 días	100
2.8	**Sandbox para análisis**	
	Que cuente con un sandbox que se pueda integrar a la seguridad en el endpoint como una capa de protección adicional para identifica amenazas de día cero	1
2.9	**Parchado y gestión de endpoints.**	

	Que cuente con la capacidad de parchado automático o con la capacidad de integrar a un tercero para realizarlo. Debe poder instalar parches de infraestructura Windows y Linux, así como de aplicaciones y/o plataformas comunes como adobe. Debe tener mecanismos alternos a los estándares para poder realizar la instalación de los parches en específico los de seguridad. La solución deberá contar con la capacidad de llevar a cabo la instalación de builds. La solución deberá contar además con la capacidad de proveer control y administración remota de dispositivos, inventario detallado de hardware y software, automatización de tareas repetitivas como instalaciones o actualizaciones, monitorización en tiempo real del desempeño de los equipos para detectar y solucionar problemas proactivamente, así como la configuración de alertas y notificaciones personalizables basadas en eventos críticos o condiciones específicas, todo con compatibilidad para sistemas Windows, macOS y Linux, la gestión de endpoints deberá estar disponible en la misma consola de gestión de parches.	
3	**INTEGRACIÓN DE INTELIGENCIA DE PREVENCIÓN DE INTRUSOS DE RED** Contar con una plataforma de detección y prevención de intrusiones que, a partir del análisis de registros y eventos, bloquee comportamientos maliciosos o direcciones IP maliciosas en tiempo real.	**CANTIDAD**
3.1	**Integración con mecanismos de respuesta avanzada** En lugar de solo “bloquear IP,” el sistema podría ejecutar acciones específicas según la amenaza detectada (por ejemplo, aislar el servidor, generar notificaciones a un SIEM, iniciar contención en un WAF). Uso de “bouncers” sofisticados que apliquen reglas de contención a nivel de firewall, WAF, proxy inverso, contenedores, etc.	1
3.2	**Análisis de patrones y colaboración**	

	La solución deberá basarse en la detección de patrones de comportamiento (fuerza bruta, escaneo de puertos, DDoS, etc.) y en el intercambio de inteligencia con la comunidad global, aportando y recibiendo indicadores de amenaza (IP maliciosas, TTPs). Debe permitir personalizar reglas para protocolos sensibles (HTTP, HTTPS, SSH, RDP) y emitir alertas o tomar acciones de bloqueo según la criticidad.	
3.3	**Protección frente a ataques dirigidos** Capacidades de detectar tácticas y técnicas propias de amenazas avanzadas (APT), más allá del simple escaneo o fuerza bruta. Registros y políticas específicas para detectar patrones sigilosos, por ejemplo: enumeración paulatina de usuarios, accesos persistentes, escaladas de privilegio. Integración con inteligencia de amenazas externa (feeds especializados en APT).	
3.4	**Resiliencia ante ataques de larga duración** Capacidad de almacenamiento extendido de logs y eventos para detectar ataques de evolución lenta (low-and-slow). Políticas de retención de datos y análisis histórico para descubrir campañas con un factor de latencia (por ejemplo, un bot en reposo que se activa tras semanas).	
3.5	**Perfiles de ataque para servicios críticos** Escenarios predefinidos o “templates” de protección para aplicaciones de misión crítica (servicios web sensibles, entornos de bases de datos) que brinden configuraciones específicas de detección y bloqueo. Monitorización reforzada de endpoints que alojan aplicaciones con un riesgo superior (servidores de autenticación, portales financieros, etc.).	
4	**Pruebas de Penetración** Se solicita la realización de pruebas de penetración tanto externas como internas, con el objetivo de identificar vulnerabilidades y riesgos en la infraestructura del Municipio. Se deberán cubrir, como mínimo, los siguientes apartados:	CANTIDAD
4.1	**Pruebas de Penetración Externas**	128 IPs Publicas / Urls

	Alcance Realizar pruebas hasta **128 IPs Públicas/Urls** de servicios expuestos a internet (portales web, interfaces de acceso remoto, etc.). Incluir pruebas de fuerza bruta, escaneo de puertos, enumeración de servicios, análisis de vulnerabilidades en aplicaciones web (inyecciones SQL, XSS, CSRF, configuraciones inseguras) y cualquier otro mecanismo que un atacante remoto pudiera utilizar. **Objetivo** Simular un escenario de ataque externo para identificar caminos de intrusión, vulnerabilidades críticas y mecanismos de escalada de privilegios o robo de información. **Metodología:** La metodología de pruebas estará fundamentada en las mejores prácticas y estándares reconocidos a nivel internacional: ● PTES (Penetration Testing Execution Standard) ● OWASP Testing Guide ● NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) ● MITRE ATT&CK Framework, para la emulación de técnicas de adversarios reales. **Requisitos:** Es indispensable que el proveedor del servicio cuente con personal con experiencia comprobable y altamente calificado en escenarios avanzados de hacking ético, análisis de aplicaciones web, desarrollo de exploits y emulación de adversarios. Se requiere que el personal con el que brindara el servicio cumpla con las siguientes certificaciones: ● OffSec Exploit Developer (OSED) ● OffSec Experienced Penetration Tester (OSEP) ● OffSec Web Expert (OSWE) ● OffSec Certified Expert 3 (OSCE3) ● Offensive Security Certified Professional (OSCP) ● Web Application Penetration Tester eXtreme (eWPTX v2.0) ● Certified Penetration Tester eXtreme v2 (eCPTX) ● Certified Secure Web Application Engineer (SWAE)	

	Debiendo anexar currículos con los cuales su personal acredite que cuenta con las certificaciones y acreditar las mismas con copias simples y número de folio. **Entregables** Informe detallado con todas las vulnerabilidades detectadas, su nivel de riesgo, evidencia (logs, capturas de pantalla), posible impacto e instrucciones de remediación priorizada.	
4.2	**Prueba de Penetración Internas** **Alcance** Realizar pruebas hasta **1600 IPs Privadas** dentro de la red interna, cubriendo servidores, bases de datos, equipo de cómputo, servicios de Directorio Activo, dispositivos de red, entre otros. Incluir técnicas de escalada de privilegios, movimiento lateral y exfiltración de información, considerando un escenario de atacante con acceso local o de usuario interno malintencionado. **Objetivo** Identificar fallas de seguridad internas, configuraciones débiles, brechas en la segmentación de red, y oportunidades de mejora en los controles existentes. **Metodología:** La metodología de pruebas estará fundamentada en las mejores prácticas y estándares reconocidos a nivel internacional: ● PTES (Penetration Testing Execution Standard) ● OWASP Testing Guide ● NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) ● MITRE ATT&CK Framework, para la emulación de técnicas de adversarios reales. **Requisitos:** Es indispensable que el proveedor del servicio cuente con personal con experiencia comprobable y altamente calificado en escenarios avanzados de hacking ético, análisis de aplicaciones web, desarrollo de exploits y emulación de adversarios. Se requiere que el personal cumpla con las siguientes certificaciones: ● OffSec Exploit Developer (OSED) ● OffSec Experienced Penetration Tester (OSEP) ● OffSec Web Expert (OSWE)	1600 IPs Privadas

	• OffSec Certified Expert 3 (OSCE3) • Offensive Security Certified Professional (OSCP) • Web Application Penetration Tester eXtreme (eWPTX v2.0) • Certified Penetration Tester eXtreme v2 (eCPTX) • Certified Secure Web Application Engineer (SWAE) Debiendo anexar currículos con los cuales su personal acredite que cuenta con las certificaciones y acreditar las mismas con copias simples y numero de folio. **Entregables** Reporte con resultados de la evaluación, descripción de cada vulnerabilidad o hallazgo, su criticidad, ejemplos de explotación y recomendaciones específicas para mitigar riesgos.	
5	**MONITOREO DE EVENTOS DE CIBERSEGURIDAD**	
5.1	**Detección Avanzada de Amenazas** La plataforma deberá incluir análisis de comportamiento y algoritmos de aprendizaje automático para identificar actividades inusuales, permitiendo la detección temprana de amenazas internas y externas. Se espera que: Correlacione y consolide eventos de múltiples orígenes (endpoints, dispositivos de red, sistemas operativos, aplicaciones) en una única consola. Incluya alertas inteligentes para priorizar las amenazas más críticas y agilizar la respuesta. Ofrezca inteligencia global que ayude a distinguir incidentes relevantes de falsos positivos o eventos de bajo riesgo. Permite la automatización de acciones de respuesta (por ejemplo, bloquear IPs, deshabilitar cuentas comprometidas, etc.).	1,600 dispositivos
5.2	**Integración y Correlación de Registros** El sistema deberá funcionar como una solución de correlación (similar a un SIEM), capaz de unificar: Registros y eventos de sistemas operativos (Windows/Linux), firewalls, WAF, routers, bases de datos, aplicaciones internas, etc. Alertar en caso de cadenas de eventos que, combinadas, indiquen una posible intrusión o abuso de privilegios.	

	Proporcionar reglas personalizables para detectar comportamientos específicos del entorno del municipio.	
5.3	**Gestión de Incidentes y Respuesta**	
	Deberá contar con un módulo de gestión de incidentes que: Asigne y clasifique los eventos detectados como “incidentes”, permitiendo al equipo de ciberseguridad llevar un seguimiento (registro de acciones, tiempos de resolución, etc.). Permite flujos de trabajo que automaticen la atención de incidentes repetitivos (por ejemplo, bloqueo de cuentas tras numerosos intentos fallidos). Ofrezca la trazabilidad completa de las acciones realizadas, facilitando las auditorías post-incidentes.	
5.4	**Auditoría de Directorio Activo (AD) y Cumplimiento**	
	La plataforma deberá brindar capacidades para auditar cambios en Directorio Activo o servicios análogos, facilitando: Monitoreo de movimientos en grupos privilegiados, creación o eliminación de cuentas, alteraciones de políticas de contraseñas. Detección de inicios de sesión anómalos o intentos masivos de acceso fallido. Generación de reportes de cumplimiento (por ejemplo, alineados a buenas prácticas o normativas de seguridad), además de alertas inmediatas si se detectan desviaciones graves.	
5.5	**Paneles de Control y Reportes**	
	La herramienta deberá contar con paneles de control que muestren indicadores clave (incidentes activos, hosts afectados, etc.) en tiempo real, así como: Reportes automáticos programables, con la opción de enviarlos a distintos perfiles (administradores, auditores, alta dirección). Alertas en tiempo real (notificaciones vía correo, mensajes, etc.) sobre incidentes de alta criticidad. Capacidad de personalizar los paneles según las necesidades de cada rol dentro de la organización.	

6	AUDITORIA DE CUENTAS CON ALTOS PRIVILEGIOS Y GESTIÓN DE CUENTAS DE SERVICIO	CANTIDAD
6.1	**Auditoría de Cuentas Privilegiadas** Se requiere supervisar de forma continua las acciones que involucren cuentas con altos privilegios, como Domain Admins y Enterprise Admins. Así mismo la capacidad de monitorear los movimientos en grupos privilegiados, la creación o eliminación de usuarios con derechos especiales y las modificaciones de políticas de contraseñas. También se busca el registro de inicios de sesión para identificar patrones anómalos o accesos fuera de horario, y la generación de informes que muestren el nivel de cumplimiento de la organización frente a normativas de seguridad.	100
6.2	**Análisis de Contraseñas y Fortalecimiento de Políticas** La solución debe permitir escanear las contraseñas almacenadas en Directorio Activo (o sistemas análogos) para detectar credenciales débiles, repetidas o filtradas en brechas públicas. Se busca un reporte que muestre qué cuentas incumplen las políticas de complejidad y caducidad, así como las contraseñas que no cumplen los estándares mínimos establecidos. Adicionalmente, se requiere la posibilidad de exigir cambios inmediatos y de reforzar las políticas cuando se hallen vulnerabilidades.	1,500
6.3	**Control y Auditoría de Cuentas de Servicio** Se necesitan capacidades para identificar y documentar las cuentas de servicio asociadas a aplicaciones, bases de datos o sistemas internos, verificando que no tengan permisos excesivos o contraseñas obsoletas. Es deseable que se monitoree cada acceso que realicen, con alertas si se detectan patrones inusuales. También se solicita la elaboración de recomendaciones para la rotación periódica de credenciales y la adopción de prácticas seguras (por ejemplo, cuentas gestionadas).	100
6.4	**Consola de Reportes y Paneles de Control** La plataforma deberá ofrecer un método de unificación de la información obtenida de la auditoría de cuentas privilegiadas, del análisis de contraseñas y de la gestión de cuentas de servicio. Esto implica contar con paneles de control que muestren indicadores	1

	clave (por ejemplo, cantidad de cuentas privilegiadas con contraseñas débiles o cambios no autorizados), así como la programación de informes automáticos para directivos y auditores. Asimismo, se requiere la capacidad de personalizar alertas y reportes según los roles, facilitando el cumplimiento de normativas y la toma de decisiones basadas en riesgos.	
7	**FIREWALLS Y VPNS DE SSL**	**CANTIDAD**
7.1	**Firewall Principal y VPN SSL (Clúster en Sitio Principal)** Se solicita un clúster activo-pasivo de 2 dispositivos de firewall de última generación (NGFW) que cumpla con: Capacidad de inspección con estado (stateful inspection), filtrado de puertos y sesiones. Módulos de seguridad como IPS (detección y prevención de intrusiones), filtrado de contenido web, control de aplicaciones, antivirus (detección de malware) y opción de SD-WAN. Rendimiento mínimo: ~14 Gbps en modo firewall básico, ~7.5 Gbps con IPS activo y ~6.6 Gbps con inspección SSL, con unas 145,000 conexiones concurrentes. Interfaces: al menos 10 puertos de cobre (1 Gbps) y 8 puertos de fibra (hasta 10 Gbps). Capacidad de VPN SSL de ~200 sesiones simultáneas, con licenciamiento o suscripción que lo habilite. Sandbox (local o en la nube) para analizar archivos desconocidos y amenazas de día cero.	2 Firewalls en clúster
7.2	**FW Sitio Alterno y VPNs** Se requiere otro clúster activo-pasivo de 2 dispositivos NGFW, que incluya: Stateful inspection y funciones integradas de seguridad (IPS, filtrado web, antivirus). Rendimiento similar al del sitio principal (≥14 Gbps firewall, ~7.5 Gbps con IPS, ~6.6 Gbps con inspección SSL, ~145k conexiones). Al menos 10 puertos de 1 Gbps (cobre) y 8 puertos de 10 Gbps (fibra). Soporte para ~200 sesiones concurrentes de VPN SSL. Suscripciones que mantengan los motores de IPS, filtrado y antivirus actualizados.	2 Firewalls en clúster
7.3	**Consola de administración**	2 por cada Cluster

	Además de los firewalls, se requiere una consola de administración que permita: Gestión remota de ambos clústeres (sitio principal y alterno), aplicando cambios de configuración, políticas de seguridad y actualizaciones de firmware de forma unificada. Soporte de alta disponibilidad (un nodo en cada sitio) para asegurar la continuidad y la sincronización de políticas	
7.4	**Consola de Reportes y Correlación de Eventos** Para la recolección de logs, análisis y reportes, se solicita un sistema de correlación o analítica de eventos que: Recoja eventos de los firewalls: detecciones de IPS, bloqueos de antivirus, filtrado web, etc. Genere reportes ejecutivos y dashboards en tiempo real (uso de la red, amenazas bloqueadas, etc.). Permite correlacionar incidentes y almacenar los registros para investigación forense, con una retención acorde a la política del Municipio.	1
7.5	**Módulos Avanzados de Seguridad** Cada dispositivo de firewall deberá incluir las licencias o suscripciones para: IPS (Intrusion Prevention System): inspeccionar tráfico en todas las capas, incluidas las comunicaciones cifradas (SSL/TLS). Antivirus / Anti-Malware: escanear archivos y flujos de datos para detectar y bloquear código malicioso. Filtrado web: categorizar y restringir el acceso a sitios según política o reputación. Control de aplicaciones: regular el uso de aplicaciones en la red (p. ej., redes sociales, servicios de almacenamiento). Sandbox: análisis avanzado de archivos desconocidos o de día cero.	4
8	**FIREWALLS DE APLICACIONES WEB**	**CANTIDAD**
	WAF basado en la nube	

	Web Application Firewall basado en la nube para proteger hasta 130 portales o aplicaciones web, con despliegue flexible en nubes públicas, privadas, híbridas y entornos Kubernetes. Que ofrezca protección continua y adaptable, funcionando tanto como proxy inverso como en configuraciones fuera de ruta, según los requerimientos del entorno. Que lleve a cabo inspección a tráfico HTTPS y brinde protección contra los ataques listados en OWASP Top 10, incluyendo amenazas emergentes, integrando capacidades de aprendizaje automático (machine learning) para identificar patrones de comportamiento típicos y que contenga desviaciones maliciosas. Además, deberá incluir mecanismos automáticos para adaptarse a cambios en los sitios protegidos, ajustando dinámicamente las políticas de seguridad. La solución deberá soportar esquemas de despliegue que incluyan integración con servicios CDN y balanceo de carga avanzado, asegurando alta disponibilidad y óptimo rendimiento. Una consola de administración en nube, que permita la administración del WAF que protege las aplicaciones tanto el del sitio principal como el del sitio alterno, cuya función principal sea la de mantener la configuración uniforme y ofrecer reportes de actividad maliciosa y desempeño. Protección integral de API. La plataforma debe poder identificar y bloquear amenazas que busquen explotar vulnerabilidades específicas de servicios REST, SOAP u otros protocolos de intercambio de datos, aplicando reglas de validación para parámetros, encabezados y métodos HTTP. Inspección de tráfico y heurísticas avanzadas. El sistema deberá analizar el comportamiento del tráfico hacia las APIs, utilizando heurísticas y patrones de amenazas conocidos para detectar inyecciones de SQL, cross-site scripting (XSS) y tentativas de enumerar endpoints de forma maliciosa. Posibilidad de definir transformaciones de encabezados, redirecciones específicas, bloqueo o desafío basado en atributos como IP, país, agente de usuario, patrones de URL, etc. Detección temprana de actividad maliciosa y retroalimentación. Además de bloquear ataques en tiempo real, el sistema deberá notificar a la consola central sobre patrones repetitivos o intentos de explotación, facilitando la retroalimentación constante para ajustes en las reglas y la expansión de su base de conocimientos.	130 Aplicaciones

8.2	**Integración con Red Global y Mitigación DDoS** Para mejorar el rendimiento y la resiliencia ante ataques volumétricos, se solicita un servicio que ofrezca: Una red distribuida de puntos de presencia (PoP) para reducir la latencia y distribuir contenido (CDN). Mitigación DDoS a gran escala, interceptando ataques en la periferia antes de saturar la red interna. Interceptar ataques volumétricos a gran escala (SYN flood, amplificación UDP, ataques layer 7) en la periferia de la red, antes de que saturen el enlace local. Adaptar automáticamente la defensa en función del tipo y escala del ataque (L3, L4, L7), sin requerir intervención manual en la mayoría de los casos. Gestión de bots que filtre tráfico automatizado malicioso sin afectar a los motores de búsqueda legítimos. Distinguir bots legítimos (p. ej., motores de búsqueda) de bots maliciosos (scrapers, spam bots, intentos de fuerza bruta) usando heurística avanzada, reputación IP y validación de comportamiento. Permitir acciones de bloqueo, desafío (CAPTCHA) o limitación de velocidad (rate limiting) según la criticidad del tráfico detectado. Reglas personalizadas de bloqueo o modificación de encabezados y parámetros, según la conveniencia de cada aplicación. Ubicar copias (caché) del contenido estático de los portales en varios puntos de presencia (PoP) alrededor del mundo, reduciendo la latencia para usuarios y descarga de ancho de banda en el origen. Permitir configuraciones de “cache rules” y “page rules” ajustables según subdominios, rutas o encabezados.	
	Consola de Administración y Reportes Unificados	
8.3	La solución deberá incluir: Reportes y paneles de control con indicadores de amenazas bloqueadas, tipos de ataques y volumen de peticiones procesadas. Alertas en tiempo real cuando se detecten eventos críticos o se alcancen umbrales inusuales de tráfico o actividad maliciosa. Capacidad para personalizar la seguridad según el perfil de cada sitio, ajustando el nivel de protección y las reglas aplicadas. Posibilidad de integración con sistemas de monitoreo y soluciones SIEM para correlación de incidentes en todo el entorno.	
9	**SEGURIDAD DNS**	**CANTIDAD**

	Contar con un servicio o dispositivo de DNS Sinkhole que intercepte peticiones a dominios catalogados como maliciosos, phishing, de spam o con contenido no autorizado, y desvíe dichas consultas a una dirección o servidor controlado (sinkhole). Esto impide que los usuarios o sistemas internos del municipio establezcan conexiones con dichos dominios maliciosos, mitigando riesgos de infección, fugas de información o consumo de ancho de banda innecesario.	
9.1	**DNS Sinkhole** El municipio requiere la incorporación de un DNS Sinkhole que intercepte peticiones a dominios maliciosos, de phishing, spam o contenido prohibido, y desvíe dichas solicitudes a un servidor controlado. Con ello se evitará que los usuarios y sistemas internos establezcan conexiones con dichos destinos peligrosos, reduciendo los riesgos de infección, robo de información o consumo innecesario de ancho de banda. Se deberá configurar este sinkhole como servidor DNS principal o intermediario (proxy) para las redes del municipio, de modo que todas las resoluciones pasen por él. Las listas de bloqueo deberán actualizarse de manera periódica (automática) desde fuentes reconocidas de inteligencia de amenazas. La solución no deberá exigir la instalación de agentes en los endpoints ni cambios significativos en la programación de las aplicaciones.	1
9.2	**Consola de Administración** La solución deberá: Disponer de una consola de administración que permita ver el detalle de las consultas bloqueadas, los dominios más solicitados y las categorías de bloqueo (malware, phishing, etc.). Ofrecer la posibilidad de crear listas blancas (exclusiones) para dominios que, por motivos operativos, requieran acceso a pesar de aparecer en listas negras externas.	

LIBERTAD 101 CENTRO
SPGG / NL

SAN PEDRO
GARZA GARCÍA

TEL
81 8400 4400

	Permitir la configuración de alertas cuando se detecte un pico de solicitudes hacia un dominio catalogado como malicioso, lo que puede indicar la infección de uno o varios equipos en la red. Garantizar un rendimiento adecuado para las necesidades de la organización, con una latencia mínima en la resolución de nombres y soporte para esquemas de alta disponibilidad (redundancia en DNS). Paneles de control (dashboards) con indicadores en tiempo real (por ejemplo, cantidad de bloqueos recientes, origen de las peticiones, etc.).	
10	**ADMINISTRACIÓN DE VULNERABILIDADES**	**CANTIDAD**
10.1	**Administración de Vulnerabilidades Infraestructura** Se requiere una plataforma de escanéo que identifique vulnerabilidades en equipos de cómputo, dispositivos de red y bases de datos, tanto desde una perspectiva externa (Internet) como interna (red corporativa). La herramienta deberá: Permitir la detección y catalogación de fallas de seguridad (sistema operativo, software de terceros, configuraciones erróneas). Relacionar dichas fallas con las amenazas conocidas, aportando un puntaje de riesgo (por ejemplo, CVSS) que priorice qué vulnerabilidades deben abordarse primero. Escanear cada activo tanto desde la vista externa (Internet) como dentro de la red local, facilitando una visión global de la postura de seguridad. Mantener una base de datos de plugins o reglas de detección constantemente actualizada, cubriendo nuevas CVE y amenazas emergentes.	1600 IPs Privadas
10.2	**Administración de Vulnerabilidades Servidores Web** Plataforma con los módulos de escaneo para identificar vulnerabilidades en los servidores web desde la perspectiva de Internet y desde la red interna, relacionarla con amenazas existentes y proponer la priorización de las que deben resolverse inicialmente. Asimismo, que pueda escanear los activos desde la perspectiva de Internet y desde la red interna.	128 Publicas.
11	**REVISIÓN DE SEGURIDAD DE CÓDIGO FUENTE**	**CANTIDAD**
11.1	**Plataforma de Pruebas estáticas de seguridad de aplicaciones (SAST)**	

	La solución deberá ser una plataforma de segmentación avanzada, gestionada desde la nube, que permita proteger los entornos tecnológicos mediante el control del tráfico este-oeste dentro de la infraestructura. Debe admitir un **número ilimitado** de repositorios o proyectos privados, lo que implica que no se establece un tope fijo en la cantidad de aplicaciones que puedes dar de alta para análisis. Capacidad hasta **5 usuarios de seguridad** quienes sean los responsables de realizar las revisiones de seguridad. Deberá ofrecer capacidades para identificar, visualizar y segmentar flujos de datos y aplicaciones críticas, limitando la propagación de amenazas al reducir significativamente la superficie de ataque. Asimismo, deberá proporcionar visibilidad en tiempo real y permitir la implementación de políticas basadas en el contexto, asegurando que las conexiones entre cargas de trabajo estén estrictamente reguladas y alineadas con las necesidades del negocio y los requisitos de cumplimiento. La arquitectura de la solución deberá facilitar una gestión centralizada y eficiente, adaptable a entornos dinámicos y heterogéneos. Lanzar escaneos manualmente o de manera automática en proyectos seleccionados. Recibir alertas y notificaciones cuando aparezcan nuevas vulnerabilidades tras una actualización de código o dependencia.	
11.2	**Integración con el Ciclo de Desarrollo (CI/CD)**	
	Se requiere que la herramienta de SAST: Ofrezca conectores o plugins para pipelines de integración continua (CI), permitiendo que el escaneo de seguridad se ejecute de manera automática en cada commit o pull request. Permite bloquear la promoción de código al siguiente ambiente si se detectan vulnerabilidades críticas o de alta severidad. Genere reportes dentro de la misma interfaz de desarrollo o repositorio, facilitando la corrección temprana de los fallos.	
11.3	**Análisis de Dependencias y Contenedores**	

	Deberá incluir un módulo de análisis de dependencias que: Identifique bibliotecas de terceros con fallas conocidas, catalogadas en bases de datos de CVE u otras fuentes de inteligencia de amenazas. Suministre una guía concreta de actualización o parcheo para cada dependencia vulnerable. Ofrezca la capacidad de analizar la seguridad de imágenes de contenedores, detectando software obsoleto o configuraciones inseguras en Dockerfiles.	
11.4	**Consola de Administración y Gestión de Hallazgos**	
	La plataforma deberá disponer de una consola que incluya: Revisar la lista de vulnerabilidades encontradas por lenguaje, severidad y módulo de la aplicación. Asignar los hallazgos a integrantes específicos del equipo, estableciendo plazos o prioridades de remediación. Ver tendencias de seguridad (reducción o aumento de vulnerabilidades) a lo largo del tiempo y generar reportes ejecutivos. Exportar los resultados en formatos estándar (PDF, CSV), así como integrar los eventos de seguridad a una herramienta de correlación (SIEM) o sistema de tickets.	
12	**Servicio de Implementación**	**CANTIDAD**
12.1	Se requiere un **Servicio de Implementación** que abarque la puesta en marcha de todas las soluciones de seguridad adquiridas (antivirus endpoint y servidores, firewall, WAF, gestión de vulnerabilidades, parches, SAST, SIEM, IPS, DNS Sinkhole, etc.), cubriendo desde la **planificación** inicial (recolección de requerimientos, validación de infraestructuras) hasta la **configuración y despliegue** en entornos de prueba y producción. Este servicio deberá incluir la **coordinación** con las áreas de TI del municipio para asignar ventanas de mantenimiento y definir la secuencia de instalación y migración de políticas, asegurando una **transición ordenada** y minimizando el impacto en la operación. Se espera que el proveedor brinde la **creación de perfiles de seguridad** adaptados a las necesidades (p. ej., reglas de firewall, políticas de WAF, configuración del SIEM, módulos de antimalware y parches). Durante la fase de ejecución, se contemplará la **capacitación** necesaria al personal local para que conozcan las	

	funciones básicas de administración. El proveedor será responsable de la **validación funcional** (pruebas de seguridad, confirmación de bloqueos y alertas) y de un periodo de estabilización en el que se optimicen reglas, se reduzcan falsos positivos y se afinen los umbrales de alerta. Finalmente, deberá presentar un **informe de cierre** que confirme la correcta implementación de cada componente, las lecciones aprendidas y las **recomendaciones finales** de mejores prácticas para la operación continua de la solución.	
13	**Servicios Administrados de Seguridad**	**CANTIDAD**
13.1	**Servicio Administrado de Antivirus en Endpoint y Servidores** Se requiere un Servicio Administrado de Antivirus en Endpoint y Servidores que, con apoyo del equipo de ciberseguridad, proporciona protección continua y monitoreo en tiempo real de los dispositivos del municipio, de modo que se obtenga información de amenazas mediante indicadores de compromiso y se implementen acciones de bloqueo y contención de forma proactiva, contemplando el diseño de una configuración base personalizada, el mantenimiento y la actualización de firmas, la administración centralizada de la solución, la gestión de políticas y exclusiones, la programación de escaneos y la ejecución de flujos de respuesta a incidentes. Adicionalmente, el servicio deberá incluir el control de CPU para procesos de escaneo, la ejecución de análisis en segundo plano sin ralentizar los equipos, la disponibilidad de un mecanismo de rollback para restaurar cambios que puedan afectar la estabilidad del sistema, la detección de nuevas clases de malware mediante técnicas de comportamiento, la gestión de cuarentena para eliminar amenazas sin intervención del usuario final y el control de permisos para prevenir la desinstalación no autorizada del software de seguridad. Deberá administrarse una sola consola unificada que permita la configuración y monitorización tanto de servidores como de endpoints, con escaneos automáticos para dispositivos extraíbles y correos electrónicos, supervisión de procesos en memoria y la capacidad de bloquear puertos, direcciones IP, protocolos y sitios web a través de un firewall integrado, así como filtrar contenido por palabras clave y monitorear aplicaciones con acceso a internet. Además, el	1

	servicio se encargará de la creación y despliegue de plantillas de políticas, la gestión de grupos e implementación de agentes, la generación de reportes con formatos .doc, .pdf o .xls, la protección activa con mecanismos de análisis de comportamiento, la puesta en cuarentena de amenazas, la generación de exclusiones específicas, la desinfección manual de malware (sin restauración de archivos cifrados por ransomware) y la vigilancia constante del rendimiento para asegurar que las actualizaciones no causen interrupciones, todo complementado con la capacidad de integrarse con sistemas de correlación de eventos (SIEM) y de producir entregables periódicos que incluyan indicadores de cumplimiento y resúmenes ejecutivos.	
13.2	**Servicio Administrado de Firewall** Se requiere un Servicio Administrado de Firewall que garantice la operación continua y la máxima eficacia de la solución de seguridad perimetral del municipio, proporcionando un equipo especializado en ciberseguridad que supervise y administre de manera centralizada la configuración, las políticas y las actualizaciones del dispositivo, de modo que se asegure el filtrado de puertos, la inspección de tráfico cifrado (SSL/TLS), la detección y prevención de intrusiones (IPS), el control de aplicaciones y el bloqueo de contenido web, así como la gestión de licenciamientos y renovaciones necesarios. Adicionalmente, el servicio deberá abarcar la elaboración de una configuración base adaptada a las necesidades específicas del municipio, la aplicación de cambios rutinarios (reglas, NAT, VPN, segmentación), la implementación y actualización de firmwares, la monitorización permanente de eventos y registros para la detección proactiva de amenazas y anomalías, y la generación de reportes periódicos con indicadores de seguridad y métricas de rendimiento. Se solicita también la coordinación de respuesta a incidentes, con acciones de contención o bloqueo inmediato ante intentos de intrusión o actividad maliciosa, y la opción de exportar registros a una herramienta de correlación (SIEM), facilitando la integración con el ecosistema de ciberseguridad. El proveedor deberá ofrecer asistencia experta las 24 horas o según el esquema acordado, asegurando la continuidad del servicio ante fallos de hardware, reconfiguraciones urgentes o cambios en la topología de red, y presentando informes de estado a intervalos predefinidos,	1

	detallando la disponibilidad, las amenazas neutralizadas y las recomendaciones de mejora continua en la política de seguridad perimetral.	
13.3	**Servicio Administrado de Web Application Firewall (WAF)**	
	Se requiere un Servicio Administrado de Web Application Firewall (WAF) que garantice la protección continua de los portales y aplicaciones del municipio frente a amenazas de capa 7, ofreciendo una plataforma que supervise y filtre el tráfico HTTP/HTTPS para bloquear inyecciones de código, intentos de acceso indebidos, ataques de denegación de servicio y cualquier vulnerabilidad listada en OWASP Top 10; el proveedor deberá diseñar una configuración inicial adecuada a las necesidades del entorno (manejando despliegue tipo proxy inverso, modo fuera de ruta o esquemas mixtos), integrar funciones de CDN para optimizar el rendimiento y la disponibilidad de las aplicaciones, y administrar las actualizaciones y reglas de seguridad para detectar patrones de ataque emergentes. Adicionalmente, el servicio administrado incluirá la monitorización en tiempo real de eventos y registros, la correlación de incidentes con indicadores de compromiso y la capacidad de respuesta inmediata ante anomalías o ataques masivos, presentando reportes periódicos con métricas de amenazas bloqueadas, análisis de tráfico y recomendaciones de ajuste; asimismo, se prestará soporte en la configuración de políticas finas (por ejemplo, protección de API, control de bots, bloqueo de geolocalización), sin requerir cambios significativos en el código de las aplicaciones protegidas. El equipo asignado deberá coordinarse con la infraestructura del municipio para asegurar la continuidad operativa, proveer asistencia experta en la administración del WAF y permitir la exportación de registros a plataformas de correlación (SIEM) para una visión más amplia de la postura de seguridad.	1
13.4	**Servicio Administrado de Gestión de Vulnerabilidades**	1
	Se solicita un Servicio Administrado de Gestión de Vulnerabilidades que, mediante una plataforma de escaneo y un equipo de expertos en ciberseguridad, realice evaluaciones periódicas de la infraestructura y las aplicaciones del municipio (servidores, dispositivos de red, equipos de cómputo, portales web), generando un inventario de fallas clasificadas por criticidad y correlacionadas	

	con las amenazas más relevantes, de modo que se prioricen las correcciones y se mantenga un ciclo de mejora continua; además de identificar brechas y configuraciones inseguras, el servicio deberá entregar reportes ejecutivos y técnicos que evidencien la evolución de la postura de seguridad, coordinar la elaboración y seguimiento de planes de remediación para cada vulnerabilidad detectada y, en caso de que se requiera, exportar los hallazgos a la plataforma de correlación (SIEM) para un análisis más amplio de incidentes, ofreciendo asesoría especializada para la configuración de escaneos, el refinamiento de políticas de detección, la definición de ventanas de mantenimiento y la integración con otras áreas de la infraestructura del municipio.	
13.5	**Servicio Administrado de Gestión de Parches en Servidores** Se requiere un Servicio Administrado de Gestión de Parches en Servidores Windows que garantice la revisión, aprobación, implementación y seguimiento de las actualizaciones críticas en los sistemas operativos y aplicaciones del municipio, con el objetivo de mitigar vulnerabilidades y asegurar la estabilidad de la infraestructura. El equipo responsable deberá llevar a cabo un inventario continuo de los parches pendientes, evaluar su criticidad y priorizar su instalación en coordinación con las áreas operativas, verificando en entornos de prueba cuando sea necesario y programando ventanas de mantenimiento para minimizar el impacto en la operación. Además, se solicita la generación de reportes periódicos que muestren el estado de cumplimiento y el porcentaje de servidores parchados, así como la correlación con cualquier hallazgo previo de vulnerabilidad para comprobar la efectividad de las acciones tomadas. El servicio también deberá contemplar la posibilidad de retroceder cambios (rollback) en caso de que un parche cause inestabilidad, ofreciendo soporte experto en la resolución de conflictos y facilitando la integración con otras herramientas de seguridad (por ejemplo, escáner de vulnerabilidades o SIEM) para contar con una visión global de la postura de seguridad de la organización.	1
13.6	**Servicio Administrado de herramienta SAST**	

1

	Se requiere un Servicio Administrado de herramienta SAST (análisis estático de seguridad de aplicaciones) que permita a la organización integrar la verificación de vulnerabilidades en el código fuente durante todas las etapas del ciclo de desarrollo, con el fin de identificar y corregir fallas lo antes posible. El equipo asignado deberá encargarse de configurar la herramienta, establecer las políticas y reglas de análisis, e integrar los repositorios de código o pipelines de CI/CD, a fin de garantizar que cada commit o cambio de versión se analice automáticamente en busca de inyecciones, ulnerabilidades de bibliotecas, configuraciones inseguras y otras deficiencias. Asimismo, se deberá ofrecer asesoría especializada para la interpretación de hallazgos, priorizando la remediación con base en el nivel de riesgo y el posible impacto sobre las aplicaciones críticas, presentando reportes ejecutivos y técnicos que resuman la evolución de las vulnerabilidades detectadas y las correcciones implementadas. El servicio también abarcará la administración de usuarios y proyectos en la plataforma, la actualización continua de los motores de análisis (para cubrir nuevos lenguajes o librerías), y la integración con otras soluciones de seguridad para correlacionar eventos y notificar de forma proactiva ante fallas críticas, todo ello con el propósito de introducir la cultura de la seguridad en el desarrollo desde etapas tempranas y minimizar la presencia de defectos en producción. **Requisitos:** Es indispensable que el proveedor del servicio cuente con personal con experiencia comprobable y altamente calificado en desarrollo seguro. Se requiere que el personal cumpla con la siguiente certificación: • Certified Secure Programmer Associate	
13.7	**Servicio Administrado de Correlacionador de Eventos (SIEM), Prevención de Intrusos (IPS), DNS SInkhole**	
	Se requiere un **Servicio Administrado** que unifique la correlación de eventos (SIEM), la prevención de intrusiones (IPS) y un servicio de DNS Sinkhole, de manera que los registros de seguridad provenientes de diferentes dispositivos (firewalls, endpoints, servidores, aplicaciones) se centralicen y analicen para identificar	1

	patrones de ataque o anomalías, recibiendo una respuesta coordinada que bloquee las amenazas antes de que se propaguen; el equipo responsable deberá implementar, configurar y monitorear el SIEM, ajustando reglas de correlación y priorizando alertas para reaccionar de forma oportuna, administrar el IPS que inspeccione el tráfico e intercepte intentos de explotación (inclusive SSL si es requerido), y desplegar el DNS Sinkhole que impida a los sistemas resolver dominios maliciosos o fraudulentos, cortando la comunicación con servidores de comando y control, todo complementado con la elaboración de reportes periódicos y el soporte experto para la optimización continua de la protección en base a indicadores de compromiso e inteligencia de amenazas, integrándose con los procesos de la organización sin exigir cambios radicales en la infraestructura existente.	
14	**Servicio de Gestión de Incidentes**	**CANTIDAD**
14.1	Se solicita un Servicio de Gestión de Incidentes que cubra la identificación, clasificación, contención, análisis y resolución de los eventos de seguridad que afecten la infraestructura del municipio, brindando soporte experto en un esquema 24/7 o según los SLAs definidos. El proveedor deberá establecer un proceso formal de respuesta a incidentes, asignando un equipo de analistas L1/L2 y un responsable de escalación para los casos críticos; además, administrará la bitácora de incidentes y la documentación de lecciones aprendidas, garantizando la trazabilidad de cada evento desde su detección hasta su cierre. Se espera que este servicio se integre con las herramientas de monitoreo y correlaciones existentes (SIEM, IPS, WAF, etc.), recibiendo alertas de manera automática y ejecutando acciones de contención (bloqueo de IP, cuarentena de hosts, aislamiento de segmentos) cuando sea necesario, en coordinación con el personal de TI del municipio. Adicionalmente, se elaborarán reportes post-incidente con un análisis de causa raíz, un plan de remediación y recomendaciones para fortalecer la postura de seguridad y evitar recurrencias, promoviendo un ciclo de mejora continua en la gestión de la ciberseguridad.	1
15	**Servicio de Monitoreo SOC**	**CANTIDAD**

15.1	Se requiere un **Servicio de Monitoreo SOC** que, de forma complementaria a los servicios administrados existentes (antivirus, firewall, WAF, gestión de vulnerabilidades, etc.), realice la supervisión continua de la infraestructura y la correlación de eventos para detectar incidentes de seguridad; el proveedor deberá operar en un horario 8x5 para la mayoría de actividades de monitoreo y gestión, pero asegurar una atención 24x7 en caso de alertas críticas que pongan en riesgo la disponibilidad o la confidencialidad de los activos del municipio. Este servicio contemplará la recepción y análisis de logs provenientes de distintas fuentes (SIEM, IPS, WAF, endpoints), la generación de alertas con escalado al personal de seguridad o de TI cuando se presenten indicadores de compromiso, y la coordinación con los servicios administrados para ejecutar acciones de bloqueo, contención o mitigación de amenazas. Asimismo, se emitirán reportes periódicos sobre el estado de la seguridad, las incidencias atendidas, las tendencias de amenazas y las recomendaciones de mejora, a fin de mantener informada a la alta dirección y garantizar una postura de seguridad alineada con las mejores prácticas.	1

ANEXO B. REQUERIMIENTOS DE INSTALACIÓN Y CONFIGURACIÓN DE LOS PRODUCTOS

El servicio otorgado deberá incluir la TRANSFERENCIA DE CONOCIMIENTO y herramientas necesarias para el monitoreo de la seguridad de acuerdo con las necesidades expresadas por parte del municipio, adicional a los requerimientos descritos en la tabla. Si se solicita, los cambios hechos en los dispositivos de seguridad se realizarán en sesión compartida (con el control y operación del proveedor) con el municipio.

Tiempo de implementación 60 días naturales.

PLATAFORMA DE SEGURIDAD PARA LA NAVEGACIÓN, LAS APLICACIONES SAAS Y EL ACCESO SEGURO A LA RED.
Control en la navegación

Servicios de habilitación de licencias de navegación web, se requiere de: ● La habilitación del servicio de proxy en la nube. ● La distribución de hasta 1500 agentes en las PCs del municipio, incluyendo el certificado requerido para la inspección de HTTPS. ● La integración al dominio para el reconocimiento de los usuarios. ● La configuración/migración de hasta 10 políticas de navegación web asociada los diferentes perfiles incluyendo el control de acceso a "tenants", el control de "shadow IT", la habilitación de "remote browser isolation" para sitios maliciosos, e identificación y contención de fuga de información en el canal web, alineadas y en complemento a las reglas establecidas en la previsión de fuga de información en las computadoras. ● La habilitación del filtrado de HTTPS, incluyendo la distribución del certificado en las estaciones (PCs). ● La integración con el firewall designado por el municipio para la redirección del tráfico HTTP y HTTPS en caso de requerirse. ● La estabilización de la operación, apoyada con personal en sitio por al menos 5 días posteriores a la finalización de la instalación y configuración.
Cloud Access Security Bróker
Servicios de Habilitación de "Cloud Access Security Bróker" para la protección de aplicaciones SaaS funcionamiento y liberación. Se requiere: ● La integración vía API de hasta 2 aplicaciones SaaS durante la vigencia del proyecto, considerando Google Drive y Gmail. ● La distribución de agentes al total de los usuarios (1500) y su habilitación silenciosa en las computadoras. ● La configuración/migración de hasta 20 reglas de protección para hasta 20 perfiles diferentes que pueden incluir, el bloqueo de actividades, el control de acceso a módulos específicos de Google Drive y Gmail, a la fuga de información en el servicio Google Drive y Gmail, la tokenización y/o cifrado de la información. ● La integración con el módulo de previsión de fuga de información en la navegación web para administrar esta amenaza de manera unificada, tanto en la definición de reglas de protección, como en el reporteo y alertamiento. ● Todas las tareas de afinación requeridas para evitar detener la operación o evitar cualquier falla. ● El alertamiento vía correo electrónico.

Servicios de Habilitación de acceso a la red con el mínimo privilegio para la protección de aplicaciones internas del municipio: ● La distribución del agente a todas las computadoras (1,500) ● La integración al dominio para la provisión del acceso basado en identidad. ● La habilitación de gateways de conectividad en el sitio principal y el sitio alterno. ● La generación de hasta 20 perfiles de acceso para los cuales les pueda configurar la autenticación de doble factor, la validación de una postura que al menos revise el antivirus activo y la versión del sistema operativo ● La configuración/migración de todas las reglas para dar el acceso a las aplicaciones internas del municipio, en su perfil. ● Todas las tareas de afinación requeridas para evitar detener la operación o evitar cualquier falla con apoyo en sitio al menos 5 días posteriores a la habilitación ● La integración con el control de navegación web para ser administrado desde la misma consola. ● La solución deberá tener puntos de presencia en México (Datacenters) para baja latencia y alto rendimiento.
PLATAFORMA ANTI MALWARE
La plataforma deberá estar configurada para soportar la ejecución de campañas antimalware, considerando que se deberá tener visibilidad y cruce de información entre el estado de seguridad de los servidores y todas las computadoras, que permita identificar si existen indicadores de compromiso que puedan representar impacto o posible impacto en el ambiente del municipio. Adicionalmente, deberá proveer visibilidad del tráfico malicioso para señalar indicadores de compromiso de alguna campaña de malware que no haya afectado las estaciones de trabajo o servidores pero que esté presente en el tráfico de la red.
Se requiere la habilitación de los productos de antimalware, anti ransomware y parcheo virtual en 1600 estaciones considerando: ● La distribución de todos los productos en todas las estaciones, de acuerdo con su compatibilidad ● Se deberá habilitar una consola en premisa y todas las estaciones de trabajo y servidores deberán poderse gestionar a través de ella.
Para el antimalware: ● El antivirus deberá estar configurado para identificar las estaciones en la red y autoinstalarse. ● La instalación del antivirus deberá tener configuradas políticas para que se actualice de manera regular ya sea diaria, semanal, mensual, semestral y/o anual, para el módulo que lo amerite. ● El antimalware deberá estar habilitado en modo protección, alineado con los parámetros

y políticas de protección actualmente existentes.

- El módulo de machine learning y mecanismos de análisis de reputación deberán estar activos para identificar y contener.
- El módulo anti ransomware deberá está habilitado en todas las estaciones (1500) al finalizar su habilitación deberá poderse validar su correcto funcionamiento, es decir, conducir pruebas de cifrado y regresar la estación de trabajo al estado inicial antes de ser cifrada.
- El módulo de parcheo virtual deberá estar activo en todas las estaciones de trabajo (1500), protegiendo al menos ante las amenazas de alta criticidad.

Para el control de dispositivos:

- Deberá estar activo en todas las estaciones de trabajo
- Deberá de incluir una de dos políticas: bloqueado o permitido. El proveedor deberá replicar el esquema actual de control y el municipio indicará cuál aplicar para los equipos que actualmente no estén siendo gestionados.

Se requiere la habilitación del producto del control de cambios para todos los servidores Windows, 50:

- El levantamiento del inventario de las aplicaciones y directorios
- La configuración de listas “blancas” y listas “negras”
- La habilitación de directorios de sólo lectura
- La habilitación de los usuarios para hacer modificaciones en los directorios
- La definición y establecimiento de un proceso de control de aplicaciones regulado por “los administradores de las aplicaciones” del municipio que considere un estadío de actualización de listas blancas y negras para la instalación de nuevas versiones o nuevas aplicaciones permitidas por el municipio
- La habilitación progresiva con las siguientes consideraciones:
  - La habilitación en modo observación sin que aparezcan problemas de compatibilidad, bloqueo, bajo desempeño o “pantallas azules” en 4 etapas:
    - Habilitación de 1 servers (laboratorio)
    - Habilitación de 3 servers (prueba)
    - Habilitación de 6 servers (piloto): La habilitación progresiva en modo solidificado, asegurando la continuidad operativa y la resolución de problemas sin afectar la operación de los servidores y las aplicaciones del Municipio
    - Habilitación en el resto de los servidores

Servicios de habilitación para el control de aplicaciones o listas blancas:

- Deberá distribuirse a todas las estaciones para recopilar un inventario de todas las aplicaciones del municipio
- Deberá validarse las aplicaciones permitidas y las que no, generando al menos 3 perfiles de usuarios y sus aplicaciones permitidas
- Deberá aplicarse el control de aplicaciones permitidas de acuerdo a los perfiles generados basados en los inventarios
- La habilitación deberá ser progresiva considerando
- Distribución en todas las estaciones, 1,500
- Habilitación en modo de observación para la identificación del inventario
- Habilitación en modo de restricción en las siguientes etapas
- Un grupo piloto de 5 estaciones
- Un grupo laboratorio de 25 estaciones que incluyan al menos una PC de cada perfil y de cada departamento del municipio
- Un grupo inicial adicional de 50 PCs
- Habilitación masiva en grupos de 40 PCs

Servicios de habilitación para el firewall personal

- Deberá estar activo en todas las estaciones con excepción de las administradas en la nube
- Deberá contener una política de inspección sobre la cual se definan las políticas de restricción
- Deberá poder aplicar hasta 5 políticas de restricción en el acceso, las cuales deberán aplicarse de acuerdo a las instrucciones del Municipio

Servicios de habilitación el Endpoint Detection and Response para servers

- Deberá distribuirse a todos los servidores Windows y Linux, hasta 100 servidores
- Deberá configurarse para identificar y alertar de anomalías y desviaciones
- Deberá configurarse para poder establecer mecanismos de reacción, aislamiento, cuando se requiera
- Deberá configurarse para poder establecer una investigación guiada que permita llegar a conclusiones de una manera más rápida

Servicios de habilitación de sandbox para ofrecer una capa adicional de análisis para la identificación y contención de malware de los llamados de “día cero”, tanto en el antimalware de las PCs como en el IPS de red: ● La integración con la consola de administración del antivirus ● La configuración para el envío de código o archivos con posible malware de día cero desde la consola del antivirus de manera automática ● La contención del malware de día cero como resultado del análisis del sandbox tanto en las computadoras ● Estabilización de la integración y el correcto funcionamiento
Los servicios de habilitación de la herramienta de parcheo para el total de las estaciones, 1600: ● La distribución de los productos al total de las computadoras y servidores ● La definición y habilitación de un proceso regular (mensual) de parcheo para el total de las PCs y servidores. ● La habilitación y el parcheo del mes en curso con los parches críticos de seguridad de Microsoft debe ser progresiva. ● La actualización de builds mayores o Para PCs: ● Habilitación de 10 estaciones (laboratorio) ● Habilitación de 20 estaciones (prueba) ● Habilitación de 40 estaciones (piloto) ● La habilitación masiva en grupo de los parches críticos de Microsoft, asegurando la continuidad operativa y la resolución de problemas sin afectar de manera masiva a la operación de las PCs del municipio ● Para los servidores: ● Habilitación de 1 servers (laboratorio) ● Habilitación de 3 servers (prueba) ● Habilitación de 6 servers (piloto) ● La habilitación de los 90 servers restantes
INTEGRACIÓN DE INTELIGENCIA DE PREVENCIÓN DE INTRUSOS DE RED

Implementación de Plataforma de detección y respuesta: ● Convertir las reglas y configuraciones existentes del IPS anterior (firmas, perfiles de ataque) en escenarios y definiciones para la nueva plataforma, de modo que el comportamiento de bloqueo o alerta se mantenga acorde a las políticas vigentes. ● Instalar y configurar la solución colaborativa (en servidores o contenedores adecuados) que analice los registros (logs) de los dispositivos y servicios críticos. En lugar de un modo “transparente” con hardware dedicado, se emplearán módulos de “bouncers” que apliquen decisiones de bloqueo en el firewall y el WAF. ● Activar una política estándar de observación para recopilar información sin bloquear el tráfico, minimizando la posibilidad de falsos positivos. ● Con base en la información obtenida, habilitar mecanismos de respuesta (reset de conexión, denegación de IP) para detener intentos de explotación masiva o ataques volumétricos, priorizando la mitigación de denegación de servicio (DoS).
Cobertura en DMZ y servidores: ● Recopilar registros desde los servidores de la DMZ y la granja interna, enviándolos a la consola colaborativa para detectar fuerza bruta, enumeraciones y otros patrones maliciosos. ● Implementar los módulos necesarios para que la plataforma de detección ordene al firewall y al WAF bloquear o poner en cuarentena las direcciones IP maliciosas. ● Ajustar reglas y excepciones para evitar falsos positivos, incluyendo la configuración de perfiles de protección contra ataques volumétricos en los enlaces de mayor capacidad. ● Aplicar perfiles específicos para la detección de ataques de saturación, bloqueando tráfico volumétrico antes de que afecte la continuidad del servicio.
● Se requiere la habilitación de una infraestructura central (servidor de la solución, base de datos) con redundancia o respaldos, para asegurar que las reglas y bloqueos permanezcan operativos ante fallas de hardware. ● La consola debe mostrar la lista de reglas o “escenarios” activos, los bloqueos en curso y las direcciones IP maliciosas detectadas, ofreciendo reportes de actividad y la posibilidad de afinar reglas de respuesta. ● La inteligencia deberá proporcionar reglas y listas de IP en tiempo real, nutridas por la comunidad global (opcional según la política del municipio), para mejorar la capacidad de detección de ataques masivos. ● Ajustar los umbrales de volumetría, los tiempos de bloqueo y las excepciones, reduciendo falsos positivos y mejorando la eficacia ● Definir reglas de exclusión para servicios esenciales y flujos internos tras observar la operación real, garantizando un equilibrio entre seguridad y continuidad.

PRUEBAS DE PENETRACIÓN

Pruebas de penetración Internas y Externas

Alcance Externo
Realizar pruebas hasta **128 IPs Públicas/Urls** de servicios expuestos a internet (portales web, interfaces de acceso remoto, etc.).
Incluir pruebas de fuerza bruta, escaneo de puertos, enumeración de servicios, análisis de vulnerabilidades en aplicaciones web (inyecciones SQL, XSS, CSRF, configuraciones inseguras) y cualquier otro mecanismo que un atacante remoto pudiera utilizar.

Alcance Interno
Realizar pruebas hasta **1600 IPs Privadas** dentro de la red interna, cubriendo servidores, bases de datos, equipo de cómputo, servicios de Directorio Activo, dispositivos de red, entre otros.

El proveedor deberá:

- Identificar las vulnerabilidades de manera interna y pública, clasificarlas por nivel de riesgo y definir las acciones correctivas para el cierre de las brechas de seguridad identificadas.
- Comprobar la eficacia de las políticas de seguridad existentes.
- Evaluar los aplicativos y/o servicios expuestos públicamente ante ataques automatizados y manuales.
- Identificar datos sensibles.
- Identificar y establecer vectores de ataque específicos a la infraestructura tecnológica.
- Evaluar la autenticación de usuarios para verificar que las cuentas no puedan comprometer los datos (escalación de privilegios).

Identificación, análisis, priorización, verificación y explotación de las vulnerabilidades a la infraestructura actual, en el Centro de Datos Principal y el Centro de Datos Alterno; Se deberán realizar pruebas manuales y automatizadas como, por ejemplo:

- Reconocimiento de la red. Información IP, DNS.
- Transferencias de zona. Open source Intelligence a través de SHODAN, GHDB.
- Extracción de metadatos de documentos, imágenes, etc.
- Identificación de vectores de ataque.
- Detección de puertos, servicios, versiones.
- Enumeración de cadenas de comunidad SNMP.
- Banner Grabbing.

- Detección de contraseñas por defecto en servicios de Red y de Aplicación.
- Obtención de credenciales de protocolos sin capa de cifrado (inseguros) FTP, HTTP, IMAP, POP3, Telnet, VNC, SMTP, RPC, MYSQL.
- Obtención de credenciales a través de SSL implementando suplantación de certificados y aplicando técnicas de Bypass HSTS y Preloaded HSTS sites (HTTP Strict Transport Security)
- Obtención de Hashes NTLMv1 y v2 a través de SMBRelay
- Obtención de credenciales vía proxy WPAD.
- Obtención de credenciales POP, IMAP, SMTP, SQL.
- Detección de vulnerabilidades en diferentes tecnologías de acuerdo al entorno de las pruebas.
- Ataque de fuerza bruta a protocolos de Red y aplicación
- Generación de Diccionario Personalizado.
- Ataque vía diccionario a protocolos de Red y Aplicación.
- Crackeo de hashes vía fuerza bruta, diccionario y Rainbow Tables.
- Ejecución de exploits, comprometimiento de sistemas y obtención de acceso vía Shell.
- Compilación de códigos de exploits externos.
- Escalación de privilegios Via Exploits
- Escalación de privilegios a través de la recuperación de contraseñas almacenadas en el equipo.
- Escalación de privilegios a través de la obtención de credenciales mediante técnica forense de lsass dump.
- Escalación de privilegios a través de la búsqueda de contenido de archivos en el equipo con contraseñas.
- Escalación de privilegios a través de Password cracking.
- Movimientos laterales a redes aisladas o fuera del alcance a través de un equipo comprometido.
- Abuso del mecanismo de control de elevación
- Manipulación de tokens de acceso
- Scripts de inicio de sesión o de arranque
- Creación o modificación de procesos del sistema
- Modificación de la política de dominio
- Secuestro del flujo de ejecución
- Abuso de mecanismos de control de elevación
- Desofuscar/Decodificar archivos o información
- Explotación para la evasión de defensas
- Modificación de permisos de archivos y directorios
- Modificación del proceso de autenticación
- Modificación de la infraestructura de computación en la nube
- Subvertir los controles de confianza

- Evasión de Virtualización/Sandbox
- Descubrimiento y reconocimiento de información expuesta.
- Fingerprint al Servidor Web.
- Revisión de Metadatos en archivos expuestos.
- Identificación de puntos de entrada.
- Reconocimiento de Arquitectura y Frameworks.
- Prueba sobre la configuración de la Infraestructura.
- Prueba sobre la configuración de la plataforma.
- Pruebas sobre Métodos HTTP.
- Pruebas sobre manejo de extensiones de archivos con información confidencial.
- Enumeración de interfaces de administración.
- Prueba sobre cross domain policy.
- Pruebas sobre Roles.
- Pruebas sobre el proceso de registro.
- Pruebas sobre el proceso de aprovisionamiento de cuentas.
- Pruebas sobre la enumeración de cuentas y cuentas de usuario visitante.
- Pruebas sobre la debilidad en la política de usuario.
- Prueba del transporte de credenciales y canales cifrados.
- Prueba sobre credenciales por defecto.
- Prueba sobre mecanismos de bloqueo débiles.
- Prueba para bypass de esquema de autenticación.
- Pruebas sobre recuperación o reseteo de contraseñas.
- Pruebas de directorio transversal
- Pruebas de bypass al esquema de autorización
- Pruebas de escalación de privilegios
- Prueba sobre referencias inseguras a objetos.
- Prueba sobre el bypass de la gestión de sesiones.
- Pruebas sobre atributos en las cookies.
- Prueba sobre Session Fixation
- Pruebas sobre la exposición de variables en las sesiones.
- Pruebas sobre Cross Site Request Forgery.
- Pruebas sobre funcionalidades de logout
- Pruebas sobre Cross Site scripting reflejado
- Pruebas sobre Cross Site Scripting almacenado
- Pruebas sobre HTTP Tampering
- Pruebas sobre HTTP Parameter Pollution
- Pruebas sobre Inyecciones SQL
- Pruebas sobre Local File Inclusion
- Pruebas sobre Remote File Inclusion
- Análisis de código de errores
- Pruebas sobre debilidades en cifrados con SSL/TLS

- Pruebas sobre Padding Oracle
- Pruebas sobre información sensible enviada a través de canales sin cifrar.

Metodologías requeridas y aceptadas:

- Open Web Application Security Project (OWASP)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Penetration Testing Execution Standard (PTES)
- NIST SP 800-115

La Priorización de las vulnerabilidades y fallos tecnológicos identificados se documentará conforme a su clasificación y nivel de riesgo determinado por el estándar internacional para la puntuación de vulnerabilidades CVSS.

Requisitos:

Es indispensable que el proveedor del servicio cuente con personal con experiencia comprobable y altamente calificado en escenarios avanzados de hacking ético, análisis de aplicaciones web, desarrollo de exploits y emulación de adversarios. Se requiere que el personal cumpla con las siguientes certificaciones:

- OffSec Exploit Developer (OSED)
- OffSec Experienced Penetration Tester (OSEP)
- OffSec Web Expert (OSWE)
- OffSec Certified Expert 3 (OSCE3)
- Offensive Security Certified Professional (OSCP)
- Web Application Penetration Tester eXtreme (eWPTX v2.0)
- Certified Penetration Tester eXtreme v2 (eCPTX)
- Certified Secure Web Application Engineer (SWAE)

Debiendo anexar currículos con los cuales su personal acredite que cuenta con las certificaciones y acreditar las mismas con copias simples y numero de folio.

Entregables:

- Reporte Ejecutivo de Resultados
- Reporte Técnico de Resultados
- Plan de Remediación de Vulnerabilidades.

MONITOREO DE EVENTOS DE CIBERSEGURIDAD

Servicios de integración de registros (correlación de eventos). Se requiere:

- Integración de 3 portales, 5 aplicaciones, 50 equipos de red que incluyen switches, call manager, routers, 4 firewalls, WAF, 1 administrador de vulnerabilidades, VPNs, IPSs, Filtrado de contenido web, 50 servidores que pudieran ser Windows, Linux y que pudieran incluir IIS, Apache, SQL y MySQL, consola de antivirus, 1 consola de EDR.
- Configuración de 10 Tableros (dashboards)
- Debe incluir al menos pero no limitado a:
  - La integración de los elementos mencionados, en caso de no ser posible vía Syslog.
- Los tableros deberán ser de:
  - Eventos de los portales y la información contextual de todos los elementos de seguridad relacionada a los mismos e incluidos en el presente documento.
  - Eventos de las aplicaciones e información contextual de las herramientas de seguridad
  - Eventos de malware o Eventos de actividad inusual
  - Eventos de actividad maliciosa conocida como resultado de ejercicios de penetración
  - Eventos de alta criticidad de seguridad mostrado por las herramientas de seguridad y no contenido o bloqueado
  - Eventos anómalos, de falla o de riesgo de seguridad asociado a las 5 aplicaciones más importantes y 3 portales ya sea de manera directa o a través de los WAF
  - Las 30 reglas de correlación deberán incluir al menos los siguientes eventos/criterios y

serán definidas por el municipio al cierre de esta licitación:

- Accesos y modificaciones no autorizados a la red
- Accesos y modificaciones no autorizados a la infraestructura
- Accesos y modificaciones no autorizados a las aplicaciones
- Accesos y modificaciones no autorizados a los portales o Accesos y modificaciones remotos no autorizados o La creación de cuentas con altos privilegios o La modificación de reglas de firewalls
- La modificación a las políticas de los web application firewalls
- La modificación a las políticas de protección de control de cambios en los servidores
- Control o La modificación a las políticas de protección contra malware
- Violaciones a las políticas de navegación
- Violaciones a las políticas de protección en las aplicaciones SaaS
- Actividad anómala o inusual en la red.
- Indicadores de riesgo asociados con cambios realizados a los registros del sistema operativo de los endpoints o servidores.

AUDITORÍA DE CUENTAS CON ALTOS PRIVILEGIOS Y GESTIÓN DE CUENTAS DE SERVICIO
Servicios de auditoría de cuentas y privilegios deben incluir: El descubrimiento de cuentas con altos privilegios de dominio y locales en los servidores Windows y Linux ● Identificar los servidores destinados a alojar la herramienta y planificar la integración con el Active Directory existente. ● Desplegar la herramienta de auditoría de cuentas en los servidores designados, asegurando su instalación. ● Instalar la herramienta de análisis de contraseñas en el mismo entorno o en servidores complementarios, garantizando la conectividad con el Active Directory. ● Configurar la conexión segura y la sincronización entre el Active Directory y las herramientas instaladas. ● Establecer políticas de monitoreo para detectar cambios en grupos privilegiados, creación o eliminación de cuentas y modificaciones en permisos críticos. ● Configurar la herramienta de análisis de contraseñas para evaluar la fortaleza de las credenciales, definiendo parámetros de complejidad, caducidad y bloqueo para contraseñas débiles. ● Configurar la herramienta de auditoría de cuentas para que detecte y registre en tiempo real cambios relevantes, generando alertas automáticas cuando se superen umbrales críticos. ● Realizar análisis de contraseñas en los repositorios de credenciales, verificando el cumplimiento de las políticas de complejidad y caducidad.
FIREWALLS
Servicios de habilitación del firewall principal en clúster, incluyendo la habilitación de todas sus capacidades, incluyendo, pero no limitado a: firewall, VPN de usuario a sitio, Identificación de usuarios, IPS, control de aplicaciones de red, Antivirus, Protección contra redes robot y sandbox en modo de protección: ● La instalación de los equipos físicos a la red eléctrica y la red local de datos. ● La instalación de conectividad en sitio en la localidad central Para el cluster de sitio principal: ● La integración a la consola de administración. ● La configuración de alta disponibilidad de los equipos. ● La configuración de alta disponibilidad de al menos 2 enlaces de Internet

- La configuración de hasta 100 reglas de acceso incluyendo la traducción necesaria de IP (Network Address Translation) tanto para la navegación como para la navegación del servicio.
- La habilitación del módulo para identificación de usuarios del directorio activo.
- La habilitación de los módulos de antivirus y antibot.
- La habilitación de las capacidades de IPS, inicialmente en modo monitoreo y posteriormente en modo protección o bloqueo.
- La habilitación del sandbox integrado en modo protección.
- La habilitación de una VPN SSL usuario a sitio con autenticación a través del directorio activo.
- La habilitación del sandbox integrado en modo protección para la inspección del tráfico protegido a través del proxy.
- La habilitación de SDWAN para redundancia de enlaces de ISP.
- La estabilización de la operación de cada uno de los firewalls.

Para el cluster de sitio alterno:
Servicios de habilitación del firewall alterno en clúster , incluyendo la habilitación de todas sus capacidades, incluyendo, pero no limitado a: firewall, VPN de usuario a sitio, Identificación de usuarios, IPS, control de aplicaciones de red, Antivirus, Protección contra redes robot y sandbox en modo de protección:

- La instalación de los equipos físicos a la red eléctrica y la red local de datos.
- La instalación de conectividad en sitio en la localidad central.
- La integración a la consola de administración.
- La configuración de alta disponibilidad de los equipos.
- La configuración de alta disponibilidad de al menos 2 enlaces de Internet.
- La configuración de hasta 100 reglas de acceso incluyendo la traducción necesaria de IP (Network Address Translation) tanto para la navegación como para la navegación del servicio.
- La habilitación del módulo para identificación de usuarios del directorio activo.
- La habilitación de los módulos de antivirus e IPS.
- La habilitación de capacidades de IPS, inicialmente en modo monitoreo y posteriormente en modo protección o bloqueo.
- La habilitación del sandbox integrado en modo protección.
- La habilitación de una VPN SSL usuario a sitio con autenticación a través del directorio activo.
- La habilitación del sandbox integrado en modo protección para la inspección del tráfico protegido a través del proxy.
- La estabilización de la operación de cada uno de los firewalls.

La habilitación de redundancia de enlaces de ISP.

Servicios de habilitación de la consola de administración:

- Debe instalarse una consola para el sitio principal y otra para el sitio alterno.
- Debe tener integrados los clústers del sitio principal, del sitio alterno

Debe tener habilitada las capacidades de administración de todos los elementos, alertamiento, reporteo respaldo automático.

FIREWALL DE APLICACIONES WEB

Servicios para la habilitación de Web Application Firewall para la protección de 130 portales, incluyendo:

- La habilitación de una consola en nube para la gestión del WAF
- La integración de 130 portales
- La habilitación en modo de monitoreo/aprendizaje, de 20 en 20 portales, hasta completar 100 para la identificación de amenazas.
- La identificación de vulnerabilidades y capacidades de protección del WAF para habilitarlas en modo monitoreo, de 20 en 20, portales hasta completar 130.
- Afinación/validación/migración de las políticas de protección.
- Cambio a modo protección sin causar disrupción, de 20 en 20 portales, hasta completar 130
- Estabilización de la operación de las aplicaciones y el WAF.

SEGURIDAD DNS

- Servicios de instalación del DNS Sinkhole
- Definir el alcance del proyecto, identificando los servidores DNS internos, el entorno del Directorio Activo y la cantidad de dispositivos que deberán utilizar el nuevo servicio.
- Revisar la arquitectura DNS actual, tanto la resolución directa en el entorno local como la integración con el Directorio Activo, para establecer la estrategia de redirección.
- Recopilar y validar las fuentes de listas negras (dominios maliciosos, phishing, spam) y establecer criterios y frecuencia de actualización.
- Instalar la solución de DNS Sinkhole en un servidor o dispositivo dedicado, configurado con seguridad y respaldos para evitar puntos únicos de falla.
- Configurar el servidor para interceptar peticiones y redirigir aquellas que correspondan a dominios bloqueados a una dirección IP controlada (sinkhole).
- Integrar automáticamente las listas negras desde fuentes confiables, programando actualizaciones periódicas o en tiempo real.
- Definir y configurar listas blancas y excepciones para garantizar que dominios esenciales no sean bloqueados.
- Configurar la solución para que se integre con el DNS del Directorio Activo, de modo que la resolución de nombres en el entorno interno se realice a través del servidor de DNS Sinkhole.
- Ajustar la configuración de los controladores de dominio para que redirija las consultas DNS hacia la nueva solución, sin interrumpir la autenticación y otros servicios críticos.

- Verificar que la integración permita la sincronización de registros y que las actualizaciones en el Directorio Activo se reflejen correctamente en el sistema de resolución.
- Actualizar la configuración DNS en equipos, routers y controladores de dominio para que apunten al servidor que aloja el DNS Sinkhole.
- Realizar pruebas de resolución de nombres para confirmar que las peticiones legítimas se resuelven correctamente, mientras que aquellas dirigidas a dominios bloqueados son redirigidas al sinkhole.
- Ejecutar simulaciones de tráfico y escaneos de peticiones para validar que la solución opera con baja latencia y sin afectar la conectividad de la red interna.
- Configurar una consola de administración que muestre estadísticas en tiempo real, como el número de consultas bloqueadas, dominios más recurrentes y tendencias de tráfico sospechoso.
- Establecer alertas que notifiquen a los administradores en caso de picos anómalos en solicitudes bloqueadas o intentos persistentes de acceder a dominios maliciosos.
- Ajustar las políticas y reglas del sinkhole en base a la retroalimentación del tráfico, incorporando excepciones o reglas adicionales según se requiera.

ADMINISTRACIÓN DE VULNERABILIDADES

Servicio para identificar vulnerabilidades, que tengan las siguientes capacidades:

- Habilitación de la plataforma e integración con plataforma centralizada para gestionar el monitoreo de eventos de ciberseguridad.
- Configuración de tareas de escaneo de vulnerabilidades para 10 grupos y hasta 128 direcciones IPs Públicas y 1600 direcciones IPs privadas.
- Definición y habilitación de tareas de identificación periódica (mensual o trimestral) de vulnerabilidades alineado a los grupos definidos por el municipio: sistemas operativos, bases de datos, aplicaciones, portales, etc. Considerando la aparición de nuevas amenazas publicadas por el fabricante. Descubriendo el mayor volumen de vulnerabilidades sin causar disrupción en la operación.
- Configuración de un panel de control que señale las amenazas prioritarias a resolver en los activos prioritarios que defina el municipio.
- Definición e implementación de un proceso de administración de vulnerabilidades que asegure el descubrimiento y corrección oportuna de las vulnerabilidades, alineado a las capacidades de “seguimiento” de la herramienta.
- Definición de reportes y los alertamientos correspondientes alineados a los grupos de activos escaneados y las vulnerabilidades escaneadas mensualmente.

- Configuración de un panel de control que señale las amenazas prioritarias a resolver en los portales prioritarios que defina el municipio.
- Definición e implementación de un proceso de administración de vulnerabilidades que asegure el descubrimiento y corrección oportuna de las vulnerabilidades, alineado a las capacidades de “seguimiento” de la herramienta.

REVISIÓN DE SEGURIDAD DE CÓDIGO FUENTE

- Revisar los requerimientos de seguridad del código fuente y definir los objetivos de la evaluación (por ejemplo, detectar vulnerabilidades, errores lógicos y configuraciones inseguras).
- Identificar los lenguajes de programación y los repositorios de código que serán objeto del escaneo.
- Determinar la integración deseada con el pipeline de integración continua (CI/CD) y definir políticas de escalado en caso de encontrar vulnerabilidades críticas.
- Desplegar la solución SAST en el entorno de desarrollo o en un servidor dedicado, asegurando la conectividad con los repositorios.
- Configurar conectores o plugins para la integración con herramientas de CI/CD, de modo que cada commit o pull request active un escaneo automático.
- Establecer la sincronización con el sistema de control de versiones, permitiendo la revisión de resultados directamente en el flujo de desarrollo.
- Definir y aplicar políticas de análisis: establecer umbrales de severidad, reglas de bloqueo y criterios para identificar vulnerabilidades en el código.
- Configurar el análisis de dependencias y bibliotecas de terceros, para detectar fallas conocidas en paquetes o módulos.
- Ajustar la frecuencia y los parámetros del escaneo (por ejemplo, en cada commit, diariamente, o en ciclos programados) según las necesidades del proyecto.
- Ejecutar escaneos piloto en proyectos seleccionados para validar que la herramienta detecte correctamente las vulnerabilidades sin generar excesivos falsos positivos.
- Revisar y ajustar las reglas y políticas basadas en los resultados obtenidos en la fase de prueba.
- Configurar actualizaciones automáticas de las reglas y plugins de la herramienta, asegurando que se mantenga al día con nuevas vulnerabilidades y cambios en el código.
- Programar revisiones periódicas de la configuración, ajustando umbrales y políticas según la evolución del entorno de desarrollo.

Los requerimientos de gestión de las herramientas son los señalados:

SERVICIOS ADMINISTRADOS DE SEGURIDAD
Generales: • El proveedor deberá proporcionar soporte L1 y L2 en un esquema 5x8, de lunes a viernes, en un horario definido por el municipio. • Para incidentes operativos o de seguridad de carácter crítico, se deberá proveer una cobertura 24x7x365. • Se deberá proveer apoyo en sitio, especializado, para el diagnóstico, solución y si se requiere, escalación con el fabricante proveyendo seguimiento hasta su resolución. • Se deberán proveer métricas que permitan determinar la efectividad de las herramientas, incluyendo, mas no limitado a la cobertura de la solución y de los motores de protección. • Se deberá cumplir con las especificaciones del servicio, definidas en el apartado “Servicios de gestión de herramientas de seguridad” de esta convocatoria. • Se deberán proveer servicios de mantenimiento de cobertura de las herramientas, reportando de manera periódica (mensual) el estado de estas y los pasos necesarios para fortalecer (en caso de que aplique) su efectividad. **Servicio Administrado de Antivirus en Endpoint y Servidores** • Supervisar en tiempo real la actividad de los agentes instalados en endpoints y servidores, detectando malware, ransomware, spyware, troyanos, rootkits y otras amenazas emergentes. • Recoger y correlacionar registros de actividad para identificar patrones inusuales y comportamientos sospechosos en toda la infraestructura. • Gestionar actualizaciones diarias de firmas, algoritmos de detección y módulos de seguridad, garantizando que todos los dispositivos reciban las definiciones de amenazas más recientes. • Asegurar la correcta distribución de actualizaciones y realizar pruebas de verificación periódicas para confirmar su efectividad sin interrumpir la operatividad de los sistemas.

- Automatizar la puesta en cuarentena de archivos sospechosos o infectados, coordinando con los equipos de respuesta para iniciar procesos de recuperación.
- Realizar análisis forense de incidentes detectados, documentando la cadena de eventos, determinando el origen del ataque y generando recomendaciones para la remediación.
- Generar informes diarios, semanales y mensuales que incluyan estadísticas de detecciones, incidentes resueltos, tasa de falsos positivos y tendencias de amenazas.
- Configurar alertas automáticas en caso de eventos críticos y ofrecer paneles de control actualizados en tiempo real para facilitar la toma de decisiones.
- Ajustar la asignación de recursos (por ejemplo, CPU y memoria) en los equipos escaneados para evitar ralentizaciones en sistemas con capacidad limitada.
- Proveer soporte técnico 24x7 para resolver incidencias críticas, coordinar ventanas de mantenimiento y gestionar actualizaciones urgentes.

Servicio Administrado de Firewall

- Revisar y actualizar las reglas de filtrado, NAT, VPN, y segmentación en función de los cambios en la infraestructura y las amenazas emergentes.
- Aplicar políticas de inspección con estado (stateful inspection) y ajustar configuraciones de cortafuegos para optimizar la protección y minimizar falsos positivos.
- Supervisar en tiempo real el flujo de datos a través del firewall, identificando patrones de tráfico anómalo, intentos de intrusión o actividades inusuales.
- Ejecutar pruebas periódicas de penetración interna para confirmar la efectividad de las reglas y realizar ajustes en función de los resultados.
- Administrar la consola central del firewall para realizar cambios de configuración, actualizaciones de firmware y distribución de nuevas políticas a dispositivos en clúster o en diferentes ubicaciones (sitio principal y alterno).
- Coordinar la integración del firewall con otros dispositivos de seguridad (por ejemplo, WAF, IPS, SIEM) para una respuesta unificada ante incidentes.

- Configurar la generación de reportes detallados sobre el rendimiento del firewall, número de amenazas bloqueadas, tráfico inusual y estadísticas de conexión.

- Establecer alertas automáticas que notifiquen al SOC ante eventos críticos, facilitando la respuesta inmediata.

Servicio Administrado de Web Application Firewall (WAF)

- Definir y aplicar una configuración base adaptada a los portales y aplicaciones web del municipio, estableciendo reglas de protección que cubran los ataques listados en OWASP Top 10 y otras amenazas emergentes.
  Configurar la protección de APIs, el filtrado de bots, geo-blocking y controles específicos para aplicaciones según su criticidad.

- Diseñar reglas personalizadas para situaciones de vulnerabilidades o funcionalidad

- Monitorear y analizar el tráfico HTTP/HTTPS en tiempo real, incluyendo el descifrado de conexiones seguras para la detección de inyecciones, XSS, CSRF y otros ataques.

- Implementar ajustes automáticos de las políticas de seguridad cuando se detecten cambios en la estructura o comportamiento del sitio, utilizando modos de aprendizaje para minimizar falsos positivos.

- Coordinar la integración del WAF con servicios de CDN, balanceadores de carga y almacenamiento en caché para optimizar la entrega de contenido sin comprometer la seguridad.

- Supervisar la latencia y el rendimiento del tráfico web, asegurando que la protección no afecte la experiencia del usuario final.

- Generar informes en tiempo real y paneles de control que muestren estadísticas de bloqueos, intentos de intrusión, actividad sospechosa y desempeño general del WAF.

- Configurar notificaciones automáticas para eventos críticos que requieran intervención inmediata.

Servicio Administrado de Gestión de Vulnerabilidades

- Programar y ejecutar escaneos automáticos en toda la infraestructura (servidores, dispositivos de red, aplicaciones web), tanto desde la perspectiva interna como externa.

- Clasificar las vulnerabilidades encontradas utilizando escalas de riesgo (por ejemplo, CVSS) y priorizar las que deben ser remedidas de inmediato.
- Consolidar los hallazgos en una consola central, permitiendo la integración de resultados con otras herramientas de seguridad (SIEM), para un análisis global de incidentes.
- Generar reportes detallados y dashboards que muestren tendencias, avances en la remediación y áreas críticas de la infraestructura.
- Colaborar con el equipo de TI para coordinar la remediación de vulnerabilidades, estableciendo flujos de trabajo y asignando responsabilidades.
- Realizar escaneos de verificación tras la aplicación de parches o modificaciones, asegurando la efectividad de las acciones correctivas.
- Realizar un plan de remediación en conjunto con las áreas de TI para establecer acciones de mitigación
- Dar seguimiento a las remediaciones efectuadas y revalidar la correcta mitigación.

Servicio Administrado de Gestión de Parches en Servidores

- Realizar un inventario actualizado de servidores y aplicaciones críticas, identificando aquellos que requieren actualizaciones urgentes.
- Configurar escaneos automáticos para detectar parches pendientes y vulnerabilidades asociadas en sistemas operativos y software de terceros.
- Planificar ventanas de mantenimiento para aplicar actualizaciones en entornos críticos, minimizando la interrupción de los servicios.
- Ejecutar pruebas en entornos de laboratorio para validar la aplicación de parches antes de su despliegue en producción, y gestionar procedimientos de rollback en caso de incidencias.
- Supervisar el estado de los parches aplicados y generar informes de cumplimiento y avance, con métricas sobre la reducción de vulnerabilidades.
- Integrar la información de parches con el sistema global de gestión de vulnerabilidades para una visión unificada.

Servicio Administrado de Herramienta SAST (Análisis Estático de Seguridad de Aplicaciones)

- Conectar la herramienta de análisis estático con los repositorios de código y configurar integraciones automáticas con pipelines de integración continua, de modo que cada commit o pull request dispare un análisis de seguridad.
- Establecer conectores o plugins que permitan la revisión automática del código sin interrumpir el flujo de desarrollo.
- Definir políticas y reglas de escaneo que detecten vulnerabilidades, errores lógicos y configuraciones inseguras, incluyendo el análisis de dependencias y bibliotecas de terceros.
- Programar escaneos automáticos y manuales, y establecer umbrales de alerta que impidan la promoción del código a entornos de producción si se encuentran fallas críticas.
- Generar informes detallados que clasifiquen los hallazgos por severidad y proporcionen recomendaciones de remediación.
- Permitir la asignación de tareas y el seguimiento del estado de remediación de cada vulnerabilidad, facilitando la integración con el flujo de trabajo de desarrollo.
- Capacitar al equipo de desarrollo en la interpretación de los reportes y en la integración de la herramienta dentro del ciclo de vida del software.
- Establecer procedimientos para la actualización periódica de las reglas de análisis y la adaptación a nuevas amenazas.

Servicio Administrado de Correlacionador de Eventos (SIEM), Prevención de Intrusos (IPS) y DNS Sinkhole

- Recolectar logs y eventos de las distintas herramientas de seguridad (antimalware, firewall, WAF, SAST, gestión de vulnerabilidades y parches) y consolidarlos en una consola central.
- Configurar reglas de correlación personalizadas para identificar incidentes críticos, basadas en indicadores de compromiso y patrones de ataque.

- Administrar la plataforma de prevención de intrusos para analizar el tráfico a nivel de red y bloquear automáticamente actividades maliciosas, aplicando políticas definidas para diferentes tipos de ataques (por ejemplo, inyecciones, fuerza bruta).

- Establecer flujos de trabajo automáticos para la contención de incidentes, como el bloqueo de direcciones IP, reinicio de conexiones o aislamiento de segmentos afectados.

- Desplegar un servidor DNS Sinkhole que intercepte peticiones a dominios maliciosos y redirija dichas consultas a una dirección controlada, evitando que se establezcan conexiones a sitios con alto riesgo.

- Configurar listas negras actualizadas automáticamente, con la posibilidad de definir excepciones y listas blancas según la política de la organización.

- Integrar la salida de la plataforma con herramientas de análisis forense o SIEM para un seguimiento global de los incidentes.

- Configurar paneles de control y reportes periódicos que muestren la actividad de la red, incidentes detectados, respuestas ejecutadas y tendencias en las amenazas, con alertas en tiempo real para incidentes críticos.

- Establecer procedimientos de revisión periódica de las reglas y políticas de correlación, asegurando la actualización constante ante nuevas amenazas.

- Capacitar al personal de seguridad en el uso de la consola y en la interpretación de los eventos, garantizando la capacidad de respuesta inmediata ante incidentes.

Los requerimientos de gestión de respuesta a incidentes son los siguientes:

GESTIÓN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD

- Se identificará el proceso de gestión de respuesta y esquemas de comunicación ante incidentes de seguridad en conjunto con el municipio.
- La gestión de incidentes deberá estar disponible durante la vigencia del servicio, considerando al menos 1 incidente crítico por año, bajo demanda, en un esquema 24x7x365.
- Se deberá asignar a un responsable de la gestión, por parte del proveedor y el fabricante.
- Se deberá llevar a cabo el levantamiento inicial correspondiente para garantizar la correcta ejecución de los planes de comunicación y respuesta del municipio.
- Se deberán cubrir todas las características mencionadas en el apartado “Gestión de respuesta a incidentes” de este documento.

Los requerimientos del servicio de monitoreo de eventos de ciberseguridad son los siguientes:

MONITOREO SOC Y REPORTE DE INCIDENTES DE CIBERSEGURIDAD
• El proveedor deberá contar con un equipo de especialistas, dedicados a esta actividad, con el conocimiento de reporteo y análisis de información de seguridad informática. • Los reportes de ciberseguridad deberán ser enviados de acuerdo con el plan de comunicación y a los SLAs autorizados por el municipio para eventos anómalos y de seguridad. • El proveedor deberá contar con un SOC especializado, el cual podrá ser verificado en cualquier momento por el municipio. • El proveedor se encargará de dar mantenimiento a las integraciones, reglas de detección y elementos correspondientes a la tecnología que se implemente. • El proveedor deberá llevar a cabo, de manera progresiva, la implementación de flujos de trabajo de automatización, a través de la herramienta de monitoreo. • El proveedor deberá llevar a cabo el análisis de la operación del municipio para asegurar que aquellos falsos positivos no se reporten posterior a su identificación. • El proveedor deberá alertar la detección de indicadores de compromisos que indiquen la presencia de un incidente de seguridad de manera inmediata y presentar un reporte de los hallazgos, una vez se haya informado a los involucrados asociados con el plan de comunicación definido por el municipio. • El proveedor deberá proporcionar respuesta ante incidentes de seguridad en aquellas herramientas que administre, en colaboración con el área de SOC. • Se deberán enviar reportes periódicos (mensual) de las actividades realizadas durante el periodo, incluyendo, mas no limitado a: cobertura de agentes, hits en

honeypots, incidentes de seguridad identificados, estado de implementación de recomendaciones.
- El municipio será responsable de implementar las recomendaciones de reforzamiento de seguridad provistas por el SOC, siempre y cuando no sea una herramienta que gestione el proveedor.

ANEXO D. REQUERIMIENTOS DE SERVICIOS ADMINISTRADOS

Herramienta	Validación correcto funcionamiento	Requerimiento de migración a la nueva versión	Tareas Diarias	Requerimiento de respaldo mensual	Sesión Semanal	Reporteo diario vía correo electrónico	Reporte mensual en documento y reportado en una junta
Filtrado de contenido	Del filtrado.	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio. En el escenario en la nube, la migración deberá ser de los	Modificación de políticas de navegación sin límite de modificaciones.	Debe respaldarse la configuración de la consola políticas y reportes.	Para revisión de eventos, incidentes y fallas.	De salud de la herramienta	De navegación
	De la consola de administración		Modificación de políticas de DLP en el canal web, sin límite de modificaciones.			De eventos de seguridad.	De salud de la herramienta, consolidada, al mes.
			Reporteo de navegación de usuarios específicos como se requiera, sin límite.			De eventos de falla	De eventos de seguridad, consolidados, al mes

		agentes si así aplica	Validación del correcto funcionamiento.			De correcciones	De eventos de falla, consolidados, al mes
Cloud Access Security Brocker	Del tennant	No aplica	Modificación de políticas de protección, sin límite de modificaciones.	Debe respaldarse la configuración de la consola políticas y reportes.	Para revisión de eventos, incidentes y fallas.	De eventos de seguridad.	De eventos de seguridad, consolidados, al mes
	Del registro de actividades anomalías, incidentes		Modificación de políticas de DLP en el canal web, sin límite de modificaciones.			De eventos de falla	De eventos de falla, consolidados, al mes
			Reporte de incidentes de seguridad, sin límite.			De correcciones	De correcciones, consolidades, al mes
			Validación del correcto funcionamiento.				De recomendaciones, consolidadas, al mes.
Control de acceso a la red con mínimos privilegios	Del tennant	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del	Modificación de políticas de protección, sin límite de modificaciones.	Debe respaldarse la configuración de la consola políticas y reportes.	Para revisión de eventos, incidentes y fallas.	De eventos de seguridad.	De eventos de seguridad, consolidados, al mes
	Del gateway		Reporte de incidentes de seguridad, sin límite.			De eventos de falla.	De eventos de falla, consolidados, al mes
			Validación del correcto			De correcciones	De correcciones,

		requerimiento del municipio. Aplica para el gateway y los agentes.	funcionamiento.				consolidades, al mes
							De recomendaciones, consolidadas, al mes.
Prevención ante campañas de malware	De los motores de prevención	No aplica	Identificación de estaciones expuestas ante campañas de malware	No aplica	Para revisión de eventos, incidentes y fallas.	La aparición de una nueva campaña de malware vs las estaciones desprotegidas y las acciones de protección	De las campañas aparecidas en el mes en curso vs las acciones realizadas
Antimalware, antiransomware y parcheo virtual	De la consola de administración	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio. Aplica para el	Validación del correcto funcionamiento.	La configuración.	Para revisión de eventos, incidentes y fallas.	Coberturas	Cobertura del producto
			Cobertura de producto y patrones (antimalware, parcheo virtual.	La base de datos para la consola en sitio.			Cobertura de patrones o firmas
			Identificación, resolución y reporte de incidentes.			Incidentes de seguridad y/o falla	Eventos de seguridad
							Eventos de falla
						Correcciones realizadas y/o	Acciones realizadas
							Recomendaciones

		gateway y los agentes.				recomendaciones	
Control de dispositivos periféricos	Sobre demanda	Debe realizarse al menos una vez al año, como fundamento de una mejora o como resultado del requerimiento del municipio	Validación del correcto funcionamiento.	La configuración.	Para revisión de eventos, incidentes y fallas.	De eventos de seguridad.	De evento de seguridad, consolidados, al mes.
			Cobertura del producto.	La base de datos para la consola en sitio.		De eventos de falla.	De eventos de falla, consolidados, al mes
						De correcciones.	De correcciones, consolidades, al mes
							De recomendaciones, consolidadas, al mes.
Control de aplicaciones / Controles de cambios en los servidores	Cobertura de la solución en modo bloqueo	Debe realizarse al menos una vez al año, como fundamento de una mejora o como resultado del requerimiento del municipio	De la cobertura de productos en modo bloqueo.	La configuración.	Para revisión de eventos, incidentes y fallas.	Coberturas	Cobertura del producto
							Cobertura de modo protección: bloqueo o no bloqueo.
				El inventario		Incidentes de seguridad y/o falla	Eventos de seguridad
							Eventos de falla
						Correcciones realizadas y/o	Acciones realizadas
							Recomendaciones

						recomendaciones	
Control de aplicaciones	Cobertura de la solución en modo bloqueo	Debe realizarse al menos una vez al año, como fundamento de una mejora o como resultado del requerimiento del municipio	De la cobertura de productos en modo bloqueo.	La configuración.	Para revisión de eventos, incidentes y fallas.	Coberturas	Cobertura del producto
							Cobertura de modo protección: bloqueo o no bloqueo.
				El inventario		Incidentes de seguridad y/o falla	Eventos de seguridad
							Eventos de falla
						Correcciones realizadas y/o recomendaciones	Acciones realizadas
							Recomendaciones
Firewalls para las computadoras	Sobre demanda	Debe realizarse al menos una vez al año, como fundamento de una mejora o como resultado del requerimiento del municipio	De la cobertura de productos.	La configuración.	Para revisión de eventos, incidentes y fallas.	No aplica	De cobertura

Endpoint detection & Response EDR	De la consola de administración	Debe realizarse al menos una vez al año, como fundamento de una mejora o como resultado del requerimiento del municipio	Identificación de eventos de seguridad	No aplica	Para revisión de eventos, incidentes y fallas.	Eventos de seguridad extraños o anómalos	De eventos anómalos, consolidados, al mes.
			Investigaciones de los eventos de seguridad			De las investigaciones realizadas.	De las recomendaciones realizadas durante el mes.
Cifrado para las computadoras	Del motor de protección	Debe realizarse al menos una vez al año, como fundamento de una mejora o como resultado del requerimiento del municipio	De la cobertura de productos	La configuración.	Para revisión de eventos, incidentes y fallas.	No aplica	De fallas o habilitaciones, consolidadas, al mes.
				La llave de cifrado, cada vez que cambie o se agregue una			
Sandbox para PCs y previsor de intrusos	De disponibilidad del motor de protección	Sobre demanda, cuando aplique	Identificación del correcto funcionamiento	No aplica	Para revisión de eventos, incidentes y fallas.	Eventos de seguridad	Volúmen de eventos administrados por el sandbox, incluído en reporte de
						Fallas	

							antivirus y/o previsores de intrusos de propósito específico
Parchado	Cobertura de parches	Debe realizarse al menos una vez al año, como fundamento de una mejora o como resultado del requerimiento del municipio	Avance en la cobertura de los parches de acuerdo a la métrica.	Configuración	Para revisión de eventos, incidentes y fallas.	No aplica	Cobertura de parches vs métrica
	Salud de la herramienta de parcheo			Eventos de parcheo			Eventos de falla Acciones realizadas Recomendaciones
Previsores de intrusos de red de propósito específico, físicos y virtuales y su consola de administración	De los equipos y la consola	Debe realizarse al menos una vez al año, como fundamento de una mejora o como resultado del requerimiento del municipio	Alertamiento	Configuración	Para revisión de eventos, incidentes y fallas.	Eventos de seguridad	De salud de la solución.
			Reporteo sobre demanda, sin límite de eventos.				Eventos de seguridad
			Modificación, adición a las reglas de protección, sin límite de eventos.	Eventos de parcheo		Fallas	Cobertura de patrones o firmas
							De acciones

							De recomendaciones, consolidadas, al mes.
SIEM/XDR	De la disponibilidad de la consola de administración	No aplica	Monitoreo de eventos de seguridad.	Configuración	Para revisión de eventos, incidentes y fallas.	Eventos de seguridad	Actividad anómala identificada, consolidada, al mes.
	De los componentes desplegados (honeypots, sensores, colectores)		Configuración de reglas de monitoreo/correlación, sin límite de eventos.				
			Modificación o creación de dashboards, sin límite de eventos.				
Firewalls y VPN con todos sus módulos	De la consola de administración	Debe realizarse al menos una vez al año, como fundamento de una mejora o como resultado del requerimiento del municipio	Modificación de reglas, sin límite de eventos.	Configuración	Para revisión de eventos, incidentes y fallas.	Eventos de seguridad	De salud de la solución.
			De configuración asociada a cualquiera de sus módulos.	Eventos			Eventos de seguridad
			De habilitación de componentes y su configuración, sin límite de eventos			Fallas	Acciones realizadas
							Recomendaciones

Firewalls de web	De la consola de administración	No aplica	Modificación de reglas de protección a los servidores web, sin límite de eventos.	Configuración	Para revisión de eventos, incidentes y fallas.	Eventos de seguridad en los servidores web	Salud de la solución.
				Eventos			Eventos de seguridad
						Fallas	Acciones
							Recomendaciones
Administración de vulnerabilidades de infraestructura y web	De la consola de administración	No aplica	Seguimiento a las vulnerabilidades reportadas, con los responsables del equipo interno del municipio, para que sean resueltas.	No aplica	Para la corrección de vulnerabilidades	Sobre demanda, para servidores y/o equipos activos a punto de ser liberados y/o mensual	De las vulnerabilidades de los activos.
							Del score de riesgo y su comportamiento contra el mes anterior.

ANEXO E. CARACTERÍSTICAS Y/O CAPACIDADES DE TODOS LOS PRODUCTOS

Las capacidades y/o características específicas de los mismos se encuentran en el presente anexo E.

Vale la pena señalar que las capacidades y/o características que deben cumplirse en su totalidad es incluyendo las descritas en Anexo A y el anexo E.

1 PLATAFORMA DE SEGURIDAD PARA LA NAVEGACIÓN, LAS APLICACIONES SAAS, LA FUGA DE INFORMACIÓN, LA CLASIFICACIÓN DE INFORMACIÓN Y EL ACCESO
La solución se implementará como una plataforma unificada, administrada desde la nube, que protege la navegación, controla el acceso a aplicaciones SaaS y garantiza un modelo Zero Trust para el acceso a recursos internos. La solución se basa en la inspección del tráfico en tránsito y la gestión centralizada de políticas, sin requerir la instalación de agentes complejos en los endpoints, pero aprovechando un agente ligero (como WARP) y configuraciones DNS/Proxy

para redirigir el tráfico a la nube. Que cuente con las características de "Cloud Access Security Broker" y Control de acceso con el mínimo privilegio (Zero Trust Network Access).
1.1 Control de la Navegación
La solución de filtrado de contenido Web, debe incluir funcionalidades nativas integradas de: filtrado URL, control de aplicaciones Web, antimalware y prevención de fuga de información (DLP). La solución deberá contar con un servicio Web Proxy en modalidad nube para la utilización de filtrado web de los usuarios móviles de la organización con el fin de contar con seguridad en todos los sitios, dentro y fuera de la red corporativa, a través de la nube La solución deberá contar con la opción de que el tráfico web de usuarios pueda enrutar de forma automática hacia la nube a través de agentes para su análisis fuera de sitio La solución debe brindar un mecanismo para que los usuarios no manipulen el proxy de navegación, sea independiente del navegador y aplicaciones que utilicen internet para que sean filtrados de forma transparente Solución de filtrado de contenido Web debe proveerse a través de un servicio SaaS en nube de tipo gateway con la opción de desplegar localmente instancias virtuales del Gateway El servicio de Proxy SaaS debe ser administrado (tanto creación de políticas como gestión de incidentes) desde la misma consola de administración en nube que la solución de CASB solicitada en los numerales anteriores La solución deberá permitir la inspección del tráfico SSL, HTTPS. La solución debe permitir importar certificados propios de la entidad para realizar la inspección de SSL El servicio de Proxy SaaS debe garantizar un SLA de disponibilidad del 99.999% La solución debe permitir implementar la cantidad necesaria de Proxy On-Prem en modalidad virtual sin incurrir en costos adicionales de licenciamiento El servicio de Proxy SaaS debe contar con puntos de presencia (centros de datos) en México
Protección Antimalware en la navegación web:
La solución deberá contar con un motor Antimalware basado en firmas, comportamiento y emulación de navegadores, Malware en PDF, Detección de inyecciones de código para la detección de amenazas avanzadas, botnets y malware avanzado La solución deberá permitir la detección heurística proactiva.

La solución deberá permitir la detección y bloqueo de Proxies anónimos

El escáner proactivo deberá inspeccionar en profundidad el HTML y el código script utilizado por URLs hostiles, explotación de buffer overflow y shellcode injection.

Filtrado de Contenido web:
El administrador podrá sobrescribir la categoría de una URL o aplicaciones vs. La categoría dada por el fabricante

La solución deberá permitir el filtrado basado en reputación de los sitios web, para ello deberá contar con un sistema de reputación "en la nube" administrado y mantenido por el mismo fabricante que permita bloquear de forma dinámica contenido Web malicioso

La plataforma debe contar con un sistema de categorización de la navegación, aplicaciones y contenido basado en: Metadatos, fuentes de terceros (TrustedSource URL Lookup, DCC - Dynamic Content Categorization

La solución deberá contar con protección contra sitios web sin categorizar La solución deberá tener la capacidad de filtrado por:

- Revisión por reputación de archivos
- Tamaño del archivo
- Extensión del archivo
- Encabezados
- Usuario o Grupo que realiza la descarga

La solución deberá analizar en tiempo real una página y basándose en el contenido de la misma y catalogarla en tiempo real.
Las actualizaciones de los filtros por reputación de URL deben actualizarse en tiempo real continuamente, inmediatamente después que hayan sido descubiertas por el fabricante.

Control de Aplicaciones y Shadow IT:

La solución debe contar con un equipo dedicado a inspeccionar nuevos servicios Cloud, así como nuevos cambios dentro de los servicios ya evaluados en el registro, de tal manera que el registro se mantenga siempre al día.

Se debe mostrar en la consola la fecha de la última vez que se verificó el análisis de cada servicio Cloud

La solución debe permitir personalizar el criterio de clasificación de riesgo de los servicios cloud de acuerdo con las necesidades de cada empresa

La solución debe permitir añadir nuevos servicios cloud al registro, y estos deben ser accesibles para el demás cliente de la solución

La solución debe identificar intentos de fuga de información por servicios no corporativos a través del análisis de Machine Learning, correlacionado con la actividad de los usuarios en los servicios Sancionados

La solución debe permitir la comparación, atributo a atributo de hasta 4 servicios cloud en simultáneo para análisis del equipo de seguridad y riesgo

La solución debe tener la capacidad de integrarse con la solución de control web existente para generar bloqueos sin necesidad de instalar un nuevo proxy.

La solución debe contar con la capacidad de control (Bloquear/Permitir) con base en atributos de Riesgo de Shadow IT

La solución debe tener la capacidad de ejecutar control de instancias. Por ej, que los usuarios puedan ingresar únicamente a su cuenta corporativa de O365, y no a una cuenta personal de Hotmail o Outlook.

Capacidad de bloqueo de aplicaciones cloud por tipo de acción. Por Ej, permitir We Transfer para descargas, pero no para cargas

La solución debe tener la capacidad de aplicar políticas de DLP al tráfico Web y de prevención de Shadow IT.

La solución deberá tener la capacidad de realizar bloqueos de inicio de sesión a cuentas personales para los servicios de: AWS, Box, Google, M365, Dropbox, Slack, esto para evitar la fuga de información en el canal web.

1.2 Cloud Access Security Broker

Debe de tener la capacidad de aplicar políticas a la información en la nube basado en: Diccionarios, palabras clave, grupos de usuarios y expresiones regulares.

Debe poder incluir identificadores inteligentes de información, más allá de expresiones regulares simples.

Debe permitir el uso de validaciones de proximidad entre diferentes tipos de Identificadores de información

Cuenta con la capacidad de crear roles de usuario diferentes al del administrador global de la solución, para que usuarios específicos tengan la capacidad de:

- Definir o activar políticas de DLP y Compliance

- Crear, Acceder y remediar incidentes
- Administrar (acceder, restaurar, eliminar) documentos en cuarentena.

Debe poder configurar políticas de control de colaboración basadas en usuarios y grupos de usuarios

Debe poder mostrar un resumen de colaboración que incluya colaboración con: dominios externos, correos personales, usuarios internos.

Prevención de Amenazas:Debe proveer una auditoría detallada de las acciones ejecutadas por usuarios y administradores de los servicios Cloud integrados, inclusive servicios cloud desarrollados in house

Cada log de actividad debe ser complementado por la solución con metadata que informe sobre elementos como Geolocalización, Reputación de IP o agente de usuario

Se debe poder filtrar las actividades de los usuarios por: servicio cloud, rango de fecha, nombre de la actividad, categoría de la actividad y nombre de usuario

Se deben poder monitorear las actividades realizadas a través de diferentes tipos de dispositivos, como equipos móviles o computadores personales

La solución debe estar en la capacidad de ingerir y categorizar nuevos tipos de actividad recibidos desde el servicio Cloud integrado de manera automática, e incluirlos dentro del análisis de anomalías y amenazas

La solución debe poder identificar anomalías dentro del servicio Cloud y generar alertas basado en:

- Comportamiento de usuarios
- Localización
- Actividad de usuarios privilegiados
- Fuga de información
- Cuentas comprometidas
- Reputación de IP

No se debe requerir una configuración previa para que la solución empiece a identificar las anomalías mencionadas en el punto anterior

La solución debe poder identificar uso anómalo de cuentas privilegiadas, basado en escalamientos de privilegios, creación/eliminación masiva de cuentas, y exceso de actividades administrativas para un usuario

- La solución debe correlacionar anomalías a través de varios servicios Cloud integrados con la solución, inclusive servicios cloud desarrollados in house.

Prevención de Amenazas: Debe proveer una auditoría detallada de las acciones ejecutadas por usuarios y administradores de los servicios Cloud integrados, inclusive servicios cloud desarrollados in house.

Cada log de actividad debe ser complementado por la solución con metadata que informe sobre elementos como Geolocalización, Reputación de IP o agente de usuario

Se debe poder filtrar las actividades de los usuarios por: servicio cloud, rango de fecha, nombre de la actividad, categoría de la actividad y nombre de usuario

Se deben poder monitorear las actividades realizadas a través de diferentes tipos de dispositivos, como equipos móviles o computadores personales

La solución debe estar en la capacidad de ingerir y categorizar nuevos tipos de actividad recibidos desde el servicio Cloud integrado de manera automática, e incluirlos dentro del análisis de anomalías y amenazas

La solución debe poder identificar anomalías dentro del servicio Cloud y generar alertas basado en:

- Comportamiento de usuarios
- Localización
- Actividad de usuarios privilegiados
- Fuga de información
- Cuentas comprometidas
- Reputación de IP

No se debe requerir una configuración previa para que la solución empiece a identificar las anomalías mencionadas en el punto anterior

La solución debe poder identificar uso anómalo de cuentas privilegiadas, basado en escalamientos de privilegios, creación/eliminación masiva de cuentas, y exceso de actividades administrativas para un usuario

La solución debe correlacionar anomalías a través de varios servicios Cloud integrados con la solución, inclusive servicios cloud desarrollados in house.

Control de acceso a aplicaciones SaaS:

La solución debe tener la capacidad de aplicar políticas de control de acceso basado en:

- Grupo de usuarios
- Geografía
- Dispositivos gestionados/no gestionados
- Tipo de actividad
- Información sensible

La solución debe poder aplicar las políticas de control de acceso tanto a PCs como a dispositivos móviles

No se debe requerir el despliegue o instalación de ningún tipo de agente para aplicar las políticas de control de acceso si está cuenta con un mecanismo para provocar el control a través de la identidad del usuario

Se debe permitir otorgar acceso de solo lectura a conexiones realizadas al servicio cloud desde dispositivos no gestionados

La solución no debe requerir estar en modo Forward Proxy entre los clientes y el servicio cloud para aplicar control de acceso a estos servicios

No se debe requerir ningún tipo de desarrollo ni construcción de APIs por parte de la entidad para integrar aplicaciones desarrolladas in house

Google Enterprise específico:

La solución debe permitirles a los administradores personalizar vistas y reportes basados en la información que deseen ver.

La consola debe permitir programar la ejecución de reportes y que estos sean enviados vía correo en formato pdf, csv o xls

La solución debe presentar un dashboard de madurez de implementación de la misma, donde se muestre el nivel de adopción de la herramienta en la entidad, comparativas anónimas con otros clientes de la misma vertical y recomendaciones de funcionalidades a implementar de la solución

La solución debe contar con un Dashboard ejecutivo que muestre métricas detalladas trimestre a trimestre de todos los elementos monitoreados a nivel de SaaS/IaaS/PaaS, usuarios involucrados, incidentes generados, acciones de remediación ejecutadas, etc.

La solución debe mostrar en un Dashboard la matriz detallada de cómo se mapean todos los incidentes de seguridad identificados a nivel de fallas de configuración, DLP, Vulnerabilidades, Apps conectadas y Malware contra el Framework de MITRE ATTACK

LIBERTAD 101 CENTRO
SPGG / NL

SAN PEDRO
GARZA GARCÍA

TEL
81 8400 4400

La solución debe permitir la creación de roles de administración con funciones específicas de Administración, Gestión de Incidentes y Gestión de Políticas para cada una de las secciones ofrecidas en la solución

La solución debe permitir la creación de jurisdicciones de administración basadas en atributos de AD de tal manera que un Administrador solo pueda ver los incidentes asociados a los usuarios pertenecientes a un grupo específico de AD asignado a la jurisdicción

Deberá permitir capacidad multitunel.

Deberá tener la capacidad de conectar a diferentes sitios (diferentes nubes, diferentes centros de datos, oficinas, etc.) con una sola autenticación sin la necesidad de que el usuario requiera autenticarse en cada sitio al que se conecte.

Deberá brindar acceso seguro a recursos sin necesariamente hacer modificaciones en los dispositivos de red como: switches, firewalls, routers, entre otros.

Deberá soportar los protocolos TCP

Deberá ser capaz de re-enrutar el tráfico entre el cliente y el recurso que requiere utilizar.

Deberá tener la capacidad para establecer reglas de acceso de manera individual por cada recurso o grupo de recursos de red.

Deberá brindar las capacidades para que la comunicación entre servicios cloud, datacenter públicos y datacenter privados debe estar cifrada en todo momento.

Deberá admitir la configuración de reglas entrantes entre el usuario y los recursos a ser protegidos. Deberá asignar los permisos a los usuarios de acuerdo con la estrategia de mínimo privilegio.

Deberá permitir otorgar los mínimos privilegios requeridos por el usuario para el cumplimiento de sus funciones.

Deberá permitir que las políticas y controles de acceso se definen alrededor de la identidad del usuario.

Deberá garantizar que solo los usuarios verificados (identificados y correctamente autenticados) pueden comunicarse con los recursos corporativos.

Deberá tener la capacidad de controlar que los usuarios solo podrán establecer canales de comunicación con los sitios protegidos que fueron autorizados para cada usuario tras el proceso de autenticación.

Deberá permitir que los privilegios de usuario se ajusten en tiempo real de ser necesario. Deberá permitir establecer controles dinámicos de acuerdo con la postura de seguridad del usuario y su dispositivo de conexión. Deberá proveer la capacidad de gestionar el onboarding de los usuarios en una base de datos propia o proveer las capacidades para integrarse con un proveedor de identidad provisto por el cliente. Deberá poder integrarse con proveedores de identidad que utilicen los protocolos SAML Deberá tener la capacidad de registrar el tráfico y accesos de usuarios que se conectan a través de ella. Deberá permitir el reenvío del syslog a herramientas de correlación tipo SIEM. Deberá hacer registro (logs) de todos los accesos de los usuarios, tanto el tráfico permitido como el tráfico denegado. Deberá tener un agente de tipo software que pueda ser instalado en los equipos de los usuarios con los sistemas operativos más utilizados, tales como: windows 7 o superior, OSX/macOS 10.13.6 o superior Deberá poder implementarse en ambientes virtuales, tales como: VMware ESX (6.0 or 6.5U2), KVM (libvirt 4.0.0 o superior), Microsoft Hyper-V (10.0.14393 o superior), Servicios Cloud: Amazon Web Services (AWS), Microsoft Azure and Google Compute Engine. Deberá tener soporte para implementarse tanto en ambientes nube como en sitios (on-premise). Deberá permitir agregar nuevos recursos o usuarios sin provocar indisponibilidad en los servicios. Deberá ser basada en un componente central (consola), pop y agentes. Deberá contar con modos de instalación de agentes para equipos desatendidos, la instalación deberá ejecutarse desde la línea de comandos. Deberá admitir el acceso basado en roles para la consola de administración. Deberá permitir la visualización gráfica de dashboards, e información del registro de actividad de los usuarios
1.4 Control de Acceso a la Red con el mínimo privilegio
Deberá de ser administrado por la misma consola de administración de los controles anteriores para asegurar la centralización y la unificación de configuración Deberá estar basada en el modelo Zero Trust.

Deberá garantizar que el proceso de autenticación de los usuarios para acceder a los recursos protegidos y a los diferentes componentes que controlan el acceso a los recursos de red, se realice de manera independiente y previo al establecimiento de cualquier canal de comunicación hacia los recursos privilegiados. Deberá garantizar que el acceso a los recursos se haga de forma segura. Deberá establecer canales de comunicación seguros, usando criptografía fuerte. Deberá garantizar que la conexión se realice sólo a los recursos autorizados. Deberá garantizar que los recursos a los que el usuario no tiene acceso permanezcan inaccesibles. Deberá garantizar que se elimine el movimiento lateral - movimiento este - oeste. Deberá permitir capacidad multitunel.

Deberá tener la capacidad de conectar a diferentes sitios (diferentes nubes, diferentes centros de datos, oficinas, etc.) con una sola autenticación sin la necesidad de que el usuario requiera autenticarse en cada sitio al que se conecte.

Deberá brindar acceso seguro a recursos sin necesariamente hacer modificaciones en los dispositivos de red como: switches, firewalls, routers, entre otros.

Deberá soportar los protocolos TCP

Deberá ser capaz de re-enrutar el tráfico entre el cliente y el recurso que requiere utilizar.

Deberá tener la capacidad para establecer reglas de acceso de manera individual por cada recurso o grupo de recursos de red.

Deberá brindar las capacidades para que la comunicación entre servicios cloud, datacenter públicos y datacenter privados debe estar cifrada en todo momento.

Deberá admitir la configuración de reglas entrantes entre el usuario y los recursos a ser protegidos. Deberá asignar los permisos a los usuarios de acuerdo a la estrategia de mínimo privilegio.

Deberá permitir otorgar los mínimos privilegios requeridos por el usuario para el cumplimiento de sus funciones.

Deberá permitir que las políticas y controles de acceso se definen alrededor de la identidad del usuario.

Deberá garantizar que solo los usuarios verificados (identificados y correctamente autenticados) pueden comunicarse con los recursos corporativos.

Deberá tener la capacidad de controlar que los usuarios solo podrán establecer canales de comunicación con los sitios protegidos que fueron autorizados para cada usuario tras el proceso de autenticación.

Deberá permitir que los privilegios de usuario se ajusten en tiempo real de ser necesario.

Deberá permitir establecer controles dinámicos de acuerdo con la postura de seguridad del usuario y su dispositivo de conexión.

Deberá proveer la capacidad de gestionar el onboarding de los usuarios en una base de datos propia o proveer las capacidades para integrarse con un proveedor de identidad provisto por el cliente.

Deberá poder integrarse con proveedores de identidad que utilicen los protocolos SAML

Deberá tener la capacidad de registrar el tráfico y accesos de usuarios que se conectan a través de ella.

Deberá permitir el reenvío del syslog a herramientas de correlación tipo SIEM.

Deberá hacer registro (logs) de todos los accesos de los usuarios, tanto el tráfico permitido como el tráfico denegado.

Deberá tener un agente de tipo software que pueda ser instalado en los equipos de los usuarios con los sistemas operativos más utilizados, tales como:

- windows 8 o superior
- OSX/macOS 10.13.6 o superior

Deberá poder implementarse en ambientes virtuales, tales como:

- VMware ESX (6.0 or 6.5U2), KVM (libvirt 4.0.0 o superior)
- Microsoft Hyper-V (10.0.14393 o superior)
- Servicios Cloud: Amazon Web Services (AWS),
- Microsoft Azure and Google Compute Engine.

Deberá tener soporte para implementarse tanto en ambientes nube como en sitios (on-premise).

Deberá permitir agregar nuevos recursos o usuarios sin provocar indisponibilidad en los servicios.

Deberá ser basada en un componente central (consola), pop y agentes.

Deberá contar con modos de instalación de agentes para equipos desatendidos, la instalación deberá ejecutarse desde la línea de comandos.

Deberá admitir el acceso basado en roles para la consola de administración.

Deberá permitir la visualización gráfica de dashboards, e información del registro de actividad de los usuarios.

2. PLATAFORMA DE SEGURIDAD PARA EL ENDPOINT

Que sea una plataforma que se tenga la opción para instalarse en la nube y en una consola en sitio, para administrar controles específicos o solventar cualquier requerimiento normativo

2.1 Anticipación de campañas de malware

La solución debe proporcionar la información global más reciente sobre las campañas más importantes que los actores de amenaza utilizan para dirigirse a sectores empresariales y organizaciones de todo el mundo de ser posible consultar las métricas por industria.

La solución debe permitir la calificación de la postura de seguridad, permitiendo visualizar su calificación actual según su Contenido, Ataques de día cero, Configuración y Prevalencia de detección.

La solución debe permitir visualizar el número de dispositivos de su entorno que están expuestos y aquellas campañas de malware detectadas o cuya cobertura de contenido es insuficiente para campañas ya conocidas.

Permitir la visualización de posibles amenazas dentro de la misma consola de gestión facilitando la integración y visualización de los eventos, al igual que permitiendo tener información de la amenaza dentro del mismo panel para entender su comportamiento

La solución debe poder establecer un % de postura de seguridad frente a amenazas de alto riesgo y actuar como una especie de auditor a fin de dar a conocer el estado actual de cobertura y correcto
despliegue de las soluciones licenciadas, permitiendo de manera general evaluar el parque computacional gestionado frente al riesgo de amenazas.

La solución debe tener opciones de implementación de servidor flexibles para adaptarse a varios tipos de entornos.

- On-prem
- SaaS
- Hybrid

La solución debe de mostrar los endpoint con riesgo frente a las campañas de

malware la solución debe de mostrar las campañas de malware por severidad

La solución debe de mostrar el número de las últimas campañas de malware detectadas
La solución deberá de mostrar los endpoint afectados por alguna campaña de malware dentro del ambiente
La solución debe de mostrar cuándo fue la última detección de la campaña de malware en el ambiente
La solución debe de mostrar el detalle del impacto de la campaña de malware
La solución debe de mostrar información detallada de la campaña de malware como:

- MD5
- SHA256
- IP Address

- URL
- Domains

La solución debe de mostrar información del comportamiento de la amenaza de acuerdo a las técnicas de MITRE y su descripción

La solución debe de mostrar información de las soluciones donde ha sido detectada la campaña de malware

La solución debe de tener integración con mecanismos como EDR dentro de la misma plataforma para poder realizar la búsqueda de indicadores de compromiso en el ambiente.

2.2 Antimalware con anti ransomware y parcheo virtual

La solución deberá soportar los siguientes sistemas operativos de servidores:

- Windows Server 2022 (incluyendo Server Core mode)
- Windows Server 2019 (incluyendo Server Core mode)
- Windows Server 2016 RS3, 2016 (incluyendo Server Core mode)
- Windows Server 2012, 2012 R2, and 2012 R2 Update 1: Essentials, Standard, Datacenter (incluyendo Server Core mode)
- Windows Storage Server 2012 and 2012 R2
- Windows Server 2008 y 2008 R2: Standard, Datacenter, Enterprise, Web (incluyendo Server Core mode)
- Windows Storage Server 2008 and 2008 R2
- Windows Small Business Server 2011
- Windows Small Business Server 2008
- Linux CentOS 7.4, 7.3, 7.2, 7.1 (64-bit)
- Red Hat Enterprise Linux 7.x, 6.x
- Linux Ubuntu 18.X, 20.X, 21.X (64-bit)

La solución deberá soportar los siguientes sistemas operativos de clientes:

- Windows 11
- Windows 10 Anniversary Update o superior
- Windows 10
- Windows 8.1 Update 1
- Windows 8 (no incluyendo Windows RT edition)
- Windows 7
- Windows To Go (All versions)

- Windows Vista SP2
- Windows Embedded 8: Pro, Standard, Industry
- Windows Embedded Standard 7
- macOS 10.9 Mavericks
- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma
- macOS 15 Sequoia
- Linux Ubuntu 16.X ,18.X, 20.X, 21.X, 22.X, 24.X (64-bit)
- Amazon Linux AMI 2017.9, 2016 and later
- Debian 10.0, 9.0, 8.0

La solución debe ser administrada de forma centralizada.

La solución debe permitir la gestión y manejo de políticas de mecanismos de defensa integrados a Windows 10 (Firewall, Defender) y las subsecuentes actualizaciones

La solución debe ofrecer distintos modelos de gestión: On-Premises, IaaS o SaaS.

La solución deberá ser administrada en la misma consola que el resto de los componentes de seguridad mencionados en este documento, así como podrá utilizar un modelo híbrido on-prem y nube.

- Microsoft Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Se debe poder desplegar el agente de la solución desde la consola de administración y este debe ser el componente administrativo único de todas las funcionalidades solicitadas en este documento.

La solución debe contar con los mecanismos de protección para no poder ser desinstalada o desactivada por el usuario.

La solución debe avisar sobre los posibles conflictos que existan de la solución a otras soluciones de antivirus y firewall instalados previamente en la máquina.

Se deben poder habilitar o deshabilitar los módulos de protección sin ser desinstalados del sistema.

Se debe poder restringir completa o parcialmente al acceso a la consola cliente para configurar parámetros individuales sobre el host.

La desinstalación de la aplicación puede ser protegida mediante contraseñas desplegadas por políticas configuradas por el administrador.

Puede existir más de una configuración de idioma para la aplicación cliente.

La solución debe basarse en una plataforma común sobre la cual se incorporan módulos de Prevención de Amenazas, control web, y Firewall de escritorio, y que permita el intercambio de información entre cada uno de los módulos.

Para antimalware (antivirus):
La solución debe de poder configurarse para realizar escaneos por demanda o programados, desde la consola de administración o desde la consola cliente.

Se debe poder configurar acciones sobre infecciones identificadas:

- Denegar acceso
- Limpiar
- Eliminar
- Ninguna

Debe tener la opción de detectar actividad del usuario, teniendo en cuenta el funcionamiento del disco, mouse y teclado para activar escaneos y no afectar la productividad.

La solución debe ofrecer opciones de envío de infecciones a cuarentena y ejecutar acciones sobre ítems enviados allí.

Se deben reportar eventos de amenazas directamente sobre la consola cliente, de forma consolidada (AV, Web e IPS/FW), priorizada y bajo un lenguaje específicamente descriptivo donde de manera natural cada registro explique cuál fue el elemento que causante, cuál fue la acción realizada por este, que componentes estuvieron involucrados, que regla de protección fue violada. No se admiten tablas, archivos tabulados en texto plano, listas o cualquier tipo registro que no sea fácilmente entendido por el usuario final.

La solución debe poder habilitar la opción de escaneo de clic-derecho sobre carpetas específicas.

Es requerido que la solución en equipos Windows reciba actualizaciones de seguridad bajo un único componente (archivo) consolidado que incluya lo correspondiente a: Antivirus, Protección Web e IPS, con el fin de disminuir la carga administrativa y de red que supondría realizarlos de forma independiente

Debe contar con mecanismos de protección de exploits Generic Buffer Overflow Overflow Protection (GBOP) o integración con Microsoft DEP (Data Execution Prevention).

La solución debe contar con mecanismos de protección contra la ejecución de scripts maliciosos de IE, sean JavaScript o VBScript.

La solución debe de contar con detección de inyección de código en memoria

La solución debe de contar con mecanismos de protección contra vulnerabilidades y exploits, actuando como un parcheo virtual ofreciendo seguridad de día cero y debe de estar constantemente actualizándose basado en los anuncios de vulnerabilidades nuevas

La solución debe poder configurar mediante reglas o políticas de protección de:

- Entradas y llaves de registro de Windows.
- Prevención de creación de ejecutables portables (.INI, .PIF).
- Creación de archivos autorun.
- Prevención de uso de archivos TFTP (Trivial File Transfer Protocol).
- Creación y modificación remota de archivos o carpetas.
- Acceso remoto de archivos o carpetas.

.EXE, .BAT y otros ejecutables bajo la llave de registro HKEY_CLASSES_ROOT.

- Modificación de procesos core de Windows.
- Modificación de configuraciones de exploradores y navegadores web.
- Proteger procesos con subreglas personalizadas
- Asignar las reglas por nombre de usuario

Para Protección contra amenazas avanzadas (antivirus de nueva generación)

Debe estar basado en reglas de comportamiento configurables tanto desde la consola cliente como la consola central

Debe poder integrarse con herramientas tipo EDR (Endpoint Detection and Response)

La funcionalidad debe poder liberar una aplicación contenida mediante:

- Cambio en la reputación dentro del sistema de inteligencia contra amenazas

- Exclusión en la política

La solución deberá permitir generar una infraestructura colaborativa entre puntos de protección ya sea a nivel perimetral, contenido, virtual o en los equipos de usuario final puedan intercambiar información sobre nuevas amenazas detectadas en tiempo real mediante un protocolo abierto diseñado para este propósito.

La solución deberá permitir reputar archivos localmente (de forma manual o a través de reglas de comportamiento) y mediante distintas fuentes de reputación dentro de la infraestructura de seguridad como: Sandbox y Proxys Web)

Para la protección de amenazas de día cero, la solución debe permitir enviar automáticamente archivos a un sandboxing para análisis de amenazas avanzadas y de día cero a fin de inspeccionar la amenaza y ofrecer un veredicto (Malicioso / No-Malicioso) y basado en dicha detección compartir los resultados en tiempo real, alimentado al ecosistema de Endpoint y Red de la organización. Todo esto desde la misma consola de gestión.

La solución debe permitir asignar diferentes niveles de reputación a aplicaciones y certificados que se ejecutan en un ambiente con un punto de análisis a nivel local, la difusión de esta asignación debe realizarse en tiempo real mediante un protocolo diseñado para este propósito sin requerir que los agentes realicen un proceso de actualización firmas o configuraciones.

En caso de generarse un evento, la comunicación de este debe ser en tiempo real mediante el protocolo de comunicación diseñado para este fin, no debe depender de los ciclos de actualización de eventos a la consola central ni del "llamado/despertar de agentes"

La solución no deberá ser un sistema de antivirus, control de aplicativos y/o control de cambios, pero debe poder integrarse con estos dispositivos en caso de que se encuentren presentes

La solución al determinar la reputación de un archivo ejecutable, deberá comunicar al resto de los equipos de usuarios finales con el objetivo de crear una inteligencia de seguridad en la red.
La solución deberá tener una funcionalidad específica diseñada para inspeccionar archivos y actividad sospechosa con el fin de detectar patrones maliciosos mediante el uso de técnicas de “Machine Learning”.

Debe tener dos modos de análisis: en la nube y en el cliente, dependiendo de la conectividad de los equipos

Debe incluir contexto de la causal de detecciones de amenazas

Debe recolectar información de los atributos de los archivos y su comportamiento para realizar el análisis

La solución debe tener la capacidad de detectar y tomar acción sobre amenazas "fileless"

La solución debe tener la capacidad de realizar acciones de remediación y rollback ante ataques de ransomware Esta funcionalidad debe ser opcional y deberá poder ser desactivada tanto en la consola cliente como mediante política centralizada a través de la consola central de administración Debe permitir seleccionar que las aplicaciones con una reputación específica deben ser ejecutadas en modo “contenido”, es decir que esta funcionalidad no le permitirá realizar ciertas acciones que hayan sido consideradas como maliciosas dentro del sistema operativo La solución deberá poder tomar acciones o de bloqueo o registro según su configuración Debe estar en la capacidad de integrarse y recibir actualizaciones de reputación de un sistema de inteligencia contra amenazas mediante el uso de protocolo abierto de comunicación diseñado específicamente para esta finalidad, con la capacidad de actualizar todas las máquinas del ambiente en tiempo real, sin necesidad de actualizar políticas o comunicarse con la consola de administración Este módulo debe permitir la ejecución de las aplicaciones potencialmente maliciosas permitiéndoles la ejecución dentro del ambiente (punto final), mientras que limita los cambios en el sistema operativo que esta puede realizar.

2.3 Control de dispositivos periféricos
La solución debe ser soportada en sistemas operativos Windows y MacOS La solución debe permitir el monitoreo o bloqueo total de los dispositivos conectados En los casos que aplique, la solución debe permitir la creación de políticas unificadas para sistemas operativos Windows y MacOS. La gestión de control de dispositivos debe estar unificada en la misma consola utilizada para la gestión de anti-malware. La solución debe permitir la extensión de sus funcionalidades hacia Prevención de Fuga de Datos, con el propósito de evitar despliegues adicionales Cada regla debe permitir la configuración basada en localización del usuario, de tal forma que permita tomar distintas acciones cuando el usuario está dentro o fuera de la organización.

La solución debe permitir la desactivación de una regla o un conjunto de reglas. La solución debe permitir el control de los siguientes tipos de dispositivos:

- Almacenamiento Removible;
- Bluetooth;
- Dispositivo Multimedia;
- Smartphones;
- Dispositivos Plug and Play;

La solución debe permitir el bloqueo de ejecución de aplicaciones desde dispositivos removibles, permitiendo también configurar excepciones.

La solución debe permitir el control de dispositivos bajo los siguientes criterios:

- Clase de Dispositivo;
- Medio de conexión;
- Fabricante y/o modelo;
- Número de serie;

La solución debe permitir crear políticas de bloqueo, monitoreo o solo lectura para dispositivos de almacenamiento removible.

La solución debe permitir la configuración de definiciones de dispositivos bajo las siguientes categorías:

- Gestionado;
- No gestionado;
- Lista Blanca;

La solución debe permitir el agrupamiento de dispositivos por medio de propiedades comunes, como: Vendor ID, Product ID o Device Class.

La solución debe ser capaz de identificar los dispositivos Plug and Play bajo las siguientes propiedades:

- Tipo de Bus;
- Clase de Dispositivo (Device Class)
- ID de fabricante (Vendor ID)
- ID de producto (Product ID)

La solución debe ser capaz de identificar los dispositivos removibles bajo las siguientes propiedades:

- Tipo de Bus;
- Sistema de Archivo;
- Número de Serie;
- Permisos de lectura/escritura;

La solución debe poseer las siguientes clases de dispositivos de manera nativa:

- Batería;
- Lectores de huella y dispositivos biométricos;
- Bluetooth;
- Drives de CD/DVD;
- Impresoras y scanners;
- Adaptadores de video;
- Disco Duro;
- Controladoras y drives de disquete;
- Infrarrojo;
- IEEE 1394;
- Mouse;
- Modem;
- Adaptadores de Red;

Debe ser posible habilitar o deshabilitar una determinada regla de protección de acuerdo a la localización del equipo (ej. Dentro o fuera de la red organizacional)

La solución debe poseer los siguientes tipos de dispositivos de manera nativa:

- Dispositivos Apple;
- Dispositivos Bluetooth;
- Drives CD/DVD;
- Dispositivos de almacenamiento removible;
- Lectores de tarjetas SD;
- Dispositivos Windows Portable;
- Dispositivos Plug and Play;

La solución debe permitir la creación de clases y tipos de dispositivos personalizados, utilizando, como mínimo, los siguientes criterios:

- Clase de Dispositivo;
- Tipo de Bus;
- Número de Serie;
- ID de fabricante;
- ID de producto;
- Sistema de Archivo

La solución debe permitir la creación de los siguientes tipos de controles:

- Regla para control de discos duros;
- Regla para dispositivos Plug and Play;
- Regla para dispositivos de almacenamiento removible;
- Regla de acceso de archivos a dispositivos de almacenamiento removible;
- Cada regla debe tener la capacidad de ser aplicada a:
- Cualquier usuario (All);
- Usuario que pertenece a un grupo específico (OR);
- Usuario que pertenezca a todos los grupos (AND);
- Usuario local o usuario fuera del dominio;

Durante la definición de las reglas, la solución debe permitir la creación de objetos LDAP en base a:

- SID de Objeto;
- Nombre de Objeto;
- Dominio de Objeto;
- Cada regla debe permitir crear exclusiones para, como mínimo:
- Usuarios;
- Dispositivos;
- Cada regla debe permitir la asignación de los siguientes niveles de severidad:
- Información;
- Warning;
- Minor;
- Major;
- Crítico;

2.4 Control de cambios para servers

Se requiere de una solución que realice el control de las aplicaciones, así como la prevención de modificaciones en archivos de los sistemas

La solución permitirá proteger servidores y dispositivos de propósito específico mediante el control de la ejecución de aplicaciones, realizado a través de listas blancas dinámicas, y por medio de la prevención de modificaciones hacia los archivos

La solución debe emplear un modelo dinámico de confianza para bloquear las aplicaciones no autorizada

La solución deberá de entregar una protección completa contra aplicaciones y código no deseado

Se requiere de una solución que refuerce la administración de aplicaciones, incremente la seguridad, y de mayor visibilidad de lo que sucede en diferentes tipos de equipos

La solución debe contar con técnicas que disminuyan la administración de las listas haciéndolo de manera dinámica.

Debe proteger contra las amenazas persistentes avanzadas y de tipo zero-day sin actualizaciones de firmas.

Debe contar con mecanismos de protección de memoria para contrarrestar los ataques de buffer overflow sobre las aplicaciones en lista blanca

La solución debe proveer métodos para agregar aplicaciones como confiables (lista blanca) o no confiables (lista negra)

El producto debe proveer mecanismos para agregar aplicaciones en base a información como el nombre o el checksum

la solución deberá contar con monitoreo en tiempo real de cambios de archivos y registros en los sistemas

La solución deberá tener un repositorio central de las aplicaciones confiables que corren en el sistema.

La solución deberá proteger el sistema contra ataques de malware.

La solución deberá realizar un inventario de archivos que contienen código ejecutable, los cuales deberán ser clasificados por aplicación y por fabricante.

La solución deberá permitir a usuarios específicos que puedan instalar nuevo software en caso de que sea necesario, sin necesidad de autorización adicional.

La solución deberá tener protección contra lectura y escritura de archivos.

La solución debe proveer un único agente que permita la comunicación entre la consola de administración para la actualización de políticas de listas blancas y protección de cambios

Dicho agente puede ser utilizado para otras soluciones de endpoint del mismo fabricante con el objetivo de eliminar la necesidad de múltiples agentes en el sistema

Se deberá contar con herramientas que faciliten el despliegue de la solución, haciendo de este un proceso sencillo y eficiente.

La solución deberá integrar un sistema de gestión centralizado que consolide toda la información producida por el sistema de control de aplicaciones.

Deberá ejecutarse de forma transparente con una configuración inicial impactando de forma mínima los ciclos de CPU

La solución deberá poder extender la visibilidad de lo que sucede en dispositivos legacy como plataformas Windows 2003, Linux Rhel 5, SLES 10, Opensuse 11, etc. y 64 bits

La solución deberá soportar los siguientes sistemas operativos Linux: CentOS, SUSE, OEL, Ubuntu.

La solución deberá soportar Sistemas Operativos tanto de plataformas de 32, como de 64 bits.
La solución deberá reforzar y blindar el sistema contra amenazas o cambios indeseados sin necesidad de escaneo de archivos o actividades periódicas que puedan impactar el rendimiento del sistema.

Debe bloquear aplicaciones no autorizadas o vulnerables

La solución debe apoyar a la organización a cumplir con requerimientos de cumplimiento como PCI DSS

Deberá contar con mecanismos de protección contra lectura y escritura a archivos específicos en los sistemas endpoint para control de los usuarios

Se deberá contar con la capacidad de especificar programas que pueden selectivamente sobrepasar las protecciones de lectura y escritura, así como usuarios tambien

La función de protección de escritura y cambios a los sistemas deberá proteger de:

- *Eliminar
- *Renombrar
- *Modificar Contenidos
- *Truncar
- *Cambiar Propietario

La funcionalidad de control de aplicaciones realizara listas dinámicas blancas para asegurar que solo aplicaciones confiadas se ejecuten en dispositivos de propósito único, servidores

El control de aplicaciones apoyara a la institución a enforzar cumplimiento de licenciamiento al prevenir la ejecución de software no autorizado en los endpoint

Para el control de cambios se deberá contar con la funcionalidad de crear políticas de monitoreo de cambios

Si el sistema detecta que un archivo crítico es modificado se deberá contar con una respuesta automática para el envío de un correo para notificar

La solución deberá permitir realizar políticas de monitoreo de cambios a archivos en base a tamaño de archivos. Las reglas de prevención de ejecución de aplicaciones deberán permitir la ejecución de controles ActiveX con el objetivo de permitir al usuario utilizar páginas interactivas en los exploradores El sistema de administración deberá contar con una integración hacia una red de reputación que permita obtener información de la reputación de los archivos Deberá poder integrarse con sistemas de colección de eventos via syslog Deberá poder integrarse con sistemas de administración de cambios (CMS) Se deberá contar con la capacidad de permitir usuarios autorizados a sobrepasar las reglas de protección mediante la adición de usuarios confiables por medio de detalles de directorio activo Se deberá contar con la opción de utilizar mediante línea de comando cambios de contraseña Se deberá poder personalizar las notificaciones visuales que saltan a los usuarios finales La solución debe proveer un panel de monitoreo para poder visualizar los cambios y violaciones en los endpoint Los tableros deben de poder ser creados, modificados, duplicados y exportados La solución deberá permitir la ejecución de consultas en el sistema de administración para revisar información de los endpoints
2.5 Control de aplicaciones para las computadoras
La solución permitirá proteger estaciones de trabajo mediante el control de la ejecución de aplicaciones, software y código ejecutable, realizado a través de listas blancas dinámicas y por medio de la prevención de modificaciones hacia los archivos de la máquina. La solución debe emplear un modelo dinámico de confianza para bloquear las aplicaciones no autorizadas. La generación de listas blancas dinámicas debe ser un proceso automático sin necesidad de intervención manual. La solución debe tener en cuenta ejecutables, activeX, Java, Pearl Scripts, archivos .bat, archivos VBS, dll y archivos .SYS. Debe proteger contra las amenazas persistentes avanzadas y de tipo zero-day sin actualizaciones de firmas.

Debe contar con mecanismos de protección de memoria para contrarrestar los ataques de buffer overflow sobre las aplicaciones en lista blanca. No debe permitir que las aplicaciones denegadas se ejecuten desde el disco o desde memoria. La solución debe soportar el control mediante: listas blancas, listas negras, inventario y modo híbrido (combinación entre las anteriores). Debe soportar flujos de auto aprobación (usuario final) cuando se presente el bloqueo de una aplicación. La solución debe estar en capacidad de hacer un inventario de todas las aplicaciones incluyendo sus códigos asociados y dll de forma centralizada para su catalogación. La solución debe estar en capacidad de investigar un inventario de aplicaciones y clasificarlas basado en su reputación de manera que se puedan aislar las buenas de las malas. La solución no debe requerir una actualización de políticas para aprobar la ejecución de una aplicación. La solución debe soportar estaciones de trabajo y equipos de propósito específico. La solución debe estar diseñada para funcionar en modo desconectado (offline mode) La solución debe soportar un modo de observación luego de la creación de la lista blanca, donde las aplicaciones, software y código no permitido puedan ser monitoreados sin afectar su ejecución, con el fin de identificar posibles nuevos ítems que sean agregados a la política. Debe estar en la capacidad de integrarse y recibir actualizaciones de reputación de un sistema de inteligencia contra amenazas mediante el uso de protocolo abierto de comunicación diseñado específicamente para esta finalidad, con la capacidad de actualizar todas las máquinas del ambiente en tiempo real, sin necesidad de actualizar políticas o comunicarse con la consola de administración. La autorización de aplicaciones permitidas se debe poder realizar a través de: Checksum, certificados, editor, nombre, adición manual a través de inventario La solución deberá soportar la administración mediante línea de comandos en caso de ser necesario
2.6 Firewall para las computadoras

El módulo debe permitir/bloquear tráfico de red para protocolos no soportados.

Permitir o bloquear tráfico solo hasta que el módulo y servicios de firewall este

arriba.

Habilitar/deshabilitar alertas de intrusión de Firewall

La solución debe poder recopilar log en eventos lanzados directamente sobre el cliente y reportar incidentes en la consola de administración central.

Debe proteger ataques tipo “Generic Buffer Overflow” en aplicaciones de 32bits Debe soportar reglas de protección de acceso para registro, procesos y servicios Debe tener la funcionalidad “Data Execution Prevention”

Debe soportar la funcionalidad “Generic Privilege Escalation Protection”

Cada una de las reglas debe ser aplicable tanto para tráfico entrante como para tráfico saliente del cliente.

Las reglas de tráfico deben ser soportadas para protocolos IP:

- Ipv4
- Ipv6

La solución debe aplicar reglas de tráfico para conexiones:

- Alámbricas
- Inalámbricas
- Virtuales

Las reglas de tráfico deben poder extenderse a ejecutables por medio de la especificación de ruta (se pueden utilizar wildcards).

El módulo debe poder incluir reglas en base a los protocolos y puertos más conocidos del mundo.
Se debe poder administrar redes y ejecutables de confianza desde la interfaz de usuario de los endpoints.
La herramienta debe contar con un mecanismo de conocimiento global de amenazas que permita configurar el bloqueo de conexiones de alto riesgo en base a reputación.

2.7 EDR para los servidores

La solución ofertada debe ser basada en cloud, es decir, todo el procesamiento de datos se debe realizar en la nube.

La solución debe utilizar el mismo agente de comunicación con la consola central usado en la protección para los servidores

La herramienta debe permitir la búsqueda de información en tiempo real de distintos elementos sospechosos dentro de los computadores

La herramienta debe permitir tener un historial de búsqueda para poder realizar búsquedas en estos datos centralizados (independientemente del estado actual, online u offline, de cada server)

La solución debe permitir la creación de procesos de investigación, carga de información y análisis directamente desde la consola de monitoreo.

La solución debe tener la capacidad de monitorear posibles anomalías en tiempo real y reportarlas a la plataforma para que sean analizadas.

La solución debe permitir aplicar mecanismos de contención directamente de la consola y sin la necesidad de contar con herramientas de terceros para estos efectos

La solución debe utilizar distintos mecanismos de análisis los cuales deben incluir el uso de playbooks, información de terceros para detectar posibles incidentes dentro del ecosistema

La solución deberá poder informar qué o cuáles otros dispositivos del ecosistema tienen el mismo comportamiento previamente identificado en un servidor (es decir, poder decir los hostnames que comparten cierto comportamiento) sea o no, anómalo.

La solución debe utilizar The MITRE Attack Framework para el análisis de posibles incidentes dentro de la organización.

En el proceso de análisis de un posible incidente, la herramienta debe permitir asignar distintos estados al proceso de evaluación para determinar la etapa en que se encuentra un incidente.

La solución debe poder realizar Investigación del phishing y correos sospechosos por medio del análisis con una red de inteligencia externa.

La solución debe permitir tomar instantáneas de un equipo particular para poder analizarlas cuando se requiera.

La herramienta debe permitir la creación de colectores para realizar acciones sobre los nodos.

La solución deberá permitir generar una infraestructura colaborativa entre puntos de protección ya sea a nivel perimetral, contenido, virtual o en los equipos de usuario final puedan intercambiar

información sobre nuevas amenazas detectadas en tiempo real mediante un protocolo abierto diseñado para este propósito.

La solución debe permitir comunicarse con la solución de protección del servidor de manera nativa.
La solución debe permitir poner en cuarentena a los hosts comprometidos con el objetivo evitar movimientos laterales de códigos maliciosos. Como también se pueden detonar acciones como:

- parar,
- terminar un proceso
- eliminar o modificar archivos, llaves de registro,
- ejecutar un script en lenguajes como: C+, VB, Python, powershell, CMD)

La plataforma debe integrarse a una red de reputación basado en el análisis de campañas de ataques de forma que pueda evaluar el impacto de en la red y emita las recomendaciones para poder proteger la infraestructura. Debe contener los IOCs para que el EDR pueda consultar por demanda y tomar acción en caso de hallarlos.

La investigación de un incidente debe ser basado en motores de Inteligencia Artificial brindando una investigación guiada ayudando a la documentación e investigación.

La solución debe permitir poner en cuarentena a los hosts comprometidos con el objetivo evitar movimientos laterales de códigos maliciosos.

La solución debe permitir detener y/o eliminar un proceso en ejecución o persistente en las estaciones de trabajo.

La solución ofertada debe permitir la segmentación de políticas para la operación de la plataforma, es decir, la herramienta debe permitir aplicar distintos tipos de políticas para un mismo ecosistema cliente.

La solución debe contar con un panel de visualización de métricas de uso de la plataforma.

La solución debe permitir la creación de distintos roles de usuarios dentro de la consola de gestión para el perfilamiento de usuarios.

La herramienta debe permitir la vinculación de procesos mediante mecanismos de trace.

La solución debe permitir la visualización de información en distintos modelos, desde vistas gráficas de los hallazgos hasta el detalle de la información recolectada.

La herramienta debe permitir la visualización de los hallazgos mediante vistas gráficas. La herramienta debe permitir visualizar eventos históricos, de cada uno de los equipos. La herramienta debe permitir visualizar eventos históricos hasta 30 días. La solución debe poseer integración con una herramienta para la gestión de políticas usada localmente. La solución ofertada debe poder integrarse con diferentes soluciones de correlación. La solución debe ser compatible con plataformas, Windows, Linux Ubuntu, Debian y Fedora y Mac. El análisis de información debe solo ser en metadata y no en archivos o datos personales. La comunicación debe ser cifrada usando el protocolo cifrado TLS 1.2 como mínimo. El almacenamiento debe estar cifrado. Cuando se borre información almacenada en la nube esta no debe ser recuperable. Para esto se necesita un documento oficial del fabricante describiendo este proceso.
2.8 Sandbox para el endpoint
La solución de análisis avanzado de malware del tipo sandboxing que permita probar en ejecución una muestra de código malicioso y generar un veredicto con información detallada. La solución deberá ser un appliance de Propósito Específico o plataforma SaaS para la detección y control de malware avanzado. Deberá ser capaz de obtener muestras de los endpoints (estaciones y servidores) y en base a su resultado, determinar si se permite o no su ejecución. Deberá soportar trabajar en cluster u ofrecer un mecanismo de alta disponibilidad. La “Solución de análisis y prevención de Malware Avanzado” deberá ser ofertada con licenciamiento, garantías, mantenimiento, actualización y soporte técnico del fabricante para todos sus componentes. Deberá entregar información clave para poder detectar sistemas que hayan sido comprometidos con anterioridad al análisis (Indicadores de Compromiso). **Especificaciones Generales**

Deberá contar con la capacidad de recibir emails para análisis sin estar en línea y extraer los archivos adjuntos para poder realizar el análisis. Una vez realizado, deberá enviar el resultado mediante la incorporación con un conector de correo propietario en el protocolo SMTP del servidor de correo.

La solución deberá proporcionar detección y protección en las comunicaciones desde y hacia Internet contra los ataques basados en Web de Malware día cero, polimórfico, “botnets” y Ataques Persistentes Avanzados (APT).

Deberá contar con técnicas de Machine Learning y Deep Neural Network.

La solución deberá brindar un flujo detallado de la ejecución de la amenaza, indicando modificaciones al sistema operativo, creación de archivos, procesos en memoria, conexiones externas, captura de paquetes, etc.; con el objetivo de medir el impacto de la amenaza en el sistema operativo y brindar las medidas necesarias para la remediación.

La solución deberá contar con integración a una consola de administración del endpoint de siguiente generación para las tareas de remediación de Malware Avanzado.

Debe ser capaz de analizar URLs embebidas en páginas HTML.

La solución deberá poder realizar análisis de código estático para garantizar profundidad en el descubrimiento de código latente.

La solución deberá contar con un modo interactivo de análisis para que el usuario administrador pueda interactuar en el proceso del análisis de Malware Avanzado.

La solución deberá brindar información en forma de archivos descargables para visualizar los componentes de código analizado y caminos lógicos de ejecución.

La solución debe tener la capacidad de poder recibir muestras para análisis de Malware de forma manual mediante el ingreso a una consola web, automáticamente desde soluciones de seguridad en red y mediante protocolo SFTP.

Performance

La solución deberá contar con múltiples motores de detección, las cuales deberán encontrarse priorizadas por consumo de recursos, de manera que entregue la posibilidad de analizar en profundidad sólo cuando esto sea requerido, optimizando los recursos necesarios para la detección.

Efectividad

La solución deberá poseer la capacidad de análisis dentro de ambientes virtuales sandbox con los siguientes sistemas operativos los cuales son estándar en la Entidad:

- Microsoft Windows 7 32 y 64 bits
- Microsoft Windows 8 Professional 32 y 64 bits
- Microsoft Windows 8.1 64 bits Enterprise
- Microsoft Windows 10 Enterprise 64 bits Enterprise
- Microsoft Windows Server 2003 32 bits
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2 Standard
- Microsoft Windows Server 2016 Standard
- Microsoft Windows Server 2019 Standard
- Microsoft Windows Server 2022 Standard

Deberá soportar el análisis de Código estático de las muestras.

La solución dentro de sus componentes de análisis podrá consultar información de reputación hacia una red de colaboración global para la identificación de malware avanzado.

La solución deberá tener la capacidad de poder seleccionar automáticamente el sistema operativo que utilizará para analizar de malware avanzado las muestras basándose en el sistema operativo de la víctima.

La solución debe ser capaz de conectar a internet las máquinas virtuales para identificar comunicaciones maliciosas.

La solución deberá contar con capacidad de almacenar listas blancas y listas negras para análisis de malware avanzado.

La solución deberá soportar los siguientes tipos de archivo para análisis:

a. Executables (.exe, .dll, .scr, .ocx, .sys, .com, .cgi, .cpl)
a. MS Office Files (.doc, .docx, .xls, .xlsx. .ppt, .pptx)
b. PDF Files (PDF files, Adobe Flash files (SWF))
c. Compressed Files (.zip, .cab, .7z, .zip, .rar , msi, .lzh, .lzma,)
d. Android Application Package (.apk)
e. Java Archives (JAR), CLASS, Java Script, Java bin files
f. Images (.jpeg, .png, .gif)
g. Other files (.cmd, .bat, .vbs, .xml, .url, .htm, .html, .eml, .msg, .vb, .vba, .vbe, .vbs, .ace, . .arj,.chm, .inf, .ins, .ink, .mof, .ocx, .potm, . potx, .ps1, .reg, .wsc, .wsf, .wsh)

Integración

La solución deberá contar con la capacidad de integrar a la consola de administración de endpoint para obtener información de los hosts administrados.

La solución deberá contar con la capacidad de integrarse a un sistema de administración centralizada de endpoint y reputación interna de la organización, permitiendo la remediación de malware día cero detectado en esta solución en los endpoints de la organización.

La solución deberá contar con una integración a una red de reputación global en la nube para obtener información más certera de las amenazas que puedan estar presentes en archivos y conexiones desde o hacia sitios externos determinados por esta.

La solución deberá contar con una integración al dispositivo de seguridad proxy de red actual de la institución para recibir muestras de archivos para su análisis de malware avanzado y proveer la capacidad de bloqueo.

La solución debe permitir exportar Indicadores de Compromiso a una solución SIEM.

Gestión

La solución deberá permitir la creación de diferentes usuarios administrativos para las tareas de mantenimiento y envío de muestras de malware.

La solución debe poder contar con una consola gráfica donde se pueda visualizar el estado del análisis de las muestras para su posterior revisión.

Deberá ser una solución administrable vía web y cli.

Se debe contar con los siguientes roles de administración: Admin User, Web Access, FTP Access, Log User Activities, y Sample Download Access.

Las tareas de actualización de versiones de sistema operativo podrán ser realizadas por medio de la interfaz gráfica.

Reporteo

La solución debe contar con módulo o tablero de reportes gráficos visible desde su ingreso para conocer el estado actual de amenazas en el sistema.

La solución deberá brindar información de reportes en forma de archivos descargables para visualizar los componentes de código analizado y caminos lógicos de ejecución.
La solución deberá contar con reportes avanzados donde muestre:

- Nivel de severidad de la muestra analizada
- Características del malware como: Persistencia, supervivencia a eliminación, conexiones a red, capacidades de replicación, etc.
- Modificaciones a registros de Windows
- Imagen de pantallas de interacción que pueda haber requerido el malware dentro del Sistema

- Operaciones de red
- Archivos DLL de tiempo de ejecución
- Operaciones de Archivo
- Familia a la que pertenece el malware detectado
- La solución debe poder brindar resultados de los análisis de forma gráfica que contengan:
- Resumen de Análisis en formato HTML y PDF
- Archivos Depositados
- Resultados de des-ensamblaje
- Gráfico de ruta lógica
- Registros de ejecución dinámica
- Resultados completos

La solución entregará una valoración de la amenaza, basada en el resultado de distintos motores de análisis, ponderando en este indicador el potencial compromiso del malware en cuestión.

La solución deberá contar con paneles de monitores para poder visualizar diferentes estados de la misma, entre ellos:

- Archivos analizados por tipo de archivo
- Ranking de malware por nombre de archivo
- Uso de perfil de análisis
- Información del sistema

2.09 Parchado

Deberá ser capaz de parchar ambientes tanto windows como Linux.

Deberá de tener la capacidad de enviar parches hacia desktop, laptops y servidores.

Deberá de poder ver el software instalado en el equipo y los parches que ya tiene instalados.

Deberá tener escalabilidad empresarial: entrega de parches a organizaciones grandes, medianas y pequeñas.

Monitoreo y mantenimiento de cumplimiento de parches en toda la empresa.

Deberá de poder aplicar los parches de acuerdo con los plazos de seguridad.

Deberá de cumplir con las regulaciones y políticas corporativas y gubernamentales. Deberá de ser 100% preciso ayudándole a pasar auditorías de seguridad.

Deberá de escanear e informar todas las aplicaciones de software en su red.
Deberá contar con la opción para aprobar actualizaciones de software automáticamente cuando los parches estén disponibles.
Deberá de tener la capacidad para programar parches para toda la empresa, grupos, individuos o máquinas del sitio.

Deberá de poder permitir que el administrador controle la programación de escaneo y distribución de parches para minimizar las interrupciones del usuario final.

Deberá de poder generar informes detallados sobre qué parches están disponibles, el estado actual de los parches y qué equipos tienen qué parches y cuáles no.

Deberá de tener la habilidad de automatizar para obtener la máxima eficiencia, ahorrando tiempo de administración, esfuerzo y reduciendo costos.

Deberá de poder desplegar parches de Microsoft y de terceros (Adobe, Java, Firefox, etc.) y personalizados para aplicaciones de software.

Deberá de contar con la opción de que el administrador puede optar por forzar las instalaciones o permitir que el usuario retrase las instalaciones.

Deberá tener la posibilidad de desinstalar parches.

Deberá de contar con las siguientes opciones de repositorio de parches:

- Repositorio de parches remotos usando relés de parches y servidores proxy de parches
- Sincronización de contenido del repositorio remoto programado
- Repositorio distribuido de parches que aprovecha Windows DFS
- Posibilidad de configurar Windows IIS como almacén de repositorio

Deberá de poder mostrar un estatus del parcheo en cada equipo desktop, laptop o servidor.

Deberá incluir capacidades de soporte remoto a dispositivos de manera no intrusiva, permitiendo la resolución de problemas sin interrumpir al usuario.

Deberá permitir el acceso remoto a escritorios de usuarios con opción de control compartido o completo.

La herramienta deberá ofrecer acceso remoto basado en navegador a sistemas Windows y macOS, sin necesidad de instalar un agente adicional.

La herramienta deberá ser compatible con múltiples sesiones de Escritorio Virtual y Servidores de Escritorio Remoto para una administración IT eficiente y segura.

La herramienta deberá garantizar comunicaciones seguras mediante autenticación de dos factores y cifrado para las conexiones con el servidor.

La herramienta deberá ser capaz de realizar transferencias de archivos, gestión de tareas, edición de registros, acceso al registro de eventos y ejecución de comandos en dispositivos remotos.

Deberá permitir la gestión y reparación de dispositivos incluso cuando estén apagados, utilizando herramientas y diagnósticos avanzados.

Deberá contar con capacidad para automatizar el despliegue de actualizaciones y parches en los sistemas operativos y software instalados.

Deberá incluir funciones de despliegue centralizado de software y actualizaciones en múltiples dispositivos desde una consola única.

Deberá contar con monitoreo en tiempo real de dispositivos, incluyendo métricas como uso de CPU, memoria, discos duros, estado de impresoras, entre otros.

Deberá permitir la creación y ejecución de scripts personalizados, así como la descarga y modificación de scripts preexistentes desde un repositorio (ComStore).

Deberá ofrecer una solución 100% basada en la nube, sin requerir infraestructura adicional, accesible desde cualquier ubicación y dispositivo mediante un navegador compatible.

Deberá incluir un panel de control personalizable con información de dispositivos como tipo, estado del antivirus, actualizaciones de sistema operativo y alertas.

Deberá soportar capacidades de soporte remoto para plataformas Windows, macOS y Linux, y ser compatible con navegadores como Google Chrome, Mozilla Firefox, Microsoft Edge, Vivaldi, Brave y Safari.

3. INTEGRACIÓN DE INTELIGENCIA DE PREVENCIÓN DE INTRUSOS DE RED

Detección y Prevención en Tiempo Real
Debe contar con análisis continuo de logs y eventos para identificar patrones de ataque como fuerza bruta, escaneo de puertos e inyecciones SQL.

Debe bloquear automáticamente direcciones IP maliciosas en tiempo real, integrando con firewalls, WAFs y balanceadores de carga.

Debe utilizar detección basada en comportamiento, no solo firmas, para identificar amenazas desconocidas (zero-day).

Mecanismos de Respuesta Avanzada
Debe ejecutar acciones contextuales según el tipo de amenaza, incluyendo:

Aislamiento de servidores comprometidos.

Notificaciones a SIEM/SOAR mediante Syslog, Webhooks o API REST.

Modificación dinámica de reglas en WAFs (ej: OWASP CRS).

Debe incluir "bouncers" distribuidos para aplicar políticas en:

Firewalls (iptables, nftables, Cloudflare).

Proxys inversos (NGINX, Traefik, Envoy).

Entornos de contenedores/Kubernetes (kube-proxy, Cilium).

Bases de datos (bloqueo de consultas maliciosas).

Análisis de Patrones e Inteligencia Colectiva
Debe soportar reglas personalizables en YAML para protocolos sensibles (SSH, RDP, HTTP/HTTPS) y ataques de capa 7 (scraping, API abuse).
Debe integrarse con una red global de inteligencia para compartir y recibir:

IPs maliciosas (botnets, scanners, APTs).

Indicadores de compromiso (IOCs) asociados a campañas activas.

Debe implementar un sistema de reputación en tiempo real con puntuación dinámica de amenazas.

Protección contra Amenazas Avanzadas (APT)
Debe detectar técnicas evasivas como:

Enumeración lenta de usuarios (low-and-slow).

Movimiento lateral en redes (escalada de privilegios).

Tráfico cifrado malicioso (evasión de inspección SSL).

Debe integrarse con feeds de inteligencia externos (MISP, AlienVault OTX, Anomali).

Debe incluir reglas basadas en MITRE ATT&CK para tácticas APT.

Resiliencia ante Ataques Persistentes
Debe almacenar logs hasta por 12 meses para análisis forense retrospectivo.

Debe permitir la detección de bots dormidos que activan acciones tras largos períodos.

Debe ofrecer políticas de retención ajustables con exportación a SIEM/data lakes.

Perfiles de Ataque para Servicios Críticos
Debe incluir templates predefinidos para:

Servidores web (OWASP Top 10, DDoS).

Bases de datos (SQL injection, brute force).

APIs REST/GraphQL (abuso de endpoints).

Debe priorizar la monitorización de portales financieros y sistemas de autenticación.

Escalabilidad y Despliegue
Debe soportar entornos on-premise, cloud (AWS/Azure/GCP) e híbridos.

Debe utilizar agentes ligeros (<1% CPU) compatibles con:

Linux (Debian, RHEL, Ubuntu).

Windows (via integración con Wazuh/Osquery).

Contenedores (Docker, Kubernetes).

Personalización y Automatización
Debe permitir reglas adaptables en YAML, con:

- Umbrales dinámicos (ej: bloquear IP tras 3 intentos fallidos de SSH en 5 minutos).

- Whitelists granulares (IPs/ASNs).

Debe ofrecer APIs RESTful para integración con Ansible, Terraform, Splunk y Elastic

5. CORRELACIONADOR DE EVENTOS SIEM/XDR
5.1 Correlacionador de eventos
Arquitectura Debe ser una solución ofrecida en esquema de Software as a Service (SaaS), cuya consola y repositorio de información se encuentren en una nube pública o privada provista por el fabricante, y con opción de instalar componentes on-premise.. Los componentes on-premise deben ser complementarios a la solución SaaS y en ningún caso serán un reemplazo de la consola y repositorio en nube. Todos los componentes on-premise deben ser del mismo fabricante y deben conectarse de forma segura con la consola y repositorio de nube. Las fuentes enviarán información a un componente instalado en la red del municipio. Para fuentes on-premise, en ningún caso se permitirá que las fuentes envíen información directamente a la consola o repositorio en nube del fabricante. Para fuentes de eventos en nube, se deberá brindar la posibilidad de envío de eventos de nube a nube o a través del componente on-premise. La solución debe proveer capacidad de instalar tantos componentes que recibirán la información de las fuentes como considere necesario, sin que aumentar la cantidad de dispositivos de este tipo implique costo adicional de licenciamiento para la Convocante. La información enviada por todos los componentes on-premise hacia la nube será transmitida cifrada para garantizar la confidencialidad de esta. Debe contar con una consola basada en Web, que permita el acceso simultáneo de un número ilimitado de usuarios sin que haya degradación en su operación, y sin que agregar más usuarios administradores a la consola Web implique costo adicional de licenciamiento para la Convocante. La consola Web debe contar con opción de arquitectura multi-tenant. El repositorio de información en nube debe brindar retención de información durante al menos los últimos 3 meses. Debe proveer al menos una alternativa para brindar a la Convocante la posibilidad de contar con periodos de retención más largos. La solución debe proveer capacidad de agregar todas las fuentes que enviarán eventos a la solución propuesta sin que implique pago de licenciamiento extra por fuente. Los eventos generados en fuentes on-premise y de otros servicios de nube en esquema SaaS, deberán ser almacenados en el mismo repositorio de nube del fabricante.

Funcionalidades generales de administración

La consola Web debe permitir realizar búsquedas de eventos con las siguientes opciones:

- Búsqueda por rango de tiempo
- Búsqueda por tipo de fuente que envía información
- Búsqueda por query (usando sintaxis)

Debe brindar la posibilidad de hacer queries incluso sin conocimiento de la sintaxis, para que los administradores se vayan familiarizando con el uso de queries con sintaxis.
Debe permitir a los administradores guardar los queries que deseen reutilizar.
Debe permitir construir queries directamente desde la visualización de los eventos, de forma visual e intuitiva.

Debe de contar con paneles de información predefinidos y personalizables, de manera que los analistas obtengan un vistazo rápido del estado de la solución y los eventos recopilados.

Debe incluir un panel de información que muestre la tendencia de tiempo en el manejo de las alertas reportadas por la solución, para permitir a la Convocante determinar si se están atendiendo de manera más o menos efectiva.

Los paneles de información deberán servir de base para la creación de reportes

personalizables. Los reportes deberán poder exportarse al menos en los siguientes formatos:

- HTML
- PDF
- CSV

Debe permitir definir la zona horaria por cada fuente de eventos.

Debe permitir establecer la zona horaria del perfil de los usuarios de la

solución. Debe tener varios niveles de acceso basado en roles, considerando

al menos:

- Administrador (acceso completo),
- Investigador (acceso sólo de incidente) o
- Sólo lectura.

Debe permitir etiquetar equipos de alta importancia para darles un tratamiento diferente al resto de los equipos monitoreados.

Debe permitir definir políticas de detección basadas en redes específicas.

Debe mostrar el listado de agentes instalados y el estatus que reportan a consola.

Debe incluir la posibilidad de recibir alertas en caso de que alguna fuente que envía información a la solución deje de enviar datos por un periodo de tiempo configurable por el administrador.

Debe brindar acceso a la documentación del fabricante directamente en los apartados en que los administradores podrían requerir información acerca de cómo realizar una configuración en particular.

Debe de contar con API que permita a la Convocante realizar tareas adicionales a las provistas por el fabricante de forma nativa en la consola.

El fabricante debe proporcionar información relacionada al uso de la API.

Fuentes que enviarán información a la solución

La solución debe incluir al menos 100 integraciones preconfiguradas para agregar fuentes de terceros (líderes en el ámbito de Seguridad Informática) que le enviarán información.

Para garantizar la continuidad de la operación y flexibilidad que el municipio necesita para mantener una base instalada de herramientas de seguridad actualizada, la herramienta debe incluir la
capacidad de agregar al menos las siguientes fuentes que le enviarán información dentro de las integraciones preconfiguradas,:

- Directorio Activo:
  - On-premise.
  - En Azure (Entra ID).
- Consolas de Antivirus/Antimalware/EDR:
  - Crowdstrike
  - Cylance
  - Kaspersky
  - McAfee
  - Palo Alto
  - SentinelOne
  - Sophos
  - Symantec
  - Trend Micro
- Firewall:
  - Barracuda

    - Check Point
    - Cisco
    - Forcepoint
    - Fortinet
    - Juniper
    - McAfee
    - Palo Alto
    - SonicWall
- IDS:
    - Cisco
    - F5
    - McAfee
    - Snort
    - Trend Micro
- Servicios de nube (SaaS):
    - AWS
    - Box
    - Google
    - Microsoft
    - Salesforce
    - Zoom

- Servidores de DHCP:
    - Cisco
    - Infoblox
    - Microsoft

- Servidores de DNS:
    - Cisco
    - Infoblox
    - Microsoft

- Servidores Proxy:
    - Cisco
    - McAfee
    - Websense

- Zscaler
- Servidores VPN:
  - Barracuda
  - Cisco
  - F5
  - Microsoft
- Servicios adicionales:
  - CyberArk
  - Darktrace

Debe incluir además la capacidad de agregar fuentes de terceros de manera personalizada (es decir, aunque no esté incluida en las integraciones preconfiguradas).

La recopilación de información proveniente de las fuentes debe poder realizarse en al menos las siguientes opciones:

- Utilización de puerto para recepción tipo Syslog
- Monitoreo de archivo en la fuente
- Monitoreo de carpeta en la fuente

La solución debe contar con un almacén de contraseñas que se utilizan para conectar a las diferentes fuentes que envían información a la solución y pueden ser reutilizadas en diferentes fuentes si así es requerido.

Debe contar con un mecanismo que permita a los administradores observar rápidamente si hay algún problema con la recolección de información en una o más fuentes.

La información recopilada de las fuentes deberá ser procesada por la solución y presentada en formato JSON dentro de la misma.

Debe de contar con un módulo de análisis de tráfico de red, que se integrará en la red de la Convocante sin que implique interrupción en el flujo de datos en la red, sin que haya limitante en cuanto al número de dispositivos que realizarán el análisis del tráfico de red, y sin que aumentar la cantidad de dispositivos de este tipo implique costo adicional de licenciamiento para la Convocante.

No se aceptará que este módulo sea de otra marca o fabricante, ni que sea un appliance físico.

Los dispositivos que analizan el tráfico de red deberán conectarse a la consola en nube y la información recopilada deberá integrarse en el mismo repositorio de información en nube

6. Administración de cuentas con altos privilegios y gestión de cuentas de servicio

Arquitectura e Implementación

Debe tener una arquitectura on-premise, compatible con sistemas Windows Server 2016 o superiores.

Debe ofrecer opción de despliegue en la nube (SaaS) sin requerir infraestructura local adicional.

Debe soportar escalamiento horizontal para entornos con más de 10,000 usuarios sin degradación de rendimiento.

Debe permitir la instalación en entornos virtualizados (VMware, Hyper-V, Azure VM, AWS EC2).

Integración con Directorio Activo

Debe tener integración nativa con Active Directory (LDAP/LDAPS) para recopilar eventos en tiempo real.

Debe soportar Azure AD (Entra ID) para entornos híbridos.

Debe monitorear cambios en GPOs, incluyendo creación, modificación y eliminación.

Debe auditar modificaciones en atributos críticos (ej: adminCount, userAccountControl).

Monitoreo y Detección de Amenazas

Debe registrar todos los inicios de sesión (éxito/fallo) en equipos y servidores.

Debe detectar movimientos laterales, como accesos sospechosos entre estaciones de trabajo.

Debe alertar sobre intentos de fuerza bruta en cuentas privilegiadas.

Debe rastrear cambios en membresías de grupos (ej: Domain Admins, Enterprise Admins).

Debe identificar actividades anómalas de PowerShell (ej: ejecución de scripts no autorizados).

Auditoría de Contraseñas

Debe analizar contraseñas en Active Directory para detectar:

Contraseñas débiles o comunes (ej: "Password123").

Reutilización de contraseñas en múltiples cuentas.

Contraseñas que no cumplen con políticas de complejidad.

Debe generar reportes de riesgo con niveles de criticidad (bajo, medio, alto).

Debe permitir la exportación de resultados en formatos CSV, PDF y HTML.

Cumplimiento y Reportes Debe incluir plantillas preconfiguradas para normativas: PCI DSS (accesos a datos sensibles). ISO 27001 (gestión de accesos). NIST (fortaleza de contraseñas). Debe permitir la programación de reportes automatizados (diarios, semanales, mensuales). Debe ofrecer dashboards personalizables con métricas clave (ej: intentos de acceso fallidos, cambios críticos). **Alertas y Respuesta** Debe enviar notificaciones en tiempo real (email, Syslog, Webhooks). Debe permitir acciones automatizadas, como bloquear usuarios tras múltiples intentos fallidos. Debe integrarse con SIEM/SOAR (Splunk, IBM QRadar, Microsoft Sentinel). **Usabilidad y Gestión** Debe contar con una consola web intuitiva con búsquedas avanzadas (filtros por fecha, usuario, tipo de evento). Debe soportar multi-usuario con roles definidos (Administrador, Auditor, Solo Lectura). Debe incluir documentación técnica detallada y soporte para API (RESTful). Debe funcionar sin agentes en los endpoints (solo conexión a controladores de dominio). Debe soportar retención de logs por 12+ meses (con opción a extensión). Debe ser compatible con Windows Server 2008 R2+ y Windows 10/11.
7. FIREWALLS Y VPNs
7.1 Firewalls y VPN sitio principal
Capacidades de Rendimiento y Hardware Throughput de NGFW: mínimo de 14 Gbps. Throughput con Threat Prevention activo: mínimo de 7.5 Gbps.

Throughput con sandbox activo: mínimo de 1.8 Gbps.

Conexiones concurrentes: al menos 1.4 millones.

Sesiones por segundo: soportar 145,000.

Interfaces físicas:

Al menos 12 interfaces en cobre 1G/10G-T.

Al menos 10 interfaces SFP/SFP+ (1G/10G).

1 interfaz dedicada para la sincronización del clúster (HA).

1 interfaz dedicada para la administración fuera de banda.

El equipo deberá permitir alta disponibilidad (HA) en modo activo-activo o activo-pasivo y contar con mecanismos de balance de enlaces WAN si se requiere. Asimismo, deberá garantizar cifrados robustos (3DES, AES-256) en VPN IPsec y soportar protocolos y algoritmos modernos (IKEv2, Diffie-Hellman grupos 14, 19, 20, Perfect Forward Secrecy, AES-GCM, etc.).

Funcionalidades Generales del Firewall

Filtrado de Puertos y Control de Aplicaciones

- Permitir la creación de reglas de seguridad basadas en direcciones IP, usuarios, grupos, horarios, protocolos y aplicaciones.
- Identificar aplicaciones independientemente del puerto o protocolo, sin necesidad de abrir puertos específicos.

Integración de Identidad (Active Directory, RADIUS, LDAP)

- Adquirir la identidad del usuario mediante consultas a Microsoft Active Directory (eventos de seguridad) o navegadores (portal cautivo).
- Soportar autenticación Kerberos transparente para inicio de sesión único (SSO), uso de grupos anidados en LDAP y la integración con RADIUS para granularidad de políticas basadas en usuarios o grupos.

0. Módulo VPN (IPsec, SSL VPN)

- Soportar VPN de sitio a sitio (full mesh, estrella, hub-and-spoke) y VPN de acceso remoto (SSL VPN) para al menos 500 usuarios concurrentes.

- Integración con Active Directory y RADIUS para autenticar usuarios, con la opción de asignar permisos basados en grupos.
- Permitir redirigir todo el tráfico de los usuarios remotos a través del túnel, o dividir el tráfico si así se requiere.

Alta Disponibilidad y Balanceo de Enlaces

- Permitir la configuración en HA (activo-activo o activo-pasivo) con sincronización de estado para conmutar sin interrumpir las conexiones.
- Manejar múltiples enlaces WAN, realizando balanceo y failover de manera transparente.

IPS (Sistema de Prevención de Intrusos)

Integración con el Firewall

- El IPS debe estar embebido en la plataforma Fortinet, evitando la necesidad de un equipo externo.
- Permitir la habilitación de perfiles de protección en modo “detectar” o “prevenir” para distintos segmentos o políticas de firewall.

Mecanismos de Detección y Respuesta

- Soporta firmas de explotación, detección de anomalías de protocolo y comportamiento, con la posibilidad de crear reglas personalizadas.
- Actualizaciones automáticas de las firmas de IPS, con capacidad de “fail open” configurable ante sobrecarga de CPU o memoria.
- Opciones para definir excepciones de inspección según fuente, destino o servicio, y perfiles predefinidos de protección (cliente, servidor, mixto).

0. Cobertura de Amenazas

- Detectar y bloquear ataques a nivel de red y capa de aplicación, protegiendo servicios de correo (SMTP, IMAP, POP), DNS, FTP, SSH, Telnet, HTTP(S), Windows (SMB) y protocolos VoIP.
- Incluir protecciones SCADA, detección de túneles DNS, C&C (Command and Control), envenenamiento de caché DNS y ataques genéricos sin firmas predefinidas.

Integración con Firmas Externas y Correlación

- Poder convertir o importar reglas SNORT.

- Integrarse con la consola de administración centralizada y con un SIEM para correlación de eventos.

Control y Filtrado de URLs / Application Control

Base de Datos de Filtrado Web

- Más de 200 millones de URL categorizadas, con actualizaciones constantes en la nube.
- Posibilidad de crear reglas de filtrado que combinen múltiples categorías, y de sobrescribir la categoría asignada por el fabricante (excepciones).
- Bloqueo y/o limitación de ancho de banda para aplicaciones P2P, streaming o redes sociales, según la necesidad.

0. Políticas Basadas en Usuarios y Grupos

- Integración con AD, LDAP o RADIUS para aplicar políticas según la identidad del usuario, horario y ubicación.
- Capacidad de definir excepciones de red, listas blancas y negras para URL específicas, y un modo de “continuar” (bypass) con notificación al usuario.

Reportes y Alertas

- Generación de estadísticas de uso, bloqueos, actividad por categoría o aplicación, y envío de reportes automáticos.
- Interfaz gráfica intuitiva para navegar entre políticas, con posibilidad de buscar y filtrar reglas por usuario, aplicación, IP, etc.

Anti-Bot y Anti-Virus (Malware Inspection)

Análisis de Tráfico

- Motor de reputación de direcciones IP, URL y DNS, detectando patrones de botnets o actividad maliciosa.
- Detección y bloqueo de archivos infectados (incluyendo ransomware y variantes de cryptors) en tránsito HTTP/HTTPS, con capacidad de inspeccionar archivos archivados.

0. Protección contra Phishing y Spear Phishing

- Bloqueo de sitios web maliciosos basados en reputación y heurística, inspección de enlaces dentro de correos electrónicos cuando se habilita la inspección SSL y las reglas de escaneo adecuadas.
- Mecanismos de detección de DGA (Domain Generation Algorithm) y exfiltración a servidores C&C.

Integración con Servicios en la Nube

- Actualizaciones de reputación y firmas en tiempo real desde la nube de Fortinet, garantizando protección inmediata contra amenazas emergentes.
- Opción de análisis y bloqueo de tráfico cifrado (SSL) con la importación del certificado raíz y la configuración de políticas granuladas de inspección.

Sandbox

Detección Avanzada de Día Cero

- Integración con FortiSandbox (local o en la nube), enviando archivos sospechosos para emulación antes de su entrega.
- Bloqueo proactivo del primer ejemplar de malware (evitando paciente cero), compartiendo inteligencia con el motor de antimalware en tiempo real.

0. Arquitectura Multicapa

- Filtrado estático inicial (por reputación, heurística) y emulación dinámica en un entorno Windows con distintas versiones de sistema operativo y suites de Office.
- Capacidad de preconfigurar cuánto tiempo dedicar a la descompresión de archivos anidados, previniendo ataques de denegación de servicio.

Modo de Implementación

- Soporte para modo bridge (L2) sin alterar la topología, así como TAP/monitoring, o integrado con la pasarela de correo.
- Integración con la consola central y con API REST para que aplicaciones internas soliciten análisis bajo demanda.

Inspección SSL (Inbound / Outbound)

Alto Rendimiento con Cifrado Avanzado

- Soporte para Perfect Forward Secrecy (PFS, ECDHE Cipher Suites), AES-NI y AES-GCM, optimizando la inspección de tráfico cifrado sin degradar significativamente el rendimiento.
- Configuración granular de políticas de inspección SSL, permitiendo exenciones por categoría de URL o dominio.

Compatibilidad con Protocolos Modernos

- Manejo de TLS 1.3, con la posibilidad de configurar suites de cifrado según las políticas de la organización.
- Desactivación selectiva de la inspección en servicios o dominios críticos que no deben ser descifrados por razones de privacidad o cumplimiento normativo.

Funciones de Alta Disponibilidad y Gestión Centralizada

Consola Unificada de Administración

- Interfaz gráfica intuitiva para gestionar políticas de firewall, IPS, antivirus, URL filtering y sandbox, con búsqueda y filtrado de reglas.
- Soporte de alta disponibilidad para la consola, en modo activo-pasivo, con sincronización automática de la configuración y de los objetos de seguridad.

0. Políticas Programables y Programación de Caducidad

- Permitir que ciertas reglas de seguridad entren en vigor o caduquen en una fecha/hora específica.
- Generación de estadísticas sobre el número de hits de cada regla, facilitando el refinamiento de la política.

VPN IPsec y SSL

- Creación de comunidades VPN (full mesh, hub-and-spoke, etc.) con arrastrar y soltar, soporte de IPs dinámicas y topologías complejas.
- Integración con la consola para definir la aplicación de reglas de seguridad en el tráfico VPN, permitiendo un control granular.

7.2 Firewalls y VPNs sitio alterno

Capacidades de Rendimiento y Hardware

Throughput de NGFW: mínimo de 14 Gbps.

Throughput con Threat Prevention activo: mínimo de 7.5 Gbps.

Throughput con sandbox activo: mínimo de 1.8 Gbps.

Conexiones concurrentes: al menos 1.4 millones.

Sesiones por segundo: soportar 145,000.

Interfaces físicas:

Al menos 12 interfaces en cobre 1G/10G-T.

Al menos 10 interfaces SFP/SFP+ (1G/10G).

1 interfaz dedicada para la sincronización del clúster (HA).

1 interfaz dedicada para la administración fuera de banda.

El equipo deberá permitir alta disponibilidad (HA) en modo activo-activo o activo-pasivo y contar con mecanismos de balance de enlaces WAN si se requiere. Asimismo, deberá garantizar cifrados robustos (3DES, AES-256) en VPN IPsec y soportar protocolos y algoritmos modernos (IKEv2, Diffie-Hellman grupos 14, 19, 20, Perfect Forward Secrecy, AES-GCM, etc.).

Funcionalidades Generales del Firewall

Filtrado de Puertos y Control de Aplicaciones

- Permitir la creación de reglas de seguridad basadas en direcciones IP, usuarios, grupos, horarios, protocolos y aplicaciones.
- Identificar aplicaciones independientemente del puerto o protocolo, sin necesidad de abrir puertos específicos.

0. Integración de Identidad (Active Directory, RADIUS, LDAP)

- Adquirir la identidad del usuario mediante consultas a Microsoft Active Directory (eventos de seguridad) o navegadores (portal cautivo).
- Soportar autenticación Kerberos transparente para inicio de sesión único (SSO), uso de grupos anidados en LDAP y la integración con RADIUS para granularidad de políticas basadas en usuarios o grupos.

Módulo VPN (IPsec, SSL VPN)

- Soportar VPN de sitio a sitio (full mesh, estrella, hub-and-spoke) y VPN de acceso remoto (SSL VPN) para al menos 500 usuarios concurrentes.

- Integración con Active Directory y RADIUS para autenticar usuarios, con la opción de asignar permisos basados en grupos.
- Permitir redirigir todo el tráfico de los usuarios remotos a través del túnel, o dividir el tráfico si así se requiere.

0. Alta Disponibilidad y Balanceo de Enlaces

- Permitir la configuración en HA (activo-activo o activo-pasivo) con sincronización de estado para conmutar sin interrumpir las conexiones.
- Manejar múltiples enlaces WAN, realizando balanceo y failover de manera transparente.

IPS (Sistema de Prevención de Intrusos)

Integración con el Firewall

- El IPS debe estar embebido en la plataforma Fortinet, evitando la necesidad de un equipo externo.
- Permitir la habilitación de perfiles de protección en modo “detectar” o “prevenir” para distintos segmentos o políticas de firewall.

0. Mecanismos de Detección y Respuesta

- Soportar firmas de explotación, detección de anomalías de protocolo y comportamiento, con la posibilidad de crear reglas personalizadas.
- Actualizaciones automáticas de las firmas de IPS, con capacidad de “fail open” configurable ante sobrecarga de CPU o memoria.
- Opciones para definir excepciones de inspección según fuente, destino o servicio, y perfiles predefinidos de protección (cliente, servidor, mixto).

Cobertura de Amenazas

- Detectar y bloquear ataques a nivel de red y capa de aplicación, protegiendo servicios de correo (SMTP, IMAP, POP), DNS, FTP, SSH, Telnet, HTTP(S), Windows (SMB) y protocolos VoIP.
- Incluir protecciones SCADA, detección de túneles DNS, C&C (Command and Control), envenenamiento de caché DNS y ataques genéricos sin firmas predefinidas.

Integración con Firmas Externas y Correlación

- Poder convertir o importar reglas SNORT.

- Integrarse con la consola de administración centralizada y con un SIEM para correlación de eventos.

Control y Filtrado de URLs / Application Control

Base de Datos de Filtrado Web

- Más de 200 millones de URL categorizadas, con actualizaciones constantes en la nube.
- Posibilidad de crear reglas de filtrado que combinen múltiples categorías, y de sobrescribir la categoría asignada por el fabricante (excepciones).
- Bloqueo y/o limitación de ancho de banda para aplicaciones P2P, streaming o redes sociales, según la necesidad.

0. Políticas Basadas en Usuarios y Grupos

- Integración con AD, LDAP o RADIUS para aplicar políticas según la identidad del usuario, horario y ubicación.
- Capacidad de definir excepciones de red, listas blancas y negras para URL específicas, y un modo de “continuar” (bypass) con notificación al usuario.

Reportes y Alertas

- Generación de estadísticas de uso, bloqueos, actividad por categoría o aplicación, y envío de reportes automáticos.
- Interfaz gráfica intuitiva para navegar entre políticas, con posibilidad de buscar y filtrar reglas por usuario, aplicación, IP, etc.

Anti-Bot y Anti-Virus (Malware Inspection)

Análisis de Tráfico

- Motor de reputación de direcciones IP, URL y DNS, detectando patrones de botnets o actividad maliciosa.
- Detección y bloqueo de archivos infectados (incluyendo ransomware y variantes de cryptors) en tránsito HTTP/HTTPS, con capacidad de inspeccionar archivos archivados.

Protección contra Phishing y Spear Phishing

- Bloqueo de sitios web maliciosos basados en reputación y heurística, inspección de enlaces dentro de correos electrónicos cuando se habilita la inspección SSL y las reglas de escaneo adecuadas.
- Mecanismos de detección de DGA (Domain Generation Algorithm) y exfiltración a servidores C&C.

Integración con Servicios en la Nube

- Actualizaciones de reputación y firmas en tiempo real desde la nube de Fortinet, garantizando protección inmediata contra amenazas emergentes.
- Opción de análisis y bloqueo de tráfico cifrado (SSL) con la importación del certificado raíz y la configuración de políticas granuladas de inspección.

Sandbox

Detección Avanzada de Día Cero

- Integración con FortiSandbox (local o en la nube), enviando archivos sospechosos para emulación antes de su entrega.
- Bloqueo proactivo del primer ejemplar de malware (evitando paciente cero), compartiendo inteligencia con el motor de antimalware en tiempo real.

Arquitectura Multicapa

- Filtrado estático inicial (por reputación, heurística) y emulación dinámica en un entorno Windows con distintas versiones de sistema operativo y suites de Office.
- Capacidad de preconfigurar cuánto tiempo dedicar a la descompresión de archivos anidados, previniendo ataques de denegación de servicio.

Modo de Implementación

- Soporte para modo bridge (L2) sin alterar la topología, así como TAP/monitoring, o integrado con la pasarela de correo.
- Integración con la consola central y con API REST para que aplicaciones internas soliciten análisis bajo demanda.

Inspección SSL (Inbound / Outbound)

Alto Rendimiento con Cifrado Avanzado

- Soporte para Perfect Forward Secrecy (PFS, ECDHE Cipher Suites), AES-NI y AES-GCM, optimizando la inspección de tráfico cifrado sin degradar significativamente el rendimiento.
- Configuración granular de políticas de inspección SSL, permitiendo exenciones por categoría de URL o dominio.

Compatibilidad con Protocolos Modernos

- Manejo de TLS 1.3, con la posibilidad de configurar suites de cifrado según las políticas de la organización.
- Desactivación selectiva de la inspección en servicios o dominios críticos que no deben ser descifrados por razones de privacidad o cumplimiento normativo.

Funciones de Alta Disponibilidad y Gestión Centralizada

Consola Unificada de Administración

- Interfaz gráfica intuitiva para gestionar políticas de firewall, IPS, antivirus, URL filtering y sandbox, con búsqueda y filtrado de reglas.
- Soporte de alta disponibilidad para la consola, en modo activo-pasivo, con sincronización automática de la configuración y de los objetos de seguridad.

Políticas Programables y Programación de Caducidad

- Permitir que ciertas reglas de seguridad entren en vigor o caduquen en una fecha/hora específica.
- Generación de estadísticas sobre el número de hits de cada regla, facilitando el refinamiento de la política.

VPN IPsec y SSL

- Creación de comunidades VPN (full mesh, hub-and-spoke, etc.) con arrastrar y soltar, soporte de IPs dinámicas y topologías complejas.
- Integración con la consola para definir la aplicación de reglas de seguridad en el tráfico VPN, permitiendo un control granular.

7.3 Consola de administración de firewalls

La solución debe incluir una opción de búsqueda para poder consultar fácilmente qué objeto de red contiene una dirección IP específica o parte de ella.

La solución debe incluir la opción de segmentar la base de reglas usando etiquetas o títulos de secciones para organizar mejor la política.

La solución debe proporcionar la opción de guardar toda la política o parte específica de la política.

La solución debe tener un mecanismo de verificación de la política de seguridad antes de la instalación de la política.

La solución debe tener un mecanismo de control de revisión de la política de seguridad.

La solución debe proporcionar la opción de agregar alta disponibilidad de administración, utilizando un servidor de administración en espera que se sincroniza automáticamente con el activo, sin la necesidad de un dispositivo de almacenamiento externo.

La solución debe incluir la capacidad de distribuir de forma centralizada y aplicar nuevas versiones de software de los firewalls.

La solución debe incluir una herramienta para administrar centralmente las licencias de todas las puertas de enlace controladas por la estación de administración.

La solución debe tener las capacidades para la administración multi-dominio y respaldar el concepto de política de seguridad global en todos los dominios.

La GUI de administración debe tener la capacidad de excluir fácilmente la dirección IP de la definición de firma IPS.

El Visor de registro debe tener la capacidad de excluir fácilmente la dirección IP de los registros de IPS cuando se detecta como falso positivo.

La GUI de administración debe tener la capacidad de acceder fácilmente a la definición de firmas IPS a partir de los registros de IPS.

El Visor de registro debe tener la capacidad de ver todos los registros de seguridad (fw, IPS, url ...) en un panel de visualización (útil cuando se soluciona un problema de conectividad para una dirección IP).

El Visor de registro debe tener la capacidad en el visor de registro de crear un filtro utilizando los objetos predefinidos (hosts, red, grupos, usuarios)

El Visor de registro debe tener la capacidad en el visor de registro para crear múltiples "filtros guardados" personalizados para usar en un momento posterior.

La solución debe combinar la configuración de políticas y el análisis de registros en un solo panel, para evitar errores y lograr la confianza del cambio.

La solución de administración de políticas debe proporcionar registros de reglas similares para el usuario a medida que crea o modifica reglas (registros de contenido)

La GUI de la solución debe proporcionar una navegación fácil entre cientos de políticas, cada una con hasta 2000 reglas. Se deben proporcionar saltos entre sub-políticas y títulos de sección, así como una búsqueda exhaustiva.

La administración de políticas debe proporcionar la búsqueda de reglas por paquetes, incluso sin tener registros de ese paquete en el sistema. La búsqueda debe estar integrada en el mismo panel que la configuración de la política y devolver todos los resultados en pocos segundos.

La solución de administración de seguridad debe proporcionar la búsqueda de todas las referencias a cualquier objeto de red dado en todas sus políticas y configuraciones (donde se usa).

El servidor de administración de seguridad debe contener todas las validaciones, desencadenantes y procesos comerciales para proporcionar un servicio estable y confiable para cualquier cliente definido por el usuario que esté operando a través de su API.

8. WEB APPLICATION FIREWALLS

8.1 Firewall de aplicaciones Web

El servicio de WAF debe proteger un total de 130 aplicaciones web con un ancho de banda máximo de 100 Mbps

Debe ser en la nube o en nuestras instalaciones que funcione de manera transparente o como proxy reverso.

La instalación del servicio debe ser simple, a través de modificación DNS o montado en línea.

La solución debe ofrecer protección de aplicaciones WEB contra amenazas registradas OWASP Top Ten vulnerabilities.

El proveedor deberá proporcionar y asegurar la protección de los aplicativos web; dicha protección debe incluir:

- Web Application Firewall
- Content Delivery Network (CDN)
- Monitoreo de Logs
- Protección contra ataques de Denegación de Servicio Distribuidos,
- Protección contra vulnerabilidades explotación de software
- Virtual patching

- Bloqueo de ataques dirigidos de hackers.
- IDS/IPS
- Protección contra APT
- Análisis de Comportamiento
- DDOS protección
- Doble factor de autenticación
- Control de carga de archivos.
- Protección contra fuerza bruta
- Balanceo de Carga Fail Over

El proveedor deberá incluir un monitoreo continuo y respuesta a incidentes durante la duración del servicio que incluya:

- Ataques a nivel aplicación
- Ataques de explotación de Software
- Infecciones de Malware
- Listas Negras
- SEO Spam
- Almacenamiento de Phishing
- Vencimiento de certificados SSL
- Cambios en los registros DNS
- Redirecciones maliciosas
- Defacements

En caso de alguna afectación a la seguridad de los servicios web, el proveedor deberá desplegar las acciones de identificación y contención de los ciberataques, incluyendo también la restauración de los servicios afectados eliminando cualquier tipo de código malicioso que sea incrustado de manera no autorizada.

Para red de distribución de contenido (CDN) deberá ser implementada en centros de datos seguros que cuenten con las siguientes certificaciones:

- SSAE16
- ISO 9001:2008
- OHSAS 18001:2007
- ISO 14001:2004
- PCIDSS PAYMENT CARD INDUSTRY STANDARD
- ISO / IEC 27001:2005 AND 27001:2013
- ISO CERTIFICATION ISO 50001:2011

La solución propuesta debe proteger contra mínimo los siguientes ataques en capa de aplicación WEB:

- XSS
- SQL injections
- OS command injections
- LDAP injections
- SSI injections
- XPath injections
- Sensitive information leakage
- Application DoS
- CSRF
- Parameter tampering
- From field manipulation
- Session hijacking
- Cookie poisoning
- Application buffer overflows
- Brute Force attacks
- Access to predictable resource locations
- Unauthorized navigation
- Web server reconnaissance
- Directory/path traversal
- Forceful browsing
- Hotlink
- HTTP response splitting
- Evasion and illegal encoding
- XML validation
- Web services method restrictions and validation
- HTTP RFC violations
- HTTP request format and limitation violations
- Use of revoked or expired client certificates
- File upload violations
- Clickjacking

La solución debe inspeccionar el tráfico cifrado, terminando la sesión SSL/TLS del cliente y enviando el tráfico en texto claro o cifrado al servidor protegido.

La solución debe incluir una suscripción que permita actualizar las firmas de ataques conocidos, base de datos de geolocalización e IP de proxies anónimos.

La solución debe permitir extraer la dirección IP origen de la conexión (IP Cliente) de un encabezado HTTP configurable.

La solución debe permitir configurar una página de bloqueo interna o utilizar una página de bloqueo externa por cada aplicación configurada.
La solución debe soportar los siguientes modos operacionales por cada aplicación configurada:

- Modo log
- Modo Bloqueo
- Modo bypass

Las protecciones individuales dentro de una política de seguridad deben soportar los siguientes modos operacionales:

- Modo log
- Modo Bloqueo
- Modo bypass

La solución debe incluir un mecanismo que permita priorizar los recursos de procesamiento otorgados a las aplicaciones más críticas.

La solución debe permitir añadir la dirección IP origen en el encabezado HTTP.

La solución debe permitir especificar el número máximo de conexiones activas que soporta una determinada aplicación protegida.

La solución debe permitir los hostnames (virtual hosts) asociados a una aplicación, permitiendo usar wildcards en la definición de los hostnames.

La solución debe permitir configurar las políticas de seguridad por cada virtual host configurado.

La solución debe permitir mensajes que contengan valores de parámetros que no fueron completamente normalizados y evaluarlos como una cadena de bytes.

La solución debe controlar el tiempo timeout de conexión de los clientes a nivel HTTP, definiendo para cada aplicación protegida:

- El tiempo que espera por datos de solicitud del cliente.
- El tiempo que se espera por una respuesta por parte del servidor.

La solución debe permitir específica el carácter usado por queries strings para delimitar el inicio de los parámetros dentro de un query específico.

La solución debe bloquear queries con valores de parámetros definidos, pero sin un nombre de parámetro asociado al valor (NULL parameter name).

La solución debe permitir purgar múltiples slashes en las urls y cambiarlos por un solo slash. Este comportamiento podrá ser modificado por cada aplicación.
La solución debe permitir analizar las cookies como parámetros restringiendo el tamaño y los caracteres permitidos dentro de ellas.

La solución debe permitir añadir headers personalizados a los requests de los clientes.

La solución debe permitir firmar los mensajes enviados al servidor para que este chequee la autenticidad y solo permita la comunicación enviada desde el WAF.

La solución debe proteger contra ataques de denegación de servicio de tipo low and slow a través de análisis de comportamiento.

La solución debe permitir reemplazar los mensajes de respuesta HTTP por mensajes personalizados por cada aplicación protegida.

La solución debe enmascarar la identidad del servidor web protegido.

La solución debe configurar los tamaños de mensajes permitidos para los requerimientos del cliente y las respuestas enviadas por el servidor, permitiendo definir como mínimo:

- El tamaño del cuerpo del mensaje
- El tamaño total de los encabezados
- El tamaño total de un solo encabezado
- El tamaño total de los encabezados individuales.

La solución debe permitir configurar listas blancas y listas negras de direcciones IP.

La solución debe permitir la configuración de las listas para toda la aplicación o para un path específico dentro de la aplicación.

La solución debe permitir configurar políticas basadas en geolocalización.

La solución debe permitir la configuración de políticas basadas en geolocalización para toda la aplicación o para un path específico dentro de la aplicación.

La solución debe contar con un mecanismo de bloqueo por origen que cuente con las siguientes características mínimas:

- Debe hacer seguimiento a los ataques generados por una dirección IP en particular.
- Debe hacer seguimiento a los ataques generados por un fingerprinting de un dispositivo particular.
- Dependiendo del nivel de ataque, la IP o el Fingerprinting serán bloqueados por un tiempo en minutos configurable.

- Las IP o los fingerprinting de los dispositivos se podrán desbloquear desde el WBI de la solución

La solución debe enviar las IP bloqueadas por el mecanismo de source blocking a un mitigador de ataques DDoS del mismo fabricante, para que este efectúe el bloqueo en el perímetro.

La solución debe descubrir de forma automática y a través del tráfico que cursa a través de ella, la estructura de cada aplicación web configurada.
La solución debe incluir una vista en donde se muestre al menos la siguiente información del descubrimiento realizado sobre la aplicación:

- Hosts
- URIs
- páginas
- Cookies
- Parámetros (path y queries)

La solución debe permitir importar sitemaps para agilizar el proceso de auto descubrimiento del sitio.

La solución debe incluir un mecanismo de generación automática de política basado en el auto descubrimiento y en un análisis de amenazas realizado sobre los paths descubiertos.

El mecanismo de generación automática de políticas debe realizar como mínimo las siguientes acciones sin intervención humana:

- Generar automáticamente los paths de cada aplicación
- Configurar las protecciones para cada path configurado
- Refinar las protecciones
- Cambiar las protecciones de modo monitoreo a modo bloqueo

La generación automática de políticas permitirá definir el tipo de tráfico de cliente a utilizar: Tráfico Productivo o Tráfico de Staging.

La solución debe continuar auto descubriendo el sitio, modificando la política de seguridad y refinando las protecciones, aun estando sus protecciones en modo bloqueo.

La generación automática de políticas también debe ser capaz de ajustar automáticamente parámetros del protocolo HTTP, como mínimo:

- Definición del tamaño de los mensajes HTTP permitidos.
- Las propiedades de parsing del protocolo HTTP en URLs específicas o de forma global

La solución debe permitir definir los métodos permitidos hacia una determinada aplicación o path dentro de la aplicación.

La solución debe contar con una protección que evalúe las solicitudes de los clientes y bloquee aquellas que no hagan match con las expresiones definidas, las cuales deben contar como mínimo con las siguientes opciones de configuración:

- host
- Path dentro de la aplicación
- Método HTTP
- Página
- Expresión Regular

La solución debe contar con una protección contra ataques de fuerza bruta que bloquee intentos de atacantes de hallar el usuario y password de un usuario autorizado.
La protección contra ataques de fuerza bruta debe validar las respuestas de autenticación enviadas por los servidores WEB y bloquear la IP origen en caso que se genere un número configurable de respuestas de autenticación inválidas.

La protección de ataques de fuerza bruta debe identificar direcciones IP compartidas, por ejemplo, en caso de que la IP origen pertenezca a un proxy desde donde se están conectando varios usuarios.

La solución debe usar un motor de análisis de consulta de base de datos para detectar comandos de tipo SQL que los hackers puedan usar para realizar una manipulación de datos.

La solución debe aplicar múltiples heurísticas en valores de parámetros para detectar valores codificados en Base64. Los parámetros codificados, deben decodificarse y luego se debe aplicar la política de seguridad sobre los mismos.

La solución debe permitir crear reglas para controlar el upload de archivos con al menos los siguientes parámetros:

- Path de la aplicación.
- Extensión del archivo
- Método HTTP
- Permitir descarga de los archivos

La solución debe evaluar las respuestas de los servidores para determinar si estas están exponiendo información sensible, con al menos las siguientes características:

- Debe redirigir a página de bloqueo o ocultar los caracteres, si la respuesta del servidor incluye información de tarjetas de crédito.
- Debe redirigir a página de bloqueo o ocultar los caracteres, si la respuesta del servidor incluye un parámetro personalizado por el administrador a través de expresiones regulares.

La solución debe permitir bloquear el acceso a path específicos dentro de la aplicación.

La solución debe prevenir que los remotos manipulen la información del estado de la sesión y que envíen la información al servidor.

La solución debe permitir firmar la información de cookies para mitigar ataques que busquen manipular el estado de la sesión.

La solución debe permitir cifrar la información de cookies para mitigar ataques que busquen manipular el estado de la sesión.
La solución debe permitir firmar o cifrar la información en parámetros de tipo form, path y query para bloquear ataques que busquen manipular el estado de la sesión.

La solución debe permitir cifrar la información en parámetros de tipo form, path y query para bloquear ataques que busquen manipular el estado de la sesión.

La solución debe incluir una base de datos de firmas de vulnerabilidades conocidas.

La solución validar las solicitudes contra la base de datos de firmas de vulnerabilidades conocidas en al menos:

- La URL
- El encabezado
- El cuerpo del mensaje
- Parámetros

La solución debe permitir crear patrones personalizados para que sean validados junto con los incluidos en la base de datos de firmas de ataques conocidos.

La solución debe permitir configurar protección contra ataques de tipo CSRF para un grupo de hosts o para un host en particular.

La solución debe permitir configurar protección contra ataques de tipo Hotlink para un grupo de hosts o para un host en particular.

La solución debe permitir configurar protección contra ataques de tipo Directory Listing para un grupo de hosts o para un host en particular.

La solución debe permitir ofuscar la estructura real de la aplicación de un atacante potencial a través de la configuración de reescritura de la URL (URL Rewrite).

La solución debe proteger contra ataques DDoS a través del seguimiento de la actividad de una IP.

La solución debe permitir definir si el seguimiento de la actividad de la IP se realizará a nivel de host o a nivel global.

La solución debe soportar device fingerprinting para realizar seguimiento a las actividades utilizando un identificador de dispositivo y no la dirección IP origen.

La solución debe detectar bots de tipo motores de búsqueda para excluirlos de la lista de orígenes a los cuales se les hará seguimiento.

La solución debe registrar al menos los siguientes eventos de auditoría:

- Modificaciones de configuración.
- Intentos de acceso no autorizados.
- Reinicios de la solución o servicios.

La solución debe registrar los eventos de seguridad detectados o bloqueados incluyendo como mínimo la siguiente información:

- Severidad del evento
- Fecha

Descripción corta del evento
- El tipo de ataque.
- Dirección IP origen
- Geolocalización
- Puerto Origen
- Host
- Path de la aplicación
- URI
- Nombre del Parámetro
- Valor del Parámetro
- Tipo de Parámetro

La solución debe permitir filtrar los eventos utilizando por lo menos los siguientes parámetros:

- Nivel de severidad
- Aplicación Web
- Fecha y hora del evento
- Host
- Ruta de la aplicación
- Geolocalización
- IP Origen

- URI
- Tipo de Amenazas

La solución debe permitir refinar las políticas desde la vista de los eventos de seguridad.

La solución debe permitir agrupar los eventos a través de:

- Dirección IP: Agrupando eventos que hayan sido originados por la misma IP de origen.
- Ataques: Agrupando eventos de un mismo tipo de ataques.

La solución debe permitir visualizar, para cada evento registrado, el header HTTP de la solicitud.

La solución debe permitir visualizar, para cada evento registrado y si la protección específica está en modo monitoreo, el header HTTP de la respuesta del servidor.

9. SEGURIDAD DNS

• Se debe filtrar consultas DNS hacia dominios no deseados, devolviendo una dirección local (sinkhole) en lugar de la IP real.

• Se debe ofrecer una interfaz web de administración para visualizar estadísticas, incluyendo el número de consultas procesadas, bloqueos realizados y dominios más solicitados.

• Se debe soportar la carga de múltiples blocklists, permitiendo la actualización automática y la integración de listas personalizadas de dominios maliciosos o publicitarios.

• Se debe instalar en servidores físicos o virtuales que ejecuten distribuciones basadas en Debian o Ubuntu, aprovechando recursos mínimos (bajo consumo de CPU, RAM y almacenamiento).

• Se debe combinar un resolutor DNS interno con almacenamiento en caché para acelerar la resolución y reducir la latencia.

• Se debe permitir la configuración de listas blancas y excepciones para asegurar que dominios esenciales sean resueltos correctamente.

• Se debe integrar con servidores DNS corporativos para reenviar consultas de dominios internos, garantizando la resolución de nombres del entorno del Directorio Activo.

• Se debe ofrecer la opción de actuar como servidor DHCP en redes pequeñas, asignando direcciones IP y designándose como resolutor principal.

• Se debe proporcionar una API local que permita extraer información de logs y estadísticas para la generación de reportes personalizados o su integración con sistemas de correlación de eventos. • Se debe actualizar de forma periódica el software y las listas de bloqueo mediante comandos o tareas programadas, garantizando protección contra nuevas amenazas. • Se debe soportar la implementación en redes complejas, permitiendo la configuración de múltiples instancias en modo redundante para alta disponibilidad.

10. ANÁLISIS DE VULNERABILIDADES
10.1 Análisis de vulnerabilidades
La solución deberá ofrecer constante actualización a la plataforma durante todo el periodo de tiempo que dure el contrato del servicio. Las actualizaciones del servicio deben ser transparentes para el administrador de la solución, sin afectar ninguno de los datos almacenados o servicios suministrados. Toda comunicación entre componentes, transferencia y sincronización de datos de la solución debe estar cifrada de extremo a extremo, haciendo uso como mínimo de TLS 1.2. La solución debe permitir descubrir, evaluar, priorizar vulnerabilidades / configuraciones en toda la infraestructura de la red, incluyendo estaciones de trabajo, servidores, dispositivos de red, telecomunicaciones y seguridad, hipervisores, máquinas virtuales y nubes (Azure, GCP, AWS), brindando una única interfaz web de usuario para todos los activos, permitiendo la gestión centralizada de todos los componentes de la solución desde un único punto, sin necesidad de incurrir a consolas adicionales o componentes fuera de la misma para la administración de los servicios ofertados. Permite la detección y crear un inventario de todos los activos conocidos y desconocidos que se conectan al entorno de TI híbrido global de la organización, incluidos los dispositivos y aplicaciones locales, móviles, estaciones de trabajo, servidores, dispositivos de red / telecomunicaciones / seguridad, nubes. Permite descubrir dispositivos, aunque no sea permitido hacer ping o traceroute. Permite generar vistas gráficas de los dispositivos descubiertos a través de visualizaciones de mapas de la red.

Permite descubrir todos los activos conectados a la red, incluso en segmentos con entornos aislados y en infraestructuras críticas.

Permite descubrir activos ofreciendo las siguientes alternativas:

- Escaneo pasivo de la red
- Escaneo activo de la red no autenticado
- Escaneo activo de la red autenticado
- Agente

Ofrecer un inventario de activos que cubra como mínimo los siguientes puntos:

Inventario de activos de la red local: Debe detectar todos los dispositivos conectados a la red, incluidos servidores, estaciones de trabajo, routers, dispositivos de seguridad y redes, impresoras y dispositivos móviles.

Inventario de Certificados: Debe detectar y catalogar todos los certificados TLS/SSL digitales (internos y externos) de cualquier autoridad de certificación.

Inventario de Nube: Debe permitir supervisar los usuarios, instancias, redes, almacenamiento, bases de datos, ACL, ELB y sus relaciones para tener un inventario continuo de los recursos y activos en al menos las siguientes plataformas de nube pública:

- Amazon
  AWS,
- Google Cloud Platform
- Microsoft Azure.

Inventario de dispositivos móviles: Debe permitir detectar y catalogar los dispositivos móviles, con todos los detalles de versión de OS (Android, IOS, Ipad OS) y hardware sobre el dispositivo

La solución propuesta deberá permitir, a través de un agente instalado en los servidores, recopilar información detallada del activo, la misma debe detallar al menos los siguientes datos para cada activo:

- Software instalado
- Puertos abiertos
- Versión de sistema operativo
- Hostname
- F
  Q
  D
  N

- IP v4/v6
- MAC Address
- Ubicación del Activo

Permitir de forma automática clasificar los activos por familias tecnológicas, tipo de dispositivo, tipo de plataforma y fabricante.

Permitir el etiquetado de activos para facilitar la identificación, debe permitir generar etiquetas al menos utilizando los siguientes parámetros:

- Estática / manual.
- Palabras clave
- Dirección IP y rangos de IPs
- Segmento de Red
- Puertos abiertos
- ID de Vulnerabilidad específica

La solución debe permitir ejecutar escaneos de vulnerabilidades basados en:

- Sistemas Operativos
- Servicios WEB
- Puertos TCP y UDP
- Servicios
- Aplicaciones
- Bases de Datos

Detectar y analizar vulnerabilidades de al menos los siguientes sistemas operativos:

- Microsoft Windows
- UNIX
- LINUX
- MacOS
- Cisco
- VMware

Detectar y analizar vulnerabilidades en las principales versiones de Bases de Datos, al menos:

- Microsoft SQL Server
- MySQL
- Oracle
- Sybase

Detectar y analizar vulnerabilidades en plataformas WEB, al menos:

- IIS
- Apache Tomcat

Detectar y analizar vulnerabilidades por puertos y servicios como:

- TCP
- UDP

Buscar vulnerabilidades en al menos las siguientes aplicaciones y/o plataformas:

- Adobe
- Apple
- HP
- McAfee
- Microsoft (Office, IIS, Exchange)
- Oracle
- Oracle Java
- VMware

Permitir descubrir vulnerabilidades en la red ofreciendo las siguientes alternativas de escaneo

- Escaneo activo de la red no autenticado
- Escaneo activo de la red autenticado
- Agente

El motor de escaneo debe contar con una tasa de precisión para detección de vulnerabilidades del 99.99966%.

La base de conocimiento de vulnerabilidades debe ser actualizada automáticamente, y debe contar con al menos una base de conocimiento de 35,000 CVEs relacionados incluyendo tecnologías viejas y actuales.

La solución debe admitir el soporte estándar de la industria para la puntuación de vulnerabilidades Common Vulnerability Scoring System (CVSS)

La solución debe admitir el soporte estándar de la industria para la adición de detecciones personalizadas utilizando Open Vulnerability Assessment Language (OVAL).

La solución debe permitir vincular las vulnerabilidades detectadas e indicar su relación con amenazas como Virus, Troyanos y Malware.

La base de datos debe relacionar la mayoría de las vulnerabilidades con CVE y Bugtraq.

Debe soportar integración para autenticación con herramientas de bóvedas de contraseña líderes de la industria.

La solución debe permitir la configuración del tipo de escaneo que se va a realizar, permitiendo como mínimo definir las siguientes configuraciones al definir el mismo:

- Configuración de puertos
- Consumo de ancho de banda y recursos (Alto, Medio, Bajo)
- Escaneo a dispositivos que no soportan ping o traceroute
- Detección de balanceadores de carga
- Configuración de fuerza bruta a utilizar para los passwords
- Utilización de un header HTTP personalizado

La solución debe ofrecer evaluación de configuraciones basado en el estándar de industria CIS Benchmark, dando cobertura de esta funcionalidad en las siguientes categorías:

- Sistemas operativos
- Software de servidor
- Dispositivos de red
- Software de escritorio

Evaluación de certificados

La solución debe permitir la evaluación de certificados digitales (internos y externos) y configuraciones TLS en busca de problemas y vulnerabilidades de certificados brindando como resultado distintos grados de conformidad de acuerdo con los resultados de evaluación de su emisor, fecha de expiración, tipo de certificado, robustez del algoritmo y suite de cifrado utilizada.
Complejidad de la contraseña, caracteres alfanuméricos y numéricos a utilizar.

Forzar el cambio de contraseña en el inicio de sesión inicial

Notificación de contraseña caducada antes de varios días.

Admitir la capacidad de restringir el acceso desde la red interna o cualquier ubicación fuera de la red interna.

Admitir la capacidad de rastrear la actividad del usuario por nombre de cuenta de usuario, fecha, acción e información de acción.

Ser compatible con la capacidad de distribuir PDF informes de forma segura a través de una contraseña o un número restringido de informe de descarga a través del enlace.

Soporta acceso mediante SSO (Single Sign-on) utilizando SAML 2.0.

Generar reportes mediante IP, Grupo o Etiquetas

Permitir generar reportes de cualquier IP o Host escaneado previamente.

Permitir programar reportes diarios, semanales, mensuales o bajo demanda.

Permitir el envío de notificaciones por correo electrónico cada vez que un reporte esté disponible al administrador de la solución, usuarios específicos o distintos perfiles creados dentro de la herramienta.

Permitir al menos los siguientes tipos de reportes:

- Reporte de parches
- Reporte para toma de decisión
- Reporte de vulnerabilidades de alta criticidad
- Reporte ejecutivo
- Reporte técnico
- Reporte de autenticación
- Reporte de cumplimiento normativo y regulatorio
- Reporte de remediación

Proporcionar informes de remediación: tendencias de tickets por grupo de activos, usuario y vulnerabilidad.

Permite crear reportes basándose en direcciones IPv4, IPv6, Hostname, Grupo de activos y etiquetas personalizadas por el administrador.

Permitir reportes con cálculo de riesgo de seguridad, permitiendo un cálculo de riesgo global para todos los activos incluidos en el reporte.

Permitir reportes que permitan realizar un cálculo de riesgo empresarial, utilizando como base para calcular el mismo el riesgo de impacto al negocio y el riesgo de seguridad de los activos incluidos en el reporte.

Permitir reportes de hallazgos basando en el estado de las vulnerabilidades detectadas y su estado.

- Nuevas
- Resueltas
- Reabiertas
- Activas

Permitir reportes que incluyan vulnerabilidades en función de su fecha de publicación.

Permitir excluir vulnerabilidades encontradas en un puerto o servicio que no se está ejecutando.

Permitir excluir vulnerabilidades que no son explotables debido a la configuración del sistema / plataforma donde fue detectado.

Permitir excluir parches de Microsoft que fueron reemplazados por un nuevo parche o un parche acumulativo del mismo fabricante.

Proporcionar informes diferenciales y de tendencias automatizados.

Proporcionar múltiples opciones de distribución de informes, incluido PDF cifrado.

Admitir la personalización de la plantilla del informe según sea necesario.

Permitir exportar informes a formatos HTML, MHT, PDF, DOC, CSV y XML

Los reportes e informes deben ser mostrados en tablas y en gráficos mostrando los incidentes ocurridos, permitiendo la personalización detallada de cada reporte.

Permitir comparar el nivel de cumplimiento entre políticas, tecnologías y activos.

Contar con un tablero de control por defecto que permita ver las tendencias de vulnerabilidades por severidad, plataforma, antigüedad y estado de remediación las mismas.

Permitir la personalización de los tableros de control haciendo uso de cualquiera de los datos disponibles asociados a los activos escaneados para seleccionar diferentes tipos de gráficos, tablas, gráficas de tendencia o vistas sobre la priorización de vulnerabilidades.

Proporcionar tableros de control ejecutivos personalizables y con una vista unificada de todos los componentes de la solución.

Ofrecer un agente de bajo impacto en los sistemas donde se encuentre instalado y el consumo de ancho de banda que realice en la red.

- Debe instalarse en servidores y estaciones de trabajo, soportando su despliegue en una red local, en equipos remotos (tipo home office) y en la nube.

Ofrecer soporte para su despliegue en al menos los siguientes sistemas operativos:

- Windows 7/Windows Server 2003 SP2 and later (x86, x64)
- Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64)
- Ubuntu 14, 16,18,19,20 (x64)
- Oracle Enterpise Linux 8, Oracle Enterprise Linux (OEL) 7 through 7.5, Oracle Enterprise Linux (OEL) 6
- Amazon Linux 2, Amazon Linux 2018.03, Amazon Linux 2017.09, Amazon Linux 2017.03
- SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 11
- Actualizarse automáticamente y gestionarse de forma centralizada.

Soportar plataformas en la nube AWS, GCP, Azure.

Debe tener funciones de gestión de vulnerabilidades y cumplimiento de

políticas Poder recopilar información sobre el inventario de activos.

En el caso del despliegue de un escáner virtual, el mismo debe estar compuesto de un sistema operativo cerrado y seguro.

El escáner virtual debe poder desplegarse en los siguientes ambientes de virtualización:

- Localmente: VMware Workstation, Player, Workstation Player, Fusion, Oracle VM VirtualBox, VMware vSphere: vCenter Server, ESXi, Citrix XenServer, Microsoft Windows Server (Microsoft Hyper-V)
- En la nube Cloud: Amazon EC2-Classic, Amazon EC2-VPC, Microsoft Azure Cloud Platform (ARM), Google Cloud Platform, OpenStack, OCI, OCI-Classic, Alibaba Cloud Compute

10.2 Análisis de vulnerabilidades web

La solución propuesta deberá:

Permitir escaneos en profundidad dinámicos para descubrir, catalogar todas las aplicaciones web y APIs en el perímetro de la red empresarial, redes internas e instancias en la nube.

Permitir escaneo autenticados, complejos y progresivos.

Detectar, identificar, evaluar, rastrear y remediar los 10 riesgos principales de OWASP, como inyección de SQL, secuencias de comandos entre sitios (XSS), entidades externas XML (XXE), autenticación interrumpida y configuraciones incorrectas, también las amenazas de WASC, las debilidades de CWE y los CVE asociados en aplicaciones web.

Admitir la capacidad de volver a probar una vulnerabilidad específica que se haya detectado antes en la aplicación web.

Encontrar aplicaciones web homologadas y no homologadas en su red generando un proceso continuo de catalogación y descubrimiento de aplicaciones web.

Generar etiquetas para facilitar la búsqueda y el uso de los activos de aplicaciones web hallados.

Escanear aplicaciones web de gran tamaño haciendo uso de un mecanismo de escaneo progresivo, que debe permitir escanear en etapas incrementales y evitar cualquier restricción que pueda generarse al intentar escanear una aplicación de una sola vez.

Establecer la hora de inicio y la duración exactas de los escaneos.

Permitir gestionar múltiples escaneos de aplicaciones web combinando múltiples escáneres para acelerar el proceso de escaneo y obtener resultados de forma más rápida.

Consolidar los datos de escaneo automatizado de la solución con datos de herramientas que permiten la evaluación manual de vulnerabilidades a través de Burp Suite y Bugcrowd, para

obtener una vista unificada de las vulnerabilidades de la aplicación web detectadas automática y manualmente.

La solución debe proporcionar informes resumidos y de escaneo del sitio que se puedan exportar a formato HTML y PDF.

La solución debe admitir la creación de roles y ámbitos definidos por el usuario y permitir la asignación de los permisos adecuados a cada rol.

La solución propuesta deberá:

Tener la capacidad de escanear e identificar infecciones de malware a partir de las propiedades web.

Proporcionar una vista completa de la actividad de los escaneos, las páginas infectadas y las tendencias de infección de malware.

Admitir la capacidad de etiquetado con fines de categorización.

11. REVISIÓN DE SEGURIDAD DE CÓDIGO FUENTE

Alcance

Debe contemplar 5 usuarios con acceso a la consola de administración y la capacidad de ejecutar escaneos ilimitados, revisar hallazgos y gestionar la remediación.

Repositorios y proyectos: Debe permitir un número ilimitado o amplio de repositorios/proyectos en el entorno, de modo que no se restrinja el volumen de aplicaciones escaneadas.

Acceso multirol: Debe ofrecer roles diferenciados (administrador, desarrollador, seguridad, etc.) para los 5 usuarios, con permisos ajustables en cuanto a creación de políticas, asignación de vulnerabilidades y visualización de reportes.

Integración con el Ciclo de Desarrollo (CI/CD)

Conectores para repositorios

Debe contar con integración nativa para plataformas como GitHub, GitLab o Bitbucket, de forma que cada commit, pull request o push active un escaneo automático de vulnerabilidades.

Plugins de CI/CD

Debe ofrecer complementos para herramientas de integración continua (Jenkins, Azure DevOps, CircleCI, etc.), facilitando la ejecución de análisis SAST en cada pipeline.

Políticas de bloqueo

Debe permitir el bloqueo de la promoción del código al siguiente ambiente en caso de detectar vulnerabilidades críticas, evitando que fallas graves lleguen a producción.

Soporte para Múltiples Lenguajes y Entornos

Lenguajes de Programación

Debe cubrir al menos Java, JavaScript/TypeScript, .NET, Python, Go y otros lenguajes populares del mercado.

Marcos y Frameworks

Debe reconocer librerías y frameworks (Spring, Express, Django, Angular, React, etc.) para detectar patrones de vulnerabilidad específicos.

Escaneo de dependencias

Debe analizar bibliotecas de terceros para CVEs conocidas y relacionarlas con versiones vulnerables, permitiendo la actualización a versiones seguras.

Políticas de Análisis y Configuración

Reglas de Detección Personalizables

Debe ofrecer la posibilidad de definir reglas propias para el análisis estático, ajustando la sensibilidad y la clasificación de fallas.

Políticas de severidad

Debe permitir la definición de umbrales de severidad (crítica, alta, media, baja) y configurar acciones automáticas según el nivel detectado.

Configuración de análisis incremental

Debe soportar escaneos parciales en proyectos de gran tamaño, optimizando el tiempo de ejecución en cada ciclo de integración continua.

Análisis de Dependencias y Licencias

Inventario de dependencias

Debe generar un listado de las librerías, módulos y frameworks utilizados en cada repositorio, indicando su versión y las CVEs asociadas.

Alertas de licencias

Debe detectar licencias conflictivas (GPL, AGPL) en el código abierto incluido, generando alertas para el equipo legal o de cumplimiento.

Actualizaciones sugeridas

Debe indicar la versión segura o parche recomendada para cada dependencia vulnerable, facilitando la remediación y el rastreo de actualizaciones.

Gestión de Hallazgos y Remediación

Dashboard de Vulnerabilidades

Debe contar con una consola central que muestre las fallas encontradas, clasificadas por severidad, fecha de descubrimiento y repositorio.

Asignación de Tareas

Debe permitir asignar vulnerabilidades a miembros específicos del equipo, generando notificaciones y seguimiento del estado (abierta, en progreso, resuelta).

Integración con sistemas de tickets

Debe ofrecer conectores o webhooks para herramientas de gestión de proyectos (Jira, Trello, Slack, etc.), facilitando la colaboración entre desarrolladores y analistas de seguridad.

Reportes y Alertas

Reportes Personalizables

Debe proporcionar informes técnicos (listado detallado de vulnerabilidades, rutas de código) y ejecutivos (resumen de riesgos, tendencias de remediación) en formatos como PDF o CSV.

Alertas en Tiempo Real

Debe habilitar notificaciones por correo o mensajería cuando se detecten nuevas fallas críticas o cuando una dependencia con CVE alto se agregue a un proyecto.

Paneles de Control

Debe ofrecer vistas gráficas de las vulnerabilidades por severidad, antigüedad, repositorio y responsable de corrección, permitiendo análisis y priorización ágiles.

Funciones de Cumplimiento y Conformidad

Soporte para Estándares

Debe mapear las vulnerabilidades a OWASP Top 10, CWE, CVE y CVSS, facilitando la correlación con estándares de la industria.

Comparativas de Conformidad

Debe generar vistas o reportes de alineación con marcos normativos (PCI-DSS, HIPAA, etc.), cuando aplique.

Trazabilidad de Cambios

Debe mantener un historial de aparición y corrección de vulnerabilidades, mostrando en qué commit se resolvió y quién ejecutó la acción.

Seguridad y Actualizaciones

Actualizaciones Automáticas de la Base de Datos

Debe actualizar su motor de análisis y base de reglas de forma constante, incorporando nuevos patrones de vulnerabilidad y CVEs.

Seguridad de la Consola

Debe ofrecer la opción de Multi-Factor Authentication (MFA) y cifrado TLS 1.2 o superior para las comunicaciones.

Roles de Usuario

Debe permitir definir permisos granulados (administrador, auditor, desarrollador), limitando la visibilidad y acciones según el rol asignado.

Resumen de servicios y/o funcionalidades requeridas

- Cloud Web Application Firewall (1)
- Licencias de Parcheo (1,600)
- Licencias de Firewall Personal (1,600)
- Sandbox para el endpoint (1)

- Previsor de Intrusos de Red (2)
- Scanner de vulnerabilidades (1600)
- Scanner de vulnerabilidades web (128)
- Acceso a la red ZTNA (1,500)
- URL filtering (1,500)
- CASB (1,500 Aplicaciones)
- Seguridad DNS Interno (1)
- Sandbox para los IPSs (1)
- Change Control para servers (100)
- Antivirus de nueva generación (1,600)
- Administrador de parcheo virtual (1,600)
- Pruebas de Penetración (1600 ips privadas 128 ips públicas)
- XDR/Correlacionador de eventos (1)
- Auditoría de cuentas de Active Directory (1500 usuarios de AD)
- Next Generation Firewalls principales (4)
- Consola de administración para los Firewalls (2)
- EDR para Servers (100)
- Control de aplicaciones para pcs (1,500)
- Revisión de seguridad código fuente SAST (5 usuarios seguridad / SCANs ilimitados)
- Seguridad en aplicaciones de Google Enterprise (Google Drive y Gmail) sin instalación de agentes.
- Instalación, soporte y servicios administrados por 2 años

El proveedor deberá de proporcionar soluciones a todo lo mencionado en esta lista. La descripción a detalle se proporciona para ilustrar lo que se espera puedan hacer para la seguridad de la información del municipio.

Las características descritas de los servicios y equipos mencionados deberán ser considerados como un requerimiento mínimo para calificar. Se podrá presentar soluciones de distintos fabricantes y mayores capacidades

SUB-PARTIDA	CONCEPTOS	UNIDAD DE MEDIDA	CANTIDAD
1.1	CONTROL EN LA NAVEGACIÓN Y SEGURIDAD WEB	LICENCIA	1500
1.2	"CLOUD ACCESS SECURITY BROKER"	LICENCIA	1500
1.3	CONTROL DE ACCESO A LA RED CON EL MÍNIMO PRIVILEGIO	LICENCIA	1500

1.4	ANTICIPACIÓN DE CAMPAÑAS DE MALWARE	LICENCIA	1500
1.5	CONTROL DE ACCESO A LA RED CON EL MÍNIMO PRIVILEGIO	LICENCIA	1500
1.6	CONTROL DE DISPOSITIVOS PERIFÉRICOS EN LAS COMPUTADORAS	LICENCIA	1500
1.7	CONTROL DE CAMBIOS PARA SERVERS	LICENCIA	100
1.8	CONTROL DE APLICACIONES PARA COMPUTADORAS	LICENCIA	1500
1.9	FIREWALL PARA LAS COMPUTADORAS	LICENCIA	1500
1.10	EDR PARA SERVIDORES	LICENCIA	100
1.11	SANDBOX PARA ANÁLISIS	LICENCIA	1
1.12	PARCHADO Y GESTIÓN DE ENDPOINTS.	LICENCIA	1600
1.13	INTEGRACIÓN CON MECANISMOS DE RESPUESTA AVANZADA	LICENCIA	1
1.14	ANÁLISIS DE PATRONES Y COLABORACIÓN	LICENCIA	1
1.15	PROTECCIÓN FRENTE A ATAQUES DIRIGIDOS	LICENCIA	1
1.16	RESILIENCIA ANTE ATAQUES DE LARGA DURACIÓN	LICENCIA	1
1.17	PERFILES DE ATAQUE PARA SERVICIOS CRÍTICOS	LICENCIA	1
1.18	PRUEBAS DE PENETRACIÓN EXTERNAS	SERVICIO	128 IPs Publicas / Urls
1.19	PRUEBAS DE PENETRACIÓN INTERNAS	Servicio	1600
1.20	DETECCIÓN AVANZADA DE AMENAZAS	LICENCIA	1600
1.21	INTEGRACIÓN Y CORRELACIÓN DE REGISTROS	LICENCIA	1600
1.22	GESTIÓN DE INCIDENTES Y RESPUESTA	LICENCIA	1600
1.23	AUDITORÍA DE DIRECTORIO ACTIVO (AD) Y CUMPLIMIENTO	LICENCIA	1600
1.24	PANELES DE CONTROL Y REPORTES	LICENCIA	1600
1.25	AUDITORÍA DE CUENTAS PRIVILEGIADAS	LICENCIA	100
1.26	ANÁLISIS DE CONTRASEÑAS Y FORTALECIMIENTO DE POLÍTICAS	LICENCIA	1500
1.27	CONTROL Y AUDITORÍA DE CUENTAS DE SERVICIO	LICENCIA	100
1.28	CONSOLA DE REPORTES Y PANELES DE CONTROL	LICENCIA	1

1.29	FIREWALL PRINCIPAL Y VPN SSL (CLÚSTER EN SITIO PRINCIPAL)	LICENCIA	2 Firewalls en cluster
1.30	FW SITIO ALTERNO Y VPNS	LICENCIA	2 Firewalls en cluster
1.31	CONSOLA DE ADMINISTRACIÓN	LICENCIA	2 Por cada cluster
1.32	CONSOLA DE REPORTES Y CORRELACIÓN DE EVENTOS	LICENCIA	1
1.33	MÓDULOS AVANZADOS DE SEGURIDAD	LICENCIA	4
1.34	WAF BASADO EN LA NUBE	LICENCIA	130
1.35	INTEGRACIÓN CON RED GLOBAL Y MITIGACIÓN DDOS	LICENCIA	130
1.36	CONSOLA DE ADMINISTRACIÓN Y REPORTES UNIFICADOS	LICENCIA	1
1.37	DNS SINKHOLE	LICENCIA	1
1.38	CONSOLA DE ADMINISTRACIÓN	LICENCIA	1
1.39	ADMINISTRACIÓN DE VULNERABILIDADES INFRAESTRUCTURA	LICENCIA	1600 IPS PRIVADAS
1.40	ADMINISTRACIÓN DE VULNERABILIDADES SERVIDORES WEB	LICENCIA	128 IPS PUBLICAS
1.41	PLATAFORMA DE PRUEBAS ESTÁTICAS DE SEGURIDAD DE APLICACIONES (SAST)	LICENCIA	5
1.42	INTEGRACIÓN CON EL CICLO DE DESARROLLO (CI/CD)	LICENCIA	5
1.43	ANÁLISIS DE DEPENDENCIAS Y CONTENEDORES	LICENCIA	5
1.44	CONSOLA DE ADMINISTRACIÓN Y GESTIÓN DE HALLAZGOS	LICENCIA	5
1.45	SERVICIO DE IMPLEMENTACIÓN	SERVICIO	1
1.46	SERVICIO ADMINISTRADO DE ANTIVIRUS EN ENDPOINT Y SERVIDORES	SERVICIO	1
1.47	SERVICIO ADMINISTRADO DE FIREWALL	SERVICIO	1

1.48	SERVICIO ADMINISTRADO DE WEB APPLICATION FIREWALL (WAF)	SERVICIO	1
1.49	SERVICIO ADMINISTRADO DE GESTIÓN DE VULNERABILIDADES	SERVICIO	1
1.50	SERVICIO ADMINISTRADO DE GESTIÓN DE PARCHES EN SERVIDORES	SERVICIO	1
1.51	SERVICIO ADMINISTRADO DE HERRAMIENTA SAST	SERVICIO	1
1.52	SERVICIO ADMINISTRADO DE CORRELACIONADOR DE EVENTOS (SIEM), PREVENCIÓN DE INTRUSOS (IPS), DNS SINKHOLE	SERVICIO	1
1.53	SERVICIO DE GESTIÓN DE INCIDENTES	SERVICIO	1
1.54	SERVICIO DE MONITOREO SOC	SERVICIO	1

GARANTIAS: En caso de que se produzca cualquier incidente de ciberseguridad que impacte la prestación de los servicios o la integridad de los equipos suministrados, el proveedor se compromete a activar de inmediato su plan de respuesta ante incidentes en un término que no podrá variar de 1 a 3 horas como máximo, debiendo notificar al personal de la Dirección de Tecnologías en un plazo máximo de 1 hora en que se registre el incidente y proporcionando informes periódicos hasta la completa resolución del incidente.

Ejecutar todas las acciones correctivas y preventivas necesarias para mitigar y erradicar el incidente, restaurando la normalidad en las operaciones sin costo adicional para la convocante. Asumir la obligación de indemnizar a la convocante por cualquier daño, perjuicio o pérdida económica directa o indirecta ocasionada por el monto del 100%, en la medida en que se determine que dichos perjuicios surgieron a consecuencia del incumplimiento de las medidas de ciberseguridad contratadas.

El participante deberá garantizar que, ante una falla en el servicio y la consecuente rescisión del contrato, la empresa se compromete a facilitar la migración del servicio durante un período de **dos (2) meses**, brindando el soporte, servicio y servidores necesarios para que el convocante pueda adaptarse sin contratiempos a una nueva plataforma o proveedor.

A t e n t a m e n t e,

_____

Firma de la persona física o
del Representante Legal (en caso de ser persona moral)

ANEXO 2
PROPUESTA ECONÓMICA

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS

SUB-PARTIDA	CONCEPTOS	UNIDAD DE MEDIDA	CANTIDAD	IMPORTE MENSUAL	IMPORTE TOTAL POR 2 AÑOS
1.1	CONTROL EN LA NAVEGACIÓN Y SEGURIDAD WEB	LICENCIA	1500	$	$
1.2	"CLOUD ACCESS SECURITY BROKER"	LICENCIA	1500	$	$
1.3	CONTROL DE ACCESO A LA RED CON EL MÍNIMO PRIVILEGIO	LICENCIA	1500	$	$
1.4	ANTICIPACIÓN DE CAMPAÑAS DE MALWARE	LICENCIA	1500	$	$
1.5	CONTROL DE ACCESO A LA RED CON EL MÍNIMO PRIVILEGIO	LICENCIA	1500	$	$
1.6	CONTROL DE DISPOSITIVOS PERIFÉRICOS EN LAS COMPUTADORAS	LICENCIA	1500	$	$
1.7	CONTROL DE CAMBIOS PARA SERVERS	LICENCIA	100	$	$
1.8	CONTROL DE APLICACIONES PARA COMPUTADORAS	LICENCIA	1500	$	$
1.9	FIREWALL PARA LAS COMPUTADORAS	LICENCIA	1500	$	$
1.10	EDR PARA SERVIDORES	LICENCIA	100	$	$
1.11	SANDBOX PARA ANÁLISIS	LICENCIA	1	$	$
1.12	PARCHADO Y GESTIÓN DE ENDPOINTS.	LICENCIA	1600	$	$
1.13	INTEGRACIÓN CON MECANISMOS DE RESPUESTA AVANZADA	LICENCIA	1	$	$
1.14	ANÁLISIS DE PATRONES Y COLABORACIÓN	LICENCIA	1	$	$
1.15	PROTECCIÓN FRENTE A ATAQUES DIRIGIDOS	LICENCIA	1	$	$
1.16	RESILIENCIA ANTE ATAQUES DE LARGA DURACIÓN	LICENCIA	1	$	$

1.17	PERFILES DE ATAQUE PARA SERVICIOS CRÍTICOS	LICENCIA	1	$	$
1.18	PRUEBAS DE PENETRACIÓN EXTERNAS	SERVICIO	128 IPs Publicas / Urls	$	$
1.19	PRUEBAS DE PENETRACIÓN INTERNAS	Servicio	1600	$	$
1.20	DETECCIÓN AVANZADA DE AMENAZAS	LICENCIA	1600	$	$
1.21	INTEGRACIÓN Y CORRELACIÓN DE REGISTROS	LICENCIA	1600	$	$
1.22	GESTIÓN DE INCIDENTES Y RESPUESTA	LICENCIA	1600	$	$
1.23	AUDITORÍA DE DIRECTORIO ACTIVO (AD) Y CUMPLIMIENTO	LICENCIA	1600	$	$
1.24	PANELES DE CONTROL Y REPORTES	LICENCIA	1600	$	$
1.25	AUDITORÍA DE CUENTAS PRIVILEGIADAS	LICENCIA	100	$	$
1.26	ANÁLISIS DE CONTRASEÑAS Y FORTALECIMIENTO DE POLÍTICAS	LICENCIA	1500	$	$
1.27	CONTROL Y AUDITORÍA DE CUENTAS DE SERVICIO	LICENCIA	100	$	$
1.28	CONSOLA DE REPORTES Y PANELES DE CONTROL	LICENCIA	1		
1.29	FIREWALL PRINCIPAL Y VPN SSL (CLÚSTER EN SITIO PRINCIPAL)	LICENCIA	2 Firewalls en cluster	$	$
1.30	FW SITIO ALTERNO Y VPNS	LICENCIA	2 Firewalls en cluster	$	$
1.31	CONSOLA DE ADMINISTRACIÓN	LICENCIA	2 Por cada cluster	$	$
1.32	CONSOLA DE REPORTES Y CORRELACIÓN DE EVENTOS	LICENCIA	1	$	$
1.33	MÓDULOS AVANZADOS DE SEGURIDAD	LICENCIA	4	$	$
1.34	WAF BASADO EN LA NUBE	LICENCIA	130	$	$

1.35	INTEGRACIÓN CON RED GLOBAL Y MITIGACIÓN DDOS	LICENCIA	130	$	$
1.36	CONSOLA DE ADMINISTRACIÓN Y REPORTES UNIFICADOS	LICENCIA	1	$	$
1.37	DNS SINKHOLE	LICENCIA	1	$	$
1.38	CONSOLA DE ADMINISTRACIÓN	LICENCIA	1	$	$
1.39	ADMINISTRACIÓN DE VULNERABILIDADES INFRAESTRUCTURA	LICENCIA	1600 IPS PRIVADAS	$	$
1.40	ADMINISTRACIÓN DE VULNERABILIDADES SERVIDORES WEB	LICENCIA	128 IPS PUBLICAS	$	$
1.41	PLATAFORMA DE PRUEBAS ESTÁTICAS DE SEGURIDAD DE APLICACIONES (SAST)	LICENCIA	5	$	$
1.42	INTEGRACIÓN CON EL CICLO DE DESARROLLO (CI/CD)	LICENCIA	5	$	$
1.43	ANÁLISIS DE DEPENDENCIAS Y CONTENEDORES	LICENCIA	5	$	$
1.44	CONSOLA DE ADMINISTRACIÓN Y GESTIÓN DE HALLAZGOS	LICENCIA	5	$	$
1.45	SERVICIO DE IMPLEMENTACIÓN	SERVICIO	1	$	$
1.46	SERVICIO ADMINISTRADO DE ANTIVIRUS EN ENDPOINT Y SERVIDORES	SERVICIO	1	$	$
1.47	SERVICIO ADMINISTRADO DE FIREWALL	SERVICIO	1	$	$
1.48	SERVICIO ADMINISTRADO DE WEB APPLICATION FIREWALL (WAF)	SERVICIO	1	$	$
1.49	SERVICIO ADMINISTRADO DE GESTIÓN DE VULNERABILIDADES	SERVICIO	1	$	$
1.50	SERVICIO ADMINISTRADO DE GESTIÓN DE PARCHES EN SERVIDORES	SERVICIO	1	$	$

1.51	SERVICIO ADMINISTRADO DE HERRAMIENTA SAST	SERVICIO	1	$	$
1.52	SERVICIO ADMINISTRADO DE CORRELACIONADOR DE EVENTOS (SIEM), PREVENCIÓN DE INTRUSOS (IPS), DNS SINKHOLE	SERVICIO	1	$	$
1.53	SERVICIO DE GESTIÓN DE INCIDENTES	SERVICIO	1	$	$
1.54	SERVICIO DE MONITOREO SOC	SERVICIO	1	$	$
				Sub-total	
				I.V.A.	
				Total	

Favor de asegurarse que los cálculos de su propuesta económica estén correctos, conforme a lo solicitado en las bases.

A t e n t a m e n t e,

_____

Firma de la persona física o del Representante Legal (en caso de ser persona moral)

FORMATO I

_____(Nombre)_____, manifiesto bajo protesta de decir verdad que los datos aquí asentados, son ciertos y han sido debidamente verificados, así como que cuento con facultades suficientes para suscribir la propuesta en la presente Licitación Pública Nacional, a nombre y representación de: (persona física o moral)

No. de Licitación Pública Nacional:

de Registro en el Padrón de Proveedores: Registro Federal de Contribuyentes: Domicilio: Calle y número: Colonia: Delegación o Municipio: Código Postal: Entidad Federativa: Teléfono institucional y del Representante Legal: Correo electrónico institucional y del Representante Legal: Página Web:
No. de la escritura pública en la que consta su Acta Constitutiva: Fecha: Nombre, número y lugar del Notario Público ante el cual se dio fe de la misma. Relación de accionistas de su última modificación: Apellido Paterno: Apellido Materno: Nombre(s) (Denominación) Descripción del objeto social: Reformas al Acta Constitutiva: Número: Fecha:

Nombre del apoderado o representante: Datos del documento mediante el cual acredita su personalidad y facultades: Escritura pública número: Fecha: Nombre, número y lugar del Notario Público ante el cual se otorgó:

Declarando además que las facultades otorgadas no le han sido revocadas ni modificadas a la fecha.

(Lugar y fecha)
Protesto lo necesario

(Firma)

Nota: El presente formato podrá ser reproducido por cada **PARTICIPANTE** en el modo que estime conveniente, debiendo respetar en todo momento su contenido y en el orden indicad

FORMATO II

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
“SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS”

C A R T A C O M P R O M I S O

MUNICIPIO DE SAN PEDRO GARZA GARCÍA NUEVO LEÓN.
DIRECCIÓN DE ADQUISICIONES
COORDINACIÓN DE LICITACIONES, CONCURSOS Y EXCEPCIONES

Me refiero a la Licitación Pública Nacional No. _____, relativa al_____.

Sobre el particular _____ por mi propio derecho (en caso de ser persona física) o como Representante Legal de _____ manifiesto a usted que:

Oportunamente he verificado el pliego de requisitos correspondientes a esta Licitación Pública Nacional y he tomado debida nota de las reglas generales, requisitos y especificaciones a que se sujetará dicha Licitación Pública Nacional y conforme a los cuales se llevará a cabo el servicio o suministro licitado, en virtud de lo anterior, mi representada se somete expresamente y acepta íntegramente los requisitos contenidos en los citados pliegos y para tal efecto se devuelven debidamente firmados por el suscrito, igualmente expongo que se han tomado las providencias a que se contrae en los mismos así como en las bases de la Licitación Pública Nacional.

Habiendo manifestado lo anterior, declaro bajo protesta de decir verdad, que la propuesta presentada se apega estrictamente a lo solicitado por **LA CONVOCANTE** y que fue revisada y presentada respetando todas y cada una de las especificaciones y requisitos establecidos en las bases, por lo que dicha propuesta no contiene alternativas y/o vicios ocultos que difieran de lo solicitado o lo modifiquen de manera alguna.

Que tengo conocimiento de todas y cada una de las etapas señaladas en las bases para el procedimiento de adjudicación, así como las reuniones y actas derivadas de las mismas (Junta de Aclaraciones, Acto de Presentación de Propuesta Técnica y Económica y Apertura de Propuesta Técnica, Resultado de la Evaluación Técnica y Apertura de propuesta Económica y Fallo Definitivo y Adjudicación), por lo que al firmar las actas por mí mismo o por el representante que yo asigne para

asistir en mi nombre y representación a cada reunión, doy por hecho, acepto y estoy de acuerdo con el procedimiento y determinaciones tomadas y asentadas por **LA CONVOCANTE** en actas hasta el momento de su elaboración.

Además, declaro también, que estoy de acuerdo en la decisión que **LA CONVOCANTE**, dictamine en el fallo, siendo que las bases y procedimiento se establecen apegados a la normatividad aplicable, de acuerdo con el siguiente criterio de adjudicación:

“CRITERIO DE ADJUDICACIÓN.- Se considerarán para la emisión del fallo lo siguiente:

LA CONVOCANTE adjudicará la licitación al **PARTICIPANTE** que haya ofertado la propuesta más conveniente en cuanto a precio y que previamente haya cumplido con los requisitos legales y técnicos solicitados en las presentes bases.

Declaro y manifiesto mi compromiso moral y solidario con el Municipio de San Pedro Garza García, Nuevo León, en la asignación de esta Licitación Pública Nacional, puesto que el suministro o servicio a contratar se verá reflejado en un beneficio a la comunidad del Municipio.

Ratificamos nuestro compromiso y conformidad con el proceso ejecutado y por ejecutar por el Municipio de San Pedro Garza García, Nuevo León, en las determinaciones que sean tomadas y avaladas, firmando toda acta elaborada para la adjudicación de esta Licitación Pública Nacional.

De conformidad con lo manifestado y declarado anteriormente, se presenta la propuesta respectiva.

A t e n t a m e n t e,

_____

Firma de la persona física o
del Representante Legal (en caso de ser persona moral)

FORMATO III

CARTA DE ACEPTACIÓN DE LA CONVOCATORIA, BASES, CONTENIDO DE JUNTA DE ACLARACIONES Y VALIDEZ DE PROPUESTA

San Pedro Garza García, Nuevo León a (mes) del 2025.

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
"SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS"

Bajo protesta de decir verdad manifiesto que he revisado y analizado cada uno de los puntos que contienen las bases de la Licitación Pública Nacional número **SAIA-DA-CL-43/2025** para el **SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS** emitidas por el Municipio de San Pedro Garza García Nuevo León y por ende las conozco y estoy de acuerdo con ellas, sin tener reclamación o duda alguna en torno a las mismas. Así mismo, manifiesto que por medio de la presente me comprometo a darle validez a la propuesta y oferta económica presentada por el suscrito.

Del mismo modo, manifiesto que conozco y estoy de acuerdo con el contenido del acta del Junta de Aclaraciones.

NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL
SELLO DE LA EMPRESA

El presente formato deberá ser presentado previo al evento de Presentación de Propuesta Técnica y Económica y Apertura de Propuesta Técnica.

FORMATO IV

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
“SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS”

MUNICIPIO DE SAN PEDRO GARZA GARCÍA NUEVO LEÓN.
DIRECCIÓN DE ADQUISICIONES
COORDINACIÓN DE LICITACIONES, CONCURSOS Y EXCEPCIONES

Carta de no impedimento legal para contratar

El firmante y mi representada manifestamos bajo protesta de decir verdad que no nos encontramos en alguno de los supuestos establecidos por los artículos 37 y 95 de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León y 38 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León, para participar o celebrar contratos, lo anterior con fundamento en lo dispuesto por el artículo 31, fracción XI de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León, así como el artículo 117 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León.

Sin más por el momento, quedando a sus apreciables órdenes para cualquier aclaración o duda de la presente.

Atentamente

NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL
NOMBRE DE LA EMPRESA PARTICIPANTE

FORMATO V

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
“SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS”

MUNICIPIO DE SAN PEDRO GARZA GARCÍA NUEVO LEÓN
DIRECCIÓN DE ADQUISICIONES
COORDINACIÓN DE LICITACIONES, CONCURSOS Y EXCEPCIONES

Declaración de integridad

El firmante y mi representada manifestamos bajo protesta de decir verdad, nuestro compromiso de conducirnos honestamente en las diversas etapas de la licitación y que por sí mismos o a través de interpósita persona, nos abstendremos de adoptar conductas para que los servidores públicos de la Dirección de Adquisiciones, induzcan o alteren las evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que le puedan otorgar condiciones más ventajosas con relación a los demás participantes, lo anterior con fundamento en lo dispuesto por el artículo 131, fracción VIII, inciso f) del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León.

Sin más por el momento, quedando a sus apreciables órdenes para cualquier aclaración o duda de la presente.

Atentamente

NOMBRE Y FIRMA DEL
REPRESENTANTE LEGAL
NOMBRE DE LA EMPRESA PARTICIPANTE

FORMATO VI

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
“SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS”

Política de Integridad

Manifieste “Bajo protesta de decir verdad”, que contamos con una política de integridad de conformidad con el artículo 130 fracción XII del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León y la proporcionaremos en caso de resultar adjudicados.

NOTA: En el caso de que los participantes no cuenten con tal política, deberán acudir a la Contraloría a suscribir compromiso de su implementación, para lo cual, la Contraloría a través de la Unidad Anticorrupción propondrá un modelo de programa de integridad empresarial y entregará constancia que acredite tal compromiso de conformidad con el artículo 130 fracción XII del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León. (SOLO PERSONAS MORALES)

Sin más por el momento, quedando a sus apreciables órdenes para cualquier aclaración o duda de la presente.

Atentamente

NOMBRE Y FIRMA DEL
REPRESENTANTE LEGAL
NOMBRE DE LA EMPRESA PARTICIPANTE

FORMATO VII

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
“SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS”

MUNICIPIO DE SAN PEDRO GARZA GARCÍA NUEVO LEÓN.
DIRECCIÓN DE ADQUISICIONES
COORDINACIÓN DE LICITACIONES, CONCURSOS Y EXCEPCIONES

Certificado de determinación independiente de propuestas

El firmante y mi representada manifestamos bajo protesta de decir verdad y declaramos que hemos determinado nuestra propuesta de manera independiente, sin consultar, comunicar o acordar con ningún otro participante. Además, manifestamos que conocemos las infracciones y sanciones aplicables en caso de cometer alguna práctica prohibida por la Ley Federal de Competencia Económica, lo anterior con fundamento en lo dispuesto por el artículo 131, fracción VIII, inciso g) del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León.

Sin más por el momento, quedando a sus apreciables órdenes para cualquier aclaración o duda de la presente.

Atentamente

NOMBRE Y FIRMA DEL
REPRESENTANTE LEGAL
NOMBRE DE LA EMPRESA PARTICIPANTE

FORMATO VIII

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
“SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS”

MUNICIPIO DE SAN PEDRO GARZA GARCÍA NUEVO LEÓN.
DIRECCIÓN DE ADQUISICIONES
COORDINACIÓN DE LICITACIONES, CONCURSOS Y EXCEPCIONES

Origen extranjero de los bienes que oferten

El firmante y mi representada manifestamos bajo protesta de decir verdad y declaramos que el origen extranjero de los bienes que ofertamos son de la siguiente procedencia:

-

Lo anterior con fundamento en lo dispuesto por el artículo 131, fracción VIII, inciso b) del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León.

Sin más por el momento, quedando a sus apreciables órdenes para cualquier aclaración o duda de la presente.

Atentamente

NOMBRE Y FIRMA DEL
REPRESENTANTE LEGAL
NOMBRE DE LA EMPRESA PARTICIPANTE

FORMATO IX

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
“SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS”

MUNICIPIO DE SAN PEDRO GARZA GARCÍA NUEVO LEÓN.
DIRECCIÓN DE ADQUISICIONES
COORDINACIÓN DE LICITACIONES, CONCURSOS Y EXCEPCIONES

Origen nacional de los bienes o servicios que oferten

El firmante y mi representada manifestamos bajo protesta de decir verdad y declaramos que el origen nacional de los bienes o servicios que ofertamos son de la siguiente procedencia:

-

Lo anterior con fundamento en lo dispuesto por el artículo 131, fracción VIII, inciso d) del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León.

Sin más por el momento, quedando a sus apreciables órdenes para cualquier aclaración o duda de la presente.

Atentamente

NOMBRE Y FIRMA DEL
REPRESENTANTE LEGAL
NOMBRE DE LA EMPRESA PARTICIPANTE

FORMATO X

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
“SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS”

MANIFESTACIÓN DE ESTRATIFICACIÓN POR SECTOR Y NÚMERO DE TRABAJADORES Y RANGO DEL MONTO DE VENTAS ANUALES

_____ de _____ de _____ (1)

MUNICIPIO DE SAN PEDRO GARZA GARCÍA NUEVO LEÓN.
P r e s e n t e.

Me refiero al procedimiento de Licitación Pública Nacional No. **SAIA-DA-CL-43/2025** en el que mi representada, la empresa _____ (2) participa a través de la propuesta que se contiene en el presente sobre.
Sobre el particular, y en los términos de lo previsto por el artículo 3 fracción III de la Ley para Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa en los procedimientos de adquisición y arrendamiento de bienes muebles, así como la contratación de servicios que realicen las dependencias y entidades de la Administración Pública Federal”, declaro bajo protesta de decir verdad, que mi representada pertenece al sector _____(3), cuenta con _____(4) empleados de planta registrados ante el IMSS y con _____(5) personas subcontratadas y que el monto de las ventas anuales de mi representada es de _____(6) obtenido en el ejercicio fiscal correspondiente a la última declaración anual de impuestos. Considerando lo anterior, mi representada se encuentra en el rango de una empresa _____(7), atendiendo a lo siguiente:

Estratificación				
Tamaño (10)	Sector (6)	Rango de número de trabajadores (7) + (8)	Rango de monto de ventas anuales (mdp) (9)	Tope máximo combinado*
Micro	Todas	Hasta 10	Hasta $4	4.6
Pequeña	Comercio	Desde 11 hasta 30	Desde $4.01 hasta $100	93
	Industria y Servicios	Desde 11 hasta 50	Desde $4.01 hasta $100	95
Mediana	Comercio	Desde 31 hasta 100	Desde $100.01	235
	Servicios	Desde 51 hasta	Hasta $250	

		100		
	Industria	Desde 51 hasta 250	Desde $100.01 hasta $250	250

*** Tope Máximo Combinado = (Trabajadores) X 10% + (Ventas Anuales) X 90%.**

(4) (5) El número de trabajadores será el que resulte de la sumatoria de los puntos (4) y (5).

(7) El tamaño de la empresa se determinará a partir del puntaje obtenido conforme a la siguiente fórmula: Puntaje de la empresa = (Número de trabajadores) X 10% + (Monto de Ventas Anuales) X 90% el cual debe ser igual o menor al Tope Máximo Combinado de su categoría.

Asimismo, manifiesto bajo protesta de decir verdad, que el Registro Federal de Contribuyentes de mi representada es: _____(8); y que el Registro Federal de Contribuyentes del(los) fabricante(s) de los bienes que integran mi oferta, es(son): _____(9).

A T E N T A M E N T E

_____(10)

INSTRUCTIVO PARA EL LLENADO DEL FORMATO PARA LA MANIFESTACIÓN QUE DEBERÁN PRESENTAR LOS LICITANTES.

NÚMERO	DESCRIPCIÓN
1	Señalar la fecha de suscripción del documento.
2	Citar el nombre o razón social o denominación de la empresa.
3	Indicar con letra el sector al que pertenece (Industria, Comercio o Servicios).
4	Anotar el número de trabajadores de planta inscritos en el IMSS.
5	En su caso, anotar el número de personas subcontratadas.
6	Señalar el rango de monto de ventas anuales en millones de pesos (mdp), conforme al reporte de su ejercicio fiscal correspondiente a la última declaración anual de impuestos federales.
7	Señalar con letra el tamaño de la empresa (Micro, Pequeña o Mediana), conforme a la fórmula anotada al pie del cuadro de estratificación.
8	Indicar el Registro Federal de contribuyentes del licitante.
9	Cuando el procedimiento tenga por objeto la adquisición de bienes y el licitante y fabricante sean personas distintas, indicar el Registro Federal de Contribuyentes del(los fabricante(s) de los bienes que integran la oferta.
10	Anotar el nombre y firma del representante de la empresa licitante.

Atentamente

NOMBRE Y FIRMA DEL
REPRESENTANTE LEGAL
NOMBRE DE LA EMPRESA PARTICIPANTE

FORMATO XI

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
“SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS”

DOCUMENTACIÓN ANEXADA POR EL LICITANTE

DOCUMENTACIÓN ANEXADA POR EL LICITANTE	EN RELACIÓN A LO SOLICITADO EN:	VERIFICACIÓN POR LA CONVOCANTE	OBSERVACIONES DE LA CONVOCANTE

Yo el Licitante _____ y mi Representante Legal, manifestamos que la documentación señalada es la correspondiente a la que se incluyó dentro del sobre que contiene nuestra Propuesta Técnica. Así mismo, manifestamos nuestra conformidad con lo asentado por **LA CONVOCANTE** en la verificación que se realice para tal efecto.

Atentamente
NOMBRE Y FIRMA DEL
REPRESENTANTE LEGAL
NOMBRE DE LA EMPRESA PARTICIPANTE

FORMATO XII

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
“SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS”

MUNICIPIO DE SAN PEDRO GARZA GARCÍA NUEVO LEÓN
DIRECCIÓN DE ADQUISICIONES
COORDINACIÓN DE LICITACIONES, CONCURSOS Y EXCEPCIONES

Por medio de la presente yo _____Nombre de Representante Legal_____ Manifiesto Bajo Protesta de decir verdad que no desempeño empleo, cargo o comisión en el servicio público o, en su caso, que, a pesar de desempeñarlo, con la formalización del contrato correspondiente, no se actualiza un Conflicto de Interés. Así mismo, dichas manifestaciones quedan pronunciadas a través del presente respecto a los socios o accionistas que ejerzan control sobre la sociedad. Una vez comentado lo anterior declaro que ningún socio, accionista o persona que por cualquier medio tengan facultades de tomar decisiones fundamentales de mi representada _____nombre de la empresa_____ configura lo establecido en el Artículo 49 Fracción IX de la Ley de Responsabilidades Administrativas del Estado de Nuevo León.

Sin más por el momento, quedando a sus apreciables órdenes para cualquier aclaración o duda de la presente.

Atentamente

NOMBRE Y FIRMA DEL
REPRESENTANTE LEGAL
NOMBRE DE LA EMPRESA PARTICIPANTE

FORMATO XIII

LICITACIÓN PÚBLICA NACIONAL NÚMERO SAIA-DA-CL-43/2025
“SUMINISTRO DE LICENCIAS, SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA, EQUIPAMIENTO EN SITIO NECESARIO Y SERVICIOS ADMINISTRADOS”

MUNICIPIO DE SAN PEDRO GARZA GARCÍA NUEVO LEÓN
DIRECCIÓN DE ADQUISICIONES
COORDINACIÓN DE LICITACIONES, CONCURSOS Y EXCEPCIONES

Manifiesto del Artículo 69-B del Código Fiscal de la Federación

El firmante y mi representada manifestamos bajo protesta de decir verdad, no hemos emitido comprobantes sin contar con los activos, personal, infraestructura o capacidad material, directa o indirectamente, para prestar los servicios o producir, comercializar o entregar los bienes que amparan tales comprobantes. Así mismo, manifestamos que en caso de que la autoridad fiscal lo requiera nos comprometeremos a aportar la documentación e información que consideremos pertinentes para desvirtuar los hechos que llevarán a la autoridad a notificarnos. Lo anterior en cumplimiento a lo señalado por el artículo 69-B del Código Fiscal de la Federación.

Sin más por el momento quedando a sus apreciables órdenes para cualquier aclaración o duda de la presente.

Atentamente

NOMBRE Y FIRMA DEL
REPRESENTANTE LEGAL
NOMBRE DE LA EMPRESA PARTICIPANTE

Nota: El modelo de contrato que a continuación se presenta es solo un proyecto que contiene lo mínimo que establece la normatividad aplicable, en caso de resultar adjudicado previo a la firma del contrato se le hará llegar en archivo digital el proyecto de contrato para su revisión.

MODELO DE CONTRATO

CONTRATO DE PRESTACIÓN DE SERVICIOS, QUE CELEBRAN POR UNA PARTE, EL MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ “EL MUNICIPIO”, REPRESENTADO EN ESTE ACTO POR EL C. ALBERTO HERRERA HERNÁNDEZ, SECRETARIO DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL, EN EJERCICIO DE LAS FACULTADES DELEGADAS POR EL C. PRESIDENTE MUNICIPAL Y EL C. SECRETARIO DEL REPUBLICANO AYUNTAMIENTO; Y POR OTRA PARTE, «NOMBRE», A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ “EL PRESTADOR DE SERVICIOS”; MISMOS QUE SE SUJETAN AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS:

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

I.- DECLARA “EL MUNICIPIO” POR CONDUCTO DE SUS REPRESENTANTES, LO SIGUIENTE:

Que de conformidad con lo dispuesto por los artículos 115, fracción II de la Constitución Política de los Estados Unidos Mexicanos, 120 de la Constitución Política del Estado de Nuevo León y 2 de la Ley de Gobierno Municipal del Estado de Nuevo León, tiene personalidad jurídica y capacidad legal para contratar y obligarse.

El C.----, Presidente Municipal, en términos del artículo 34 fracción II de la Ley de Gobierno Municipal del Estado de Nuevo León, es a quién le corresponde ejercer la personalidad jurídica del Municipio, en representación de la Administración Pública Municipal; además de conformidad con el artículo 35 aparado B) fracción III de la referida Ley, compete al Presidente Municipal, celebrar los actos convenios y contratos necesarios para el despacho de los asuntos administrativos y la atención de los servidores públicos.

El C.-----, Secretario del Republicano Ayuntamiento, de conformidad con lo dispuesto en el artículo 98 fracción II de la Ley de Gobierno Municipal del Estado de Nuevo León, cuenta con la facultad y obligación de acordar directamente con el Presidente Municipal, en relación con las facultades conferidas por el artículo 26 inciso a) fracciones XV y XVI del Reglamento Orgánico de la Administración Pública Municipal de San Pedro Garza García, Nuevo León, que establecen que tiene como atribución y responsabilidad, el firmar convenios y contratos en los que intervenga el Municipio, así como de los acuerdos y actos que expida el Presidente Municipal.

Que el presente Contrato cuenta con la autorización por parte de la Titular de la Secretaría de

Finanzas y Tesorería Municipal, en la que se hace constar la suficiencia presupuestal para cubrir los compromisos adquiridos mediante el presente instrumento jurídico.

Que requiere de la contratación de “EL PRESTADOR DE SERVICIOS”, cuya especialidad es «ESPECIALIDAD», por el período comprendido del _, para que atienda _ por conducto de_, cuyo pago se hará en base a _.

De conformidad con el Acta de Acuerdos de la _Sesión del Comité de Adquisiciones de “EL MUNICIPIO”, celebrada el día _, se emitió opinión favorable respecto a la contratación _, de conformidad con el artículo_, de _ con una vigencia a partir _ al_, por un monto de hasta $«MONTO»; impuestos incluidos.

H) Que para los efectos de este contrato, señala como domicilio para oír y recibir notificaciones, el ubicado en el cruce de las calles Juárez y Libertad sin número, Zona Centro, en San Pedro Garza García, Nuevo León.

II.- DECLARA “EL PRESTADOR DE SERVICIOS”, LO SIGUIENTE:

Que es «ESPECIALIDAD», lo que acredita con _», respectivamente, expedidas por _.

Que tiene los conocimientos, capacidad y experiencia necesaria para prestar el servicio que requiere “EL MUNICIPIO”.

Que para los efectos del presente contrato, señala como domicilio para oír y recibir notificaciones el ubicado en «DOMICILIO», Nuevo León.

III.- DECLARAN AMBAS PARTES LO SIGUIENTE:

ÚNICA: Que cuentan con la capacidad legal necesaria para contratar y obligarse, por lo que manifiestan su libre voluntad para celebrar el presente contrato ajustándose al tenor de las siguientes:

C L Á U S U L A S

PRIMERA: OBJETO.- El objeto del presente contrato es la Prestación de los Servicios relacionados con la especialidad en «ESPECIALIDAD» por parte de “EL PRESTADOR DE SERVICIOS” a los trabajadores de “EL MUNICIPIO” y a sus beneficiarios que le sean indicados _.

SEGUNDA: LUGAR DONDE SE PRESTARÁ EL SERVICIO.- “EL PRESTADOR DE SERVICIOS” se obliga a proporcionar los servicios en _, o bien, en el lugar que le sea requerido por “EL MUNICIPIO”.

TERCERA: INFORMACIÓN CONFIDENCIAL.- Ambas Partes convienen en que los servicios a que se refiere el presente contrato son de carácter estrictamente confidencial, por lo que de ninguna manera “EL PRESTADOR DE SERVICIOS” podrá revelar a terceros información alguna relacionada con dichos servicios, incluyendo enunciativa más no limitativamente la tecnología utilizada en el caso por “EL MUNICIPIO” para atender a sus trabajadores y sus beneficiarios, así como la aplicación de sistemas, procedimientos o políticas de servicio utilizados por “EL MUNICIPIO”, en caso contrario “EL PRESTADOR DE SERVICIOS” será responsable del pago de los daños y perjuicios que se originen.

CUARTA: SUPERVISIÓN POR PARTE DE “EL MUNICIPIO”.- “EL PRESTADOR DE SERVICIOS” tendrá en todo momento la obligación de proporcionar a “EL MUNICIPIO” toda la información que éste le requiera, pudiendo “EL MUNICIPIO” auditar o revisar en todo tiempo toda la documentación que esté en poder de “EL PRESTADOR DE SERVICIOS” derivada de la ejecución del presente contrato y así mismo, ejercer medidas de supervisión a fin de comprobar la calidad de los servicios que brindará “EL PRESTADOR DE SERVICIOS” a los trabajadores de “EL MUNICIPIO” y a sus beneficiarios con motivo del presente contrato.

QUINTA: HONORARIOS.- “EL PRESTADOR DE SERVICIOS” para el pago de sus servicios acepta los precios establecidos en _ por “EL MUNICIPIO”, el cual se agrega al presente contrato y forma parte integrante del mismo, siendo el monto autorizado para este contrato hasta la cantidad de $«MONTO» impuestos incluidos, “EL PRESTADOR DE SERVICIOS” se obliga a que cualquier asunto relacionado con sus honorarios deberá tratarlo directamente con la Dirección de _ y por ningún motivo a través de_.

SEXTA: REQUISITOS PARA EL PAGO DE HONORARIOS.- “EL MUNICIPIO” se obliga a pagar a “EL PRESTADOR DE SERVICIOS” el comprobante fiscal correspondiente por concepto de honorarios dentro de un plazo de 8-ocho días hábiles siguientes a la entrega del mismo en la Secretaría de Finanzas y Tesorería de “EL MUNICIPIO” de acuerdo a lo solicitado y autorizado por ésta última. El comprobante fiscal que entregue “EL PRESTADOR DE SERVICIOS” deberá cumplir con todos los requisitos consignados en los distintos ordenamientos fiscales para la procedencia de su cobro.

SEPTIMA: FORMA DE PAGO.- “EL PRESTADOR DE SERVICIOS” está de acuerdo en que la Secretaría de Finanzas y Tesorería municipal determine la forma de pago de los servicios contratados.

OCTAVA: NATURALEZA DE LA RELACIÓN.- Las Partes acuerdan que este contrato no podrá interpretarse de manera alguna como constitutivo de cualquier tipo de asociación o vínculo de carácter laboral entre las mismas, así como tampoco entre “EL MUNICIPIO” y los trabajadores o empleados que “EL PRESTADOR DE SERVICIOS” pudiera necesitar para el cumplimiento de las obligaciones de este contrato, por lo que las relaciones laborales se mantendrán en todos los casos entre la parte contratante y sus respectivos trabajadores, aún en los casos de los trabajos realizados conjuntamente y que se desarrollen en las instalaciones o con equipo de cualquiera de las Partes. En

ningún caso podrá considerarse a la otra Parte como patrón sustituto, ni solidario, ni tampoco intermediario, ya sea de carácter individual o colectivo, debiendo la parte que contrató al trabajador de que se trate, asumir y cumplir con todas las responsabilidades que marquen las leyes, por lo que desde este momento libera de las mismas a la otra Parte y se obliga a liberarlas de dichas responsabilidades en cualquier caso que se presente, incluso en las controversias individuales de sus empleados o de los conflictos colectivos que pudieran surgir; y de sacarla en paz y a salvo, en caso de conflictos laborales individuales o colectivos provocados por personal de la primera, respondiendo de los daños y perjuicios que resultasen.

NOVENA: VIGENCIA.- La vigencia del presente contrato inicia a partir del _, para concluir el día_.

DÉCIMA: CAUSAS DE RESCISIÓN DEL CONTRATO.- Son causas de rescisión del presente contrato las siguientes:

DÉCIMA NOVENA: TERMINACIÓN ANTICIPADA.- Es causa de terminación anticipada por parte de "EL MUNICIPIO", sin responsabilidad judicial, cuando así lo estime necesario por convenir a sus intereses, dando aviso por escrito con 30-treinta días de anticipación a la fecha efectiva de terminación en el domicilio señalado.

VIGÉSIMA: TÍTULOS DE LAS CLÁUSULAS Y ENUNCIADOS.- Las Partes convienen en que los títulos de las cláusulas y de los enunciados que aparecen en este Contrato son exclusivamente para facilitar su lectura y por consiguiente no se considera que definan o limitan el contenido de las cláusulas del mismo y de las obligaciones adquiridas.

VIGÉSIMA PRIMERA: COMPETENCIA.- En caso de controversia, las Partes se someten a la jurisdicción de los tribunales competentes en el Estado de Nuevo León, renunciando a cualesquier otro que pudiera corresponderles en razón de su domicilio, presente o futuro.

LAS PARTES MANIFIESTAN ESTAR DE ACUERDO CON EL CONTENIDO DEL PRESENTE INSTRUMENTO MEDIANTE SU LECTURA, QUE EN SU TEXTO CONTIENE LA EXPRESIÓN EXACTA DE SU LIBRE VOLUNTAD, POR LO QUE NO EXISTEN VICIOS DEL CONSENTIMIENTO COMO ERROR, DOLO, VIOLENCIA, MALA FE O CUALQUIER OTRO QUE PUDIERA INVALIDARLO, POR LO QUE LO FIRMAN DE CONFORMIDAD EN TRIPLICADO, EN EL MUNICIPIO DE SAN PEDRO GARZA, GARCÍA, NUEVO LEÓN, EL DÍA «FECHA_DE_FIRMA» DEL AÑO 2025-DOS MIL VEINTICINCO

MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN

C.-----

EN EJERCICIO DE LAS FACULTADES DELEGADAS POR EL C. PRESIDENTE MUNICIPAL Y EL C.

SECRETARIO DEL REPUBLICANO AYUNTAMIENTO Y EN SU CARÁCTER DE SECRETARIA DE ADMINISTRACIÓN E INTELIGENCIA ARTIFICIAL

“EL PRESTADOR DE SERVICIOS”

«NOMBRE»

LAS PRESENTES FIRMAS FORMAN PARTE INTEGRANTE DEL CONTRATO DE PRESTACIÓN DE SERVICIOS CELEBRADO ENTRE «ARTÍCULO» «NOMBRE» Y EL MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN.

NOTA: El presente modelo contiene las condiciones generales a contratar. Las obligaciones específicas del contrato se fijarán en base al resultado de la licitación, según los aspectos concretos de las propuestas técnica y económica del participante adjudicado en relación a las condiciones de contratación establecidas por la Unidad Convocante.

FIANZA DE CUMPLIMIENTO, PAGO Y PASIVOS CONTINGENTES
MATERIA DE ADQUISICIONES

ANTE: MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN.

PARA GARANTIZAR POR **(NOMBRE DEL PROVEEDOR)** CON REGISTRO FEDERAL DE CONTRIBUYENTES **(R.F.C.)** Y CON DOMICILIO EN **(DIRECCIÓN DEL PROVEEDOR)**, HASTA LA CANTIDAD DE $**(MONTO AFIANZADO)** INCLUYE IVA, ESTA GARANTÍA EQUIVALE AL 10% DEL MONTO TOTAL DEL CONTRATO PARA GARANTIZAR EL CUMPLIMIENTO DE TODAS Y CADA UNA DE LAS OBLIGACIONES A SU CARGO, ASÍ COMO LOS POSIBLES PASIVOS CONTINGENTES EN EL ORDEN LABORAL Y FISCAL QUE PUDIERAN LLEGAR A CUANTIFICARSE EN SU CONTRA, HASTA POR EL MONTO DE LA PRESENTE GARANTÍA Y QUE SEAN IMPUTABLES A **(EL PROVEEDOR)** COMO RESULTADO DE UNA SENTENCIA Y/O LAUDO CONDENATORIO, DERIVADAS DEL CONTRATO No. (**NÚMERO DEL CONTRATO)** DE FECHA **(FECHA DEL CONTRATO)** QUE CELEBRAN POR UNA PARTE MUNICIPIO DE SAN PEDRO GARZA GARCÍA, N.L. Y POR LA OTRA PARTE **(NOMBRE DEL PROVEEDOR)** RELATIVO A: **(DESCRIPCIÓN DEL SERVICIO)** CON UN IMPORTE DE **$(MONTO TOTAL DEL CONTRATO)** INCLUYE IVA **(NOMBRE DE LA INSTITUCIÓN AFIANZADORA),** HACE SUYAS TODAS Y CADA UNA DE LAS OBLIGACIONES DERIVADAS DEL CONTRATO Y POR LO TANTO SE COMPROMETE A CUBRIR TOTAL O PARCIALMENTE EL PAGO A ESTA INSTITUCIÓN EN CASO DE INCUMPLIMIENTO DE **(EL PROVEEDOR)**, PREVIA COMUNICACIÓN DE MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN.

LA PRESENTE FIANZA SE OTORGA DE CONFORMIDAD CON LO ESTIPULADO EN LA (**CLÁUSULA __ _____ DEL CONTRATO No. (NÚMERO DEL CONTRATO**).

LA INSTITUCIÓN DE FIANZAS HACE EXPRESAMENTE LAS SIGUIENTES DECLARACIONES:

a) Que la fianza se otorga atendiendo a todas las estipulaciones contenidas en el contrato.

b) Que la fianza garantiza la entrega total del servicio materia del contrato de acuerdo con las estipulaciones establecidas en el mismo y podrá hacerse efectiva en cualquier etapa del desarrollo de la entrega del servicio.

c) Que, para cancelar la fianza, será requisito contar con la constancia de la Dirección de --- relativa al cumplimiento total de las obligaciones contractuales. Para la cancelación de la garantía correspondiente, se requerirá la autorización previa y por escrito de **MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN.**

d) La garantía de buen cumplimiento del contrato estará vigente por un mínimo de seis meses después de que los bienes o servicios materia del mismo hayan sido recibidos en su totalidad

y quedará extendida hasta la fecha en que se satisfagan las responsabilidades no cumplidas y se corrijan los defectos o vicios ocultos en los casos en que esa fecha sea posterior al vencimiento del plazo anteriormente señalado.

e) Que la Institución Afianzadora acepta expresamente lo preceptuado en los Artículos 282 y 178 de la Ley de Instituciones de Seguros y de Fianzas.

f) La afianzadora podrá, mediante aviso por escrito que proporcione el beneficiario, ejercer las acciones contempladas en los Artículos 284 y 285 de la Ley de Instituciones de Seguros y de Fianzas.

g) Que la fianza permanecerá vigente durante el cumplimiento de la obligación que garantice y continuará vigente en caso de que se otorgue prórroga al cumplimiento del contrato, así como durante la substanciación de todos los recursos legales o de los juicios que se interpongan y hasta que se dicte resolución definitiva que quede firme y haya sido ejecutada, cuando la fianza haya sido otorgada a favor de **MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN.**

h) Que la afianzadora acepta expresamente someterse a los procedimientos de ejecución previstos en la Ley de Instituciones de Seguros y de Fianzas para la efectividad de la fianza, aun para el caso de que proceda el cobro de indemnización por mora, con motivo del pago extemporáneo del importe de la póliza de fianza requerida.

i) La fianza se cancelará cuando **EL PROVEEDOR** haya cumplido con todas las obligaciones que se derivan del contrato**.**

j) En caso de otorgamiento de prórrogas a **EL PROVEEDOR** para el cumplimiento de sus obligaciones, derivadas de la formalización de convenios de ampliación al monto o al plazo del contrato, se deberá realizar la modificación correspondiente a la fianza.

k) Cuando al realizarse el finiquito resulten saldos a cargo de **EL PROVEEDOR** y éste efectúe la totalidad del pago en forma incondicional, **MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN,** deberá cancelar la fianza respectiva.

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

m) Para la interpretación y cumplimiento de las obligaciones que se garantizan mediante la presente póliza, la institución de fianzas y el fiado se someten expresamente a la Ley de Instituciones de Seguros y de Fianzas y a la jurisdicción y competencia de las autoridades responsables en el área metropolitana de Nuevo León, así mismo designa como domicilio

para los efectos de recibir, conocer y resolver todo tipo de notificaciones, demandas, reclamaciones de fianzas y todo procedimiento legal que se derive de la presente fianza el ubicado en ----------, en el área metropolitana de Nuevo León----------fin de texto---

LIBERTAD 101 CENTRO
SPGG / NL

TEL
81 8400 4400