San Pedro Garza García
GOBIERNO MUNICIPAL

C O N V O C A T O R I A

El Municipio de San Pedro Garza García, a través de la Secretaría de Administración 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, 44 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, III, 25 fracción I, 27 tercer párrafo fracción II, 29 fracción I, 31, 32, 33, 34, 35, 37, 39, 40, 46, 48 y 50 de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León; artículos 1, 57, 58, 59 al 62, 65, 66, 67, 69, 72 al 74, 75, 78, 79, 87, 88, 90, 99, 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, CONVOCA a las personas físicas y morales a participar en el procedimiento de **LICITACIÓN PÚBLICA NACIONAL PRESENCIAL** número **SA-DA-CL-26/2022**, relativa a la **"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"** en los siguientes términos:

B A S E S

INTRODUCCIÓN.

Las presentes bases señalan las características y especificaciones que se deberán cumplir para la **"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados",** que requiere el procedimiento de Licitación Pública, los requisitos para participar, la junta de aclaraciones, la forma de presentación de las propuestas técnicas y económicas, la forma y términos en que se deberán entregar las mismas, las causas para declararla desierta, los motivos de descalificación, los criterios para la adjudicación y fallo, derechos y obligaciones, penas convencionales, garantías, recursos, sanciones y las condiciones generales de contratación.

DEFINICIONES.

Adjudicataria: Persona física o moral que resulte ganadora en la presente licitación.

Área Técnica: Dirección de Tecnologías, es la unidad Administrativa del sujeto obligado que elabora las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, evalúa las propuestas técnicas y responde en la junta de aclaraciones, las preguntas que sobre estos aspectos realicen los licitantes; el área técnica, podrá tener también el carácter de Unidad Requirente.

Bases: Documento que contiene las condiciones y requisitos que regirán y serán aplicados para esta Licitación.

Bien: Los productos y/o servicios, objeto de la licitación.

Comité: Comité de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León.

Contrato: Instrumento legal que suscribe la Unidad Convocante con la adjudicataria en el que constan los derechos para módulo al aire libre y obligaciones conforme a los cuales se regirán las partes.

Convocatoria: Documento que contiene las bases de la licitación, y los requisitos que la regirán.

Copia certificada: Documento certificado ante fedatario público (Notario).

Curso de prevención de corrupción: Curso de prevención y concientización sobre las faltas administrativas y hechos de corrupción impartido por la Secretaría de la Contraloría y Trasparencia Municipal.

Dependencia: Las dependencias administrativas que conforman la Administración Pública Municipal.

Domicilio de la Convocante: Calle Independencia Nº 316 esquina con Corregidora, 4° piso, Dirección de Adquisiciones, en el centro del Municipio de San Pedro Garza García, Nuevo León.

Firma autógrafa: Es aquella que es trazada en un documento por una persona con su puño y letra, es decir, escrita directamente por su autor.

Identificación Oficial: Credencial de elector, pasaporte, cartilla militar, cualquiera de ellas vigentes y en original o en copia certificada.

Internet: La red mundial de información electrónica.

I.V.A.- Impuesto al Valor Agregado.

Ley: Ley de Adquisiciones Arrendamientos y Contratación de Servicios del Estado de Nuevo León.

Ley de Transparencia: Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León.

Licitante: Persona física o moral que participa en cualquier procedimiento de adquisición, arrendamiento y contratación de servicios.

Lote: Grupo de cosas (productos y/o servicios) que se hace en un todo para su cotización.

Manager: Administrador.

MIPYMES: Las micro, pequeñas y medianas empresas de nacionalidad mexicana a que hace referencia la Ley de Fomento a la Micro, Pequeña y Mediana Empresa para el Estado de Nuevo León

Municipio: El Municipio de San Pedro Garza García, Nuevo León.

Padrón: Padrón de Proveedores del Municipio de San Pedro Garza García, Nuevo León.

PC: Disco duro del equipo de cómputo al que se instalará la licencia.

Política de integridad: La Política de integridad que cuente con, al menos, los elementos previstos en la Ley de Responsabilidades Administrativas del Estado de Nuevo León.

Precio Aceptable: Precio del bien o servicio materia de la contratación, conocido a través de la investigación de mercado u ofertado por los licitantes, que, según corresponda, reúne los siguientes requisitos: a) Estar dentro de los rangos de precios existentes en el mercado, en condiciones similares de contratación a la que se realiza por el sujeto obligado conforme a la Ley y al Reglamento; y b) No exceder al presupuesto máximo con que cuenta el sujeto obligado para realizar la contratación.

Reglamento de la Ley: Reglamento de la Ley de Adquisiciones, Arrendamientos y Contrataciones de Servicios del Estado de Nuevo León.

Reglamento: Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León.

Representante Legal: Persona que actúa en nombre de otra y que, siendo reconocido como tal mediante escritura o acta pública, deberá de contar con poder para actos de administración y facultades para delegar y que se encuentre acreditado como tal en el padrón de proveedores del municipio.

Sobre cerrado: Cualquier medio que contenga la proposición respectiva del licitante, cuyo contenido solo puede ser conocido en el acto de presentación de propuestas y apertura técnica o el acto de fallo técnico y apertura de propuestas económicas respectivamente en términos de la Ley.

Suficiencia Presupuestal. - El costo estimado autorizado por la Secretaría de Finanzas y Tesorería Municipal en la solicitud de contrato, de inversión o requisición correspondiente.

Sujeto Obligado: El Municipio de San Pedro Garza García, Nuevo León.

Unidad Convocante: Dirección de Adquisiciones del Municipio de San Pedro Garza García, Nuevo León.

Unidad Requirente: Dependencia que solicita la contratación de los productos y/o servicios.

Versión electrónica: Formato que es solicitado en diferentes actos, que contiene información o documentos electrónicos los cuales pueden ser según se solicite en USB o correo electrónico.

1) DATOS GENERALES DE LA LICITACIÓN PÚBLICA NACIONAL PRESENCIAL.

a. UNIDAD CONVOCANTE.

Dirección de Adquisiciones de la Secretaría de Administración del Municipio de San Pedro Garza García, Nuevo León, ubicado en el domicilio calle Independencia Nº 316 esquina con Corregidora, 4° piso, Dirección de Adquisiciones, en el centro del Municipio de San Pedro Garza García, Nuevo León.

b. OBTENCIÓN DE BASES.

Las bases se podrán adquirir a partir de la fecha de publicación de la convocatoria establecida, la cual estará publicada a partir del día **15 de junio del 2022**, de manera simultánea en el Periódico Oficial del Estado y en uno de los diarios de mayor circulación en la entidad. Las bases estarán a disposición de los interesados, de lunes a viernes de las 8:00 a las 16:00 horas en la Dirección de Adquisiciones, y estas serán entregadas en archivo electrónico acompañadas de los formatos modelo de los documentos y archivos electrónicos a los que se hace referencia esta Convocatoria, los licitantes podrán presentar para ello una USB o proporcionar un correo electrónico institucional. Previamente se deberá realizar el pago de las mismas, las cuales tienen un costo de $2,750.00 (Dos mil setecientos cincuenta pesos 00/100 m. n.), podrán realizarse en efectivo o cheque, a favor del Municipio de San Pedro Garza García, N.L., el pago deberá ser efectuado en la Dirección de Ingresos de la Secretaría de Finanzas y Tesorería Municipal, sito en Juárez y Libertad S/N, 1er. piso, Centro de San Pedro, la venta de bases será a partir de la fecha de publicación y hasta el **30 de junio a las 12:00 horas.** Así mismo las bases estarán disponibles para su consulta en la página www.sanpedro.gob.mx a partir de la misma fecha.

c. MÉTODO Y CARÁCTER DE LA LICITACIÓN.

El presente procedimiento de contratación será **PRESENCIAL**, de conformidad con lo señalado en los artículos 25 fracción I, 27, fracción II de la Ley, por lo que exclusivamente los licitantes podrán presentar sus propuestas en forma documental y por escrito, en sobre cerrado, durante el acto de presentación de propuestas y apertura técnica. No se aceptarán propuestas que sean enviadas por medios remotos de comunicación (electrónicos), servicio postal o mensajería.

De igual forma se determinó que el carácter de la presente Licitación Pública es **NACIONAL**, de conformidad con el artículo 29, fracción I de la misma, por lo que podrán participar únicamente en ella personas de nacionalidad mexicana y los bienes a adquirir deberán ser producidos en el país y contar, por lo menos, con un **50% de contenido nacional**, el que se determinará tomando en cuenta la mano de obra, insumos de los bienes y demás aspectos que determine la Secretaría de Economía del Gobierno Federal de acuerdo con la legislación aplicable y los tratados internacionales celebrados por el Estado mexicano. En consecuencia, el licitante deberá integrar como parte de su propuesta un escrito donde manifieste "Bajo protesta de decir verdad", que es de nacionalidad mexicana de conformidad con el artículo 57 del Reglamento de la Ley.

d. **NÚMERO DE CONVOCATORIA.**

SA-DA-CL-26/2022

e. **EJERCICIO FISCAL Y ORIGEN DE LOS RECURSOS.**

La presente contratación será ejecutada con recursos propios correspondiente al ejercicio fiscal **2022, 2023, 2024 y 2025** del Municipio de San Pedro Garza García, N.L., lo anterior de conformidad con la **Solicitud de contratación núm. 6800,** recibida en la Dirección de Adquisiciones para llevar a cabo el presente procedimiento. Así mismo se señala que se cuenta con la disponibilidad presupuestaria y con la autorización de Cabildo para exceder el periodo de la presente administración.

f. **IDIOMA EN QUE SERÁN PRESENTADAS LAS PROPUESTAS.**

La presentación de las propuestas deberá ser en idioma español, en caso de presentarse alguna información adicional, tales como catálogos, folletos, anexos o fichas técnicas, podrán presentarse en el idioma del país de origen, pero invariablemente deberán acompañarse de una traducción simple al español**.**

2) OBJETO Y ALCANCE DE LA LICITACIÓN PÚBLICA.

a. **DESCRIPCIÓN DE LOS SERVICIOS DE SUMINISTRO E INSTALACIÓN OBJETO DE ESTA LICITACIÓN.**

La Dirección de Adquisiciones llevará a cabo el presente procedimiento para la **"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"** las especificaciones técnicas de los mismos, los servicios, así como la demás información requerida, se precisa en los

documentos anexos a las presentes bases, que forman parte integrante de las mismas y que se identifican de la siguiente forma:

Anexo 1. "Requerimientos generales para licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados.

Anexo A. Requerimientos de productos

Anexo B. Requerimientos de instalación y configuración de los productos

Anexo C. Requerimientos de soporte

Anexo D. Requerimientos de servicios administrados

Anexo E. Características y/o capacidades de todos los productos

Anexo 2. "Cotización"

b. El licitante deberá ofrecer y cotizar al 100% los bienes solicitado, cumpliendo con las especificaciones de los anexos correspondientes.

c. La adjudicación del contrato será por lote a un solo proveedor.

3) FORMAS Y TÉRMINOS QUE RIGEN LOS ACTOS DEL PROCEDIMIENTO.

Los plazos del presente procedimiento de contratación, se encuentran fundamentados en los artículos 32 párrafo segundo, 34 párrafo sexto y 35 fracción III de la Ley.

4) FORMA DE OBTENER LA PARTICIPACIÓN EN EL PROCESO DE LICITACIÓN.

Los interesados en concursar en la presente licitación deberán acudir para obtener su participación en el proceso a las oficinas de la Dirección de Adquisiciones, **A MÁS TARDAR EL DIA 30 DE JUNIO DEL 2022 A LAS 12:00 HORAS** con los siguientes documentos, en original y por escrito en papel membretado firmados por la persona física o por el representante legal de la empresa licitante, **será requisito indispensable que los participantes presenten:**

a. Escrito en papel membretado, 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:

i. Acreditación de existencia legal: Nombre, domicilios y clave del Registro Federal de Contribuyentes; así como, en su caso, de su apoderado o representante. Tratándose de personas morales, se señalará descripción del objeto social de la empresa; número y fecha de las escrituras públicas en las que conste el acta constitutiva y, en su caso, sus reformas o modificaciones, señalando nombre, número y circunscripción del notario o

fedatario público que las protocolizó; así como fecha y datos de su inscripción en el registro público de comercio.

ii. Acreditación de la personalidad jurídica: número y fecha de las escrituras públicas en las que le fueron otorgadas las facultades para suscribir la propuesta, señalando nombre, número y circunscripción del notario o fedatario público que las protocolizó.

iii. Copia simple de la identificación oficial vigente con fotografía, tratándose de Personas Físicas y en el caso de Personas Morales copia simple de la identificación de la persona que firme las propuestas y del compareciente en el acto.

En el caso de que el licitante se encuentre inscrito y vigente en el Padrón de Proveedores, no será necesario presentar la información a que se refieren los incisos i, ii y iii de la fracción a) de este punto, sin eximir la obligación de presentar el escrito a que se refiere dicha fracción inciso a) haciendo alusión al escrito en papel membretado, 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 artículo 31, fracción IX de la Ley; además bastará únicamente con exhibir, como anexo al escrito la copia de la constancia vigente que así lo acredita como proveedor y citar en dicho escrito el número de inscripción en el Padrón de Proveedores. Adicionalmente, deberá de manifestar "Bajo protesta de decir verdad", en el mencionado escrito, que la información que proporcionó en el Padrón es cierta, veraz, oportuna y se encuentra actualizada. Favor de considerar los tiempos señalados en el artículo 353 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, para obtener la constancia, ya que de no contar con la constancia a la fecha señalada como límite para la inscripción el licitante deberá presentar toda la información y documentos solicitados en el inciso a) numerales i, ii y iii, de este punto.

b. Carta de aceptación de la convocatoria y de las bases del concurso.

c. Carta de validez de la propuesta

d. Carta de aceptación de la junta de aclaraciones.

e. Carta de cumplimiento a lo dispuesto en el artículo 49, fracción IX de la Ley de Responsabilidades Administrativas del Estado de Nuevo León, Persona física o moral según corresponda (cuyos modelos se adjuntan a las presentes bases.)

f. Copia del recibo oficial que acredite el pago de las bases.

g. Carta poder en caso de designar a una persona distinta al representante legal para la entrega de las propuestas.

5) JUNTA DE ACLARACIONES.

De conformidad con el artículo 34 de la Ley, se realizará la Junta de Aclaraciones, el día **23 de junio del 2022 a las 12:00 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 72, segundo párrafo del Reglamento de la Ley, por lo cual la inasistencia a la misma, no será causa de descalificación.

Las personas que manifiesten su interés en participar en la licitación pública mediante el escrito a que se refiere el segundo párrafo del artículo 34 de la ley y que se anexa a las presentes bases en el modelo de carta de interés en participar, serán consideradas licitantes y tendrán derecho a formular solicitudes de aclaración, mismas que deberán plantearse de manera concisa y estar directamente vinculadas con los puntos contenidos en la convocatoria de la presente licitación, indicando el numeral o punto específico con el cual se relaciona. **LA CARTA DE INTERÉS EN PARTICIPAR ASI COMO EL FORMATO DE PRESENTACIÓN DE PREGUNTAS, DEBERÁN PRESENTARSE A MÁS TARDAR EL DÍA 21 DE JUNIO DE 2022 A LAS 12:00 HORAS** de manera presencial por escrito, firmadas de manera autógrafa en papel membretado, indubitablemente acompañadas de la versión electrónica de las preguntas en formato como lo establece la Convocatoria (Word sin utilizar imágenes ni establecer contraseñas de formato), en USB.

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 párrafo anterior.

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.

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.

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 acta circunstanciada en la que hará constar los cuestionamientos y su respuesta, se señalarán los cambios acordados y que formarán parte integrante de la convocatoria; así como la fecha y hora del Acto de Presentación de Propuestas y Apertura Técnica. El acta será firmada por todos los participantes de la reunión para constancia y los efectos legales correspondientes. Se entregará una copia de dicha acta a los participantes que asistan.

Los participantes podrán recoger copia del acta 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.

6) REGISTRO DE PARTICIPANTES.

Previo a los actos a celebrarse en junta pública de la Licitación, los licitantes con intención de participar deberán presentarse de preferencia **AL MENOS UNA HORA ANTES** para su registro en el lugar y fecha señalados para la celebración de dichos actos, identificándose y firmando el registro de participación. En la inteligencia de que deberán obtener previamente su participación a la fecha y hora señaladas en el punto 4) de las presentes bases.

Cuando después de la publicación de la presente convocatoria, un licitante que aún no haya sido registrado en el Padrón solicite participar en la licitación, **sus propuestas estarán condicionadas al registro en el Padrón a más tardar el 30 de junio del 2022 a las 12:00 horas.**

7) ACREDITACIÓN DE LA PERSONALIDAD JURÍDICA.

Los licitantes deberán acreditar su existencia legal y su personalidad jurídica, mediante la presentación de la documentación legal, que así lo acredite de conformidad con el punto 4 inciso a) numeral i, ii de las presentes bases.

Los interesados deberán de igual forma proporcionar en el documento solicitado en el punto 4 incisos a) numeral i y ii de las presentes bases, al menos una dirección de correo electrónico, preferentemente del representante legal, mismo que servirá para realizar notificaciones oficiales derivadas de los actos del presente procedimiento.

8) REQUISITOS QUE DEBERÁN CUMPLIR LOS LICITANTES AL MOMENTO DE LA PRESENTACIÓN Y APERTURA DE PROPUESTAS.

a. PROPUESTA TÉCNICA.

i. Documento elaborado en papel membretado de la concursante, firmado de manera autógrafa por la persona física o por el representante legal de la empresa, donde manifieste “Bajo protesta de decir verdad”, que es de nacionalidad mexicana y, que los productos que entregará, contarán con el porcentaje de contenido nacional correspondiente. Asimismo, manifestará 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 productos ofrecidos son de producción nacional y cumplen con el porcentaje de contenido nacional requerido, de conformidad con el artículo 57 del Reglamento de la Ley.

ii. Documento elaborado en papel membretado de la concursante, firmado de manera autógrafa por la persona física o por el representante legal de la empresa, donde manifieste “Bajo protesta de decir verdad”, que no se encuentran bajo ninguno de los supuestos de los artículos 37 y 95 de la Ley.

iii. Documento elaborado en papel membretado de la concursante, firmado de manera autógrafa por la persona física o por el representante legal de la empresa, donde manifieste “Bajo protesta de decir verdad”, que los licitantes que sean personas morales cuentan con una política de integridad. En el caso de que los licitantes 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.

iv. Documento elaborado en papel membretado de la concursante, firmado de manera autógrafa por la persona física o por el representante legal de la empresa, donde manifieste “Bajo protesta de decir verdad”, que se abstendrá por sí o a través interpósita persona, de adoptar conductas para que los servidores públicos de la Dirección de Adquisiciones induzcan o alteren la evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que le pueden otorgar condiciones más ventajosas con relación a los demás participantes, de conformidad con el artículo 131 fracción VI inciso f) del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León.

v. Documento elaborado en papel membretado de la concursante, firmado de manera autógrafa por la persona física o por el representante legal de la empresa, donde manifieste “Bajo protesta de decir verdad”, que han determinado su propuesta de manera independiente, sin consultar, comunicar o acordar con ningún otro participante, además deberán manifestar que conocen las infracciones y sanciones aplicables, en caso de cometer alguna práctica prohibida por la Ley Federal de Competencia Económica, de conformidad con el artículo 31, fracción XIII de la Ley.

vi. Documento elaborado en papel membretado de la concursante, firmado de manera autógrafa por la persona física o por el representante legal de la empresa, donde manifieste “Bajo protesta de decir verdad” que cumplen con las obligaciones de acuerdo a lo dispuesto en el artículo 32-D del Código Fiscal de la Federación, debiendo de adjuntar documento vigente generado por el SAT en el que se emita la opinión del cumplimiento de obligaciones fiscales en sentido positivo, cuando menos del mes inmediato anterior a la publicación.

vii. A efecto de garantizar que el licitante cuenta con la experiencia y capacidad necesaria para el suministro de los productos objeto de la presente licitación, éste deberá acreditar dicha experiencia y capacidad, mediante la presentación de copia de 3-tres facturas electrónicas expedidas a favor de dependencias oficiales o particulares, con antigüedad mayor a 11 meses a la fecha de la presentación y

apertura de propuestas, deberán estar legibles, coincidir con el objeto de la licitación y cumplir los requisitos establecidos en el artículo 17D penúltimo párrafo y artículo 29A del código fiscal de la federación. Deberán adjuntar la impresión de la validación de cada factura emitida por la página oficial del SAT en estado VIGENTE para constatar la veracidad de las mismas.

viii. Documento elaborado en papel membretado de la concursante, firmado de manera autógrafa por la persona física o por el representante legal de la empresa, donde manifieste "Bajo protesta de decir verdad", que, en caso de resultar adjudicado, cuenta con capacidad de brindar de manera inmediata los productos requeridos, y que bajo ninguna circunstancia cederá, ni subcontratará los compromisos contraídos como resultado de esta Licitación Pública Nacional Presencial.

ix. Documento elaborado en papel membretado de la concursante, firmado de manera autógrafa por la persona física o por el representante legal de la empresa, donde manifieste "Bajo protesta de decir verdad", el domicilio o domicilios del establecimiento y las sucursales con las que cuentan, deberán indicar claramente la calle número exterior y/o interior, Colonia, Municipio y teléfono del establecimiento, así como los días y horarios de atención; en el mismo escrito deberá manifestar que cuenta con un domicilio en el Estado de Nuevo León, deberá proporcionarlo y acreditarlo como domicilio para efectos de oír y recibir notificaciones, lo anterior de conformidad con el artículo 361 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León.

x. Documento elaborado en papel membretado de la concursante, firmado de manera autógrafa por la persona física o el representante legal de la empresa concursante, "Bajo protesta decir verdad" que describa íntegramente su Propuesta Técnica debidamente llenado cada campo solicitado y preparada en base a los **Anexo 1. "Requerimientos generales para licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados; Anexo A. Requerimientos de productos, Anexo B. Requerimientos de instalación y configuración de los productos, Anexo C. Requerimientos de soporte, Anexo D. Requerimientos de servicios administrados, Anexo E. Características y/o capacidades de todos los productos.** De igual manera esta información deberá presentarla en archivo electrónico en formato editable en un CD o USB.

xi. Presentar la siguiente documentación en original y hoja membretada del fabricante firmado de manera autógrafa, dirigida al municipio:
- Carta del fabricante de seguridad Web señalando que el participante es distribuidor autorizado.
- Carta del fabricante de Previsión de Fuga de Información señalando que el participante es distribuidor autorizado.
- Carta del fabricante de Firewall de bases de datos señalando que el participante es distribuidor autorizado
- Carta del fabricante de SIEM (correlacionador de eventos) señalando que el participante es distribuidor autorizado.

· Carta del fabricante del Previsor de intrusos de red señalando que el participante es distribuidor autorizado.
· Carta del fabricante de Sandbox para endpoint señalando que el participante es distribuidor autorizado
· Carta del fabricante de antivirus y EDR señalando que el participante es distribuidor autorizado.

xii. Presentar documentación en original y hoja membretada del fabricante firmado, dirigida al municipio, en la cual se mencione que el participante es distribuidor autorizado de:
· McAfee
· Forcepoint
· Checkpoint

xiii. Documento elaborado en papel membretado de la licitante, firmado de manera autógrafa por la persona física o por el representante legal de la empresa licitante, “Bajo protesta de decir verdad”, en donde se compromete a aceptar revisiones durante el proceso licitatorio o en caso de salir adjudicado, durante la vigencia del contrato por verificadores municipales dentro de sus instalaciones, cada vez que el municipio lo estime necesario.

xiv. Documento elaborado en papel membretado de la licitante, firmado de manera autógrafa por la persona física o por el representante legal de la empresa licitante, donde manifieste “Bajo protesta de decir verdad”, que no cuenta con proceso administrativo iniciado por incumplimiento de contrato; así como tampoco se le haya notificado la recisión de un contrato, ya sea por un particular, o por autoridad federal, estatal o municipal, que cuenta con sentencia ya ejecutoriada.

Cada uno de los documentos que integren la propuesta y aquellos distintos a esta, deberán estar 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, 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 la propuesta económica son esenciales, la omisión de cualquiera de ellos no podrá subsanarse, y será motivo de desechamiento de la propuesta.

b. **DOCUMENTOS QUE DEBE CONTENER 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 preparada en base al **Anexo 2. “Cotización".** De igual manera esta información deberá presentarla en archivo electrónico en formato editable en un USB.

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 económica**, (Monto total durante la vigencia del contrato) incluyendo el Impuesto al Valor Agregado. Tratándose de cheque este podrá ser certificado o de caja de cuenta de banco nacional, deberá cumplir con lo estipulado en el artículo 199 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.

iii. Presentar la última declaración fiscal anual (2021), a fin de acreditar que cuenta con capacidad económica para cumplir las obligaciones que se deriven del contrato correspondiente, en donde se demuestre que sus ingresos son superiores al 10% del monto total de su oferta. Así mismo deberá adjuntar la última declaración fiscal provisional del impuesto sobre la renta que le corresponda al ejercicio (abril 2022) y/o su acuse de recibo.

Cada uno de los documentos que integren la propuesta y aquellos distintos a esta, deberán estar 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.

Cada uno de los documentos que integren la propuesta y aquellos distintos a esta, deberán estar 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, 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 la propuesta económica son esenciales, la omisión de cualquiera de ellos no podrá subsanarse, y será motivo de desechamiento de la propuesta.

9) DOCUMENTACIÓN DISTINTA A LAS PROPUESTAS.

La documentación distinta a las propuestas, podrá entregarse, a elección del licitante, dentro o fuera del sobre que la contenga.

10) PROPUESTAS INDIVIDUALES.

Los licitantes interesados en participar en el presente procedimiento, solo podrán presentar una sola proposición, motivo por el cual no se aceptarán propuestas conjuntas.

11) FORMA DE ENTREGA DE LAS PROPUESTAS.

Los participantes deberán presentar su propuesta técnica y económica, de acuerdo a lo establecido en el punto 12 y 13 de la presente convocatoria.

Cada uno de los documentos que integren las propuestas y aquellos distintos a esta, deberán estar foliados en todas y cada una de las hojas que los integren, deberán numerar de manera individual la propuesta técnica y económica, además deberán estar firmados por la persona que cuente con el poder para actos de administración y/o dominio.

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

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

El acto de presentación y apertura de los sobres que contienen las propuestas técnicas, se celebrará el día **01 de julio del 2022 a las 12:00 horas**, en la Sala de Juntas del domicilio de la Unidad Convocante, debiendo presentar sus propuestas técnica y económica, en **DOS SOBRES,** uno para cada propuesta, cerrados y sellados con cinta adhesiva, rotulados cada uno de ellos con la siguiente información: Nombre de la concursante, Clave alfanumérica del concurso de que se trata e indicación de la propuesta a que se refiere (técnica o económica). La asistencia a este acto es de **CARÁCTER OBLIGATORIO** para los participantes y su inasistencia será motivo de descalificación.

Se deberá considerar lo siguiente:

a. Se llevará a cabo en acto público y 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 Ley y su Reglamento.
b. Previo al inicio del acto y con al menos una hora de anticipación los licitantes que acudan podrán registrarse hasta la hora señalada para el inicio del acto, se cerrará el recinto donde se llevará a cabo el acto de presentación y apertura de propuestas, dándose inicio al evento.
c. Se pasará lista de asistencia a los licitantes y demás funcionarios presentes.
d. Se recibirán las propuestas técnica y económica, así como la documentación complementaria.
e. Se procederá a la apertura del sobre cerrado que contiene la propuesta técnica de cada participante, haciéndose constar la documentación presentada.
f. Se verificará cuantitativamente que las propuestas técnicas cumplan con los requisitos exigidos en estas bases, y las que omitan uno o más requisitos se señalará en el acta correspondiente. Los licitantes que hayan asistido, en forma conjunta con los servidores públicos designado rubricará las propuestas técnicas y económicas recibidas, incluidos los de aquellos cuyas propuestas hubieren sido desechadas, quedando en custodia de la propia convocante.
g. En este acto la revisión de la documentación se efectuará en forma cuantitativa, sin entrar al análisis detallado de su contenido, el cual se realizará durante el proceso de evaluación de la propuesta.

h. Los sobres que contienen la propuesta económica pasarán a ser firmados por cada uno de los presentes y quedarán en custodia de la convocante.
i. En el caso de propuestas desechadas o descalificadas, la convocante se quedará con toda la documentación técnica que recibió para archivo del concurso.
j. Se levantará el acta correspondiente al Acto de Presentación de Propuestas y Apertura Técnica en la que se harán constar las propuestas recibidas, así como las que hubieren sido desechadas o descalificadas y las omisiones de documentación por las que se desecharon y descalificaron.
k. El acta será firmada por todos los presentes 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 y eficacia jurídica del acta en cuestión.
l. La convocante realizará la revisión detallada y cualitativa de las Propuestas Técnicas recibidas y aceptadas, para estar en posición de dar un fallo de la fase técnica, el cual se dará a conocer en el Acto de Fallo Técnico y Apertura Económica.
m. Si no se recibe ninguna propuesta o todas las presentadas fueren desechadas o descalificadas, se declarará desierto el concurso, haciéndose constar esta circunstancia en el acta correspondiente.

13) ACTO DE FALLO TÉCNICO Y APERTURA DE PROPUESTA ECONÓMICA.

El acto de fallo técnico y apertura de los sobres que contienen las propuestas económicas, se celebrará el día **05 de julio del 2022 a las 12:00 horas**, en la Sala de Juntas del domicilio de la Unidad Convocante. Se deberá 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 Ley y su Reglamento.
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 revisión cualitativa de la documentación técnica, mencionándose a cada una de las 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.
e. 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 del concurso.
f. El funcionario que presida el acto, leerá en voz alta, cuando menos, los montos totales de cada inciso de las propuestas admitidas, las cuales deberán ser firmadas por todos los participantes del evento para constancia de la legalidad del concurso.

g. 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, así como los hechos para módulo al aire libre relevantes.
h. 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 y eficacia jurídica del acta en cuestión.
i. La concursante que retire sus propuestas una vez iniciado el acto de apertura, perderá su garantía de seriedad de la propuesta.
j. 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.

14) ACTO DE FALLO

Se llevará a cabo en acto público el día **11 de julio del 2022 a las 12:00 horas**, en la Sala de Juntas del domicilio de la Unidad Convocante, por el cual se dará a conocer el fallo de la licitación, a la que libremente podrán asistir los licitantes que hubieren presentado proposición, procediéndose de acuerdo a lo siguiente:

a. Se declarará iniciado el acto.
b. Se presentará lista de asistencia a los licitantes y a los servidores públicos asistentes.
c. Se dará lectura al fallo al que se haya llegado, en el que se hará constar una reseña cronológica de los actos del procedimiento de licitación, el análisis de las propuestas y las razones para admitirlas o desecharlas.
d. Los licitantes que se encuentren presentes en el acto de fallo, se darán por notificados del mismo y de las adjudicaciones efectuadas.
e. La omisión de la firma de algún licitante no invalidará el contenido y efectos del acta.
f. Se levantará el acta del evento la cual será firmada por los servidores públicos y licitantes asistentes, a quienes se les entregará copia de la misma.
g. Asimismo, en este acto se notificará al licitante adjudicado el lugar, fecha y hora en el que formalizará el contrato respectivo.
h. 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.

Notificado el fallo serán exigibles las obligaciones establecidas en las presentes bases, obligándose la dependencia y al licitante adjudicado a formalizar el contrato respectivo en la fecha establecida en la presente convocatoria.

15) PERIODO DE VALIDEZ DE LA PROPOSICIÓN.

Una vez presentadas las propuestas en la fecha, hora y lugar establecidos para el acto de presentación de propuestas y apertura técnica, éstas no podrán ser retiradas o dejarse sin efecto.

16) VERIFICACIÓN Y SUPERVISIÓN.

La Unidad Convocante se reserva el derecho de verificar en cualquier momento la información presentada por los licitantes, así como de visitar el local donde se ubica el domicilio de los participantes, durante el desarrollo del concurso y la vigencia del contrato. Asimismo, tendrá el derecho de recurrir a otras instancias o referencias para certificar que este cuenta con la solidez, conocimientos y experiencia necesarios para la prestación del servicio.

17) CRITERIOS DE EVALUACIÓN DE LAS PROPUESTAS Y ADJUDICACIÓN DEL CONTRATO.

El criterio de evaluación será por la oferta económica presentada donde la Unidad Convocante, previa opinión del Comité de Adquisiciones adjudicará el contrato al licitante que reúna las mejores condiciones legales, técnicas y económicas y que garantice satisfactoriamente el cumplimiento de las obligaciones respectivas.

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, N.L.

La asignación será por lote, cumpliendo con los alcances y especificaciones señaladas en cada uno de los anexos.

18) CONTRATO

a. El licitante que resulte adjudicado, deberá entregar de manera inmediata a la convocante, original o copia certificada para su archivo de los documentos siguientes:

i. Constancia de Situación Fiscal (RFC) actualizada.
ii. Copia de Acta constitutiva y en su caso modificaciones a la misma (tratándose de personas morales).
iii. Escritura Pública del poder notarial del representante.
iv. Copia de Comprobante de domicilio (no mayor a tres meses).
v. Copia de Identificación Oficial vigente.
vi. Copia de la CURP para el caso de personas físicas.
vii. Copia de la Constancia de la política de integridad o compromiso de implementación.

viii. Copia de la Constancia de curso de prevención de corrupción.

b. El contrato se formalizará por el participante adjudicado, dentro de los diez días hábiles siguientes al de la adjudicación. No obstante, lo anterior, en aquellos casos en los cuales la Dirección de Adquisiciones así lo determine, podrá ampliarse dicho plazo para la formalización del contrato, sin que la ampliación pueda ser superior a los treinta días hábiles, según lo establecido en el artículo 264 del Reglamento, la firma del contrato se realizará en el domicilio de la Dirección de Adquisiciones, ubicado en el Domicilio de la Licitante, en un horario comprendido de lunes a viernes de 8:00 a 16:00 horas.

c. **La vigencia del contrato será a partir del 11 de julio del 2022 al 06 de julio del 2025.**

19) GARANTÍAS.

a. **GARANTÍA DE SERIEDAD DE LA PROPUESTA.**

A fin de garantizar la seriedad de la propuesta, los concursantes DEBERÁN ENTREGAR DENTRO DEL SOBRE que contiene su propuesta económica 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 económica**, incluyendo el Impuesto al Valor Agregado. Tratándose de cheque este podrá ser certificado o de caja de cuenta de banco nacional, deberá cumplir con lo estipulado en el artículo 199 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.

b. **GARANTÍA DE CUMPLIMIENTO DE CONTRATO.**

El licitante adjudicado deberá garantizar el debido cumplimiento de las obligaciones que se deriven del contrato, mediante fianza emitida por una institución de fianzas debidamente constituida en los términos de la Ley de Instituciones de Seguros y de Fianzas. Dicha fianza deberá ser presentada a más tardar dentro de los 10 días naturales siguientes a la formalización del contrato, junto con la copia del recibo de pago de la misma, salvo que la entrega de los bienes se realice dentro del citado plazo y por un importe equivalente al 10% del monto total del contrato, incluido el Impuesto al Valor Agregado. Lo anterior en cumplimiento en lo dispuesto en el artículo 106 del Reglamento de la Ley.

La fianza deberá contener, además de lo señalado en las cláusulas que la Ley Federal de Instituciones de Fianzas; las siguientes declaraciones:

i. Que se otorga a favor del Municipio de San Pedro Garza García, Nuevo León.

ii. Que la fianza se otorga para garantizar todas y cada una de las estipulaciones contenidas en el contrato producto de la **Licitación Pública Nacional Presencial** número **SA-DA-CL-26/2022**, relativa a la **"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"**

iii. Que la garantía de cumplimiento estará vigente por un mínimo de seis meses después de que los bienes o servicios materia del contrato 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. Lo anterior de conformidad con lo establecido en el artículo 259 fracc. I, del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León.

20) APLICACIÓN DE GARANTÍAS.

a. **GARANTÍA DE SERIEDAD DE LA PROPUESTA.**

Se podrá hacer efectiva la garantía de seriedad de la propuesta económica cuando:

i. El concursante retire su propuesta una vez iniciado el acto de presentación de propuestas y apertura técnica.
ii. La adjudicataria no firme el contrato correspondiente dentro del plazo señalado.
iii. Cuando la adjudicataria no entregue la fianza de cumplimiento de contrato dentro de los 10 días naturales posteriores al inicio de la vigencia del contrato.
iv. Cuando se falseen datos o información proporcionada a la Unidad Convocante, con motivo del presente concurso.

b. **GARANTÍA DE CUMPLIMIENTO DE CONTRATO.**

Se podrá hacer efectiva la garantía de cumplimiento de contrato cuando la adjudicataria:

i. No cumpla con el suministro y/o servicios conforme a lo establecido en las presentes bases.
ii. Incumpla con cualquiera de las obligaciones establecidas en el contrato correspondiente al presente concurso.
iii. Se rescinda administrativamente el contrato, considerando la parte proporcional al monto de las obligaciones incumplidas.

21)DEVOLUCIÓN DE GARANTÍAS.

a. GARANTÍA DE SERIEDAD DE LA PROPUESTA.

El municipio podrá proceder a la devolución de la garantía de seriedad de la propuesta a partir de la fecha de notificación del fallo, previa solicitud por escrito de los participantes que no resulten adjudicados; en caso de resultar adjudicado, la devolución de la garantía de seriedad de la propuesta estará sujeta a la presentación y verificación de la garantía de cumplimiento del contrato.

b. GARANTÍA DE CUMPLIMIENTO DE CONTRATO.

El municipio dará al proveedor su autorización, para que este pueda cancelar la fianza correspondiente a la garantía de cumplimiento del contrato, previa solicitud por escrito de la adjudicataria en el momento que demuestre plenamente haber cumplido con la totalidad de las obligaciones establecidas en el contrato.

22) GARANTÍA POR DEFECTOS DE FABRICACIÓN Y VICIOS OCULTOS.

Los licitantes deberán considerar que los productos que ofrecen deberán contar con las garantías de acuerdo a lo siguiente: La adjudicataria se obliga a responder, de cualquier responsabilidad derivada de los bienes y servicios; de la misma manera se comprometen a solucionar cualquier problema que se presente, con la colaboración de la Unidad Convocante.

23) DEL PLAZO, LUGAR Y CONDICIONES DE LA ENTREGA DE LOS PRODUCTOS.

a. La adjudicataria deberá de entregar lo solicitado en el Anexo 1 “Especificaciones Técnicas”, a más tardar a los 60 días naturales contados a partir de la fecha de la notificación del fallo de adjudicación y el tiempo de operación de cada una de las Licencias será por 3 años a partir de la fecha de su vencimiento.

b. El servicio se entregará en la Dirección de Tecnologías, con el Ing. Daniel Oscar Dares de León en Corregidora 507 Centro, C.P. 66200 San Pedro Garza García, N.L. teléfono 81-8400-45-95.

c. La vigencia del contrato será a partir del 11 de julio del 2022 al 06 de julio del 2025.

24) ANTICIPOS.

Para la presente licitación no se otorgarán anticipos.

25) CONDICIONES DE PAGO.

a. El precio ofrecido en la propuesta económica se toma como precio fijo y no se reconocerá ningún aumento.

b. El pago del contrato se hará de forma mensual para el rubro de la operación de servicios administrados y en un solo pago para la adquisición de licenciamientos y suscripciones.

c. Los pagos se efectuarán a los 8 (ocho) días hábiles posteriores al ingreso del trámite de pago en la Secretaría de Finanzas y Tesorería Municipal. La factura deberá contener el sello de recibido, con los datos del funcionario autorizado para tal efecto, deberá adjuntar folio de surtido, generado por el sistema al momento de recibir los bienes objeto de la licitación, La factura deberá contener el sello de recibido, con los datos del funcionario autorizado para tal efecto, deberá adjuntar folio de surtido, generado por el sistema al momento de recibir los bienes objeto de la licitación, así como la validación de la misma. En caso de resultar adjudicado, se le indicará la forma de validación de sus facturas.

d. El área usuaria es la responsable de realizar en los tiempos establecidos el trámite de pago ante la Tesorería Municipal.

26) IMPUESTOS Y DERECHOS

Los impuestos y derechos que procedan con motivo de la adquisición de los productos y servicios objeto de esta licitación, serán pagados por el proveedor. El municipio solo pagará lo correspondiente al Impuesto al Valor Agregado.

27) DESCALIFICACIÓN DE LOS LICITANTES.

Se descalificará a los licitantes que incurran en una o varias de las siguientes situaciones:

a. Que no cumplan con cualquiera de los requisitos establecidos en estas bases que afecten la solvencia de la propuesta o los que se deriven del acto de aclaración del contenido de las bases.

b. Cuando no acuda representante alguno al Acto de presentación de propuesta técnica y económica y apertura de propuesta técnica, toda vez que la asistencia a este acto es de carácter obligatorio.

c. Cuando se compruebe que tiene acuerdo con otro u otros licitantes para elevar precio de los productos y/o servicios solicitados, o cualquier otro acuerdo que tenga como fin obtener una ventaja sobre los demás licitantes.
d. Cuando presenten propuestas en idioma diferente al español.

e. Cuando presenten documentos alterados o apócrifos.

f. Cuando se compruebe que el licitante no cuenta con la capacidad de producción o con el respaldo del fabricante para garantizar el suministro de los productos y/o servicios ofrecidos.

g. Cuando incurran en cualquier violación a las disposiciones de la Ley, al Reglamento o a cualquier otro ordenamiento legal en la materia.

h. Cuando el licitante haya celebrado contrato con el municipio, independientemente que éste se encuentre o no vigente y haya antecedentes de incumplimiento del contrato.

28) CANCELACIÓN DE LICITACIÓN.

La Dirección de Adquisiciones, podrá cancelar la licitación, debiendo notificar por escrito a todos los involucrados en los siguientes casos.

a. Por caso fortuito o por causas de fuerza mayor.

b. Cuando existan circunstancias, debidamente justificadas, que provoquen la extinción

de la necesidad para adquirir los productos y/o servicios, o que de continuarse con el procedimiento se pueda ocasionar daños o perjuicios al municipio.

29) DECLARACIÓN DE LICITACIÓN DESIERTA.

La Dirección de Adquisiciones podrá declarar desierta la licitación cuando:

a. Ningún interesado adquiera las presentes bases.

b. Si no se recibe propuesta alguna en el acto de presentación de propuestas y apertura técnica.

c. Si las propuestas presentadas no reúnen los requisitos establecidos en las bases de la licitación.

d. Cuando las propuestas económicas, rebasen el monto autorizado para la adquisición de los productos y/o servicios objeto de la presente licitación.

e. Cuando la mejor propuesta sea presentada por una empresa que tenga antecedentes de incumplimiento con el municipio.

De materializarse cualquiera de los supuestos anteriores, la Unidad Convocante podrá proceder, a celebrar una nueva licitación, o bien, cuando proceda, cualquiera de los demás procedimientos de contratación previstos en la ley de conformidad con el artículo 74, fracción XIII del Reglamento de la Ley.

30) SUSPENSIÓN POR CONTINGENCIA.

Para el caso de que en el presente proceso de licitación se presentara alguna disposición oficial emitida por autoridad competente en el sentido de declarar cualquier tipo de suspensión que afecte el desahogo del presente proceso, esta se acatará y se suspenderá, hasta en tanto no se declare la terminación correspondiente que permita reiniciar dicho proceso.

31) IMPLEMENTACIÓN.

La Unidad Requirente será la única responsable directo de verificar que los productos y/o servicios proporcionados por el proveedor cumplan con las calidades, cualidades y cantidades establecidas en las bases del concurso, en el contrato, ello en razón de que es el único que cuenta con el personal calificado técnicamente para verificar dichas circunstancias, asimismo deberá emitir los documentos necesarios para hacer constar fehacientemente dichas situaciones o circunstancias de la Secretaría de Finanzas y Tesorería Municipal para el trámite.

La Unidad Requirente deslinda en todo momento a la unidad convocante de cualquier responsabilidad derivada del suministro de los productos y/o servicios. Lo anterior en términos de lo señalado en el artículo 237 del Reglamento de Adquisiciones,

Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, Nuevo León.

32) INCONFORMIDADES, CONTROVERSIAS Y SANCIONES.

Se podrá interponer inconformidades de acuerdo a lo dispuesto en el Capítulo VIII, artículo 79 de la Ley, en el domicilio de la Unidad Convocante.

33) CONTROVERSIAS.

Las controversias que se susciten con motivo de la interpretación o aplicación de la Ley, de estas bases o de los contratos que se deriven de la presente licitación serán solucionadas en atención a lo estipulado en el artículo 89 de la Ley.

34) SANCIONES.

Los proveedores o participantes que infrinjan las disposiciones contenidas en esta Ley serán sancionados por la Contraloría del Estado o por el órgano de control interno de los sujetos señalados en el artículo 1, fracciones II a V. Ateniendo a la gravedad de la falta y a la existencia de dolo o mala fe, las sanciones podrán ir desde el apercibimiento hasta la inhabilitación o la multa.

35) PENA CONVENCIONAL.

Se aplicará una pena convencional a la adjudicataria por atraso en la entrega de los bienes y/o servicios, por causas imputables al proveedor, para lo que una vez que el municipio le comunique la incidencia presentada en la prestación del servicio y en caso de no ser atendida en los términos señalados en el punto Tiempos de atención y niveles de servicio descrito en el anexo 1 de las presentes bases, se hará acreedor a la aplicación de penalizaciones de acuerdo a la siguiente tabla.

TABLA DE PENALIZACIONES	
Incidencias de no cumplimiento con los niveles de servicio especificados en este documento.	Penalidad
0-1 incidencias	Sin penalidad
2-4 incidencias	3% de penalidad del pago mensual
5-9 incidencias	5% de penalidad del pago mensual
10 o más incidencias	10% de penalidad del pago mensual

Mismas que serán deducidas de las facturas pendientes por pagar a la adjudicataria, independientemente de que la Unidad Convocante opte por hacer efectiva la garantía de cumplimiento de contrato otorgada.
En el supuesto que sea rescindido el contrato, no procederá la contabilización, de la

sanción por cancelación a que hace referencia el párrafo anterior, toda vez que se deberá hacer efectiva la garantía de cumplimiento, de acuerdo a lo establecido en el artículo 99 del Reglamento de la Ley.

36) RESCISIÓN Y TERMINACIÓN ANTICIPADA DEL CONTRATO.

La Dirección de Adquisiciones rescindirá administrativamente siguiendo los lineamientos establecidos en el artículo 111, del Reglamento de la Ley.

37) TERMINACIÓN ANTICIPADA DEL CONTRATO.

La Dirección de Adquisiciones podrá dar por terminado anticipadamente el contrato, de acuerdo a lo establecido en el artículo 114 del Reglamento de la Ley.

38) NO NEGOCIACIÓN DE CONDICIONES

Bajo ninguna circunstancia podrán ser negociadas las condiciones estipuladas en estas bases y sus anexos o en las propuestas presentadas por los licitantes, de acuerdo a lo estipulado en el artículo 59, Fracc. I. inciso h) del Reglamento de la Ley.

39) SITUACIONES NO PREVISTAS EN LAS CONVOCATORIA.

Cualquier situación que no haya sido prevista en la presente convocatoria y sus anexos, será resuelta por la Dirección de Adquisiciones escuchando la opinión de las autoridades competentes, con base en las atribuciones establecidas en las disposiciones aplicables.

40) COMPETENCIA

Asimismo, para la interpretación o aplicación de estas bases, sus anexos o del contrato que se celebre, en lo no previsto en tales documentos se estará a lo dispuesto en la Ley, Reglamento de la Ley, y Reglamento Adquisiciones, Arrendamientos y Contratación de Servicios para el Municipio de San Pedro Garza García, N.L. y demás disposiciones legales vigentes en la materia.

San Pedro Garza García, Nuevo León, a 15 de junio del 2022
Ing. Carlos Romanos Salazar
Director de Adquisiciones
Rúbrica

MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN
Secretaría de Administración
Dirección de Adquisiciones

Concurso por Licitación Pública Nacional Presencial No. SA-DA-CL-26/2022
"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

OBJETO DEL CONTRATO: Suministro de servicio Administrado Compartido de hardware, licencias y suscripciones de seguridad informática con soporte de fabricante y proveedor local para nuestra infraestructura informática de equipo de cómputo y 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 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 DE SERVICIOS DE INGENIERÍA ESTRATÉGICA DE PROTECCIÓN CONTRA:

- Intrusos accediendo al Portal Oficial y/o páginas públicas del Municipio con el fin de modificarlas o dañarlas
- Ataques desde archivos consultados o bajados desde Internet
- Ataques desde archivos bajados desde correos electrónicos oficiales y no oficiales
- Intrusos accediendo a la red interna con el fin de dañar aplicaciones y/o servidores
- Intrusos accediendo a Bases de Datos con el fin de afectar, dañar o robar información confidencial sensible
- Ataques a la infraestructura de red mediante saturación accesos
- Protección contra daños de nuevos virus, nuevas versiones o variantes de ellos
- Secuestro de información de pc's del Municipio (ransomware)
- Ataques que afecten los sistemas con que se opera en el Municipio
- Código maligno (Malware) en las pc's que afecten la operación diaria
- Código maligno (Malware) para infiltrarse e intentar robar información o identidades (claves de acceso)

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

GENERALES

El servicio de monitoreo son 5x8 con al menos una junta semanal informativa de hechos, así como juntas de emergencias en caso de eventos extraordinarios y servicios de soporte 7x24.

Al menos un ingeniero en sitio de lunes a viernes en horario de 8 am a 4 pm

La Empresa es 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 ser atendido y en su caso canalizar la llamada de forma inmediata con un ingeniero certificado. Deberá proporcionarse una forma de contacto para eventos de emergencia en horas no hábiles.
LUGAR DE PRESTACIÓN DEL SERVICIO O ENTREGA DE BIENES: El servicio se entregará en la Dirección General de Tecnologías, con el Ing. Daniel Oscar Dares de León en Corregidora 507 Centro, C.P. 66200 San Pedro Garza García, N.L. teléfono 81-8400-45-95.
CRONOGRAMA DE ACTIVIDADES Y FECHAS DE ENTREGA: El período del contrato es del 07 de julio de 2022 al 06 de julio de 2025.
ENTREGABLES 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 vía correo electrónico:
- 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 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 su 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 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 éstos 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 liberación de los Servicios Contratados, el equipo de soporte del proveedor comenzará con la administración de los servicios 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.

Gestión de Incidentes

El equipo de soporte técnico atenderá los incidentes generados por parte de MUNICIPIO DE SAN PEDRO conforme al siguiente proceso:

A cada incidente, la Mesa de Servicio le asignará una prioridad para cumplir con los requerimientos y expectativas de usuario, respetando los criterios de impacto y urgencia. Esta prioridad facilitará la atención de incidentes y escalonar 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

ATENTAMENTE

_____

Nombre y firma de la persona física o representante legal

MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN
Secretaría de Administración
Dirección de Adquisiciones

Concurso por Licitación Pública Nacional Presencial No. SA-DA-CL-26/2022
"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

ANEXO A. REQUERIMIENTOS DE PRODUCTOS

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

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.

Los sitios a considerar 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 ANEXO D	DESCRIPCIÓN GENERAL DE LAS CAPACIDADES DE LA TECNOLOGÍA	CANTIDAD
1	PLATAFORMA DE SEGURIDAD PARA LA NAVEGACIÓN, LAS APLICACIONES SAAS, LA FUGA DE INFORMACIÓN, LA CLASIFICACIÓN DE INFORMACIÓN Y EL ACCESO Que sea una plataforma unificada administrada desde la nube y/o en sitio con capacidades de clasificación de información para las computadoras, previsión de fuga de información para las computadoras y la navegación web, "Cloud Access Security Broker" y Control de acceso con el mínimo privilegio (Zero Trust Network Access). La clasificación de la información en "el origen", es decir, que tenga la posibilidad de clasificar la información cuando se genera "tenga la capacidad"	
1.1	**Control en la navegación y seguridad web** Que cuente con capacidades de filtrado de contenido basado en uso de un proxy con capacidad de control de navegación basado en categorías web, control de acceso basado en riesgos o "shadow IT", "remote browser isolation" al menos para sitios maliciosos, control de acceso a "tenants" propios del municipio, limitando el acceso a otros, Previsión de Fuga de Información en el canal web. Que pueda ser instalado en dispositivos en PCs, Mac y dispositivos móviles con sistema operativo IOS y Android	**1200**

1.2	**Previsión de Fuga de Información en las computadoras y clasificación de información** El módulo de data loss prevention cuente con capacidades de: clasificación en el origen, identificación y contención de fuga de información en los canales de USB, impresión, email, web, aplicaciones de mensajería, impresión de pantalla	**1200**
1.3	**"Cloud Access Security Broker"** Que el "Cloud Access Security Broker" (CASB) se pueda integrar a través de una API o como un proxy reverso o con un agente. Que cuente con agentes para PCs y Mac, así como para dispositivos móviles IOS y Android. Que cuente con un módulo para el análisis de comportamiento de los usuarios. Que a través de API pueda tener visibilidad de todas las actividades de los usuarios y la información en todas las aplicaciones en la nube gestionadas vía SaaS y que tenga la capacidad de reaccionar en caso de una amenaza y que pueda controlar los accesos haciendo el uso de los agentes, como proxy inverso o através de un tercero que maneje la identidad de los usuarios. Es muy importante que pueda acotar la actividad en todas las herramientas de colaboración relacionadas a Google Enterprise	**1200**
1.4	**Control de acceso a la red con el mínimo privilegio** Que sea parte preferentemente de la misma plataforma con la capacidad de proveer acceso micro segmentado a cualquier protocolo que use cualquier puerto TCP, que al menos tenga la capacidad de ofrecer una autenticación de doble factor y pueda revisar en la postura previo a la validación la existencia de un antivirus ejecutándose. Asimismo que requiera de un gateway que preferentemente NO requiera ser publicado por el firewall	**1200**
2	**PLATAFORMA ANTIMALWARE** 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 señalen la presencia de malware en el ambiente y que señale los mecanismos de afectación basados en el marco de Mitre	**1200**
2.2	**Antimalware con antiransomware y parcheo virtual** Que cuente con un módulo específico antiransomware 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 que soporte los sistemas operativos Windows, Linux Ubuntu y Debian	**1200**
2.3	**Control de dispositivos periféricos en las computadoras**	**1200**

	Que cuente con el control de dispositivos periféricos en los sistemas operativos Windows y Mac, de tal modo que les detecte asi como 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, CD/DVDs, 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	**70**
2.5	**Control de aplicaciones para computadoras** Que cuenta 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 si se pueda 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	**1200**
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	**1200**
2.7	**EDR para Computadoras** Que cuente con un EDR que soporte sistemas operativos Windows, que además cuente con la capacidad de ofrecer investigaciones guiadas. Que retenga la información para su análisis al menos por 30 días	**1200**
2.8	**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	**70**
2.9	**Antimalware para dispositivos móviles** Que cuente con un módulo para identificar el nivel de seguridad o riesgo de los dispositivos móviles señalando las vulnerabilidades y riesgos del dispositivo y las aplicaciones y como mecanismos de repuesta pueda ofrecer el bloque y/o la desconexión	**1200**
2.10	**Cifrado para las computadoras** Que sea administrado desde la misma consola de antimalware que soporte sistemas operativos de Windows y Mac que pueda cifrar el disco duro con algoritmos de cifrado estándar a través de un agente propietario y/o que pueda cifrar con bitlocker y/o filevault nativo.	**1200**
2.11	**Sandbox para el endpoint**	**1**

	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	
2.12	**Parchado** 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 Microsoft 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.	**1200**
3	**PREVISORES DE INTRUSOS DE RED** Que sea una plataforma administrada centralmente con capacidad de ofrecer mecanismos de protección de manera uniforme con los previsores de intrusos de red físico y los previsores de intrusos virtuales, que pueda interactuar para ofrecer información, tomarla o responder a una amenaza con la consola de antimalware. Que preferentemente pueda consumir la información de la plataforma de anticipación de campañas para identificar indicadores de compromiso en el tráfico de la red. Que se integre con un sandbox para identificar amenazas de día cero. En los IPSs de red deberán contar con TAPs, es decir, con elementos que dejen pasar el tráfico por si se caen, pues los equipos no están en clúster y la continuidad de la operación es prioridad	**CANTIDAD**
3.1	**Previsor de Intrusos de Red físico para el Sitio principal** Que sea una tecnología de propósito específico con una marca diferente a la del firewall para reducir la posibilidad de intrusión y estar alineado a las buenas prácticas de seguridad en la red con al menos 8 interfaces Gigabit Ethernet con taps embebidos y al menos 6 interfaces 10 G con taps embebidos de las cuales cuatro deben soportar el formato **SR** de las siguientes características con un throughput de hasta 5 Gbps, la inspección de hasta 3 millones de conexiones concurrentes, con la capacidad de inspección de todos los protocolos incluyendo https y que cuente con mecanismos de protección basados en patrones de tráfico, comportamiento, la contención de archivos maliciosos, código y URLs basado en reputación la contención con un antimalware y la integración de un sandbox para la identificación y contención de archivos y código maliciosos. Asimismo que tenga la capacidad de identificar y contener ataques de alto volumen de tráfico distribuido (DDoS)	**1**
3.2	**Previsor de Intrusos de Red físico para el Sitio alterno** Que sea una tecnología de propósito específico con una marca diferente a la del firewall para reducir la posibilidad de intrusión y estar alineado a las buenas prácticas de seguridad en la red con al menos 8 interfaces Gigabit Ethernet con taps embebidos y al menos 6 interfaces 10 G con taps embebidos de las cuales cuatro deben soportar el formato **LR** de las siguientes características con un throughput de hasta 5 Gbps, la inspección de hasta 3 millones de conexiones concurrentes, con la capacidad de inspección de todos los protocolos incluyendo https y que cuente con mecanismos de protección basados en patrones de tráfico, comportamiento, la contención de archivos maliciosos, código y URLs basado en reputación la contención con un antimalware y la integración de un sandbox para la identificación y contención de archivos y	**1**

	código maliciosos. Asimismo que tenga la capacidad de identificar y contener ataques de alto volumen de tráfico distribuido (DDoS)	
3.3	**Previsores de Intrusos virtuales** Previsores de intrusos que puedan instalarse en hasta 8 hosts de VMWARE con un throughput total mínimo de 500 Mbps distribuido en todos los host con las capacidades de identificar y contener basado en patrones de tráfico malicioso, volumétricos, de mala reputación, de malware y que pueda cortar las conexiones a cualquiera de estas amenazas tirando las conexiones o mandando señales de reset	**8**
3.4	**Consola de administración IPS** La consola de administración debe administrar, monitorear, alertar y reportear todas las capacidades de los IPSs físico y virtuales, deb poder tener mecanismos para integrarse con la consola antimalware para consumir información del estado de las computadoras y servidores en cuanto a las capacidades antimalware instaladas y activas. Asimismo que se pueda integrar con el módulo de anticipación de campañas de tal forma que pueda hacer evidente la presencia indicadores de compromiso en la red	**2**
3.5	**Sandbox para los IPSs** Que cuente con un sandbox que se pueda integrar a la seguridad de los IPS como una capa de protección adicional para identificar amenazas de día cero en el tráfico de la red	**1**
4	**SEGURIDAD DE BASES DE DATOS**	CANTIDAD
4.1	**Seguridad en bases de datos** Que sea basada en un agente administrado desde una consola central para resguardar desde la perspectiva del servidor de base de datos con la capacidad para identificar y resolver vulnerabilidades, accesos no permitidos de usuarios y/o aplicaciones no permitidas, de zonas de la red no permitidas, en horarios no permitidos y que pueda identificar y contener comandos/verbos no permitidos configurados en una política de protección	**14**
5	**CORRELACIONADOR DE EVENTOS SIEM**	CANTIDAD
5.1	**Correlacionador de eventos SIEM** Que se pueda integrar a todas las herramientas de seguridad incluidas en la presente licitación y el EDR para obtener alarmas, dar contexto y correlacionar actividad que señale una amenaza. El equipo físico o virtual debe estar en sitio y debe soportar la ingesta de al menos 1000 eventos por segundo y debe poder retener la información al menos 1 año o contar con un espacio de 3TB de información	**1**

6	ADMINISTRACIÓN DE CUENTAS CON ALTOS PRIVILEGIOS Y GESTIÓN DE CUENTAS DE SERVICIO	CANTIDAD
6.1	**Administración de cuentas con altos privilegios y gestión de cuentas de servicios** Que pueda ser instalada en la nube o en sitio con exactamente las mismas capacidades. Que cuente con las capacidades de una bóveda de contraseñas que soporte la administración de hasta 10,000, un módulo para gestionar las cuentas de servicio, asimismo que pueda establecer flujos de autorización para el uso de las contraseñas cuente con capacidades para monitorear los comandos, las sesiones y si así se requiere grabar las mismas y que incluya la posibilidad de que un administrador pueda consumir varias contraseñas de manera simultánea. Debe tener alta disponibilidad asegurando el acceso al sitio principal y al sitio alterno	**20**
7	**FIREWALLS Y VPNS DE SSL**	CANTIDAD
7.1	**FW principal y VPNs** Un clúster de 2 firewalls en modo activo-pasivo con capacidades de statefull inspection con las funcionalidades de filtrado de puertos, previsor de intrusos, antibot filtrado de contenido web, control de aplicaciones, y un sandbox que tenga la capacidad de eliminar el malware "desconocido" de los archivos maliciosos. VPNs de SSL. Cada Firewall debe tener al menos: 8 interfaces de cobre que soporten 1Gbps, hasta 17.65 Gbps de throughput de paquetes UDP, 4.65 Gbps de throughput con el IPS prendido, 3.72 de throughput con todas las capacidades de NGFW inspeccionando SSL y 1.8 Gbps con el sandbox activo, con al menos 67,000 conexiones por segundo. Debe contar con el licenciamiento necesario para soportar VPNs de SSL en hasta 200 sesiones concurrentes	**2 Firewalls en clúster**
7.2	**FW Sitio Alterno y VPNs** Un clúster de 2 firewalls en modo activo-pasivo con capacidades de statefull inspection con las funcionalidades de filtrado de puertos, previsor de intrusos, antibot filtrado de contenido web, control de aplicaciones, y un sandbox que tenga la capacidad de eliminar el malware "desconocido" de los archivos maliciosos. VPNs de SSL. Cada Firewall debe tener al menos: 8 interfaces de cobre que soporten 1Gbps, hasta 20 Gbps de throughput de paquetes UDP, 3.9 Gbps de throughput con el IPS prendido, 3.4 de throughput con todas las capacidades de NGFW inspeccionando SSL y 1.4 Gbps con el sandbox activo, con al menos 67,000 conexiones por segundo. Debe contar con el licenciamiento necesario para soportar VPNs de SSL en hasta 200 sesiones concurrentes	**2 Firewalls en clúster**
7.3	**Consola de administración** Una consola de administración en clúster con un equipo ubicado en el sitio principal y otro en el sitio alterno en sitio que permita la administración de los 2 clústers señalados y los 12 firewalls distribuidos, de todos los módulos, que además pueda actualizar los sistemas operativos de manera remota, que tenga	**2**

	las capacidades de correlacionar los eventos de todos los módulos, así como de reportear toda la actividad	
8	**FIREWALLS DE WEB**	CANTIDAD
8.1	**WAF sitio principal** Un Web Application Firewall en sitio o en nube que proteja hasta 100 portales en una conexión de hasta 500 Mbps que funcione como un proxy reverso y/o de manera transparente en línea que pueda inspeccionar https, que soporte los ataques definidos en OWAS top 10, que tenga capacidades de machine learning para identificar el comportamiento típico y que pueda contener ataques que demuestren ser una desviación maliciosa. Que pueda establecer mecanismos automáticos para identificar cuando los sitios cambian y adaptar las políticas de protección	**1**
8.2	**WAF sitio alterno** Un Web Application Firewall en sitio o en nube que proteja hasta 100 portales en una conexión de hasta 500 Mbps que funcione como un proxy reverso y/o de manera transparente en línea que pueda inspeccionar https, que soporte los ataques definidos en OWAS top 10, que tenga capacidades de machine learning para identificar el comportamiento típico y que pueda contener ataques que demuestren ser una desviación maliciosa. Que pueda establecer mecanismos automáticos para identificar cuando los sitios cambian y adaptar las políticas de protección	**1**
8.3	**Consola de administración WAF** Una consola de administración en clúster ubicando una en el sitio principal y otra en el sitio alterno, que permita la administración de ambos WAF, 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	**2 consola en clúster**
9	**ANALIZADOR DE PROTOCOLOS**	CANTIDAD
9.1	**Analizador experto de protocolos** Un analizador de protocolos para instalarse en una computadora que permita capturar paquetes de red y muestre problemas con un módulo experto en el análisis de protocolos. El analizador de protocolo debe estar soportado por un fabricante, NO debe ser de uso libre	**1**
10	**ADMINISTRACIÓN DE VULNERABILIDADES**	CANTIDAD
10.1	**Admon Vulnerabilidades Infraestructura** Plataforma con los módulos de escaneo para identificar vulnerabilidades en la infraestructura de cómputo, comunicaciones y bases de datos desde la perspectiva de Internet y desde la perspectiva de 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	**256**
10.2	**Admon Vulnerabilidades Servidores Web**	**25**

	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	

ATENTAMENTE

_____

Nombre y firma de la persona física o representante legal

MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN
Secretaría de Administración
Dirección de Adquisiciones

Concurso por Licitación Pública Nacional Presencial No. SA-DA-CL-26/2022
"Requerimiento de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

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 a nuestras necesidades 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, LA FUGA DE INFORMACIÓN, LA CLASIFICACIÓN DE INFORMACIÓN Y EL ACCESO
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 todos los agentes, 1200 a todas 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 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
Previsión de Fuga de Información en las computadoras

Servicios de habilitación de -Previsión de Fuga de Información- en las computadoras (los días requeridos en sitio) validando su correcto funcionamiento y liberación. Se requiere:
• La distribución agentes al total de los usuarios, 1200, y su habilitación silenciosa en las computadoras
• La configuración de hasta 20 reglas de protección para hasta 20 perfiles diferentes que pueden incluir, el bloqueo y/o el cifrado de información de acuerdo a los requerimientos del municipio minimizando falsos positivos
• La afinación de todas las reglas hasta que muestren sólo información veraz
• El diseño de un proceso de protección de la información validado por el municipio
• Todas las tareas de afinación requeridas para evitar detener la operación o evitar cualquier falla
• El alertamiento vía correo electrónico
• La integración con el control de navegación web para establecer políticas de protección en este canal

Cloud Access Security Brocker

Servicios de Habilitación de "Cloud Access Security Brocker"- (los días requeridos en sitio) para la protección de aplicaciones SaaS funcionamiento y liberación. Se requiere:
• La integración vía API de hasta 10 aplicaciones SaaS durante la vigencia del proyecto, comenzando con Google Enterprise y Zoom
• La distribución agentes al total de los usuarios, 1200, y su habilitación silenciosa en las computadoras
• La configuración 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 Enterprise, a la fuga de información en el servicio Google Enterprise, la tokenización y/o cifrado de la información
• La integración con el módulo de previsión de fuga de información en las computadoras y 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
• La integración con el control de navegación previsión de fuga de información para establecer políticas de protección en este canal

Servicios de Habilitación de acceso a la red con el mínimo privilegio- (los días requeridos en sitio) para la protección de aplicaciones internas del municipio:
• La distribución del agente a todas las computadoras, 1,200
• La integración al dominio para la provisión del acceso basado en identidad
• La habilitación de 2 gateways: uno en el sitio principal y otro en 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 de todas las reglas microsegmentadas 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

PLATAFORMA ANTIMALWARE
El servicio de anticipación de campañas deberá ser habilitado para tener visibilidad y cruzar información con el estado de seguridad de los servidores y todas las computadoras para señalar las diferencias y las acciones para compensarla, así como para identificar si existen identificadores de compromiso que indiquen impacto o posible impacto de estas campañas en el ambiente del municipio. Asimismo, deberá ser configurado para tener visibilidad del tráfico malicioso para señalar indicadores de compromiso de alguna campaña que no haya tocado a las estaciones pero que esté en el tráfico de la red
Se requiere la habilitación de los productos de antimalware, antiransomware, parcheo virtual en todas las estaciones,1200: • La distribución de todos los productos en todas las estaciones, de acuerdo a la compatibilidad de los mismos • Se deberá habilitar una consola en sitio y una consola en la nube • El resto de las estaciones deberán ser administradas desde la consola en la nube Para el antimalware • Para la habilitación del antivirus este deberá estar configurado para identificar las estaciones en la red y autoinstalarse • La instalación del antivirus deberá tener configuradas políticas para que este se actualiza de manera regular, diaria, semanal, mensual, semestral, anual, para el módulo que lo amerite • Deberá estar habilitado en modo protección - El módulo de machine learning deberá estar activo para identificar y contener, así como los mecanismos de reputación • El módulo antiransomware deberá está habilitado en todas las estaciones, 1200, al finalizar su habilitación deberá poder validar su correcto funcionamiento, es decir, regresando la estación al estado inicial antes de ser cifrada • El módulo de parcheo virtual deberá estar activo en todas las estaciones,1200, protegiendo al menos ante las amenazas de alta criticidad
Para el control de dispositivos • Deberá estar activo en todas las estaciones con excepción de las administradas en la nube • Deberá de incluir una de dos políticas: bloqueado o permitido. El municipio indicará cuál de las dos debe aplica a cada PC

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, 1,200
- 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 • Deberá distribuirse a todas las estaciones 1,200 • 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 el Endpoint Detection and Response para servers • Deberá distribuirse a todos los servidores Windows y Linux, 70 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 antimalware para los equipos móviles • Deberá distribuirse en al menos 30 teléfonos inteligentes o tabletas con IOS o Android • Deberán configurarse políticas de protección para disminuir el riesgo asociado al dispositivo, las aplicaciones y/o la red
Servicios de habilitación para el cifrado en el total de las computadoras, 1,200: -• La distribución en todas las estaciones en sitio • La habilitación del cifrado en los archivos y folders con el siguiente alcance: • Una regla no asignada pero probada en 5 estaciones que cifre todos los archivos generados en MS Word, MS Excel, MS Power point • Una regla no asignada pero probada en 5 estaciones que cifre todos los archivos incluidos en un directorio señalado por el municipio • Una regla no asignada pero probada en 5 estaciones que cifre todos los archivos incluidos en un directorio señalado por el municipio • Una regla no asignada pero probada en 5 estaciones que cifre los USBs que se conecten a las PCs • Una regla no asignada pero probada en 5 estaciones que permita el cifrado por el usuario de un archivo resguardado por una clave de acceso, con hasta 3 llaves de cifrado diferentes • La habilitación del cifrado en los discos duros de al menos 200 estaciones en sitio, con el siguiente alcance: • Cifrado que requiera del usuario y password del dominio del municipio para acceder a la estación correspondiente a cada usuario • Se cuente con un mecanismo de descifrado ante una contingencia, mismo que se demuestre y se documente
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 : La habilitación del Sandbox: • 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 de la integración y el correcto funcionamiento

Los servicios de habilitación de la herramienta de parcheo para el total de las estaciones, 1200:
- 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, incluyendo parches de Microsoft, Adobe y JAVA
- La habilitación y el parcheo del mes en curso con los parches críticos de seguridad de Microsoft debe ser progresiva.
  - 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
  - o Para los servidores:
    - Habilitación de 1 servers (laboratorio)
    - Habilitación de 3 servers (prueba)
    - Habilitación de 6 servers (piloto)
    - La habilitación de 40 servers restantes

PREVISORES DE INTRUSOS DE RED

Se requieren los servicios de habilitación de un previsor de intrusos en línea protegiendo la granja de servidores y DMZ del sitio principal:
- La instalación en modo transparente de los 1 IPS físico y su configuración para proteger cada uno de los 8 enlaces Gigabit Ethernet y 1 de 10 G, con al menos las siguientes características:
  - La instalación en cada uno de los enlaces en modo fail open
  - La habilitación en modo monitoreo con una “política” de monitoreo estándar.
  - La habilitación progresiva de la protección para ofrecer mecanismos de respuesta de bloqueo de tráfico, "tirando los paquetes"
  - La habilitación por enlace, de un perfil para la identificación y contención de ataques de denegación de servicio (Volumétrico de tráfico)
  - En la instalación inicial deben considerarse las excepciones necesarias para evitar “falsos positivos”
- La integración a una consola de administración en alta disponibilidad
- La integración al sandbox para la identificación de malware en la red, del llamado de "día cero"
- La validación del correcto funcionamiento del bloqueo de tráfico malicioso, de ataques de DoS y de contención de malware de día cero en la red

Se requieren los servicios de habilitación de un previsor de intrusos en línea protegiendo la granja de servidores y DMZ del sitio principal:

• La instalación en modo transparente de los 1 IPS físico y su configuración para proteger cada uno de los 8 enlaces Gigabit Ethernet y 1 de 10 G, con al menos las siguientes características:

- La instalación en cada uno de los enlaces en modo fail open
- La habilitación en modo monitoreo con una “política” de monitoreo estándar.
- La habilitación progresiva de la protección para ofrecer mecanismos de respuesta de bloqueo de tráfico, "tirando los paquetes"

• La habilitación por enlace, de un perfil para la identificación y contención de ataques de denegación de servicio (Volumétrico de tráfico)

• En la instalación inicial deben considerarse las excepciones necesarias para evitar “falsos positivos”

• La integración a una consola de administración en alta disponibilidad

• La integración al sandbox para la identificación de malware en la red, del llamado de "día cero"

• La validación del correcto funcionamiento del bloqueo de tráfico malicioso, de ataques de DoS y de contención de malware de día cero en la red

Se requiere la habilitación de hasta 8 hosts virtuales en host de VMWare con el siguiente alcance:

- La instalación en modo transparente y configuración para proteger cada dominio de VMWare
- La habilitación en modo monitoreo con una “política” de monitoreo estándar.
- La habilitación progresiva de la protección para ofrecer mecanismos de respuesta de bloqueo de tráfico, tirado de paquetes o envío de reset, según sea el caso.
- La habilitación por dominio, de un perfil para la identificación y contención de ataques de denegación de servicio
- En la instalación inicial deben considerarse las excepciones necesarias para evitar “falsos positivos”

• La integración a una consola de administración en alta disponibilidad

• La integración al sandbox para la identificación de malware en la red, del llamado de "día cero"

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", en los previsores de intrusos de red:

• La habilitación del Sandbox

- La configuración para el envío de código o archivos con posible malware de día cero desde la consola de administración de los IPSs de manera automática

• La contención del malware de día cero como resultado del análisis del sandbox tanto en los IPSs

• Estabilización de la integración y el correcto funcionamiento con los IPSs

Se requiere la habilitación de la consola de administración con el siguiente alcance:

• La habilitación de 2 consolas de administración en alta disponibilidad que administren a 2 IPSs físicos y hasta 8 virtuales

• Las consolas deberán estar una en el sitio principal y otra en el sitio alterno

• Deberá estar integrada con el servicio de anticipación de campañas para la identificación de indicadores de compromiso en el tráfico de la red asociado a una campaña

• Deberá estar integrada a la consola de administración del antimalware para consumir la información de las capacidades de protección de las computadoras

SEGURIDAD DE BASES DE DATOS

Servicio para habilitación de protección para las bases de datos en hasta 14 servidores. Este debe incluir:
Servicios de afinación de módulos de Identificación de vulnerabilidades y parcheo virtual para las bases de datos (los días requeridos en sitio). Debe incluir al menos pero no limitado a:
• Definición y habilitación de tareas de descubrimiento de bases de datos
• Definición y habilitación de tareas de identificación periódica (mensual) de vulnerabilidades alineado a los tipos de bases de datos y nuevas amenazas. Descubriendo el mayor volumen de vulnerabilidades sin causar disrupción en la operación
• Definición e implementación de un proceso de administración de vulnerabilidades que asegure el descubrimiento y corrección oportuna de las vulnerabilidades
• Definir y habilitar las capacidades de virtual patching para corregir las vulnerabilidades encontradas en al menos 3 escaneos sin causar disrupción en la operación de la base de datos ni pérdida a la integridad de los datos
• Definición de 6 reportes y los alertamientos correspondientes alineados a las bases de datos escaneadas las vulnerabilidades encontradas y los ataques bloqueados con el módulo de vPatch

CORRELACIONADOR DE EVENTOS SIEM

Servicios de Integración en el SIEM (Correlacionador de eventos):
• Integración de 3 portales, 5 aplicaciones, 50 equipos de red que incluyen switches, call manager, routers, 16 firewalls, 2 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, consola de previsión de fuga de información, Consola de administración de control de acceso a la red con el mínimo privilegio, firewall de Base de datos, 1 consola de EDR, Los Web Application Firewalls, la bóveda de contraseñas

• Configuración de 10 Tableros (dashboards) y 45 reglas de correlación para SIEM (los días requeridos en sitio). Debe incluir al menos pero no limitado a:
- La integración nativa preferentemente 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 fuga de información e información contextual de las herramientas de seguridad relacionadas incluidas 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 através de los WAF
- Riesgos asociados a los escaneos de vulnerabilidades vs la protección de las herramientas de seguridad

• 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 actividad en la bóveda de contraseñas y anomalías relacionadas
- La modificación a las políticas de previsores de intrusos de host
- La modificación a las políticas de los web application firewalls
- La modificación a las políticas de protección de bases de datos
- 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 La fuga de información
- Violaciones a las políticas de protección en las aplicaciones SaaS
- Actividad anómala o inusual en la red

- Actividad anómala o inusual en la infraestructura de cómputo
- Actividad anómala o inusual en las aplicaciones y portales
- Ataques posiblemente exitosos a las plataformas más importantes

ADMINISTRACIÓN DE CUENTAS CON ALTOS PRIVILEGIOS Y GESTIÓN DE CUENTAS DE SERVICIO

Servicios de habilitación de la bóveda de contraseñas deben incluir:

• Preferentemente, la habilitación de una arquitectura en la nube que de manera nativa sea de alta disponibilidad

• La habilitación de un par de conectores en sitio, uno para el sitio principal y otro para el secundario

• El descubrimiento de cuentas con altos privilegios de dominio y locales en los servidores Windows y Linux

• El resguardo de las contraseñas con altos privilegios de dominio y locales

• La habilitación de hasta 20 administradores y las contraseñas a las que pueden tener acceso, así como el flujo de autorización para el uso de las mismas

• La configuración del bloqueo de la cuenta privilegiada para que sólo un usuario la pueda consumir a la vez

• La rotación automática de cuentas cada vez que se usen, así como su rotación semanal

• El registro de toda actividad a nivel comando y el guardado en video de las sesiones

• La habilitación del descubrimiento y uso de las cuentas denominadas de servicio en uso en todos

los servidores del municipio
• La documentación de las cuentas de servicio, su uso y su vigencia, administrada desde la bóveda de contraseñas
• La configuración para que el total de usuarios, hasta 1,200 pudiera resguardar todas sus contraseñas en la bóveda si así se requiere

FIREWALLS

Servicios de habilitación del firewall principal en clúster , incluyendo la habilitación de todas sus capacidades, incluyendo pero no limitado a : firewall, Identificación de usuarios, IPS, control de aplicaciones de red, Antivirus, Protección contra redes robot y sandbox en modo de protección (los días requeridos en sitio):
• 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 de los módulo para identificación de usuarios del directorio activo
• La habilitación de los módulos de antivirus y antibot
• La habilitación del Blade 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 ruteo dinámico a través de BGP
• La estabilización de la operación de cada uno de los firewalls

Servicios de habilitación del firewall alterno en clúster , incluyendo la habilitación de todas sus capacidades, incluyendo pero no limitado a : firewall, VPN sitio a sitio (12 sitios) y usuario a sitio, Identificación de usuarios, IPS, control de aplicaciones de red, Antivirus, Protección contra redes robot y sandbox en modo de protección (los días requeridos en sitio):

- 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 de los módulo para identificación de usuarios del directorio activo
- La habilitación de los módulos de antivirus y antibot
- La habilitación del Blade 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 ruteo dinámico a través de BGP
- La estabilización de la operación de cada uno de los firewalls

Servicios de habilitación de la consola de administración:

- Debe instalarse en alta disponibilidad instalando una en el sitio principal y otra en el sitio alterno
- Debe tener integrados los clústers del sitio principal, del sitio alterno y los 12 sitios remotos
- Debe tener habilitada las capacidades de administración de todos los elementos, alertamiento, reporteo, respaldo automático y regular semanalmente, correlación

WEB APPLICATION FIREWALLS

Servicios para la habilitación de Web Application Firewall en el sitio principal para 100 portales, incluyendo:

- La habilitación del equipo físico/o virtual
- La integración de 100 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 100
- Afinación/validación de las políticas de protección
- Cambio a modo protección sin causar disrupción de 20 en 20 portales hasta completar 100
- La estabilización de la operación de los mismos

Servicios para la habilitación de Web Application Firewall en el sitio alterno para 100 portales, incluyendo:
• La habilitación del equipo físico/o virtual
• La integración de 100 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 100
• Afinación/validación de las políticas de protección
• Cambio a modo protección sin causar disrupción de 20 en 20 portales hasta completar 100
• La estabilización de la operación de los mismos

Servicios para la habilitación de la consola de administración de los Web Application Firewall:
• Integración del WAF del sitio principal
• Integración del WAF del sitio alterno
• Configuración uniforme en modo protección de ambos equipos
• Generación automática de hasta 5 reportes señalados por el municipio
• Integración con el SIEM

ANALIZADOR EXPERTO DE PROTOCOLOS

Servicios de instalación del analizador experto de protocolos:
• Requiere sea instalado en una computadora
• Requiere se capacite al personal del municipio en su uso para usarlo cuando se tenga un problema

ADMINISTRACIÓN DE VULNERABILIDADES

Servicio para identificar vulnerabilidades, que tengan las siguientes capacidades:
• Habilitación de la plataforma
• Configuración de tareas de escaneo de vulnerabilidades para 10 grupos y hasta 256 direcciones
• Definición y habilitación de tareas de identificación periódica (mensual) de vulnerabilidades alineado a los grupos definidos en el punto previo: 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, alienado 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

Servicio para identificar vulnerabilidades, que tengan las siguientes capacidades:
• Habilitación de la plataforma
• Configuración de tareas de escaneo de vulnerabilidades para hasta 20 direcciones IP diferentes
• Definición y habilitación de tareas de identificación periódica (mensual) de vulnerabilidades web . 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 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, alienado a las capacidades de "seguimiento" de la herramienta
• Definición de reportes y los alertamientos correspondientes a los portales escaneados y las vulnerabilidades escaneadas mensualmente

ATENTAMENTE

_____

Nombre y firma de la persona física o representante legal

MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN
Secretaría de Administración
Dirección de Adquisiciones

Concurso por Licitación Pública Nacional Presencial No. SA-DA-CL-26/2022
"Requerimiento de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

ANEXO C. REQUERIMIENTOS DE SOPORTE

Los requerimientos de soporte son los señalados.

SOPORTE ESPECIALIZADO EN SITIO CON LAS SIGUIENTES CAPACIDADES
Con cobertura 7x24x365 por parte del proveedor que incluya: • Tiempo de atención en sitio para resolver eventos de ALTA CRITICIDAD que estén afectando a la continuidad operativa del municipio o la disponibilidad o correcto funcionamiento de alguna de las herramientas de seguridad • Apoyo en sitio especializado para el diagnóstico, solución, si se requiere escalación con el fabricante y seguimiento hasta la resolución • Para cada producto correspondientemente: • Atención de un ingeniero especialista en la seguridad web basada en proxy • Atención de un ingeniero especialista en la tecnología de previsión de fuga de información en el endpoint • Atención de un ingeniero especialista en la tecnología de Cloud Access Security Broker • Atención de un ingeniero especialista en la tecnología de Control de Acceso con el mínimo privilegio • Atención de un ingeniero especialista en la tecnología de identificación de vulnerabilidades • Atención de un ingeniero especialista en la seguridad en los servidores y las PCs • Atención de un ingeniero especialista en el cifrado de discos duros y files & folders • Atención de un ingeniero especialista en el parcheo en los servidores y las PCs • Atención de un ingeniero especialista en los equipos de previsión de intrusos de red de propósito específico • Atención de un ingeniero especialista en Sandbox de endpoint y de previsores de intrusos de propósito específico • Atención de un ingeniero especialista en la seguridad de las bases de datos • Atención de un ingeniero especialista en SIEM • Atención de un ingeniero especialista en firewalls y el sandbox de los mismos • Atención de un ingeniero especialista en la bóveda de contraseñas • Atención de un ingeniero especialista en Web Application Firewall

Personal certificado

El proveedor deberá contar con personal certificado al menos en lo siguientes 3 rubros

- SOLUCIÓN PERIMETRAL (FIREWALLS)
- SISTEMA DE PREVENCIÓN DE INTRUSOS
- Web Application Firewall

El proveedor deberá proporcionar un ingeniero especialista dedicado con el conocimiento de reporteo y análisis de información de seguridad informática el cual tendrá la función de preparar un informe con una frecuencia quincenal en donde de a conocer los hallazgos principales valiéndose del conjunto de toda la información proporcionada por las herramientas implementadas.

El proveedor deberá contar con un SOC especializado el cual podrá ser verificado en cualquier momento por el municipio

El proveedor deberá contar con una certificación ISO/IEC 27001:2013

ATENTAMENTE

_____

Nombre y firma de la persona física o representante legal

MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN
Secretaría de Administración
Dirección de Adquisiciones

Concurso por Licitación Pública Nacional Presencial No. SA-DA-CL-26/2022
"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

ANEXO D. REQUERIMIENTOS DE SERVICIOS ADMINISTRADOS

Los requerimientos de servicios administrados son los señalados.

HERRAMIENTA	VALIDACIÓN CORRECTO FUNCIONAMIENTO (Diario)	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 Web	Del filtrado 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. En el escenario en la nube, la migración deberá ser de los agentes si así aplica	Modificación de políticas de navegación sin límite de modificaciones Modificación de políticas de DLP en el canala web sin límiete de modificaciones Reporteo de navegación de usuarios específicos como se requiera sin límite Validación del correcto funcionamiento	Debe respaldarse la configuración de la consola políticas y reporteos	Para revisión de eventos, incidentes, fallas	De Salud de la herramienta De eventos de seguridad De eventos de falla De correcciones	De navegación De Salud de a herramienta consolidada al mes De evento de seguridad consolidados al mes De eventos de falla consolidados al mes

							De correcciones consolidadas al mes De recomendaciones consolidadas al mes
Previsión de fuga de información	De la herramienta Del registro de eventos	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 agentes si así aplica	Modificación de políticas de protección sin límite de modificaciones Reporte de incidentes de seguridad sin límite Validación del correcto funcionamiento	Debe respaldarse la configuración de la consola políticas y reportes	Para revisión de eventos, incidentes, fallas	De evento de seguridad De eventos de falla De correcciones	De evento de seguridad consolidados al mes De eventos de falla consolidados al mes De correcciones consolidadas al mes De recomendaciones consolidadas al mes
Cloud Access Security Brocker	Del Tenant Del registro de actividades, anomalías, incidentes	No Aplica	Modificación de políticas de protección sin límite de modificaciones Modificación de políticas de DLP en el canala web sin límite de modificaciones Reporte de incidentes de seguridad sin límite	Debe respaldarse la configuración de la consola políticas y reportes	Para la revisión de eventos, incidentes o fallas	De evento de seguridad De eventos de falla De correcciones	De evento de seguridad consolidados al mes De eventos de falla consolidados al mes De correcciones consolidadas al mes

			Validación del correcto funcionamiento				De recomendaciones consolidadas al mes
Control de Acceso a la Red con mínimos privilegios	Del Tenant Del gateway	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio. Aplica para el gateway y los agentes	Modificación de políticas de protección sin límite de modificaciones Reporte de incidentes de seguridad sin límite Validación del correcto funcionamiento	Debe respaldarse la configuración de la consola políticas y reportes	Para la revisión de eventos, incidentes o fallas	De evento de seguridad De eventos de falla De correcciones	De evento de seguridad consolidados al mes De eventos de falla consolidados al mes De correcciones consolidadas al mes De recomendaciones consolidadas al mes
Prevensión ante campañas de malware	Sí de correcto funcionamiento	No Aplica	Identificación de estaciones expuestas ante campañas de malware	No Aplica	Para revisión de eventos, incidentes, 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 con 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	Validación del correcto funcionamiento	La configuración		Coberturas	El reporte debe incluir:

	De los repositorios distribuidos de productos y vacunas		Cobertura de producto y patrones (antimalware parcheo virtual) Identificación, resolución y reporteo de incidentes	La base de datos para la consola en sitio	Para revisión de eventos, incidentes, fallas	Incidentes de Seguridad y/o Falla Correcciones realizadas y/o recomendaciones	- Cobertura de producto - Cobertura de patrones o firmas - Eventos de seguridad - Eventos de falla - Acciones realizadas - 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 Cobertura del producto	La configuración La base de datos para la consola en sitio	Para revisión de eventos, incidentes, fallas	De evento de seguridad De eventos de falla De correcciones	De evento de seguridad consolidados al mes De eventos de falla consolidados al mes De correcciones consolidadas 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 requerimie	De la cobertura de productos en modo bloqueo	La configuración El inventario	Para revisión de eventos, incidentes, fallas	Coberturas Incidentes de Seguridad y/o Falla Correcciones realizadas y/o recomendaciones	El reporte debe incluir: - Cobertura de producto - Cobertura modo de protección: bloqueo o no bloqueo

		nto del municipio					- Eventos de seguridad - Eventos de falla - Acciones realizadas - 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 El inventario	Para revisión de eventos, incidentes, fallas	Coberturas Incidentes de Seguridad y/o Falla Correcciones realizadas y/o recomendaciones	El reporte debe incluir: - Cobertura de producto - Cobertura modo de protección: bloqueo o no bloqueo - Eventos de seguridad - Eventos de falla - 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, fallas	No Aplica	De cobertura
Endpoint Detection & Response: EDR	Sí de correcto funcionamiento	Debe realizarse al menos una vez al año como fundament	Identificación de eventos de seguridad	No Aplica	Para revisión de eventos, incidentes, fallas	Eventos de seguridad extraños o anómalos	De eventos anómalos consolidades De acciones tomadas

		o de una mejora o como resultado del requerimiento del municipio	Investigaciones de los eventos de seguridad			De las investigaciones realizadas	Las recomendaciones Las recomendaciones realizadas durante el mes
Cifrado para las computadoras	Sí de correcto funcionamiento	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 La llave de cifrado cada vez que cambie o se adicione	Para revisión de eventos, incidentes, fallas	No Aplica	De fallas o habilitaciones consolidadas
Sandbox para PCs	Sí de correcto funcionamiento	Sobre demanda, cuando aplique	Identificación del correcto funcionamiento	No Aplica	Para revisión de eventos, incidentes, fallas	Eventos de seguridad Fallas	Incluido en el reporto de antivirus de PCs, servidores y/o previsores de intrusos de propósito específico señalando el volumen de eventos administrados por el sandbox
Parchado	Cobertura de parches Salud de la herramienta de parcheo	De la herramienta de parcheo debe realizarse una vez al año como fundamento de una	Avance en la cobertura de los parches de acuerdo a la métrica	La configuración Los eventos	Para revisión de eventos, incidentes, fallas	No Aplica	El reporte debe incluir: - Cobertura de parches vs las métrica - Eventos de falla - Acciones realizadas

		mejora o como resultado del requerimiento del municipio					- Recomendaciones
Previsores de Intrusos de red de propósito específico físicos y virtuales y su consola de administración	Sí de correcto funcionamiento	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio	Alertamiento Reporteo sobre demanda sin límite de eventos Modificación adición a las Reglas de protección sin límite de eventos	La configuración Los eventos	Para revisión de eventos, incidentes, fallas	Eventos de seguridad Fallas	De salud de la solución De eventos de seguridad De cobertura de patrones De acciones De recomendaciones
Sandbox para Previsores de intrusos	Sí de correcto funcionamiento	Sobre demanda, cuando aplique	Identificación del correcto funcionamiento	No Aplica	Para revisión de eventos, incidentes, fallas	Eventos de seguridad Fallas	Incluido en el reporteo de previsores de intrusos de propósito específico señalando el volumen de eventos administrados por el sandbox
Firewall de bases de datos	Sí de correcto funcionamiento	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	La configuración Los eventos	Para revisión de eventos, incidentes, fallas	Eventos de seguridad Fallas	De vulnerabilidades de los activos De los parches virtuales aplicaciones Las recomendaciones

SIEM (Correlacionador de eventos)	Sí de correcto funcionamiento	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio	Alertamiento Modificación, adición a los dashboards sin límite de eventos Modificación adición a las Reglas de correlación sin límite de eventos	La configuración	Para revisión de eventos, incidentes, fallas	Eventos de seguridad correlacionados extraños o anómalos	Sí de actividad anómala por mes. Incluida en los dashboards específicos
Firewalls y VPNs con todos sus módulos	Sí de correcto funcionamiento	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 De configuración asociada a cualquiera de sus módulos De habilitación de componentes y su configuración sin límite de eventos	La configuración Los eventos	Para revisión de eventos, incidentes, fallas	Eventos de seguridad Fallas	De salud de la solución De eventos de seguridad De acciones De recomendaciones
Firewalls de Web	Sí de correcto funcionamiento	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio	Modificación de reglas de protección a los servidores web sin límite de eventos	La configuración Los eventos	Para revisión de eventos, incidentes, fallas	Eventos de Seguridad en los servidores web Fallas	De salud de la solución De eventos de seguridad De acciones De recomendaciones
Administración de vulnerabilidades de	De la herramienta	Debe realizarse al menos una vez al	Seguimiento a las vulnerabilidades	No Aplica	Para la corrección de	No Aplica	De vulnerabilidades de los activos

Infraestructura		año como fundamento de una mejora o como resultado del requerimiento del municipio	"abiertas" con los responsables del equipo interno del municipio para solventarlas		vulnerabilidades	Sobre demanda para servidores y/o equipos activos a punto de ser liberados y/o mensual	Del score de riesgo y su comportamiento vs el mes anterior
Administración de vulnerabilidades Web	De la herramienta	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio	Seguimiento a las vulnerabilidades "abiertas" de hasta 5 servidores Web con los responsables del equipo interno del municipio para solventarlas	No Aplica	Para la corrección de vulnerabilidades Web	No Aplica Sobre demanda para servidores a punto de ser liberados y/o mensual	De vulnerabilidades de los servidores web Del score de riesgo y su comportamiento vs el mes anterior

ATENTAMENTE

_____

Nombre y firma de la persona física o representante legal

MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN
Secretaría de Administración
Dirección de Adquisiciones

Concurso por Licitación Pública Nacional Presencial No. SA-DA-CL-26/2022
"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

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
Que sea una plataforma unificada administrada desde la nube con capacidades de clasificación de información para las computadoras, previsión de fuga de información para las computadoras y la navegación web, "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 de 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 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.

La solución debe contar con Remote Browser Isolation para aquellos sitios sospechosos cuyo análisis no sea conclusivo a través de los métodos tradicionales de Antimalware y Emulación, así como para cualquier página con reputación desconocida o de riesgo medio

La solución debe incluir controles granulares para las sesiones de Remote Browser Isolation, que permitan controlar acciones como Copiar, Pegar, Cargar, Descargar, o el almacenar cookies en la máquina local

Filtrado de Contenido web:

La solución deberá permitir el filtrado de URL basado en categorías, para ello la solución deberá contar con más de 100 categorías pre-definidas.

El administrador podrá sobre escribir la categoría de una URL o aplicaciones vs. La categoría dada por el fabricante

La solución deberá permitir el bloqueo de aplicaciones Peer-to-Peer

La solución deberá permitir el bloqueo de Streaming Media

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.

La plataforma debe filtrar en idiomas no latinos como Japones, Arabe, Mandarin entre otros

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 Registro Cloud de análisis de riesgo para al menos 25 mil diferentes servicios Cloud

Para cada servicio cloud se deben evaluar al menos 50 atributos y 260 sub atributos de riesgo

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

Debe monitorear si los servicios Cloud cuentan con las siguientes certificaciones: EU GDPR, Trustee / BBB, Safe Harbor, ISO 27018, FISMA, FedRAMP, CSA Star, HITRUST, ISO 27017, SAS 70 / SSAE16 / ISAE 3402, ITIL, DCAA / SOC 3, ISO 27001, SOC 2, PCI Compliance y HIPAA

La solución debe poder mostrar la exposición de los servicios Cloud a vulnerabilidades de los servicios Cloud como Cloudbleed, Heartbleed, Poodle, Freak, Ghostwriter

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

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

La solución debe identificar intentos de fuga de información por servicios no corporativos a través del análisis de Machine Learning y UEBA, 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

Debe de tener la capacidad de aplicar políticas a la información al momento de tratar de subirla a cualquier página web basado en: Diccionarios, palabras clave, grupos de usuarios y expresiones regulares

1.2 Previsión de fuga de información en las computadoras

Toda solución propuesta debe ser ofrecida por un único fabricante, de modo que tanto el soporte de la solución, y sus funcionalidades, queden enteramente integradas y gestionadas a través de una única consola en la nube

La solución debe ser capaz de proteger las informaciónes críticas integrando en una solución las capacidades de clasificación de datos, monitoreo y bloqueo.

La solución debe ser capaz de compartir políticas y visibilidad de información entre estaciones de trabajo y servidores e información residente en servicios de nube.

La solución debe proteger los principales canales de fuga de datos, como, por ejemplo, dispositivos de almacenamiento removibles, almacenamiento en nube, correos, mensajería instantánea, subida a sitios web, impresión, captura de pantalla, carpetas compartidas, comunicación de red y acceso por aplicaciones no autorizadas.

La solución debe permitir que los usuarios clasifiquen manualmente los documentos desde herramientas de ofimática, como Word, Excel o Powerpoint, conforme a las definiciones configuradas desde la consola de gestión centralizada.

La clasificación manual no deberá de depender de plugins o software de terceros, siendo parte integral de la solución propuesta.

La solución debe permitir que los usuarios inicien escaneos y remediaciones para descubrimiento de información crítica.

La solución debe poseer mecanismos de clasificación de documentos, incluyendo diccionarios, expresiones regulares, registro de documentos, tipo de archivo y propiedades de los archivos.

La solución debe tener la capacidad de compartir e integrar los criterios de clasificación desde una única consola, con el propósito de unificar la protección en los distintos vectores de fuga (Endpoint, Red, Nube).

La solución debe tener capacidades de marcado para identificar documentos de acuerdo a su origen, previniendo que estos documentos sean copiados a aplicaciones web, aplicaciones de red y carpetas compartidas.

La solución debe poseer capacidades de protección para desktops físicos y virtuales (VDI).

La solución debe entregar visibilidad por medio de reportes, consultas y dashboards, sirviendo como apoyo al cumplimiento de normativas de seguridad, como PCI-DSS.

La solución debe posibilitar la educación del usuario por medio de alertas y justificaciones, en base a las políticas implementadas.

La solución debe permitir personalización de mensajes de notificación al usuario para cada regla aplicada, y debe incluir, como mínimo:

- Logo de compañía
- Texto personalizado
- Variables
- Selección de idiomas

La solución debe permitir la aplicación de políticas conforme a las acciones del día a día de los usuarios, como por ejemplo, envío de correos, copiado de archivos a dispositivos removibles, o subida de información en la nube.

La solución debe utilizar técnicas de fingerprinting para clasificar y marcar datos sensitivos y no estructurados.

La solución debe poseer, como mínimo, los siguientes módulos de protección:

- Agente de protección ante fuga de datos y control de dispositivos en estaciones Windows y MacOS.

Servicio en nube capaz de proteger la información sensitiva almacenada y transferida en los servicios de nube.

La solución debe poseer integración con herramientas de Rights Management, como por ejemplo: Microsoft Windows Rights Management Services y Seclore FileSecure.

La solución debe proveer acciones como reportar un incidente y/o bloquear el acceso a la información sensitiva,.

Por medio del agente instalado, la solución debe permitir el control de los datos en uso, como por ejemplo, acciones de usuarios relacionadas a copia y envío de documentos o impresión de documentos.

El agente debe emplear reglas para la protección de datos clasificados en los siguientes vectores:

Copiado al portapapeles (Clipboard);

Aplicaciones de almacenamiento de nube;

E-mail;

Carpetas compartidas;

Impresión;

Aplicaciones y browsers;

Subida a sitios web;

La solución debe ser capaz de aplicar reglas de protección de datos a grupos y usuarios de Active Directory.

La solución debe ser capaz de aplicar reglas de protección de datos a equipos, o grupos de equipos de Active Directory.

La solución deberá ser capaz de replicar el contenido de un documento sensible que infrinja una regla de protección de datos de forma integral, con, como mínimo, la siguiente información:

Documento integral que formó parte del incidente, accesible a través de la consola de gestión;

Correo integral que formó parte del incidente, accesible a través de la consola de gestión;

Lista de términos encontrados en el incidente;

La solución debe permitir la configuración de políticas basadas en localización, donde estas puedan enforzar acciones distintas si el usuario está dentro o fuera de la red.

La solución deberá emplear técnicas de reconocimiento de patrones de texto y diccionarios predefinidos.

Las políticas de la solución deberán abarcar el proceso de clasificación, descubrimiento, monitoreo y protección de la información sensitiva.

La solución debe permitir la creación y configuración de las clasificaciones deseadas, como por ejemplo, Confidencial, Restringido o Público.

Para cada clasificación, se debe permitir la definición de información que debe ser protegida. Los métodos de definición deben incluir:

Expresiones Regulares;

Diccionarios;

Tipo de archivo;

Origen o Destino;

Grupos de aplicaciones;

La solución debe poseer métodos avanzados de identificación y rastreamiento de contenido por medio de creación de firmas o huellas de contenido, permitiendo que estas se utilicen para el rastreo del contenido total o parcial de los documentos sensibles.

Estas firmas deberán ser almacenadas como atributo extendido de los archivos, permitiendo que la solución mantenga una persistencia en el proceso de clasificación de datos

La solución debe permitir que las clasificaciones basadas en firmas entreguen la siguiente información de contexto a los incidentes:

Aplicación web de la cual se generó el archivo;

Ruta compartida de la cual se copió el archivo;

Servicio de nube del cual se descargó el archivo;

La solución debe poseer capacidades de realizar escaneos de todos los archivos almacenados en disco, así como los correos, con el propósito de identificar y descubrir información sensitiva.

La solución debe permitir tomar acciones correctivas a partir de los escaneos, como la puesta en cuarentena o la clasificación de un documento.

La solución debe permitir la carga manual de archivos para que la solución pueda crear firmas automáticas.

La solución debe permitir la clasificación manual de archivos, desde aplicaciones, o bien desde el explorador de Windows con solo dar click derecho a los archivos.

La solución debe contar con mecanismos para evitar la desinstalación o desactivación del agente.

La solución debe permitir que los usuarios soliciten excepción temporal (bypass) de las políticas y que estas excepciones puedan ser parametrizadas con tiempos definidos, desde 5 minutos a 30 días.

El agente debe soportar la ejecución en modo a prueba de fallos en sistemas operativos Windows.

El agente debe soportar la parametrización de uso máximo de memoria RAM.

La solución debe permitir que cada módulo sea deshabilitado en caso de que no esté siendo utilizado en las reglas de protección.

La solución debe tener, como mínimo, las siguientes clasificaciones predeterminadas:

EAR

HIPAA

PCI

PHI

SOX

US PII

La solución debe poseer capacidades de identificar información sensitiva en base a patrones avanzados (expresiones regulares), incluyendo, como mínimo, los siguientes patrones:

Credit Card Numbers

Email Address

IP Address v4 y v6

MAC Address

Mexico banking standard (CLABE)

Multiple Common PCI Cards

La solución debe poseer capacidades de identificar información sensitiva en base a diccionaros, incluyendo, como mínimo:

- Profit Loss
- Sarbanes-Oxley Sensitive
- Source Code CPP
- Source Code Java
- Source Code Python
- User Name
- Wire Transfer
- Bank ABA
- Bank ACNT
- Bank STMT
- Classified
- Compensation & Benefits
- Compliance Report
- Confidential
- Credit Report
- Date Of Birth
- Drivers License
- Financial Audits
- Financial Report
- Last Name
- Legal
- Network Security
- Password
- PCI GLBA

La solución debe permitir la clasificación de documentos a raíz de sus propiedades. Debe ser posible utilizar, como mínimo, los siguientes campos:

- Author
- Category
- Comments
- Company
- Keywords (Tags)
- Last Saved By
- Manager Name
- Security
- Subject
- Template
- Title

La solución debe permitir la definición de clasificaciones en base al origen o destino del documento, soportando, como mínimo:

- Aplicación
- Usuario o Grupo de Usuario

Carpeta Compartida
URL

La solución debe incluir los siguientes templates de aplicaciones:

3ds Max
Adobe Acrobat reader
Dev Studio and Microsoft compilers
Email Client Applications
Encryption Applications
Explorer
IM Applications
Installers
Java Compiler
Lotus Notes
Media Burner Applications
Microsoft Compilers
Microsoft Office Applications
P2P Applications
Rdpclip
Safari Browser
Scanners and Indexers
Web Browsers
WinAce Archiver
Windows OS Files
WinRar Archiver
Zip Applications

Además de los templates incluidos en la solución, el administrador debe tener la capacidad de crear templates personalizados en base a los ya incluidos.

La solución debe permitir la exclusión de documentos que no deben ser detectados (lista blanca).

La solución debe permitir el registro de documentos de forma manual y automática.

El registro de los documentos debe crear una firma, la cual debe ser automáticamente distribuida desde la consola de gestión centralizada.

La solución debe tener la capacidad forzar la clasificación manual por medio de integración con aplicaciones Office. Bajo esta condición, el usuario debe ser obligado a clasificar un documento o correo al momento de la creación, modificación o envío de la información sensitiva.

La solución debe ser capaz de identificar información sensitiva en los correos, tanto en los documentos adjuntos como en el cuerpo, cabecera o pie del correo o documento.

La solución debe tener la capacidad de incluir la siguiente información al momento de clasificar un correo:

Clasificación
Clasificado por
Fecha y Hora

La solución debe ser capaz de descubrir información clasificada (ejemplo: restringido, confidencial, secreto) almacenada localmente o en la nube.

La solución debe identificar la localidad en donde la información sensitiva está almacenada, así como el propietario de dicha información.

La solución debe permitir la visualización de todos los datos descubiertos durante el análisis en una consola unificada e intuitiva.

La solución debe soportar la clasificación de más de 300 tipos de contenido, como por ejemplo:

- Almacenamiento en Nube
- Documentos Microsoft Office
- Archivos PDF
- Archivos Multimedia
- Código Fuente
- Archivos comprimidos

La solución debe permitir la calendarización de tareas periódicas para análisis y descubrimiento de información.

La solución debe poseer capacidades de ejecutar tareas de descubrimiento utilizando agentes distribuidos, permitiendo el descubrimiento en:

- Sistema de archivo local;
- Email Local (PST y OST);

Al encontrar un archivo sensible en estaciones de trabajo, la solución debe permitir tomar, como mínimo, las siguientes acciones:

- Monitoreo;
- Cifrado;
- Aplicación de política de Rights Management (RM);
- Envío a Cuarentena;

El agente de endpoint debe permitir al usuario la ejecución local de tareas de análisis para descubrimiento de información sensitiva.

La solución debe permitir que el usuario final pueda tomar acciones de remediación (self-remediation).

El agente de endpoint debe clasificar un archivo de manera automática a raíz de la detección o descubrimiento de información sensitiva.

La solución debe permitir la parametrización de consumo de ancho de banda en los escaneos de descubrimiento de información sensitiva.

La solución debe incluir reglas de protección de datos predefinidas, enfocadas a la protección de datos de estándares como PCI-DSS.

El panel de creación de reglas debe poseer los siguientes campos, como forma de facilitar la visualización de las reglas:

- Estado de Regla
- Nombre de Regla
- Descripción
- Severidad
- Cantidad de incidentes por regla
- Vector de protección
- Fecha/Hora de modificación
- Administrador que modificó la regla

La solución deberá permitir crear reglas de protección de datos, por medio de los siguientes vectores:

Acceso de Aplicación

Transferencia y almacenamiento en nube

Correo

Carpetas Compartidas

Impresión

Almacenamiento Removible

Captura de Pantalla

Web

Para cada definición de regla, la solución deberá permitir los siguientes campos:

Clasificación del dato a ser protegido;

Usuario o Grupo;

Excepciones;

Reacción;

Severidad;

La solución debe ser capaz de aplicar políticas distintas para agentes conectados en la red interna, o bien conectados desde una red externa por medio de VPN.

La solución debe permitir el almacenamiento de las evidencias que formen parte de los incidentes.

La solución debe permitir la aplicación de políticas, desde una única consola y de manera unificada, para las siguientes áreas de cobertura:

Endpoint;

Red;

Nube;

La solución debe permitir la creación de listas negras de aplicaciones, y que estas sean categorizadas de acuerdo a su funcionalidad:

Editor: Aplicaciones utilizadas para la creación y modificación de documentos.

Explorer: Aplicaciones utilizadas para la gestión de archivos, como copia o eliminación.

Trusted: Aplicaciones que requieran acceso ilimitado a la información sensitiva.

Archiver: Aplicaciones de compresión de archivos (WinZip, WinRAR).

La solución debe permitir la búsqueda de evidencias en la consola, como forma de mejorar la investigación de los incidentes.

La solución debe proveer, por medio de la consola, la información exacta del contenido sensible que causó la generación del incidente.

La consola de gestión debe almacenar la información de los incidentes en forma de metadatos, con el propósito de enmascarar la información sensitiva.

La consola de gestión debe permitir la creación de roles por grupos o usuarios (RBAC), con los siguientes permisos:

Gestor de Políticas

Analista de Incidentes, donde se pueda enmascarar la información sensitiva

Supervisor de análisis de incidentes, donde la información sensitiva no quede enmascarada (vista 4 ojos)

Gestor de reportes y alertas

La consola debe poseer, como mínimo, las siguientes funcionalidades:

- Ejecución de tareas en componentes gestionados y servidor de gestión
- Dashboards
- Políticas
- Gestión de usuarios y permisos
- Consultas y Reportes
- Gestión de incidentes
- Mesa de Ayuda

La gestión de incidentes debe tener la capacidad de entregar una vista rápida del estado de protección de datos, donde:

Debe poseer filtros capaces de identificar rápidamente el uso de la información sensitiva en cada uno de los vectores de fuga

- Dato en movimiento
- Dato en reposo
- Dato en uso

Debe permitir el uso de filtros, entre estos:

- Regla
- Tipo de incidente
- Usuario
- Destino
- Clasificaciones

Debe presentar de manera gráfica un top 10 de:

- Las reglas con más ocurrencias (hits)
- Los incidentes más comunes
- Los usuarios con un mayor número de violaciones
- Tendencias de incidentes por semana
- Clasificaciones

Debe poseer la capacidad de presentar un historial de incidentes, conteniendo:

- ID de incidente
- Módulo de detección
- Fecha y hora de incidente (UTC y zona horaria local)
- Severidad
- Tipo de Incidente
- Nombre y Apellido de colaborador
- Nombre de Usuario
- Nombre de computador
- Acción
- Reglas
- Clasificación
- Destino

Debe tener la capacidad de entregar y exportar tablas con los incidentes.

La solución debe permitir el enmascaramiento de datos sensitivos en la consola, de tal forma que esta información no sea mostrada en los incidentes.

La solución deberá permitir modificar la asignación, severidad, escalamiento y resolución de incidentes para un debido tratamiento de casos de investigación.

La solución deberá permitir la inclusión de más de un incidente en un caso de investigación.

La gestión de la solución deberá permitir la creación de dashboards y reportes para visualizar:

- Asignación de Políticas
- Eventos operacionales (instalación/desinstalación, omisión de políticas, justificaciones)
- Eventos de incidentes

Por medio de la consola de gestión unificada, la solución debe permitir el despliegue e instalación de cada uno de los componentes que forman parte de la misma.

La consola centralizada debe poseer capacidades de mesa de ayuda, con el propósito de:

Generar llaves de desinstalación de producto

Generar llaves para omisión de políticas, donde permita ingresar:

- Usuario
- Nombre de Equipo
- Correo
- Justificación
- Tiempo de omisión (5 mins – 30 días)
- Liberar archivos en cuarentena

1.3 Cloud 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

Soportar fingerprinting de información estructurada y no estructurada y utilizar dichas firmas para aplicar políticas de DLP

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

Permite la creación de identificadores completamente personalizados, compuestos de patrones, palabras clave y criterios de proximidad entre estas. Dentro de un mismo criterio de clasificación. (Por ejemplo un patrón de cédulas de ciudadanía que se activa sólo si encuentra en una proximidad de 20 caracteres las palabras "identidad" o "persona")

Permite ejecutar las siguientes acciones de remediación ante un incidente de DLP: generar un incidente, Aplicar una etiqueta, enviar notificación de correo, bloquear, remover link de colaboración, modificar permisos de colaboración, colocar en cuarentena, y eliminar. Esto para acciones realizadas desde máquinas y/o redes corporativas y no corporativas

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.

Puede integrar bajo una misma consola las soluciones de DLP on-premise (Endpoint y Red) y Cloud

Tiene la capacidad de configurar políticas de DLP vía Reverse Proxy o vía API para servicios Cloud corporativos.

Cuenta con la capacidad de ejecutar escaneos bajo demanda de DLP sobre la información en reposo en los servicios Cloud Corporativos integrados mediante API

Debe permitirle al administrador la capacidad de ejecutar un rollback sobre acciones de remediación para restaurar el documento o sus permisos de colaboración en servicios Cloud

Debe poder configurar diferentes niveles de severidad para un mismo criterio de identificación de la información

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.

Cuenta con sensores físicos y/o virtuales que apliquen los controles para tráfico web. Estos sensores deberán tener una versión de sistema operativo propia del fabricante. No se aceptarán sistemas operativos abiertos como Windows o Linux.

DLP para shadow IT debe poder integrarse con la solución de Proxy actual de la entidad, sin requerir proxys adicionales o esquemas duplicados tipo Proxy Chaining

Las políticas de DLP, clasificación e incidentes de DLP en endpoint (Capturas de pantalla, dispositivos removibles, Clipboard copy/paste), red y nube deberán poder ser administrados por una misma consola

La consola de administración de DLP podrá administrar los eventos de DLP de endpoint, de red, de cloud y tendrá la capacidad de centralizar los incidentes y gestión de CWPP para servicios de IaaS

La solución debe permitir la integración AIP para la lectura de etiquetas y la aplicación automática de las mismas vía API

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 debe poder integrar los eventos en una solución de SIEM via syslog

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 incorporar un modelo de User Behavior Analisys

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

Se debe contar con un modelo de amenazas que identifique amenazas reales automáticamente a partir de la correlación de múltiples anomalías

Debe permitir escaneos bajo demanda en busca de Malware vía API

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 soportar la inspección de archivos (bajo demanda y en tiempo real) y monitoreo de actividad de usuarios y administradores en los servicios de Gmail y Gdrive

La solución debe soportar DLP activo para GMail online sin la necesidad de desplegar agentes o instalar appliances o VMs

El control de DLP para correo en tiempo real debe aplicar para cualquier protocolo, aplicación o usuario, independiente de si es una máquina corporativa o una no corporativa

La solución debe estar en la capacidad de monitorear al menos 400 diferentes tipos de actividad de usuarios y administradores dentro de Google Enterprise

Se debe contar con la capacidad de bloquear en tiempo real los intentos de colaboración de información sensible hacia dominios externos desde GDrive tanto para máquinas corporativas como no corporativas

La solución debe poder aplicar sobre Google Enterprise todos los puntos de control de acceso

La solución debe tener la capacidad de analizar los repositorios de Google Enterprise (GDrive, GMail) en busca de Malware y limpiarlo (Cuarentena, Eliminar) vía API. Y poder reaccionar en la medida que se cargue Malware desde máquinas no corporativas o se reciba vía colaboración desde dominios externos.

La solución no debe requerir proxear o hacer inspección de contenido al tráfico de las máquinas corporativas hacia Google Enterprise para aplicar los casos de uso acá mencionados.

La solución debe realizar una auditoría de configuración sobre los servicios de Gmail y GDrive, identificando potenciales configuraciones vulnerables con base en las mejores prácticas.

La solución debe permitir el acceso desde máquinas personales controlando granularmente las acciones permitidas como por ejemplo "no puede acceder a la consola de Admin de Google Enterprise desde una máquina personal" o "No puede descargar información confidencial a un dispositivo personal"

Reportería y Gestión:

La solución debe permitirle a los administradores personalizar vistas y reportes basado 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, UEBA, Vulnerabilidades, Apps conectadas y Malware contra el Framework de MITRE ATTACK

La propuesta debe incluir servicios profesionales de implementación directo del fabricante

La propuesta debe incluir soporte 7x24

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 requiere 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 definan 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 a 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 a 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

2. PLATAFORMA DE SEGURIDAD PARA LA NAVEGACIÓN, LAS APLICACIONES SAAS, LA FUGA DE INFORMACIÓN, LA CLASIFICACIÓN DE INFORMACIÓN Y EL ACCESO
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 campañas de malware dentro del ambiente

La solución deberá de mostrar una comparación de detecciones entre:
- El ambiente
- El sector
- El País
- Mundial

La solución debe de mostrar cuándo fue la última detección de la campañas de malware en el ambiente

La solución debe de mostrar el detalle del impacto de la campañas de malware

La solución debe de mostrar información detallada de la campañas de malware como:
- MD5
- SHA256
- IP Address
- URL
- Domains

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

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

La solución debe de mostrar información de indicadores de compromiso como:
- IOC Type
- IOC Value
- Nombre de la amenaza
- Clasificación de la amenaza
- Endpoint afectados
- Sectores afectados
- Presencia en Países

La solución debe de contar con un buscador de campañas de malware

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

2.2 Antimalware con antiransomware y parcheo virtual

La solución deberá soportar los siguientes sistemas operativos de servidores:

· 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 Monterrey 12.x
· MacOS BigSur 11.x
· MacOS Catalina 10.15.x
· MacOS Mojave 10.14.x
· MacOS High Sierra 10.13.x
· MacOS Sierra 10.12.x
· MacOS El Capitán 10.11.x
· MacOS Yosemite 10.10.x
· MacOS Mavericks 10.9.x
· Linux Ubuntu 18.X, 20.X, 21.X (64-bit)
· SUSE Linux Desktop 12, 11
· Amazon Linux AMI 2017.9, 2014 and later
· Fedora 26, 25, 24, 23, 22
· Debian 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 anti-virus y firewall instalados previamente en la máquina.

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

La solución debe poder desplegar una aplicación cliente standalone que pueda gestionar cambios localmente en caso de que se necesite.
Se debe poder restringir completamente 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 click-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 características de protección Kevlar para navegadores con Active X

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 deteccion de inyeccion de codigo 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).
- Contra lectura de archivos en caché de IE.
- 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 sub reglas personalizadas
- Asignar las reglas por nombre de usuario

Para Protección contra amenazas avanzadas (antivirus de nueva generación)

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 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

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

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.

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;
- CDs/DVDs;

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;
- GPS;
- Infrarrojo;
- IEEE 1394;
- Mouse;
- Modem;
- Fax;
- Adaptadores de Red;
- PCMCIA;

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;

Al identificar un nuevo dispositivo conectado a las estaciones de trabajo, cuyo hardware es desconocido, la solución debe tener la capacidad de emitir una alerta a la consola centralizada indicando una nueva clase de dispositivo encontrado.

La solución debe permitir el control de dispositivos mediante su GUID.

La solución debe permitir la creación de los siguientes tipos de controles:
- Regla para control de dispositivo en Citrix XenApp;
- 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;
- Regla de dispositivo TrueCrypt;

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 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

La solución para el control de cambios deberá soportar el monitoreo de Alternate Data Streams (ADS)

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

La solución deberá de poder trabajar en modo escucha, de tal manera que al momento del despliegue pueda llevar el registro de las aplicaciones pero sin el riesgo de bloquear alguna aplicación válida.

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 funcion de proteccion 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 dinamicas 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

Para el control de cambios se deberá, desde la consola de administración, poder comparar entre dos archivos o versiones de archivos que existan en el mismo endpoint

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 archivo

Para el control de la ejecución de aplicaciones en el endpoint la solución deberá poder funcionar en los siguientes modos:

*Funcionalidad Habilitada

*Modo Evaluación
*Modo Actualizaciones
*Modo Deshabilitado
Para la autorización de aplicaciones permitidas a ejecutarse se deberá contar con los siguientes métodos:
*Por Checksum
*Por Certificados o Editor
*Por Nombre
*Por una adición manual a la lista blanca
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
Como mínimo se deberá contar con las siguientes consultas:
*Violaciones detectadas en las últimas 24 horas
*Violaciones en los últimos 7 días
*Estado de los endpoints con la solución que están siendo administrados por la consola
*Informe que ayude a cumplir con requerimiento 10.3.1 de PCI DSS (Resumen de cambios basados en usuario y fecha)

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 autorizada

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 solución deberá soportar los siguientes sistemas operativos:
Microsoft Windows: XP, Vista, 7, 8, 8.1 y 10, Linux: CentOS, SUSE, OEL, Ubuntu. Microsoft Windows Embedded: XPE, 7E, WEPOS, POS Ready 2009, WES 2009, 8 Industry, 8.1.

La solución deberá soportar los siguientes Sistemas Operativos de Microsoft los cuales ya no cuentan con soporte del fabricante: Windows XP.

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

Esta funcionalidad debe consumir menos de 10Mb de RAM

2.6 Firewall para las computadoras

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

Permitir o bloquear trafico solo hasta que el modulo y servicios de firewall este arriba.

Habilitar/deshabilitar protección IP Spoof
Habilitar/deshabilitar alertas de intrusión de Firewall
Agregar dominios específicos para bloqueo DNS.
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 y 2.8 EDR para las computadoras y 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 y endpoints

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 endpoint)

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 endpoint/server. (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 de 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 endpoint de manera nativa

La solución debe permitir poner en cuarentena a los host 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, o 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

En caso que los dispositivos no tengan acceso a internet se puede generar snapshots que se carguen por demanda en EDR para su análisis y complemento en las investigaciones como también determinar qué vulnerabilidades tiene la plataforma en un proceso de investigación declarado

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 host 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 una 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 equipos

La herramienta debe permitir visualizar eventos históricos hasta 30 días

La solución debe poseer integración con una herramienta para la gestion de politicas 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.

2.9 AntiMalware para dispositivos móviles

La solución debe permitir la protección de dispositivos móviles sin necesidad de desplegar componentes en sitio

La solución debe entregar la siguiente información sobre los dispositivos móviles:
- Vulnerabilidades
- Riesgo de aplicaciones
- Usuario asociado al dispositivo
- Sistema Operativo
- Estado de configuración
- Estado de Sistema Operativo (actualizable y/o vulnerable)

La solución debe recolectar la siguiente información en sus eventos:
- Vector (Dispositivo, Red, Aplicación)
- Usuario
- Ubicación en donde ocurrió el evento
- Detalle de amenaza de red (WiFi conectado, direcciones IP asociadas, redes WiFi cercanas)
- Detalle de amenaza de aplicación (riesgos de privacidad y seguridad)

La solución debe soportar dispositivos iOS y Android

La solución debe permitir la integración con las soluciones de gestión de dispositivos móviles (MDM/EMM) líderes en el mercado

La solución debe permitir la integración con soluciones de SIEM vía Syslog

La solución debe permitir controlar la información colectada sobre los eventos de amenazas, con el propósito de gestionar el nivel de privacidad de los usuarios finales de acuerdo a las políticas BYOD que tenga la organización

La solución debe permitir la gestión centralizada desde una misma consola

La solución debe analizar las amenazas en el dispositivo, garantizando que el mismo esté protegido aún estando offline o en modo avión

La solución debe utilizar mecanismos de Inteligencia Artificial para la detección de amenazas

La solución debe tomar acción en cuanto a amenazas basadas en:
- Dispositivo
- Red
- Aplicación

La solución debe permitir tomar las siguientes acciones en torno a las amenazas detectadas:
- Bloqueo y desconexión de Bluetooth o WiFi
- Bloqueo de conexiones de red (sinkhole)

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

2.10 Cifrado de computadoras

Ser administrado desde la misma consola de administración del antivirus preferentemente

Debe tener la capacidad de cifrar el disco completo, reemplazando el Master Boot Record (MBR)

La solución debe proveer mecanismos seguros que garanticen la recuperación del acceso en caso de pérdida de la contraseña. Estos mecanismos deben requerir la intervención y el intercambio de información con la consola de administración.

Debe ser capaz de descifrar el disco en forma automática, desde la consola de administración y mediante mecanismos manuales

La solución debe solicitar autenticación al usuario antes de iniciar la carga del sistema operativo (SO). Luego de iniciar el SO, la solución debe poder configurarse de manera que solicite o no, nuevamente, las credenciales de autenticación del usuario.

El producto debe soportar las siguientes máquinas clientes:
• Windows 7 and SP1 (32- and 64-bit)
• Windows 8
• Windows 10 y subsecuentes actualizaciones

El fabricante debe poseer al menos las siguientes certificaciones:
• Common Criteria EAL2 +, FIPS 140-1, FIPS 140-2
• AES CBC(e/d; 256)

La solución debe soportar al menos los siguientes algoritmos de Encripción:
• RC5-1024
• AES-256

La solución debe soportar los siguientes algoritmos de cifrado:
• RC5-12: CBC Mode, 1024 bit key, 12 rounds, 64 bit blocks. PassMark 20.7 (100%). The RC5-12 algorithm is compatible with the SafeBoot 3.x algorithm.
• RC5-18: CBC Mode, 1024 bit key, 18 rounds, 64 bit blocks, PassMark 20.7 (100%). The 18 round RC5 variant is designed to prevent the theoretical “Known Plaintext” attack.
• AES 256 (FIPS 140-2 Approved) – Recommended:
CBC Mode, 256 bit key, 128 bit blocks, PassMark 19.3 (93%) This algorithm is approved for FIPS 140-2 use.
• AES 256: CBC Mode, 256 bit key, 128 bit blocks, PassMark 19.3 (93%) Only recommended for use where support for SafeBoot 4.0 AES is required.
• DES (FIPS 140-1 Approved): CBC Mode, 56 bit key. 128 bit blocks. Passmark 16.5 (79%) Only for use in exceptional circumstances.
• Blowfish: CBC Mode, 448 bit key, 20 rounds, 64-bit blocks, PassMark 19.9 (96%) Withdrawn from general distribution - special order only.

Las actualizaciones de la solución deberán realizarse remotamente y desde una consola de administración centralizada
La arquitectura de la solución debe ser cliente-servidor
La solución debe emplear el mínimo de utilización del CPU

La solución debe interceptar el mecanismo de logon de Microsoft Windows utilizando el GINA en el Credential Manager en Windows 7/8/10

La solución debe soportar la unificación del usuario y contraseña utilizadas por el usuario en el directorio Activo de Microsoft
La solución se debe integrar con herramientas de análisis forense de externos para obtener una imagen protegida del disco encriptado, como:
• Guidance Software (EnCase)

La solución debe soportar el Trusted Platform Module (TPM) de Intel

La solución debe integrarse con Microsoft Applocker

La solución debe integrarse con la herramienta de administración de VPRO del mismo fabricante

La solución debe permitir el manejo de cifrado nativo BitLocker y FileVault, brindado por Microsoft y Apple, respectivamente

El producto debe ser administrado desde la misma consola centralizada utilizada para las demás soluciones de protección del endpoint (Antivirus, Antispyware, HIPS, DLP y Control de Aplicaciones, entre otras)

La solución debe contar con una herramienta externa que utilice las Llaves de Encripción almacenadas en la consola de administración para ejecutar cualquier actividad de recuperación de discos o archivos.

La solución debe soportar Single Sign-On (SSO) en integración con las políticas de grupo (GPO) del Directorio Activo de Microsoft.

La solución debe soportar tokens o herramientas de Autenticación SSO.

La solución solo debe poder removerse del sistema por un usuario administrador y remotamente.

La solución debe contar con la opción de generar un "código de respuesta" para la recuperación del administrador

El acceso de los usuarios administradores a la consola de administración debe poder hacerse basado en roles

La consola de administración debe permitir la creación de políticas de autenticación que no sean de alcance global

La solución debe ser capaz de generar un QR Code para auto recuperar la contraseña y acceso al sistema.

La solución debe proveer reportes del estado de la solución en las máquinas administradas. Todos estos reportes deben ser exportables vía correo o documentos XML, PDF y XLS.

La solución debe proveer un reporte de los sistemas cifrados, mostrando un estado de Cifrado o Descifrado

La solución debe permitir el cifrado de folders y archivos

El cifrado de folders y archivos debe poder hacerse con llaves de cifrado diferentes para grupos de usuarios diferentes

El cifrado debe permitir que una misma computadora consuma llaves de cifrado diferentes si así se requiere

El cifrado debe permitir establecer políticas que exijan el cifrado de archivos generados por una aplicación con una llave de cifrado específica

El cifrado debe permitir establecer políticas que exijan el cifrado de archivos incluidos en un folder en específico

El cifrado debe permitir establecer políticas para forzar el cifrado de dispositivos periféricos

El cifrado debe permitir cifrar archivos y/o folders y que estos puedan descifrarse con un password

El establecimiento de todas las políticas de cifrado de archivos y folders debe hacerse de manera centralizada desde la consola de administración

El resguardo de bitácoras de falla del cifrado de archivos y folders debe hacerse desde la consola de administración central

La solución debe ser capaz de enviar reportes y notificaciones por email en los siguientes formatos:
- HTML
- CSV
- PDF
- XML

La solución debe permitir generar reportes basados en eventos históricos

La solución debe contener contener reportes y consultas (queries) que se puedan personalizar

2.11 Sandbox para el endpoint

La solución de análisis avanzado de malware del tipo sandboxing 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 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 anteriormente 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 deberá contar con una herramienta que permita importar máquinas basadas en el entorno real de la organización. Deberá utilizar para esto el formato VMDK.

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)
b. MS Office Files (.doc, .docx, .xls, .xlsx. .ppt, .pptx)
c. PDF Files (PDF files, Adobe Flash files (SWF))
d. Compressed Files (.zip, .cab, .7z, .zip, .rar , msi, .lzh, .lzma,)
e. Android Application Package (.apk)
f. Java Archives (JAR), CLASS, Java Script, Java bin files
g. Images (.jpeg, .png, .gif)
h. 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 interno 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

La solución deberá proveer la capacidad de integrarse mediante RESTful API con otros dispositivos

Gestion

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

Reporting

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

2.12 Parchado

La solución deberá ser integrada preferentemente con la consola del antivirus con el fin de reducir los elementos para su instalación como son el servidor y la base de datos

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 informa 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

3. PREVISORES DE INTRUSOS DE RED
3.1 Previsor de intrusos de red sitio principal
Con una latencia de inspección no mayor a 100 microsegundos
Que permita contener ataques basados en patrones al menos 10,000
Que permita contener ataques distribuidos de denegación de servicio basados en la generación de perfiles estadísticos de tráfico, hasta 300
Cuente 8 interfaces de cobre con capacidad 100Mbps/1Gbps de "fail open", es decir, que si el equipo se cae la información siga fluyendo
Cuente al menos con 2 interfaces SFP con capacidad de 10Gbps
Cuente 4 interfaces 10Gbps SR con la capacidad de que si el equipo se cae el tráfico siga fluyendo, es decir, "fail open"
Deberá soportar un throughput de hasta 5 Gbps y una inspección de hasta 3,000,000 de conexiones concurrentes
Deberá soportar la inspección de https pudiendo desencriptar paquetes con hasta 1024 llaves distintas
Deberá ser administrado desde una consola centralizada

Los segmentos conectados in-line requerirán mecanismos de bypass (fail-open) a fin de que un fallo en los equipos no impacte en el normal funcionamiento de la red. Los mismos pueden ser integrados en el mismo equipo o externos proporcionados por el mismo fabricante.
El equipamiento deberá contar con discos de estado sólido (SSD).
Deberá contar con fuentes redundantes
Los sensores deberán contar con puertos seriales y para propósito de inicialización o troubleshooting.
Toda comunicación entre los sensores y la consola de gestión deberá ser autenticada y encriptada. Indicar que mecanismos se utilizan.
Las soluciones deben tener la posibilidad de crecer en desempeño por medio de licenciamiento y stacking de equipos
Se requiere una solución de prevención de intrusiones de red (IDS/IPS), capaz de proteger a la organización contra amenazas tales como Exploits, Amenazas Avanzadas Persistentes, Malware avanzado, Botnets, Ataques de Denegación de Servicio Distribuido y Ataques de reconocimiento entre otros.
Deberá estar compuesta por sensores desplegados en la red y un sistema de gestión centralizada.
Los sensores deberán ser de funcionalidad dedicada, es decir, no deberán correr en hardware compartido tales como dispositivos multifuncionales (UTM) o Firewalls.
Deberá estar basados en un sistema operativo pre-endurecido específico para seguridad. Por seguridad y facilidad de administración y operación, no se aceptarán soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows
Poseer licenciamiento ilimitado de usuarios y host en su modalidad de IPS.
Deberá incluir todos los accesorios y cables necesarios para la total instalación y puesta en operación.
El sensor deberá implementarse en la red en forma transparente, en capa 2 del modelo OSI. No requerirá cambios de topología de red ni modificaciones al esquema de ruteo.
Cada puerto del sensor deberá poder implementarse en las siguientes modalidades: - Puerto SPAN a través de Port Mirroring en un Switch -Mediante un TAP - En línea, cerrando la red en caso de falla (fail-close) -En línea, abriendo la red en caso de falla (fail-open)
Deberá contar con un puerto de gestión dedicado para la comunicación con la consola de Administración.
Deberá contar con un puerto de respuesta dedicado en caso de implementarlo en modo SPAN (IDS).

Deberá contar con la posibilidad de monitorear sin bloquear, aún estando en línea, e indicar en qué casos hubiera bloqueado (bloqueo simulado). Esta función deberá poder ser activada para el equipo entero o para interfaces individuales para aprender del tráfico y realizar actividades de tunning.
Deberá permitir la definición de reglas de control de acceso (ACLs) para establecer el tráfico permitido o denegado con los siguientes componentes - Dirección de host o red IPv4 -Protocolo y/o puerto TCP/UDP
El sensor no deberá contar con Interface de Gestión Local. Todo cambio deberá realizarse a través de la Consola de Gestión Centralizada. El sensor solo permitirá conexión SSH para troubleshooting y tareas de setup inicial.
Deberá ser capaz de inspeccionar tráfico SSL sin necesidad de hardware adicional. Informar cómo afecta la performance la activación de esta funcionalidad: -Deberá permitir definir puertos SSL no estándar, es decir, diferentes a TCP 443. -El sensor deberá mantener una copia de la clave privada del servidor Web en memoria volátil de manera que no pueda ser comprometida siendo alojada en un medio de almacenamiento. -Deberá ser posible configurar las siguientes opciones de captura:
Permitirá capturar paquetes de sesión completa que permitan servir de evidencia ante el análisis de un incidente. Tomando un número de bytes antes y después de que ocurre la amenaza
Deberá ser posible configurar las siguientes opciones de captura: - Registrar el paquete entero cuando un ataque es descubierto -Registrar solo el flujo entre origen y destino del ataque detectado - Registrar todos los nuevos flujos originados en el atacante independientemente del destino y todos los flujos iniciados en la máquina víctima del ataque. - Capturar paquetes por un período de tiempo configurable
Bajo condiciones de carga alta de tráfico en la red, el sensor deberá tener mecanismos dinámicos y automáticos para priorizar el análisis de cierto tráfico, salvando recursos para proteger segmentos importantes. Indicar cómo se logra este punto.
Deberá soportar la importación de hasta 1024 certificados SSL.
La solución deberá contar con un motor de detección basado en firmas y un servicio de suscripción que permita descargar nuevas firmas frecuentemente
Las firmas deberán tener un formato propietario y no estar expuesto al público en general de manera de que un atacante no tenga acceso a la lógica y tenga la capacidad de generar variantes de ataques que permita evadir dicha firma. No deberá utilizar SNORT o lenguajes similares como método primario de detección basado en firmas.

Deberá ser posible crear firmas personalizadas con el mismo lenguaje propietario del motor principal.
Deberá ser capaz de detectar y bloquear malware antes que produzcan una infección a través de la descarga desde Internet vía HTTP, FTP o SMTP.
El motor de análisis de malware deberá estar integrado en el mismo sensor. No requerirá de un equipo adicional para este propósito
Deberá guardar evidencia del archivo infectado, alertar y bloquear la conexión como respuesta ante un incidente de malware.
Al menos deberán ser analizados los siguientes tipos de archivos: - Ejecutables (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl) - Archivos Office (.doc, .docx, .xls, .xlsx. .ppt, .pptx) - Archivos PDF (.pdf, .xdp) -Archivos comprimidos (.zip, .rar) - Archivos Java (.jar)
Deberá detectar y bloquear hosts infectados que intenten comunicarse con servidores de comandos y control de redes BOT basado en comportamiento identificando en el flujo de tráfico que no existe un usuario interactuando con un sitio web.
Deberá detectar y bloquear hosts infectados que intenten comunicarse con servidores de comandos y control de redes BOT basado en comportamiento identificando en el flujo de tráfico que no existe un usuario interactuando con un sitio web.
Deberá utilizar técnicas para detección de redes BOT tales como: - Correlación de múltiples ataques diferentes en distintas sesiones de red -Heurística para detección por comportamiento - Anomalías en protocolos de comunicación -Respuesta de error en protocolos como DNS y SMTP -Comportamiento de escaneo de puertos -Conexiones a direcciones IP, nombres de dominio o URLs de Servidores de comandos y control conocidos a través de un servicio en la nube de reputación -Inspección de paquetes de respuesta de DNS para detección de Botnets avanzados tales como FFSN y DGA.
Deberá recibir información acerca de la reputación de los archivos analizados a través de un servicio que compare el hash del archivo con una base global del fabricante y poder responder si resulta ser malware.
Deberá contar con un motor que tenga la capacidad de analizar archivos PDF, extraer JavaScript y analizarlo mediante heurística en búsqueda de contenido malicioso y ejecutar una respuesta en caso de detectarlo. Deberá soportar archivos PDF encriptados y soportar archivos XDP.
Deberá contar con un motor que detecte contenido malicioso en archivos flash y pueda ejecutar una respuesta de bloqueo y alarma.

Deberá contar con un motor que tenga la capacidad de analizar y detectar contenido malicioso en archivos APK - Android Application Package
Deberá proteger aplicaciones Web inspeccionando HTTP y HTTPS a través de análisis heurístico que identifique inyecciones de SQL (SQL injections). No deberá utilizar string-matching para esto, sino que deberá analizar la sentencia SQL, verificar que sea válida y legítima y ,reconocer palabras claves maliciosas que alteren la estructura de una query (ej. UNION).
Deberá ser capaz de forzar a los clientes a utilizar TCP en lugar de UDP para las peticiones de DNS con el objetivo de proteger los servidores DNS de ataques de DoS spoof.
Deberá soportar la limitación de ancho de banda de un tipo de tráfico a través de políticas de rate limiting con el objetivo de limitar los efectos de un ataque de DoS (Denial of Service). Estas políticas podrán ser aplicadas por interfaz y por subinterfaz, por protocolo y puerto, por aplicación, por usuario de dominio, ubicación geográfica y direcciones IP.
Deberá ser capaz de limitar el ancho de banda de las conexiones provenientes de hosts externos basado en la reputación y geo-localización de dichos hosts. Es decir, para hosts con reputación negativa, limitar el ancho de banda a un número de conexiones por segundo y generar alerta si el umbral se supera, evitando de esa manera ataques de DoS.
Deberá soportar el uso de SYN Cookies para asegurar que el three-way handshake se realice antes de dejar pasar la conexión al servidor de destino y de esa manera bloquear ataques de SYN flood.
Deberá contar con un mecanismo de aprendizaje de tráfico para desarrollar estadísticas tales como tasas de tráfico de largo plazo y de corto plazo y cantidad de direcciones IP. Con esta información, detectar desviaciones que busquen generar impacto mediante ataques de DoS.
Deberá ser capaz de procesar información contenida en el campo XFF (X-Forwarder-For) de manera de obtener la dirección IP real del cliente cuanto la conexión proviene de un servidor proxy. Deberá utilizar esa información en las vistas de alertas, dashboards, reportes así como también en las políticas de firewall y de cuarentena para no bloquear una dirección IP de un proxy denegando el servicio a toda la red.
Deberá permitir definir la tasa de requests de URL por segundo por dirección IP a un website o a todos los websites para prevenir ataques de DoS.
El sensor tendrá la capacidad de detectar el browser web del cliente para mitigar ataques de DoS originados por bots.
Deberá recolectar datos de capa de aplicación para los protocolos más importantes como HTTP, FTP y SMTP para análisis forense. Ej. En el caso de SMTP deberá capturar la dirección del emisor, la dirección del receptor, nombre de attachment. Informar cómo afecta la performance la activación de esta funcionalidad

Deberá ser capaz de detectar ataques de reconocimiento tales como host sweeps, probes, escaneos de puertos, fuerza bruta de passwords y indexado de web servers.
Deberá detectar ataques de ARP spoofing.
La plataforma debe tener los siguientes motores de detección avanzada: - La plataforma debe tener motores de red avanzados de evasión y detecciones de amenazas. - Detección de amenazas en la inspección profunda de archivos con la emulación de browser - Motor de inspección "Suricata" Snort para tráfico cifrado https
La plataforma debe tener la opción de bloqueo inteligente basado en probabilidad de tener la vulnerabilidad, reputación de objetos, tipo de eventos donde si hay una alta probabilidad e impacto se debe bloquear el acceso y en caso de baja probabilidad el tráfico no lo debe bloquear
Deberá ser capaz de obtener detalles acerca de las estaciones de trabajo y servidores propios de la red desde algún sistema que posea esta información. Los datos deberán incluir Hostname, Nombre DNS, Nombre Netbios, Sistema Operativo, Service Packs instalados, Dirección IP, MAC Address así como también el software de seguridad instalado en el endpoint. Indicar con qué sistema puede integrarse para obtener esta información.
Deberá tener la capacidad de enviar archivos interceptados para realizar un análisis profundo a través de una solución de Sandboxing y luego bloquear en base al resultado de dicho análisis. Indicar que plataformas de sandboxing son soportadas y que mecanismo de integración utiliza. Se debe soportar la integración con solución de sandboxing en la nube Los resultados del análisis mediante Sandboxing deberán estar disponibles en la consola de la solución de IPS, junto con las evidencias y hallazgos.
Será posible identificar los usuarios de dominio conectados en una dirección IP origen o destino en un evento, a través de la integración con Active Directory. Deberá soportar múltiples dominios y no requerir instalación de agentes en los Domain Controllers.
Deberá ser capaz de realizar un análisis de impacto automático evaluando si un ataque logrará ser exitoso en un host vulnerable. Indicar que componentes adicionales se requieren para realizar dicha función.
Deberá identificar las aplicaciones que corren dentro de los protocolos de manera de aplicar políticas específicas. Ej. Bloquear Facebook y permitir el resto del tráfico HTTP/HTTPS
El fabricante actualizará periódicamente la lista de aplicaciones identificables y las categorizará de manera de aplicar políticas por tipo de aplicación
Será capaz de controlar determinadas funcionalidades de la aplicación tales como bloquear la transferencia de archivos a través de Mensajería Instantánea sin bloquear la aplicación completamente.

El sistema de gestión deberá proveer una API permitiendo que aplicaciones externas accedan a las funcionalidades de la solución. Indicar a través de que protocolo es posible acceder.
La solución deberá ser capaz de colectar información acerca de un endpoint y descifrar su sistema operativo y tipo de dispositivo a través de DHCP DISCOVER, DCHP REQUESTS, el campo de HTTP User Agent, y de los paquetes SYN y SYN + ACK de TCP. Indicar si otros componentes externos a la solución pueden colectar y enviar a la solución dicha información
Indicar si la solución puede obtener eventos de sensores de IPS basados en agentes (HIPS) instalados en estaciones de trabajo y servidores.
La solución deberá integrarse con la solución de SIEM actual y entregar datos de eventos y de registro de paquetes capturados para análisis forense.
Deberá soportar al menos el uso de SNMP, Syslog y querys de SQL para obtener los datos y reportarlos al SIEM.
Debe tener la capacidad de integrarse a un sistema de reputación local para tener un intercambio de inteligencia de amenazas extendido
Deberá permitir ejecutar respuestas en el sensor disparadas directamente desde el SIEM. Indicar si este mecanismo es nativo o requiere del desarrollo de scripts.
El sensor será capaz de exportar Netflow para análisis de tráfico en Capa 7. haya un sistema de análisis de flujos el cual debe hacerse fuera de los equipos pero del mismo fabricante sin costo adicional a través de una máquina virtual. Así mismo este análisis debe recopilar la información de procesos ejecutados en las estaciones finales mediante un agente para identificar anomalías (proceso vs tráfico de red)
Deberá contar con firmas que, si bien no constituyan un ataque, reporten un comportamiento que va en contra de las políticas de seguridad. Ej. Detección de tráfico de Mensajería Instantánea, tráfico de gestión SSH, Telnet, RDP en segmentos que no deberían tenerlo, tráfico P2P, streaming de video o música
3.2 Previsor de intrusos de red sitio secundario
Con una latencia de inspección no mayor a 100 microsegundos
Que permita contener ataques basados en patrones al menos 10,000
Que permita contener ataques distribuidos de denegación de servicio basados en la generación de perfiles estadísticos de tráfico, hasta 300
Cuente 8 interfaces de cobre con capacidad 100Mbps/1Gbps de "fail open", es decir, que si el equipo se cae la información siga fluyendo
Cuente 2 interfaces SFP con capacidad de 10Gbps
Cuente 4 interfaces 10Gbps LR con la capacidad de que si el equipo se cae el tráfico siga fluyendo, es decir, "fail open"
Deberá soportar un throughput de hasta 5 Gbps y una inspección de hasta 3,000,000 de conexiones concurrentes

Deberá soportar la inspección de https pudiendo desencriptar paquetes con hasta 1024 llaves distintas
Deberá ser administrado desde una consola centralizada
Los segmentos conectados in-line requerirán mecanismos de bypass (fail-open) a fin de que un fallo en los equipos no impacte en el normal funcionamiento de la red. Los mismos pueden ser integrados en el mismo equipo o externos proporcionados por el mismo fabricante.
El equipamiento deberá contar con discos de estado sólido (SSD).
Deberá contar con fuentes redundantes
Los sensores deberán contar con puertos seriales y para propósito de inicialización o troubleshooting.
Toda comunicación entre los sensores y la consola de gestión deberá ser autenticada y encriptada. Indicar qué mecanismos se utilizan.
Las soluciones deben tener la posibilidad de crecer en desempeño por medio de licenciamiento y stacking de equipos
Se requiere una solución de prevención de intrusiones de red (IDS/IPS), capaz de proteger a la organización contra amenazas tales como Exploits, Amenazas Avanzadas Persistentes, Malware avanzado, Botnets, Ataques de Denegación de Servicio Distribuido y Ataques de reconocimiento entre otros.
Deberá estar compuesta por sensores desplegados en la red y un sistema de gestión centralizada.
Los sensores deberán ser de funcionalidad dedicada, es decir, no deberán correr en hardware compartido tales como dispositivos multifuncionales (UTM) o Firewalls.
Deberá estar basados en un sistema operativo pre-endurecido específico para seguridad. Por seguridad y facilidad de administración y operación, no se aceptarán soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows
Poseer licenciamiento ilimitado de usuarios y host en su modalidad de IPS.
Deberá incluir todos los accesorios y cables necesarios para la total instalación y puesta en operación.
El sensor deberá implementarse en la red en forma transparente, en capa 2 del modelo OSI. No requerirá cambios de topología de red ni modificaciones al esquema de ruteo.
La solución deberá tener la alternativa de desplegar tanto sensores físicos (hardware) como sensores en modalidad appliance virtual y ser gestionados desde el mismo sistema de gestión centralizada.

Cada puerto del sensor deberá poder implementarse en las siguientes modalidades: - Puerto SPAN a través de Port Mirroring en un Switch -Mediante un TAP - En línea, cerrando la red en caso de falla (fail-close) -En línea, abriendo la red en caso de falla (fail-open)
Deberá contar con un puerto de gestión dedicado para la comunicación con la consola de Administración.
Deberá contar con un puerto de respuesta dedicado en caso de implementarlo en modo SPAN (IDS).
Deberá contar con la posibilidad de monitorear sin bloquear, aún estando en línea, e indicar en que casos hubiera bloqueado (bloqueo simulado). Esta función deberá poder ser activada para el equipo entero o para interfaces individuales para aprender del tráfico y realizar actividades de tunning.
Deberá permitir la definición de reglas de control de acceso (ACLs) para establecer el tráfico permitido o denegado con los siguientes componentes - Dirección de host o red IPv4 -Protocolo y/o puerto TCP/UDPç
El sensor no deberá contar con Interface de Gestión Local. Todo cambio deberá realizarse a través de la Consola de Gestión Centralizada. El sensor solo permitirá conexión SSH para troubleshooting y tareas de setup inicial.
Deberá ser capaz de inspeccionar tráfico SSL sin necesidad de hardware adicional. Informar cómo afecta la performance la activación de esta funcionalidad: -Deberá permitir definir puertos SSL no estándar, es decir, diferentes a TCP 443. -El sensor deberá mantener una copia de la clave privada del servidor Web en memoria volátil de manera que no pueda ser comprometida siendo alojada en un medio de almacenamiento. -Deberá ser posible configurar las siguientes opciones de captura:
Permitirá capturar paquetes de sesión completa que permitan servir de evidencia ante el análisis de un incidente. Tomando un número de bytes antes y después de que ocurre la amenaza
Deberá ser posible configurar las siguientes opciones de captura: - Registrar el paquete entero cuando un ataque es descubierto -Registrar solo el flujo entre origen y destino del ataque detectado - Registrar todos los nuevos flujos originados en el atacante independientemente del destino y todos los flujos iniciados en la máquina víctima del ataque. - Capturar paquetes por un período de tiempo configurable

Bajo condiciones de carga alta de tráfico en la red, el sensor deberá tener mecanismos dinámicos y automáticos para priorizar el análisis de cierto tráfico, salvando recursos para proteger segmentos importantes. Indicar cómo se logra este punto.
Deberá soportar la importación de hasta 1024 certificados SSL.
La solución deberá contar con un motor de detección basado en firmas y un servicio de suscripción que permita descargar nuevas firmas frecuentemente
Las firmas deberán tener un formato propietario y no estar expuesto al público en general de manera de que un atacante no tenga acceso a la lógica y tenga la capacidad de generar variantes de ataques que permita evadir dicha firma. No deberá utilizar SNORT o lenguajes similares como método primario de detección basado en firmas.
Deberá ser posible crear firmas personalizadas con el mismo lenguaje propietario del motor principal.
Deberá ser capaz de detectar y bloquear malware antes que produzcan una infección a través de la descarga desde Internet vía HTTP, FTP o SMTP.
El motor de análisis de malware deberá estar integrado en el mismo sensor. No requerirá de un equipo adicional para este propósito
Deberá guardar evidencia del archivo infectado, alertar y bloquear la conexión como respuesta ante un incidente de malware.
Al menos deberán ser analizados los siguientes tipos de archivos: - Ejecutables (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl) - Archivos Office (.doc, .docx, .xls, .xlsx. .ppt, .pptx) - Archivos PDF (.pdf, .xdp) -Archivos comprimidos (.zip, .rar) - Archivos Java (.jar)
Deberá detectar y bloquear hosts infectados que intenten comunicarse con servidores de comandos y control de redes BOT basado en comportamiento identificando en el flujo de tráfico que no existe un usuario interactuando con un sitio web.
Deberá detectar y bloquear hosts infectados que intenten comunicarse con servidores de comandos y control de redes BOT basado en comportamiento identificando en el flujo de tráfico que no existe un usuario interactuando con un sitio web.

Deberá utilizar técnicas para detección de redes BOT tales como: - Correlación de múltiples ataques diferentes en distintas sesiones de red -Heurística para detección por comportamiento - Anomalías en protocolos de comunicación -Respuesta de error en protocolos como DNS y SMTP -Comportamiento de escaneo de puertos -Conexiones a direcciones IP, nombres de dominio o URLs de Servidores de comandos y control conocidos a través de un servicio en la nube de reputación -Inspección de paquetes de respuesta de DNS para detección de Botnets avanzados tales como FFSN y DGA.
Deberá recibir información acerca de la reputación de los archivos analizados a través de un servicio que compare el hash del archivo con una base global del fabricante y poder responder si resulta ser malware.
Deberá contar con un motor que tenga la capacidad de analizar archivos PDF, extraer JavaScript y analizarlo mediante heurística en búsqueda de contenido malicioso y ejecutar una respuesta en caso de detectarlo. Deberá soportar archivos PDF encriptados y soportar archivos XDP.
Deberá contar con un motor que detecte contenido malicioso en archivos flash y pueda ejecutar una respuesta de bloqueo y alarma.
Deberá contar con un motor que tenga la capacidad de analizar y detectar contenido malicioso en archivos APK - Android Application Package
Deberá proteger aplicaciones Web inspeccionando HTTP y HTTPS a través de análisis heurístico que identifique inyecciones de SQL (SQL injections). No deberá utilizar string-matching para esto, sino que deberá analizar la sentencia SQL, verificar que sea válida y legítima y ,reconocer palabras claves maliciosas que alteren la estructura de una query (ej. UNION).
Deberá ser capaz de forzar a los clientes a utilizar TCP en lugar de UDP para las peticiones de DNS con el objetivo de proteger los servidores DNS de ataques de DoS spoof.
Deberá soportar la limitación de ancho de banda de un tipo de tráfico a través de políticas de rate limiting con el objetivo de limitar los efectos de un ataque de DoS (Denial of Service). Estas políticas podrán ser aplicadas por interfaz y por subinterfaz, por protocolo y puerto, por aplicación, por usuario de dominio, ubicación geográfica y direcciones IP.
Deberá ser capaz de limitar el ancho de banda de las conexiones provenientes de hosts externos basado en la reputación y geo-localización de dichos hosts. Es decir, para hosts con reputación negativa, limitar el ancho de banda a un número de conexiones por segundo y generar alerta si el umbral se supera, evitando de esa manera ataques de DoS.
Deberá soportar el uso de SYN Cookies para asegurar que el three-way handshake se realice antes de dejar pasar la conexión al servidor de destino y de esa manera bloquear ataques de SYN flood.

Deberá contar con un mecanismo de aprendizaje de tráfico para desarrollar estadísticas tales como tasas de tráfico de largo plazo y de corto plazo y cantidad de direcciones IP. Con esta información, detectar desviaciones que busquen generar impacto mediante ataques de DoS.
Deberá ser capaz de parsear información contenida en el campo XFF (X-Forwarder-For) de manera que obtenga la dirección IP real del cliente cuanto la conexión proviene de un servidor proxy. Deberá utilizar esa información en las vistas de alertas, dashboards, reportes así como también en las políticas de firewall y de cuarentena para no bloquear una dirección IP de un proxy denegando el servicio a toda la red.
Deberá permitir definir la tasa de requests de URL por segundo por dirección IP a un website o a todos los websites para prevenir ataques de DoS.
El sensor tendrá la capacidad de detectar el browser web del cliente para mitigar ataques de DoS originados por bots.
Deberá recolectar datos de capa de aplicación para los protocolos más importantes como HTTP, FTP y SMTP para análisis forense. Ej. En el caso de SMTP deberá capturar la dirección del emisor, la dirección del receptor, nombre de attachment. Informar cómo afecta la performance la activación de esta funcionalidad
Deberá ser capaz de detectar ataques de reconocimiento tales como host sweeps, probes, escaneos de puertos, fuerza bruta de passwords y indexado de web servers.
Deberá detectar ataques de ARP spoofing.
La plataforma debe tener los siguientes motores de detección avanzada: - La plataforma debe tener motores de red avanzados de evasión y detecciones de amenazas. - Detección de amenazas en la inspección profunda de archivos con la emulación de browser - Motor de inspección "Suricata" Snort para tráfico cifrado https
La plataforma debe tener la opción de bloqueo inteligente basado en probabilidad de tener la vulnerabilidad, reputación de objetos, tipo de eventos donde si hay una alta probabilidad e impacto se debe bloquear el acceso y en caso de baja probabilidad el tráfico no lo debe bloquear
Deberá ser capaz de obtener detalles acerca de las estaciones de trabajo y servidores propios de la red desde algún sistema que posea esta información. Los datos deberán incluir Hostname, Nombre DNS, Nombre Netbios, Sistema Operativo, Service Packs instalados, Dirección IP, MAC Address así como también el software de seguridad instalado en el endpoint. Indicar con qué sistema puede integrarse para obtener esta información.

Deberá tener la capacidad de enviar archivos interceptados para realizar un análisis profundo a través de una solución de Sandboxing y luego bloquear en base al resultado de dicho análisis. Indicar que plataformas de sandboxing son soportadas y que mecanismo de integración utiliza. Se debe soportar la integración con solución de sandboxing en la nube Los resultados del análisis mediante Sandboxing deberán estar disponibles en la consola de la solución de IPS, junto con las evidencias y hallazgos.
Será posible identificar los usuarios de dominio conectados en una dirección IP origen o destino en un evento, a través de la integración con Active Directory. Deberá soportar múltiples dominios y no requerir instalación de agentes en los Domain Controllers.
Deberá ser capaz de realizar un análisis de impacto automático evaluando si un ataque logrará ser exitoso en un host vulnerable. Indicar que componentes adicionales se requieren para realizar dicha función.
Deberá identificar las aplicaciones que corren dentro de los protocolos de manera de aplicar políticas específicas. Ej. Bloquear Facebook y permitir el resto del tráfico HTTP/HTTPS
El fabricante actualizará periódicamente la lista de aplicaciones identificables y las categoriza de manera de aplicar políticas por tipo de aplicación
Será capaz de controlar determinadas funcionalidades de la aplicación tales como bloquear la transferencia de archivos a través de Mensajería Instantánea sin bloquear la aplicación completamente.
El sistema de gestión deberá proveer una API permitiendo que aplicaciones externas accedan a las funcionalidades de la solución. Indicar a través de que protocolo es posible acceder.
La solución deberá ser capaz de colectar información acerca de un endpoint y descifrar su sistema operativo y tipo de dispositivo a través de DHCP DISCOVER, DCHP REQUESTS, el campo de HTTP User Agent, y de los paquetes SYN y SYN + ACK de TCP. Indicar si otros componentes externos a la solución pueden colectar y enviar a la solución dicha información
Indicar si la solución puede obtener eventos de sensores de IPS basados en agentes (HIPS) instalados en estaciones de trabajo y servidores.
La solución deberá integrarse con la solución de SIEM actual y entregar datos de eventos y de registro de paquetes capturados para análisis forense.
Deberá soportar al menos el uso de SNMP, Syslog y querys de SQL para obtener los datos y reportarlos al SIEM.
Debe tener la capacidad de integrarse a un sistema de reputación local para tener un intercambio de inteligencia de amenazas extendido
Deberá permitir ejecutar respuestas en el sensor disparadas directamente desde el SIEM. Indicar si este mecanismo es nativo o requiere del desarrollo de scripts.

El sensor será capaz de exportar Netflow para análisis de tráfico en Capa 7. haya un sistema de análisis de flujos el cual debe hacerse fuera de los equipos pero del mismo fabricante sin costo adicional a través de una máquina virtual. Así mismo este análisis debe recopilar la información de procesos ejecutados en las estaciones finales mediante un agente para identificar anomalías (proceso vs tráfico de red)
Deberá contar con firmas que, si bien no constituyan un ataque, reporten un comportamiento que va en contra de las políticas de seguridad. Ej. Detección de tráfico de Mensajería Instantánea, tráfico de gestión SSH, Telnet, RDP en segmentos que no deberían tenerlo, tráfico P2P, streaming de video o música
3.3 Previsor de intrusos de red virtual
Con una latencia de inspección no mayor a 100 microsegundos
Que permita contener ataques basados en patrones al menos 10,000
Que permita contener ataques distribuidos de denegación de servicio basados en la generación de perfiles estadísticos de tráfico, hasta 120
Cuente 8 interfaces virtuales con capacidad 100Mbps/1Gbps
Que el throughput total que pueda analizarse al menos de 500 Mbps distribuido en al menos 8 hosts de VMWARE
Deberá ser administrado desde una consola centralizada
Los segmentos conectados in-line requerirán mecanismos de bypass (fail-open) a fin de que un fallo en los equipos no impacte en el normal funcionamiento de la red. Los mismos pueden ser integrados en el mismo equipo o externos proporcionados por el mismo fabricante.
El equipamiento deberá contar con discos de estado sólido (SSD).
Deberá contar con fuentes redundantes
Los sensores deberán contar con puertos seriales y para propósito de inicialización o troubleshooting.
Toda comunicación entre los sensores y la consola de gestión deberá ser autenticada y encriptada. Indicar que mecanismos se utilizan.
Las soluciones deben tener la posibilidad de crecer en desempeño por medio de licenciamiento y stacking de equipos
Se requiere una solución de prevención de intrusiones de red (IDS/IPS), capaz de proteger a la organización contra amenazas tales como Exploits, Amenazas Avanzadas Persistentes, Malware avanzado, Botnets, Ataques de Denegación de Servicio Distribuido y Ataques de reconocimiento entre otros.
Deberá estar compuesta por sensores desplegados en la red y un sistema de gestión centralizada.
Los sensores deberán ser de funcionalidad dedicada, es decir, no deberán correr en hardware compartido tales como dispositivos multifuncionales (UTM) o Firewalls.

Deberá estar basados en un sistema operativo pre-endurecido específico para seguridad. Por seguridad y facilidad de administración y operación, no se aceptarán soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows
Poseer licenciamiento ilimitado de usuarios y host en su modalidad de IPS.
Deberá incluir todos los accesorios y cables necesarios para la total instalación y puesta en operación.
El sensor deberá implementarse en la red en forma transparente, en capa 2 del modelo OSI. No requerirá cambios de topología de red ni modificaciones al esquema de ruteo.
La solución deberá tener la alternativa de desplegar tanto sensores físicos (hardware) como sensores en modalidad appliance virtual y ser gestionados desde el mismo sistema de gestión centralizada.
Cada puerto del sensor deberá poder implementarse en las siguientes modalidades: - Puerto SPAN a través de Port Mirroring en un Switch -Mediante un TAP - En línea, cerrando la red en caso de falla (fail-close) -En línea, abriendo la red en caso de falla (fail-open)
Deberá contar con un puerto de gestión dedicado para la comunicación con la consola de Administración.
Deberá contar con un puerto de respuesta dedicado en caso de implementarlo en modo SPAN (IDS).
Deberá contar con la posibilidad de monitorear sin bloquear, aún estando en línea, e indicar en qué casos hubiera bloqueado (bloqueo simulado). Esta función deberá poder ser activada para el equipo entero o para interfaces individuales para aprender del tráfico y realizar actividades de tunning.
Deberá permitir la definición de reglas de control de acceso (ACLs) para establecer el tráfico permitido o denegado con los siguientes componentes - Dirección de host o red IPv4 -Protocolo y/o puerto TCP/UDPç
El sensor no deberá contar con Interface de Gestión Local. Todo cambio deberá realizarse a través de la Consola de Gestión Centralizada. El sensor solo permitirá conexión SSH para troubleshooting y tareas de setup inicial.

Deberá ser capaz de inspeccionar tráfico SSL sin necesidad de hardware adicional. Informar cómo afecta la performance la activación de esta funcionalidad: -Deberá permitir definir puertos SSL no estándar, es decir, diferentes a TCP 443. -El sensor deberá mantener una copia de la clave privada del servidor Web en memoria volátil de manera que no pueda ser comprometida siendo alojada en un medio de almacenamiento. -Deberá ser posible configurar las siguientes opciones de captura:
Permitirá capturar paquetes de sesión completa que permitan servir de evidencia ante el análisis de un incidente. Tomando un número de bytes antes y después de que ocurre la amenaza
Deberá ser posible configurar las siguientes opciones de captura: - Registrar el paquete entero cuando un ataque es descubierto -Registrar solo el flujo entre origen y destino del ataque detectado - Registrar todos los nuevos flujos originados en el atacante independientemente del destino y todos los flujos iniciados en la máquina víctima del ataque. - Capturar paquetes por un período de tiempo configurable
Bajo condiciones de carga alta de tráfico en la red, el sensor deberá tener mecanismos dinámicos y automáticos para priorizar el análisis de cierto tráfico, salvando recursos para proteger segmentos importantes. Indicar cómo se logra este punto.
Deberá soportar la importación de hasta 1024 certificados SSL.
La solución deberá contar con un motor de detección basado en firmas y un servicio de suscripción que permita descargar nuevas firmas frecuentemente
Las firmas deberán tener un formato propietario y no estar expuesto al público en general de manera de que un atacante no tenga acceso a la lógica y tenga la capacidad de generar variantes de ataques que permita evadir dicha firma. No deberá utilizar SNORT o lenguajes similares como método primario de detección basado en firmas.
Deberá ser posible crear firmas personalizadas con el mismo lenguaje propietario del motor principal.
Deberá ser capaz de detectar y bloquear malware antes que produzcan una infección a través de la descarga desde Internet vía HTTP, FTP o SMTP.
El motor de análisis de malware deberá estar integrado en el mismo sensor. No requerirá de un equipo adicional para este propósito
Deberá guardar evidencia del archivo infectado, alertar y bloquear la conexión como respuesta ante un incidente de malware.

Al menos deberán ser analizados los siguientes tipos de archivos: - Ejecutables (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl) - Archivos Office (.doc, .docx, .xls, .xlsx. .ppt, .pptx) - Archivos PDF (.pdf, .xdp) -Archivos comprimidos (.zip, .rar) - Archivos Java (.jar)
Deberá detectar y bloquear hosts infectados que intenten comunicarse con servidores de comandos y control de redes BOT basado en comportamiento identificando en el flujo de tráfico que no existe un usuario interactuando con un sitio web.
Deberá detectar y bloquear hosts infectados que intenten comunicarse con servidores de comandos y control de redes BOT basado en comportamiento identificando en el flujo de tráfico que no existe un usuario interactuando con un sitio web.
Deberá utilizar técnicas para detección de redes BOT tales como: - Correlación de múltiples ataques diferentes en distintas sesiones de red -Heurística para detección por comportamiento - Anomalías en protocolos de comunicación -Respuesta de error en protocolos como DNS y SMTP -Comportamiento de escaneo de puertos -Conexiones a direcciones IP, nombres de dominio o URLs de Servidores de comandos y control conocidos a través de un servicio en la nube de reputación -Inspección de paquetes de respuesta de DNS para detección de Botnets avanzados tales como FFSN y DGA.
Deberá recibir información acerca de la reputación de los archivos analizados a través de un servicio que compare el hash del archivo con una base global del fabricante y poder responder si resulta ser malware.
Deberá contar con un motor que tenga la capacidad de analizar archivos PDF, extraer JavaScript y analizarlo mediante heurística en búsqueda de contenido malicioso y ejecutar una respuesta en caso de detectarlo. Deberá soportar archivos PDF encriptados y soportar archivos XDP.
Deberá contar con un motor que detecte contenido malicioso en archivos flash y pueda ejecutar una respuesta de bloqueo y alarma.
Deberá contar con un motor que tenga la capacidad de analizar y detectar contenido malicioso en archivos APK - Android Application Package
Deberá proteger aplicaciones Web inspeccionando HTTP y HTTPS a través de análisis heurístico que identifique inyecciones de SQL (SQL injections). No deberá utilizar string-matching para esto, sino que deberá analizar la sentencia SQL, verificar que sea válida y legítima y ,reconocer palabras claves maliciosas que alteren la estructura de una query (ej. UNION).
Deberá ser capaz de forzar a los clientes a utilizar TCP en lugar de UDP para las peticiones de DNS con el objetivo de proteger los servidores DNS de ataques de DoS spoof.

Deberá soportar la limitación de ancho de banda de un tipo de tráfico a través de políticas de rate limiting con el objetivo de limitar los efectos de un ataque de DoS (Denial of Service). Estas políticas podrán ser aplicadas por interfaz y por subinterfaz, por protocolo y puerto, por aplicación, por usuario de dominio, ubicación geográfica y direcciones IP.
Deberá ser capaz de limitar el ancho de banda de las conexiones provenientes de hosts externos basado en la reputación y geo-localización de dichos hosts. Es decir, para hosts con reputación negativa, limitar el ancho de banda a un número de conexiones por segundo y generar alerta si el umbral se supera, evitando de esa manera ataques de DoS.
Deberá soportar el uso de SYN Cookies para asegurar que el three-way handshake se realice antes de dejar pasar la conexión al servidor de destino y de esa manera bloquear ataques de SYN flood.
Deberá contar con un mecanismo de aprendizaje de tráfico para desarrollar estadísticas tales como tasas de tráfico de largo plazo y de corto plazo y cantidad de direcciones IP. Con esta información, detectar desviaciones que busquen generar impacto mediante ataques de DoS.
Deberá ser capaz de parsear información contenida en el campo XFF (X-Forwarder-For) de manera de obtener la dirección IP real del cliente cuanto la conexión proviene de un servidor proxy. Deberá utilizar esa información en las vistas de alertas, dashboards, reportes así como también en las políticas de firewall y de cuarentena para no bloquear una dirección IP de un proxy denegando el servicio a toda la red.
Deberá permitir definir la tasa de requests de URL por segundo por dirección IP a un website o a todos los websites para prevenir ataques de DoS.
El sensor tendrá la capacidad de detectar el browser web del cliente para mitigar ataques de DoS originados por bots.
Deberá recolectar datos de capa de aplicación para los protocolos más importantes como HTTP, FTP y SMTP para análisis forense. Ej. En el caso de SMTP deberá capturar la dirección del emisor, la dirección del receptor, nombre de attachment. Informar cómo afecta la performance la activación de esta funcionalidad
Deberá ser capaz de detectar ataques de reconocimiento tales como host sweeps, probes, escaneos de puertos, fuerza bruta de passwords y indexado de web servers.
Deberá detectar ataques de ARP spoofing.
La plataforma debe tener los siguientes motores de detección avanzada: - La plataforma debe tener motores de red avanzados de evasión y detecciones de amenazas. - Detección de amenazas en la inspección profunda de archivos con la emulación de browser - Motor de inspección "Suricata" Snort para tráfico cifrado https

La plataforma debe tener la opción de bloqueo inteligente basado en probabilidad de tener la vulnerabilidad, reputación de objetos, tipo de eventos donde si hay una alta probabilidad e impacto se debe bloquear el acceso y en caso de baja probabilidad el tráfico no lo debe bloquear
Deberá ser capaz de obtener detalles acerca de las estaciones de trabajo y servidores propios de la red desde algún sistema que posea esta información. Los datos deberán incluir Hostname, Nombre DNS, Nombre Netbios, Sistema Operativo, Service Packs instalados, Dirección IP, MAC Address así como también el software de seguridad instalado en el endpoint. Indicar con qué sistema puede integrarse para obtener esta información.
Deberá tener la capacidad de enviar archivos interceptados para realizar un análisis profundo a través de una solución de Sandboxing y luego bloquear en base al resultado de dicho análisis. Indicar que plataformas de sandboxing son soportadas y que mecanismo de integración utiliza. Se debe soportar la integración con solución de sandboxing en la nube Los resultados del análisis mediante Sandboxing deberán estar disponibles en la consola de la solución de IPS, junto con las evidencias y hallazgos.
Será posible identificar los usuarios de dominio conectados en una dirección IP origen o destino en un evento, a través de la integración con Active Directory. Deberá soportar múltiples dominios y no requerir instalación de agentes en los Domain Controllers.
Deberá ser capaz de realizar un análisis de impacto automático evaluando si un ataque logrará ser exitoso en un host vulnerable. Indicar que componentes adicionales se requieren para realizar dicha función.
Deberá identificar las aplicaciones que corren dentro de los protocolos de manera de aplicar políticas específicas. Ej. Bloquear Facebook y permitir el resto del tráfico HTTP/HTTPS
El fabricante actualizará periódicamente la lista de aplicaciones identificables y las categorizará de manera de aplicar políticas por tipo de aplicación
Será capaz de controlar determinadas funcionalidades de la aplicación tales como bloquear la transferencia de archivos a través de Mensajería Instantánea sin bloquear la aplicación completamente.
El sistema de gestión deberá proveer una API permitiendo que aplicaciones externas accedan a las funcionalidades de la solución. Indicar a través de que protocolo es posible acceder.
La solución deberá ser capaz de colectar información acerca de un endpoint y descifrar su sistema operativo y tipo de dispositivo a través de DHCP DISCOVER, DCHP REQUESTS, el campo de HTTP User Agent, y de los paquetes SYN y SYN + ACK de TCP. Indicar si otros componentes externos a la solución pueden colectar y enviar a la solución dicha información
Indicar si la solución puede obtener eventos de sensores de IPS basados en agentes (HIPS) instalados en estaciones de trabajo y servidores.

La solución deberá integrarse con la solución de SIEM actual y entregar datos de eventos y de registro de paquetes capturados para análisis forense.
Deberá soportar al menos el uso de SNMP, Syslog y querys de SQL para obtener los datos y reportarlos al SIEM.
Debe tener la capacidad de integrarse a un sistema de reputación local para tener un intercambio de inteligencia de amenazas extendido
Deberá permitir ejecutar respuestas en el sensor disparadas directamente desde el SIEM. Indicar si este mecanismo es nativo o requiere del desarrollo de scripts.
El sensor será capaz de exportar Netflow para análisis de tráfico en Capa 7. haya un sistema de análisis de flujos el cual debe hacerse fuera de los equipos pero del mismo fabricante sin costo adicional a través de una máquina virtual. Así mismo este análisis debe recopilar la información de procesos ejecutados en las estaciones finales mediante un agente para identificar anomalías (proceso vs tráfico de red)
Deberá contar con firmas que, si bien no constituyan un ataque, reporten un comportamiento que va en contra de las políticas de seguridad. Ej. Detección de tráfico de Mensajería Instantánea, tráfico de gestión SSH, Telnet, RDP en segmentos que no deberían tenerlo, tráfico P2P, streaming de video o música
3.4Consola de administración de previsor de intrusos de red
El proveedor de la solución será responsable de proveer todas las actualizaciones necesarias y del soporte de todos los componentes de la misma incluyendo Sistema Operativo, Base de Datos y la aplicación en sí. Deberá ser implementada en modalidad Failover con una segunda consola que se active en caso de falla Deberá contar con una base de datos incluida en el producto. No requerirá la instalación o utilización de una base de datos externa. En caso de falla deberá incluir herramientas de respaldo que permitan recuperar la configuración ya establecida sin importar si el sistema de gestión centralizado se reubicara en un appliance de propósito específico, en un ambiente virtual o en una plataforma comercial certificada por el fabricante El acceso a la consola deberá ser vía Web a través de un navegador de uso general. No deberá requerir la instalación de ningún componente en la máquina de los administradores (cliente) Deberá soportar el acceso a través de dispositivos móviles Deberá contar con soporte de autenticación con los siguientes métodos: Base de usuarios local LDAP (Active Directory)

Deberá contar con múltiples perfiles de acceso que permita a los usuarios limitar sus acciones sobre la solución mediante privilegios entre ellos:
Administrador
Operador
Generador de Reportes
Analista o Experto

Deberá contar con diferentes dominios de gestión, permitiendo que un administrador de un dominio no tenga visibilidad sobre los dominios restantes, tal como ocurre en sistemas multi-tenant

Deberá de poder administrar diferentes dispositivos de prevención de intrusos
Deberá de ser base software y poder instalarse en un windows server
Deberá de poder contar con un control uniforme de configuraciones y directivas de control para múltiples sensores desde un único sistema

Deberá de poder contar con visualización de en tiempo real enviada de los diferentes elementos

La interfaz deberá de ser basada en WEB y gráfica
Deberá de contar con plantillas predefinidas que pueden utilizarse como base
Deberá de contar con una base de datos de firmas
Deberá de tener constantes actualizaciones de firmas
Deberá de tener la posibilidad de poder crear firmas personalizadas
Las firmas deberán de tener diferentes tipos de severidad
Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware)
Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo

Debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems

Debe de soportar excepciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma por firma
Debe de contar con una base de datos exploits conocidos
Debe de poseer firmas específicas para la mitigación de ataques DoS;
Debe de poseer firmas para bloqueo de ataques de buffer overflow

Debe de poseer firmas de C2 (Comando y control) generadas de forma automática

El informe de administración debe incluir no sólo eventos de intrusión, sino también información detallada sobre los perfiles del host, como el sistema operativo, los servicios, los puertos abiertos y las aplicaciones cliente, y las posibles vulnerabilidades del host.

La plataforma de administración debe permitir la personalización rápida de los informes mediante la importación desde paneles, flujos de trabajo y resúmenes de estadísticas.

La solución propuesta debe poder trabajar estrechamente y exportar registros a las herramientas de SIEM.

La plataforma de administración debe proporcionar múltiples tipos o formatos de salida de informes, como PDF, HTML y CSV.

Deberá permitir crear reportes personalizados seleccionando el tipo de datos y la forma de visualizarlos mediante tablas, gráfico de tortas, gráficos de barras y los campos que quieren visualizarse.

Contará con la capacidad de programar la ejecución automática de los reportes y el envío a través de correo electrónico

Deberá permitir generar reportes de auditoría con todas las actividades ejecutadas sobre la consola y los sensores.

Se deben centralizar los reportes de análisis de sandboxing en el IPS para poder tener correlación y análisis.

La plataforma de administración debe admitir múltiples mecanismos para emitir alertas (por ejemplo, SNMP, correo electrónico, SYSLOG).

La plataforma de gestión debe permitir la generación de "Informes de cumplimiento" estándar o personalizados que muestran porcentajes de activos y usuarios que cumplan con los requisitos. Al realizar un seguimiento de estas métricas a lo largo del tiempo, TI puede demostrar el progreso hacia los objetivos de cumplimiento y proporcionar a los auditores datos que demuestren el cumplimiento de las políticas de uso de la red.

La plataforma de administración debe incluir un potente diseñador de informes que automatice el diseño de las plantillas de informes. Cada plantilla de informe define las secciones individuales en el informe y específica la búsqueda en la base de datos que crea el contenido del informe, así como el formato de presentación (tabla, vista detallada, etc.) y el marco de tiempo.

La plataforma de gestión debe incluir "parámetros de entrada" en una plantilla de informe para ampliar su utilidad. Esto permitirá al administrador producir variaciones personalizadas del mismo informe. Por ejemplo, puede colocar un parámetro de entrada en el campo IP de destino de la búsqueda que produce un informe de eventos de intrusión y, al momento de generar el informe, puede especificar el segmento de red de un departamento cuando se le solicite la dirección IP de destino. El informe generado contiene sólo información relativa a ese departamento en particular.

Deberá poder integrarse con la consola de anticipación de amenazas para señalar la presencia de indicadores de compromiso en el tráfico de red, así como las recomendaciones para prever su impacto

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

3.5 Sandbox los previsores de intrusos de red

La solución de análisis avanzado de malware del tipo sandboxing permita probar en ejecución una muestra de código malicioso y generar un veredicto con información detallada.

La solución deberá detectar y controlar el malware avanzado.

La solución deberá actuar en conjunto con el IPS ofertado a través de las cuales se podrán enviar muestras de códigos maliciosos para su posterior análisis hacia una solución centralizada en red.

Deberá soportar trabajar en cluster u ofrecer mecanismos de alta disponibilidad

El sistema operativo del o los "appliance" debe ser diseñado por el fabricante para garantizar un adecuado desempeño de la solución.

Deberá entregar información clave para poder detectar sistemas que hayan sido comprometidos anteriormente 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 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.

La solución deberá permitir levantar hasta XX máquinas virtuales simultáneamente

Efectividad

La solución deberá poseer la capacidad de análisis dentro de ambientes virtuales sandbox con los últimos sistemas operativos del mercado. Tanto para servidores, estaciones de trabajo como equipo móvil.

Deberá soportar el análisis de Código estático de las muestras

La solución deberá contar con una herramienta que permita importar máquinas basadas en el entorno real de la organización. Deberá utilizar para esto el formato VMDK.

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)
b. MS Office Files (.doc, .docx, .xls, .xlsx. .ppt, .pptx)

c. PDF Files (PDF files, Adobe Flash files (SWF))
d. Compressed Files (.zip, .cab, .7z, .zip, .rar , msi, .lzh, .lzma,)
e. Android Application Package (.apk)
f. Java Archives (JAR), CLASS, Java Script, Java bin files
g. Images (.jpeg, .png, .gif)

h. 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 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 perimetral de siguiente generación IPS para recibir muestras de archivos para su análisis de malware avanzado y proveer la capacidad de bloqueo

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

La solución deberá proveer la capacidad de integrarse mediante RESTful API con otros dispositivos

Gestion

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

Reporting

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

4. SEGURIDAD DE BASES DE DATOS
4.1 Seguridad de bases de datos
La solución ofertada debe estar basada en agentes instalados en los servidores de bases de datos
La solución ofertada debe poder administrarse desde una consola centralizada, desde la cual se desplieguen políticas y se puedan ver logs de eventos. Donde la comunicación entre los agentes y la consola central debe ser cifrada mediante protocolos SSL/TLS
Debe contar con la opción de contar con una separación clara de deberes, administrador, reportes, auditoría. Así mismo separa los eventos dependiendo la regla(s) que son generadas

Está en capacidad de recolectar información de bases de datos, aplicaciones, usuarios y provee una interfaz central desde la cual se puedan configurar las políticas
No debe requerir cambios en el Kernel ni reinicio de los equipos de bases de datos. Como no se aceptan soluciones que deban trabajar en línea o sniffing de la red para poder realizar el monitoreo de transacciones de las bases de datos
La solución debe ser basada en el escaneo de transacciones de Bases de datos en la memoria , por lo que no debe requerir el uso de dispositivos o appliances de red ni modificaciones de la topología de la red
Desde el sistema central de gestión se debe tener la capacidad de realizar un descubrimiento de bases de datos en la red como también el inventario de vulnerabilidades, errores en configuración, o funcionalidades críticas que deban ser parametrizadas para evitar backdoors o evitar funcionalidades por defecto. En por lo menos una librería de 4.700 chequeos de parámetros de seguridad y vulnerabilidades
El sistema debe permitir realizar la búsqueda de información sensible o identificar tables que tenga este tipo de información
En caso que el sistema central pierda comunicación con los agentes, los eventos generados deben almacenarse localmente hasta restablecer la comunicación y evitar la pérdida y continuidad del servicio de protección de la base de datos
El monitoreo de las bases de datos por medio de sensores debe poder transportarse para activarse de acuerdo al licenciamiento disponible de forma que se pueda licenciar un grupo crítico de instancias y con el tiempo se puedan adicionar nuevos sensores a todas las bases de datos restantes
La plataforma debe soportar el monitoreo y escaneo de las siguientes bases de datos: - IBM DB2 9.5 or later for Linux, UNIX, and Windows - Microsoft SQL Server 2000 (or later) - MySQL version 5.1 or later (4.6, 4.7, 5.2, 5.3) - MariaDB version 5.5 (5.5.32 and later), 10.0, 10.1 and 10.2 on Linux - Oracle 8i (or later) - PostgreSQL version 9.3 (or later) - Sybase ASE version 12.5 (or later) - SAP HANA SPS 09, Revision 91 and later - Teradata 12, 13, 13.10, 14,15, and 15.1 on Linux - MongoDB 3.0 and later - Para Oracle 18 y 19 en ambientes como (Windows, linux, AIX, HP-UX, Solaris Intel)

Debe proveer un sistema de bloqueo de ataques o de nuevas vulnerabilidades descubiertas para las bases de datos sin que degenere en downtime del DBMS ni cambios en las bases de datos, solamente terminar la sesión.
La autenticación de usuarios debe soportar un método de acceso de usuarios basado en roles RBAC y control de múltiples roles de usuario lo que permitirá facilitar la separación de deberes
La aplicación debe registrar todas las actividades incluyendo logs detallados de cambio en políticas
Provee un sistema de monitoreo granular de las bases de datos con alertas en tiempo real, donde estas alertas se pueden almacenar en una instancia de base de datos SQL o Oracle para investigación y análsis
Facilidad para separar el monitoreo y el proceso de auditoría de todas las bases de datos incluyendo actividades del administrador
Realizar seguimiento y reportar todos los intentos fallidos de autenticación, así como también las transacciones no autorizadas habiéndose completado correctamente o no.
Provee protección tanto contra amenazas conocidas así como ataques de día cero, entre ellos: Ataques de fuerza bruta, SQL Injection entre los más relevantes
Proceso de control de cambios, debe hacer seguimiento a la ejecución de DDL, a la base de datos, hora, comando de SQL, IP del cliente e IP del servidor
Cuenta con un esquema de monitoreo granular de las actividades en las bases de datos con alertas en tiempo real y prevención de actividades que vayan en contra de las políticas de seguridad. Sin necesidad de activar la auditoría de las bases de datos
La solución monitorea el acceso local y conexiones encriptadas (Oracle ASO, SSL, SSH)
Debe soportar el monitoreo de bases de datos en ambientes virtualizados, físicos, en nube privada, nube pública sin necesidad de hacer cambios de licenciamiento
Debe detectar accesos sospechosos que violen las políticas y poner en cuarentena a usuarios sospechosos
La solución no debe tener como requerimiento o confiar en la auditoría propia de la base de datos/trace/ procedimientos almacenados/triggers de monitoreo para la generación de alertas o eventos de monitoreo
La aplicación debe contar con un set de políticas preconfiguradas y permitir la fácil creación de políticas de seguridad por medio de una ayuda de sintaxis para correcta configuración

La plataforma de contar con políticas que permitan contener ataques de ransomware para proteger la información que se encuentra en las bases de datos si un ataque o cifrado está en curso en la red
Brinda al usuario plantillas que permitan configurar políticas que lleven a la organización a cumplir con diferentes regulaciones. Estará en capacidad de permitir la creación de políticas personalizadas que permitan a la organización cumplir con regulaciones de la industria
La consola central debe ser basada en software para poder instalarse en ambientes virtuales o de nube con opción de trabajar con esquemas de alta disponibilidad sin necesidad de licenciamiento adicional. Esta consola sede debe poder instalar como aplicación en sistemas operativos: Windows Server 2012 R2,2016, 2019, RHLX 7.0, SUSE LX 11., 12.2 o superior, CentOS 7, Oracle LX 6 o 7
Debe realizar monitoreo de la actividad local de la base de datos, como procedimientos almacenados / Vistas / triggers / scripts
El sistema de protección debe permitir el monitoreo de acceso de usuarios a la base de datos asi como tambien debe alertar y prevenir sobre posibles accesos no autorizados
Está en capacidad de monitorear data encriptada o enmascarada
Está en capacidad de detectar ataques que vengan a través de la red, ataques de usuarios logeados en el servidor de bases de datos y ataques que provengan desde la misma base de datos a través de procedimientos almacenados
Debe realizar monitoreo local, no solo monitorear los accesos hechos desde la red
Al detectar un ataque debe estar en capacidad de lanzar una alerta o terminar la sesión/transacción en tiempo real
Debe poder habilitar/deshabilitar los chequeos que la solución realiza a nivel de sistema operativo en el DBMS
Podrá realizar monitoreo y reportes de los comandos de Data Manipulation Language (DML)
Debe liberar parches virtuales como máximo 48 horas después del Oracle CPU y parches de Microsoft para actuar con un módulo de Virtual patching y permitir continuar la operación de la base de datos sin tener que hacer modificaciones en ella
Debe estar en capacidad de mantener las alertas en un esquema de archivo para posteriores usos de auditoría
Cuenta con reportes predefinidos y la posibilidad de crear reportes personalizados, los reportes predefinidos deben ser mínimo (PCI-DSS, SOX, HIPAA/HITECH, GLBA, SAS70) adicional tener otros reporte predefinidos

La solución deberá permitir la generación de alertas en la consola y mediante correo electrónico ante un evento en particular o un comportamiento anómalo.

La solución deberá permitir hacer un trigger de alerta, cuando un usuario saque un determinado número de registros, de una base de datos.

La solución deberá proveer protección contra los ataques de ofuscación avanzados.
La solución deberá permitir la creación de reglas de monitoreo de acceso a las bases de datos, por horario o días hábiles.
La solución deberá poder monitorear aplicaciones que en un momento dado, estén accediendo a la base de datos y crear reglas de alerta cuando aplicaciones no permitidas, estén accediendo a la base de datos.

La solución deberá permitir la creación de objetos que faciliten su llamado en la creación de reglas.
Arquitectura

La consola deberá permitir una gestión centralizada de los agentes de monitoreo.
La solución deberá tener la flexibilidad para no ser intrusivo y solo hacer monitoreo de transacciones a nivel de red.
La solución deberá poder integrarse a una solución SIEM.

La solución deberá soportar un mecanismo para identificar usuarios detrás de conexiones hacia la base de datos, por medio de aplicaciones (opcional).
La solución deberá permitir la configuración de notificaciones vía correo, parámetros de SNMP, envío y/o almacenado de logs.

La solución deberá permitir la creación de backups de reglas configuradas.

La solución deberá consistir en una plataforma de gestión centralizada y sensores distribuidos, los cuales no deben ser intrusivos con la data de la base de datos.

La solución deberá ser basada en software, para evitar hacer un rediseño de la red de datos.
Auditoría

La solución deberá incluir una herramienta de manejo de casos (incident management) embebida.

La solución deberá poder hacer el monitoreo de actividad sobre las bases de datos sin requerir que la auditoría del motor de base de datos esté activa.
Compliance

La solución deberá permitir la creación de una línea base (wizard) asociada a parámetros normales de uso y/o regulaciones de compliance como por ejemplo PCI, para enfocar las alertas en las desviaciones de la línea base.

La solución deberá permitir el enmascaramiento de datos, usando mecanismos como expresiones regulares, para evitar la visualización de información personal identificable o sensible como números de tarjetas de crédito, que pudieran estar en los campos de las bases de datos.
Integración
La consola centralizada, debe permitir la gestión de otras soluciones de endpoint, con el objetivo de realizar consolidación de consolas.

La solución debe permitir la integración con soluciones de directorio como Microsoft AD.

La solución debe incluir como mínimo en las alertas, información de timestamp, usuario de sistema operativo, usuario de base de datos, sentencia ejecutada, aplicación, objetos accedidos, CMDTYPE, DBMS y regla que hizo match.

La solución debe permitir la generación de reportes de vulnerabilidades diferenciales, asociando valores de riesgo cualitativo (alto, medio y bajo).
La solución debe permitir la creación de reportes personalizados.

La solución debe permitir la generación de reportes de auditoría DML y archiving de eventos.
Dentro de los reportes de auditoría DML, debe existir la posibilidad de generar dichos reportes enriquecidos, con información del result set.

La solución debe contar con un módulo de construcción personalizada de queries, con el objetivo de generar reportes personalizados, asociados a dichos queries.
Tenga la capacidad de identificar vulnerabilidades específicas de las bases de datos, con al menos las siguientes características:
4,700 patrones a detectar, incluyendo claves de acceso débiles
Adicionando patrones al menos cada 72 horas

Tenga la capacidad de realizar un parcheo virtual SIN LA NECESIDAD DE INSTALAR LOS PARCHES DEL FABRICANTE DEL MOTOR DE BASE DE DATOS

5. CORRELACIONADOR DE EVENTOS SIEM
5.1 Correlacionador de eventos
Podrá ser físico o virtual. Deberá soportar una ingesta de 1000 eventos por segundo y contar con la información por al menos 1 año y/o con un espacio de 3 TB de información.

La plataforma debe permitir un crecimiento escalable tanto para distribuir sus componentes como para dar alta disponibilidad. Esta distribución puede ser una mezcla Software virtualizado o Appliances con opciones de correr en nube pública como (AWS, Azure, entre otros), plataforma virtual como (VMware, HyperV, KVM o XEN Citrix)
La solución SIEM a ofertar debe constar de uno o más appliances centralizado y/o distribuido e incluir agentes, clientes y componentes necesarios para cumplir los requerimientos técnicos y funcionales.
La arquitectura de la solución propuesta deberá ser flexible, por lo tanto puede estar compuesta por appliance endurecido y asegurado por el fabricante y/o por módulos de appliance virtuales, estos también creados y asegurados por el fabricante de la solución.
La solución SIEM debe contar de forma integrada y sin necesidad de licenciamiento aparte, un módulo para la creación de nuevos recolectores para tecnologías no soportadas por el fabricante de forma nativa.
La plataforma de SIEM debe integrar un bus de datos "Data Streaming BUS" Para la ingesta de datos de forma que estos puedan consumirse para el SIEM o para terceros sin necesidad de que sean normalizados o almacenados en la base de datos de correlación de SIEM
La solución SIEM deberá permitir entre otros usos monitorear, detectar y tomar medidas correctivas a través de la integración con elementos de seguridad en el endpoint y en el perímetro, al momento de detectar comportamientos asociados a amenazas avanzadas. La solución debe permitir agregar indicadores de compromiso (IOC) los cuales permitan incrementar las capacidad de análisis que posee la herramienta.
La solución SIEM deberá estar en capacidad detectar el mal uso de los recursos de navegación generados por los usuarios internos. Este monitoreo debe ser realizado a través de la integración con herramienta de filtro de contenido, para el monitoreo de categorías e indicadores de compromiso para identificar posibles accesos a sitios maliciosos no categorizados.
La solución SIEM debe permitir la creación de paneles y el monitoreo de actividad de usuarios privilegiados en el dominio tales como: Monitoreo del manejo de cuentas (altas, bajas, reset password, etc); elevación de privilegios, monitoreo de cuentas de usuarios VIP, monitoreo de cuentas de usuarios privilegiados entre otros.
La solución SIEM debe permitir agregar indicadores de compromiso de manera automática desde una herramienta de análisis de malware avanzado con el objetivo de enriquecer las capacidades de análisis que posee la herramienta.
La solución SIEM deberá permitir reducir falsos positivos y evaluar de forma dinámica el nivel de riesgo considerando la habilidad de unificar y correlacionar : · eventos, · información proveniente de herramientas de análisis de vulnerabilidades, y · criticidad de los activos o dispositivos. Esto mediante una fórmula parametrizable a la medida de los requerimientos de la entidad
Se requiere fortalecer la función de correlación mediante la incorporación de un motor de correlación avanzado que permita realizar al mismo tiempo de la correlación en tiempo real, correlación histórica y generación de indicadores de riesgo dinámicos sin necesidad de cambiar la plataforma base con la que se cuenta actualmente

El motor de correlación de la solución SIEM, deberá estar basado en métodos de lógica booleana, reglas personalizables, así como la detección de comportamiento anómalo mediante correlación estadística a través de cálculos de promedio. Adicionalmente la solución debe incluir reglas de correlación a nivel de seguridad preconfiguradas (Ej: Ataques de fuerza bruta)
La solución SIEM deberá contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores: · Importancia del evento · Criticidad del activo · Vulnerabilidades
La solución SIEM deberá permitir la correlación de eventos entre distintos dispositivos (Cross Device Correlation) al almacenar todos los eventos recolectados en una única tabla dentro de su base de datos, independiente del tipo de dispositivo o aplicativo que la genere, permitiendo así la definición de contenido de correlación entre distintos tipos de dispositivos (firewalls, IDPs, Sistemas Operativos) sin la necesidad de utilizar estructuras complejas o lenguajes de acceso a datos para la consulta y unión de datos.
La solución SIEM deberá proveer mecanismos para asegurar la integridad de los logs almacenados.
La solución SIEM deberá ser capaz de ofrecer acceso a los logs almacenados históricos sin la necesidad de hacer una restauración de estos (restore).
La solución SIEM deberá contar con un servicio de suscripción para la actualización y categorización de eventos durante la vigencia del contrato.
La solución SIEM deberá soportar la integración de eventos provenientes de Active Directory, DHCP y concentradores VPN para monitorear la asignación de direcciones IP y asociar eventualmente los usuarios.
La interfaz de administración de la solución SIEM deberá ofrecer herramientas necesarias para el análisis de los eventos tales como "whois", "dig", "Nslookup", "Traceroute", etc.
La solución SIEM debe proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente “fuera de la caja” (tales como aplicaciones o desarrollos hechos en casa) a través de la incorporación de un conjunto de herramientas que permitan definir la lógica para extraer, obtener, normalizar y categorizar los eventos mediante un editor de expresiones regulares:
Las herramientas para recolectar eventos de fuentes no soportadas deben proporcionar una interfaz que permita realizar las configuraciones necesarias.
La solución SIEM deberá tener la posibilidad de detectar actividad anormal en base a un línea de base detectando diferenciales
Los componentes de la solución SIEM que realizan la recolección de eventos deberán ofrecer la capacidad de ajuste en la hora de los eventos, en el caso de que el dispositivo que genere el evento no cuente con la hora correcta o no tenga configurado un servidor de NTP.
La solución SIEM deberá poder integrarse con más de 600 distintos tipos de productos y dispositivos en forma nativa sin la necesidad de definir un proceso de colección a la medida.

El componente de recolección debe proveer mecanismos que garanticen la entrega de eventos y que los eventos no se pierdan si el sistema no está disponible. Debe poder almacenar eventos en un caché local durante una situación de falla en la red y entregar los eventos cuando el sistema vuelva a estar en línea.
La solución SIEM deberá capturar información a través de: Syslog, OPSEC, WMI, RDEP, SDEE, eStreamer, CIFS, NFS, SCP, SFTP, HTTP, FTP, IPFIX, IBM Tivoli, MSSQL PULL, NETFLOW. Así mismo permitir la personalización para que también esté disponible para fuentes únicas, como aplicaciones internas.
La solución SIEM debe contar con módulo o componente de reportes que contenga plantillas predefinidas, basado en estándares internacionales. Posibilidad de manejar gráficos, tipo pie, barras, y otras características de personalización tales como incluir los logos de la compañía.
La solución SIEM debe permitir la gestión de incidentes de seguridad a través de funcionalidades de manejo de casos internos y workflow de incidentes.
La solución SIEM debe poseer una base de datos creada especialmente para la gestión de grandes volúmenes de datos
La base de datos no debe requerir ningún tipo de mantenimiento por fuera de lo que el sistema ejecuta.
Las alertas co-relacionadas deben permitir usar parámetros como delta de eventos, desviaciones, con el fin de asociar cambios en la ocurrencia de los mismos.
La solución SIEM deberá soportar la auditoría de usuarios autorizados en el sistema y registrar su actividad.
La solución SIEM deberá soportar de forma nativa la integración con soluciones de almacenamiento en red como SAN, NAS, NFS o CIFS, para el almacenamiento de la información recolectada, sin importar la marca se estos
La solución debe tener la funcionalidad de conectarse al sitio del fabricante para validar la existencia de nuevos contenidos. El contenido liberado debe tener la capacidad de agregar valor al monitoreo de la herramienta entregando distintos elementos adicionales tales como: - Reglas de correlación, Alarmas, Vistas (Dashboards), Reportes, Variables, Listas de vigilancia. Con su respectivo versionamiento. Con los siguientes casos de uso como mínimo: - Monitoreo de auditoría de Bases de Datos - Monitoreo de DNSs - Monitoreo de Explotación de Vulnerabilidades - Monitoreo de Firewall - Detección de malware en la red - Monitoreo de redes wireless - Monitoreo de autenticación de Windows - Filtrado y acceso Web por parte de los usuarios

Como requisito “mínimo”, la solución debe contar con los siguientes componentes: - Componente de gestión, administración y operación de la solución. - Componente de recolección de eventos y/o log’s de seguridad. - Componente de recolección de flujos de red. Deberá soportar al menos Netflow. - Componente de almacenamiento de eventos y/o log’s. - Agentes y conectores para recolectar eventos de seguridad de terceros. - Componente de reportes. - Componente de edición de parsers custom. - Componente de auditoría (registro de las actividades de los administradores y operadores de la solución. - Módulo avanzado de correlación (correlación histórica)
El o (los) appliance(s) deberá contar con mecanismos de redundancia, y tolerancia a fallas para resolver el caso de presentarse alguna contingencia, garantizando la recolección continua de los log’s y eventos de seguridad.
la solución deberá contar con la capacidad de consultar base de datos hadoop para enriquecer la información de que se correlaciona en el SIEM
La solución SIEM debe tener un manejador de severidad que le permita a los usuarios personalizar la criticidad de los eventos en múltiples niveles, realizando una ponderación que permita configurar dinámicamente la gravedad de un acontecimiento, o una serie de eventos, basándose en los valores de peso acostumbrados por la herramienta.
La solución SIEM debe realizar automáticamente la generación de un mapa de calor, asignándole valores de riesgo cualitativo (Alto, Medio y Bajo) a los incidentes que se estén presentando en un período de tiempo determinado.
La solución SIEM debe estar en capacidad de enlazar directamente fuentes externas como Bugtraq, ICE, CVE, OSVDB o Sequnia ID.
La solución SIEM debe estar en capacidad de utilizar datos de vulnerabilidades recolectados desde herramientas como (Nessus, Rapid7, Qualys, etc.) para vincularlos a los a los eventos. Ya que los vínculos a dichas herramientas deben ser directos, deben actualizarse constantemente 24/7.
La solución SIEM debe contar con mecanismos para realizar correlación basada en riesgo, si se llegara a requerir en un futuro por la organización.
La solución SIEM debe permitir la carga de indicadores de compromiso, ya sea por otra solución del mismo fabricante o por bases de datos abiertas como Stix o TAXII, con el objetivo de posibilitar la configuración de alertas accionables a las ciberamenazas que se puedan presentar en el entorno de red.
La solución SIEM debe permitir la configuración de listas negras, con el objetivo de posibilitar las respuestas accionables ante alertas co-relacionadas.
La solución SIEM debe estar en capacidad de comunicarse con bases de datos de reputación, con el objetivo de asociar parámetros como geolocalización a los parámetros de configuración de watchlists.
La solución SIEM debe estar en capacidad de hacer push de scripts, como parte de las opciones de respuestas accionables.

La solución debe permitir tomar indicadores de compromisos (IOC) desde fuentes remotas para acceder actividad relacionada con estos en el ambiente de la organización. Y contar con una suscripción del mismo fabricante para la descarga de listas de Ips de alto riesgo y sospechosas
La solución debe contar con un módulo para realizar la retrospección (backtrace) de los indicadores de compromiso para evaluar la presencia en el ambiente de la organización.
La solución debe tener la capacidad integrarse de forma nativa a un sistema de reputación corporativo que permita conocer la reputación local, global o de análisis de la herramienta de Sandboxing de los programas ejecutables en los equipos monitoreados.
La solución deberá integrarse al sistema de reputación corporativo a través de un protocolo de comunicación abierto multi-plataforma, que permita obtener el indicador de compromiso del archivo ejecutable analizado
La solución SIEM deberá proporcionar un módulo integrado para la administración de eventos e incidentes de seguridad permitiendo asociar reglas a acciones tales como: · enviar una notificación al equipo de operadores. · abrir y asignar un caso a un usuario para su investigación. · ejecutar un script.
La consola de administración centralizada debe proveer la configuración de controles de acceso basado en roles (RBAC) y permitir la configuración de privilegios de acuerdo a los perfiles asignados por el administrador de la solución. Permitiendo la segregación de funciones y acceso a eventos, obedeciendo al principio de mínimo privilegio.
La Solución SIEM deberá permitir desplegar más de un tablero gráfico (dashboards) de forma concurrente. Su actualización deberá ser en tiempo real sin la intervención del usuario o refresco manual. Desde el tablero de indicadores se debe tener la capacidad de visualizar los eventos base (drill down) y el detalle de cada evento.
Los tableros gráficos (dashboards) de eventos deberán ser personalizables, editables y duplicables por los usuarios de la Solución de Correlación de Eventos.
La solución SIEM deberá contar con dashboards predefinidos para regulaciones tipo PCI, HIPPA, ISO 27002,FISMA, SOX Asi como permitir la creación de grupos de Dashboards que ayuden a cumplimientos locales
La solución debe contar con la capacidad de importar e instalar paquetes de contenidos que incluyan reglas de correlación, alarmas, vistas, variables y listas de monitoreo orientadas a casos de uso específicos que ayuden a responder a las amenazas existentes de manera más eficiente.
La solución SIEM deberá proporcionar una interfaz de administración gráfica (GUI) propia, para el personal operativo, así como una interfaz de solo lectura diseñada para el personal de monitoreo y personal no técnico. Esta interfaz debe ser Web y segura (HTTPS)
La solución SIEM debe incluir contenido en modo de filtros, reglas predefinidas de correlación, monitores gráficos (dashboards) y reportes pre-configurados de monitoreo de dispositivos de red perimetral, enfocado a las mejores prácticas de seguridad y ataques más comunes.
El soporte técnico del fabricante deberá incluir las actualizaciones de producto, firmas, nuevos releases y nuevas integraciones.

La solución SIEM deberá ofrecer la capacidad de publicar reportes una vez que hayan sido ejecutados para que los reportes puedan ser consultados posteriormente sin necesidad de ejecutarlos nuevamente
La solución SIEM deberá integrar reportes tipo drill-down, es decir, a partir de los resultados de un reporte, seleccionar algún resultado y automáticamente ser transferido a un nuevo reporte que proporcione un mayor nivel de detalle.
El módulo de reportes, deberá permitir aceptar parámetros previos a la ejecución de un reporte, para poder focalizar los resultados del mismo. Ej.: Ingresar el nombre de usuario, nombre del dispositivo, etc.
El módulo de reportes deberá permitir la visualización de un panel gráfico (dashboard), que agrupe múltiples elementos y permita desplegar resultados de reportes, así como links externos. El dashboard deberá ser configurable e independiente para cada cuenta de usuario que utilice la solución.
La solución SIEM deberá contar con un módulo integrado para la ejecución de reportes sobre los eventos.
Los reportes generados podrán ser de tipo ejecutivos (gráficos), detallados (matriz/tabla) o una combinación de ambos.
El módulo de reportes, deberá permitir generar un reporte, ya sea desde cero, o bien, copiando y modificando reportes existentes.

6. Administración de cuentas con altos privilegios y gestión de cuentas de servicio
6.1 Administración de cuentas con altos privilegios y gestión de cuentas de servicio
La solución propuesta debe ser implementable en on-premise, híbrida y proporcionada como una oferta en la nube.
En las instalaciones: la solución propuesta debe admitir un método de instalación manual en los sistemas operativos estándar de la organización.
En las instalaciones: la solución propuesta debe admitir un instalador automatizado en los sistemas operativos estándar de la organización.
Híbrido: la arquitectura de la solución propuesta admite múltiples centros de datos en recursos de nube privada y locales.
Nube: la solución propuesta debe poder entregarse como un modelo de entrega de nube de software como servicio (SaaS).
La solución propuesta debe ser independiente del hipervisor y no depender de dispositivos físicos o virtuales.
La solución propuesta no puede basarse en componentes no estándar o patentados, como bases de datos o protocolos de red no disponibles comercialmente.
La solución propuesta debe incluir componentes para distribuir las cargas de trabajo en un entorno.
Describir las propiedades de la arquitectura de escalamiento horizontal de las soluciones propuestas.

La solución propuesta debe ser compatible con un proceso de actualización impulsado por un asistente y realizarse sin los servicios profesionales de los proveedores.
La solución propuesta debe ejecutarse en todo momento con la versión más reciente y con los parches completos del sistema operativo
La solución propuesta debe admitir los siguientes tipos de cuentas para el cambio de contraseña listo para usar:
Active Directory (todas las cuentas)
Usuario local de Windows y cuentas administrativas (2008 R2+)
Usuario local de Linux y cuentas administrativas (cualquier distribución)
Usuarios locales de Unix y cuentas administrativas (cualquier distribución)
Cuentas de sistemas de red (Cisco, Juniper, Blue Coat, Enterasys, etc.)
Hipervisores (Hyper-V, VMware, Xen, etc.)
Sistemas de gestión fuera de banda (iDrac, HP iLO, etc.)
Claves de acceso de AWS IAM
Cuentas MS Azure Office 365 / Azure AD
Cuentas de la fuerza de ventas
Claves SSH y dependencias con y sin contraseñas
Cuentas de bases de datos (ODBC, MySQL, MS SQL, IBM, SAP, Oracle, PostgreSQL, etc.)
Cuentas VMWare ESX/ESXi
Cuentas LDAP (OpenLDAP, Oracle Directory Server EE, etc.)
Cuentas de mainframe (RACF de z/OS)
La solución propuesta debe admitir un marco de secuencias de comandos intuitivo y fácil de usar que permita a los propietarios de la aplicación ampliar las funciones de gestión de credenciales al personal interno sin los servicios profesionales de los proveedores.
La solución propuesta debe tener una integración nativa con Active Directory y soportar LDAP(s).
La solución propuesta debe integrarse con los grupos de seguridad de Active Directory como un componente del control de acceso basado en roles.
La integración de Active Directory de la solución propuesta debe permitir un cronograma de sincronización configurable para automatizar la incorporación de nuevos usuarios.
La solución propuesta debe soportar la autenticación integrada de Windows para acceder a la plataforma.
La solución propuesta debe ser compatible con la autenticación local y los grupos de control de acceso basados en roles locales.
La solución propuesta debe ser compatible con cualquier proveedor de identidad SAML 2.0 para el inicio de sesión único.
La solución propuesta debe ser compatible con cualquier solución de autenticación de múltiples factores basada en RADIUS.
La solución propuesta debe admitir integraciones listas para usar con DUO, FIDO2, RADIUS y cualquier solución TOTP.
La solución propuesta debe ser compatible con la lista blanca de direcciones IP para los usuarios de acceso.
La solución propuesta debe admitir el enmascaramiento de los dominios de inicio de sesión disponibles durante el proceso de inicio de sesión del usuario.

La solución propuesta debe admitir un banner informativo personalizado en la pantalla de inicio de sesión sin modificaciones de CSS.
La solución propuesta debe ser configurable para hacer cumplir HTTPS a través de HSTS.
La solución propuesta debe admitir un panel único para la configuración de políticas en toda la implementación.
La configuración de la política de la solución propuesta debe incluir la capacidad de configurar los ajustes de administración de contraseñas, los ajustes de seguridad y la ubicación para la asignación de la carga de trabajo.
Las soluciones propuestas deben soportar la aplicación de políticas a nivel de cuenta y/o nivel de carpeta.
La solución propuesta debe admitir los siguientes flujos de trabajo de seguridad:
Justificación de acceso (el usuario debe presentar un motivo/comentario antes de acceder)
Aprobación de acceso: aprobación única
Aprobación de acceso: aprobación de varios pasos. Describa cómo se configura este flujo de trabajo en su plataforma.
Cuenta Check Out & Check In (contraseña de un solo uso y exclusividad)
Pago de cuenta con la capacidad de ejecutar scripts cargados (PowerShell, SSH, SQL) durante el proceso de pago previo y posterior.
La solución propuesta debe admitir un proceso de check out manual, forzado y automático basado en el tiempo.
Los flujos de trabajo de aprobación y justificación de las soluciones propuestas deben admitir la validación opcional de casos/tickets con un sistema de ticketing externo durante el proceso de justificación y aprobación.
La solución propuesta debe admitir integraciones de sistemas de tickets personalizados.
La solución propuesta debe proporcionar flujo de trabajo y gestión de políticas para la solicitud, el aprovisionamiento y el desmantelamiento de cuentas de servicio descubiertas y recién creadas.
La solución propuesta debe incluir una auditoría robusta y a prueba de manipulaciones de todas las actividades dentro y contra la plataforma.
La auditoría de la solución propuesta debe proporcionar el quién, qué, dónde y cuándo de la actividad.
La solución propuesta debe admitir el reenvío de registros a cualquier plataforma SIEM.
La solución propuesta debe admitir la captura de pulsaciones de teclas para los sistemas operativos Linux, Unix y Windows.
La solución propuesta debe admitir la búsqueda cruzada de pulsaciones de teclas y permitir la exportación a un archivo CSV.
La solución propuesta debe admitir la revisión de la pista de auditoría en un único portal de panel de vidrio.
La solución propuesta debe incluir un componente de análisis de comportamiento basado en SaaS o una solución complementaria.

La plataforma de análisis de comportamiento debe proporcionar un amplio conjunto de paneles informativos que incluya usuarios principales, cuentas principales, mapeo de direcciones IP, alertas, etc.
La plataforma de Behavior Analytics debe proporcionar una lista de vigilancia para los usuarios nuevos y los usuarios existentes cuya actividad pueda ser sospechosa.
La plataforma de Behavior Analytics debe proporcionar un registro de auditoría indefinido de la actividad dentro de la plataforma.
La plataforma de Behavior Analytics debe proporcionar una interfaz gráfica de acceso para visualizar comunidades de usuarios que acceden a cuentas similares.
La plataforma de análisis de comportamiento debe proporcionar una interfaz de mapa de IP de acceso para visualizar el comportamiento anómalo en una GUI de superposición de mapa mundial.
La plataforma de Behavior Analytics debe proporcionar una descripción general de los usuarios con cuentas activas en caché móvil.
Behavior Analytics debe proporcionar un proceso de remediación automatizado contra la actividad anómala en la solución PAM que admita:
Notificación de correo electrónico
Solicitud de MFA
Bloqueo de cuenta
Sesión de grabación
Forzar la aprobación de acceso en todas las cuentas
Hooks para integrarse con sistemas externos a través de HTTP Post
Hooks para integrarse con sistemas externos como Ticketing Systems
La solución propuesta debe proporcionar todas las funciones de generación de informes dentro del portal de panel único sin necesidad de plataformas de generación de informes externas.
La solución propuesta debe incluir varios informes listos para usar preconfigurados.
La solución propuesta debe permitir que los informes incorporados se personalicen directamente desde la interfaz de panel único sin necesidad de servicios profesionales del proveedor.
La solución propuesta debe proporcionar la capacidad de generar informes personalizados directamente desde la interfaz de panel único sin necesidad de servicios profesionales del proveedor.
La solución propuesta proporciona un seguimiento de auditoría para el flujo de trabajo de la cuenta de servicio y la aplicación de la gobernanza.
La solución propuesta debe admitir la conexión transparente de un usuario desde el portal web a un recurso de destino a través de RDP, SSH o una aplicación.
La solución propuesta debe soportar el monitoreo de una sesión sin notificar al usuario conectado.
La solución propuesta debe soportar el envío de un mensaje al usuario conectado.
La solución propuesta debe admitir la finalización de una sesión de usuario activa.
La solución propuesta debe proporcionar aplicaciones preconfiguradas para el inicio de sesión (RDP, SSH, PowerShell, SSMS, etc.).

La solución propuesta debe brindar la capacidad de agregar de forma nativa iniciadores de sesiones de aplicaciones personalizados para configurarlos desde la interfaz de panel único sin la necesidad de los servicios profesionales de los proveedores.
La solución propuesta no debe requerir aplicaciones de middleware como AutoIt, AutoHotkey u otras plataformas de automatización de GUI de Windows para agregar el inicio de sesiones de aplicaciones personalizadas.
La solución propuesta debe soportar el inicio de sesiones sin divulgación de la contraseña.
La solución propuesta debe soportar la grabación automática de sesiones con y sin notificación al usuario.
La solución propuesta debe admitir la captura de eventos de aplicaciones de Windows durante las sesiones.
La solución propuesta debe admitir la búsqueda cruzada de procesos de Windows ejecutados, por ejemplo, abrir PowerShell o MMC.
La solución propuesta debe proporcionar un agente de grabación basado en agentes para capturar sesiones de Windows. El agente debe permitir la grabación de sesiones iniciadas fuera de la plataforma PAM.
La solución propuesta debe proporcionar un método para agregar los agentes de grabación en colecciones lógicas.
La solución propuesta debe proporcionar un método para incluir en la lista blanca los comandos emitidos a los recursos basados en SSH.
La solución propuesta debe admitir la descarga de grabaciones a una SAN, NAS u otros recursos compartidos de red mientras aún se encuentra encriptada.
La solución propuesta debe admitir una configuración en la que las sesiones de RDP y SSH se negocien a través del componente "jumpbox" de PAM.
La solución propuesta debe admitir una configuración en la que las sesiones RDP y SSH no requieran un componente "jumpbox" para facilitar las conexiones.
Si la solución propuesta tiene un componente "jumpbox", debe admitir el equilibrio de carga automático y la conmutación por error automatizada sin clústeres de conmutación por error de Windows Server.
La solución propuesta debe incluir una función de detección automática de cuentas. Describa cómo la solución cumple con este requisito.
La función de descubrimiento de cuentas de la solución propuesta debe permitir la programación por horas.
La función de descubrimiento de cuentas de la solución propuesta debe proporcionar una vista de resultados de descubrimiento fácil de entender para visualizar las cuentas en todo el entorno.
La función de descubrimiento de cuentas de las soluciones propuestas debe proporcionar soporte listo para usar para cuentas de Active Directory, cuentas de Windows, cuentas de Linux, cuentas de Unix, cuentas de hipervisor.
La función de descubrimiento de cuentas de la solución propuesta debe admitir reglas para automatizar la incorporación de todas las cuentas descubiertas.
La función de descubrimiento de cuentas de la solución propuesta debe ser extensible a otras plataformas que no sean compatibles de fábrica.

El descubrimiento de cuentas de la solución propuesta brinda la capacidad de descubrir cuentas de servicio y hacer cumplir el gobierno y la propiedad.
La solución propuesta debe ofrecer una amplia API de servicios web con funciones de creación, lectura, actualización y eliminación.
La API de servicios web de la solución propuesta debe admitir la autenticación integrada de Windows y la autenticación OAuth.
La API de servicios web de la solución propuesta debe ser compatible con la lista blanca de direcciones IP.
El uso de la API de servicios web de la solución propuesta debe ser auditable por la plataforma PAM.
La solución propuesta debe ofrecer un SDK o bibliotecas de programación para su inclusión en el código fuente del software desarrollado internamente.
Las bibliotecas/SDK de la solución propuesta deben ser compatibles con la lista blanca de direcciones IP.
Las bibliotecas/SDK de la solución propuesta deben ser auditables por la plataforma PAM.
El cliente de CLI o SDK de la solución propuesta debe ofrecer una estrategia de almacenamiento en caché cifrado configurable.
La auditoría de cliente de CLI o SDK de la solución propuesta debe ser accesible dentro de la plataforma.
El SDK de la solución propuesta, el cliente CLI u otros componentes de la API no deben estar basados en Java.
La solución propuesta debe proporcionar una interfaz/conector SCIM para la integración en las plataformas IdAM.
La solución propuesta debe tener una integración directa con las soluciones de escaneo de vulnerabilidades comunes (Nessus, Rapid7, Qualsys) para descargar las credenciales requeridas en los escaneos autenticados.
La solución propuesta admite la integración lista para usar con sistemas de emisión de boletos comunes (ServiceNow, BMC, JIRA) para usar en validaciones de flujo de trabajo.
La solución propuesta debe proteger los datos en reposo.
La solución propuesta debe proteger los datos en movimiento.
La solución propuesta debe proporcionar un informe de auditoría del usuario; lo que permite a los administradores visualizar qué cuentas tocó una persona fuera de la plataforma.
La solución propuesta debe proporcionar un método fácil para rotar las cuentas divulgadas en el informe de auditoría del usuario mencionado anteriormente.
La base de datos MS SQL de la solución propuesta debe ser compatible con el cifrado de datos transparente de MS. SI es el caso en la sitio
La solución propuesta debe admitir la descarga de la gestión de la clave de cifrado maestra al módulo de seguridad de hardware.
La solución propuesta debe ofrecer una función de copia de seguridad programada integrada capaz de guardar en una SAN, NAS u otra ubicación de red.
La solución propuesta debe admitir mensajes de error de divulgación de información cero para evitar que los registros muestren información confidencial.
La solución propuesta debe admitir la configuración para permitir puertos no estándar.

La solución propuesta debe admitir un motor de políticas de reglas y complejidad de contraseña personalizable.
La solución propuesta debe permitir que nuestros Objetos de directiva de grupo organizativos estándar se apliquen en todos los componentes de la arquitectura de la plataforma.
La solución propuesta debe admitir la verificación de infracciones de seguridad conocidas de sitios cuyos inicios de sesión se almacenan en el administrador de contraseñas, para los cuales no ha cambiado su contraseña desde que ocurrió la infracción.
La solución debe proporcionar una interfaz de panel único para todos los accesos y configuraciones para todas las funciones, por ejemplo, administración, auditoría, informes, bóveda, políticas de acceso, sesiones privilegiadas, detección y API.
La solución no debe requerir complementos de navegadores (Flash, Java, etc.) para ninguna función de acceso, inicio, revisión, administración o gestión.
La experiencia de usuario de la solución propuesta debe ser la misma para todos los usuarios, pero solo debe estar restringida por roles y permisos para agilizar la capacitación y la adopción.
La administración de la solución propuesta y la experiencia del usuario deben ser intuitivas.
La segregación de cuentas de la solución propuesta debe imitar un explorador de sistemas de archivos para agilizar la capacitación y la adopción.
La jerarquía de segregación de cuentas de la solución propuesta debe admitir un modelo de herencia para recursos y políticas.
El propuesto debe proporcionar una consola de gestión para la gestión del ciclo de vida de la cuenta de servicio para admitir la funcionalidad del solicitante/aprobador.
La solución debe poder administrar e interactuar con varias sesiones remotas tanto para el Protocolo de escritorio remoto (RDP) como para SSH en un entorno unificado.
La solución debería poder administrar múltiples sesiones activas a la vez, utilizando diferentes protocolos de conexión y una variedad de cuentas privilegiadas.
La solución debería poder iniciar y configurar sesiones en múltiples entornos con credenciales inyectadas automáticamente en las sesiones según sea necesario.
La solución debe poder proporcionar un registro de extremo a extremo de acceso de usuarios privilegiados y proporcionar una colaboración entre equipos para ver en vivo y enviar mensajes.
La solución debe proporcionar banners de terminal personalizados después de un inicio de sesión exitoso con los comandos disponibles para mostrar.
La solución debe tener la capacidad de iniciar una conexión de terminal y lanzarse usando una sola línea e incluir 2FA para el acceso.
La solución debería poder utilizar capacidades integradas, como las flechas hacia arriba y hacia abajo para el historial de comandos.
La solución no debería requerir más hardware o licencias adicionales para estas funciones de conexión de terminal.
La solución deberá de proporcionar seguridad de contraseña segura en todas las cuentas
La solución deberá de controlar el acceso a las contraseñas de las cuentas de servicio La solución deberá de brindar la capacidad de cambiar contraseñas en cuentas de servicio sin que los usuarios conozcan las aplicaciones que dependen de la credencial para las operaciones diarias

La solución deberá de mantener los informes de auditoría requeridos para demostrar el cumplimiento

La solución deberá de gestionar empleados externos, contratistas y socios que también requieran necesitar contraseñas limitadas o temporales, que deben crearse, administrarse y eliminarse cuando finalice su vida útil

7. FIREWALLS Y VPNs
7.1 Firewalls y VPN sitio principal
17.55 Gbps de paquetes de UDP de 1518 byte firewall throughput 4.65 Gbps IPS de throughput 3.72 Gbps de throughput como NGFW 1.8 Gbps de throughput con "sandbox" activo Con un throughput de 2.57 Gbps de VPN AES-128 Que soporte hasta 67,000 conexiones por segundo 2/4/8 Millones de conexiones concurrentes por segundo respectivamente para FW, IPS y NGFW Deberá de contar con 8 interfaces en cobre 1000-T Deberá contar con una interfaz dedicada para la sincronización del clúster Deberá de contar con una interfaz dedicada para su administración Deberá contar con las capacidades de filtrado de puertos, previsor de intrusos, antibot, control de aplicaciones URL filtering y sandbox y VPNs de SSL para hasta 200 usuarios concurrentes Debe poder adquirir la identidad del usuario al consultar Microsoft Active Directory en función de los eventos de seguridad. Debe tener un método de autenticación de identidad de usuario basado en el navegador para usuarios o activos que no sean de dominio Debe proveer múltiples métodos de identificación de usuarios: Consulta de AD, basada en navegador o agentes de identidad, Autenticación transparente de Kerberos, portal captivo. Debe soportar entornos de servidor de terminal. La solución debe integrarse perfectamente con los servicios de directorio, IF-MAP y Radius. El impacto en los controladores de dominio debe ser inferior al 3%. La solución de identidad debe admitir servidores de terminal y Citrix. La solución debería permitir la identificación a través de un proxy (por ejemplo: encabezados X-forward). Debe poder adquirir la identidad del usuario de Microsoft Active Directory sin ningún tipo de agente instalado en los controladores de dominio. Debe admitir la autenticación transparente de Kerberos para el inicio de sesión único. Debe admitir el uso de grupos anidados LDAP. Debe poder compartir o propagar identidades de usuario entre múltiples puertas de enlace de seguridad.

Debe poder crear roles de identidad para usar en todas las aplicaciones de seguridad.

Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;

Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios.

IPS

Se deberá suministrar el servicio de IPS pudiendo brindarse con el mismo Appliance, en una configuración de alta disponibilidad, para la protección de ataques orientados a conexiones internas y externas.

IPS debe basarse en los siguientes mecanismos de detección: firmas de explotación, anomalías de protocolo, controles de aplicaciones y detección basada en el comportamiento.

IPS y el módulo de firewall deben integrarse en una plataforma.

El administrador debe poder configurar la inspección para proteger únicamente los hosts internos.

IPS debe tener opciones para crear perfiles para las protecciones basadas en el cliente o servidor, o una combinación de ambos.

IPS debe proporcionar al menos tres perfiles o políticas predefinidos que se puedan usar de inmediato.

IPS debe tener un mecanismo de fail-open basado en software, configurable basado en umbrales de CPU de Gateways de seguridad y uso de memoria.

IPS debe proporcionar un mecanismo automático para activar o administrar nuevas firmas a partir de actualizaciones.

IPS debe admitir excepciones de red basadas en la fuente, el destino, el servicio o una combinación de los tres.

IPS debe incluir un modo de solución de problemas que establece el perfil en uso para detectar sólo, con un clic sin modificar las protecciones individuales.

La aplicación IPS debe tener un mecanismo centralizado de correlación e informe de eventos

El administrador debe poder activar automáticamente nuevas protecciones, en función de parámetros configurables (impacto en el rendimiento, gravedad de la amenaza, nivel de confianza, protecciones del cliente, protecciones del servidor).

IPS debe ser capaz de detectar y prevenir las siguientes amenazas: uso indebido de protocolos, comunicaciones de malware, intentos de tunelización y tipos de ataques genéricos sin firmas predefinidas.

Para cada protección, la solución debe incluir el tipo de protección (relacionada con el servidor o con el cliente), la gravedad de la amenaza, el impacto en el rendimiento, el nivel de confianza y la referencia de la industria.

IPS debe ser capaz de recopilar paquetes de captura para protecciones específicas.

IPS debe poder detectar y bloquear los ataques a la red y a la capa de aplicaciones, protegiendo al menos los siguientes servicios: servicios de correo electrónico, DNS, FTP, servicios de Windows (redes de Microsoft).

El proveedor debe proporcionar evidencia de liderazgo para proteger las vulnerabilidades de Microsoft.

IPS y/ o Application Control deben incluir la capacidad de detectar y bloquear aplicaciones P2P y evasivas.

El administrador debe ser capaz de definir exclusiones de red y host de la inspección de IPS.

La solución debe proteger contra el envenenamiento de caché de DNS e impide que los usuarios accedan a las direcciones de dominio bloqueadas.

La solución debe proporcionar protecciones de protocolos VOIP

IPS debe detectar y bloquear las aplicaciones de controles remotos, incluidas aquellas que son capaces de crear túneles a través del tráfico HTTP.

IPS debe tener protecciones SCADA.

IPS debe tener un mecanismo para convertir firmas SNORT.

La solución debe hacer cumplir la aplicación del protocolo Citrix.

La solución debe permitir al administrador bloquear fácilmente el tráfico entrante y / o saliente en función de los países, sin la necesidad de administrar manualmente los rangos de IP correspondientes al país.

Deberá contar como mínimo con los siguientes mecanismos de detección de ataques:

Detección de ataques de RPC (Remote procedure call).

Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, POP (Post Office Protocol).

Protección contra ataques DNS (Domain Name System).

Protección contra ataques a FTP, SSH, Telnet y Rlogin.

Protección contra ataques de ICMP (Internet Control Message Protocol).

Actualizaciones periódicas durante la vigencia del contrato de nuevas definiciones, las actualizaciones deberán realizarse de forma automática, programada por fecha y hora.

Debe integrarse protección basada en firmas contra ataques de inyección de SQL.

Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad;

CONTROL DE APLICACIONES Y FILTRADO DE URLS

La base de datos de control de aplicaciones debe contener más de 8,000 aplicaciones conocidas.

La solución debe tener una clasificación de URL que supere los 200 millones de URL y cubra más del 85% de los principales sitios de 1M de Alexa.

La solución debe ser capaz de crear una regla de filtrado con múltiples categorías.

La solución debe ser capaz de crear un filtro para un solo sitio que sea compatible con múltiples categorías.

La solución debe tener granularidad de usuarios y grupos con reglas de seguridad.

El caché local del Gateway de seguridad debe dar respuesta al 99% de las solicitudes de categorización de URL dentro de las 4 semanas de producción.

La solución debe tener una interfaz de búsqueda fácil de usar para aplicaciones y URL.

La solución debe clasificar las aplicaciones y las URL y las aplicaciones por Factor de riesgo.

El control de la aplicación y la política de seguridad URLF deben poder definirse por las identidades del usuario.

El control de la aplicación y la base de datos URLF deben ser actualizados por un servicio basado en la nube.

La solución debe tener un control de aplicación unificado y reglas de seguridad URLF.

La solución debe proporcionar un mecanismo para informar o solicitar a los usuarios en tiempo real que los eduquen o confirmen acciones basadas en la política de seguridad.

La solución debe proporcionar un mecanismo para limitar el uso de la aplicación en función del consumo de ancho de banda.

La solución debe permitir excepciones de red basadas en objetos de red definidos.

La solución debe proporcionar la opción de modificar la Notificación de bloqueo y redirigir al usuario a una página de corrección.

La solución debe incluir un mecanismo de listas en blanco y negro que permita al administrador denegar o permitir URL específicas independientemente de la categoría.

La solución debe tener un mecanismo de derivación configurable.

La solución debe proporcionar un mecanismo de anulación en la categorización de la base de datos de URL.

El control de la aplicación y la política de seguridad URLF deben informar sobre el conteo de aciertos de la regla.

Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);

Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad

Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory, y la base de datos local.

Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL

Permitir página de bloqueo personalizada.

Permitir el bloqueo y continuación (que permite al usuario acceder a un sitio bloqueado potencialmente informando en la pantalla de bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).

Debe tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo

Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos.

La solución debe admitir el control de acceso para al menos 150 servicios o protocolos predefinidos.

ANTI-BOT AND ANTIVIRUS

El proveedor debe tener una aplicación integrada Anti-Bot y Anti-Virus en el firewall de próxima generación.

La aplicación Anti-Bot debe ser capaz de detectar y detener el comportamiento anormal sospechoso de la red.

La aplicación Anti-Bot debe usar un motor de detección de niveles múltiples, que incluye la reputación de direcciones IP, URL y DNS, y detectar patrones de comunicaciones de bots.

Las protecciones anti-Bot deben poder escanear en busca de acciones de bots.

La solución debe ser compatible con la detección y prevención de virus y variantes de Cryptors y ransomware (por ejemplo, Wannacry, Cryptlocker, CryptoWall ...) mediante el uso de análisis estáticos y / o dinámicos.

La solución debe tener mecanismos para proteger contra los ataques de spear phishing.

Ataques basados en DNS:

La solución debe tener capacidades de detección y prevención para los escondites DNS de C & C:

Busque patrones de tráfico C & C, no solo en su destino DNS.

Invertir malware de ingeniería para descubrir su DGA (Generación de nombres de dominio).

Característica de captura de DNS como parte de nuestra prevención de amenazas, ayudando a descubrir hosts infectados generando comunicación C & C.

La solución debe tener capacidades de detección y prevención para los ataques de túnel DNS.

La política Anti-Bot y Anti-Virus debe administrarse desde una consola central.

La aplicación Anti-Bot y Antivirus debe tener un mecanismo centralizado de correlación e informe de eventos.

La aplicación de antivirus debe poder evitar el acceso a sitios web maliciosos.

La aplicación antivirus debe poder inspeccionar el tráfico cifrado SSL.

Anti-Bot y Anti-Virus deben tener actualizaciones en tiempo real de servicios de reputación basados en la nube.

Anti-Virus debe ser capaz de detener los archivos maliciosos entrantes.

Anti-Virus debe poder escanear archivos archivados.

Las políticas de antivirus y anti-Bot se deben administrar de forma centralizada con la configuración de políticas granulares y su aplicación.

El Antivirus debería admitir más de 50 motores AV basados en la nube.

El Antivirus debería ser compatible con el escaneo de enlaces dentro de los correos electrónicos.

El Antivirus debe escanear archivos que están pasando el protocolo CIFS.

INSPECCIÓN SSL (INBOUND / OUTBOUND)

La solución ofrece soporte para la inspección / descifrado SSL con un rendimiento líder en todas las tecnologías de mitigación de amenazas.

La solución debe ser compatible con Perfect Forward Secrecy (PFS, ECDHE Cipher Suites).

La solución debe ser compatible con AES-NI, AES-GCM para mejorar el rendimiento

La solución debe aprovechar la base de datos de filtrado de URL para permitir al administrador crear una política de inspección https granular.

La solución puede inspeccionar el filtrado de URL basado en HTTPS sin necesidad de descifrado SSL.

SANDBOX

La solución debe detectar y detener de forma inmediata contra ataques de día cero y malware desconocido antes de que una firma de protección estática sea creada. Las amenazas detectadas por la solución de SandBox no deben permitir ni siquiera el acceso de la primera muestra, evitando así la existencia del paciente cero.

La solución debe ser parte de una arquitectura de protección contra amenazas multicapa.

La solución debe poder implementarse de manera local e híbrida, permitiendo al usuario seleccionar la localización más adecuada para el análisis (local o en la nube) dependiendo de la naturaleza del archivo.

La solución debe soportar su implementación en modo puente (Layer 2) sin requerir cambios en la topología de la red a proteger.

La solución debe soportar la recepción de correo electrónico como un MTA (Mail Transfer Agent), después de obtener el veredicto del archivo analizada debe tener la capacidad de entregar los datos a un servidor de correo electrónico representado por una dirección IP o un nombre de dominio, permitiendo la redundancia mediante DNS.

La solución debe soportar su implementación en modo de detección conectado a un TAP o puerto espejo.

La solución no debe requerir equipos separados para proteger web (HTTP y HTTPs) y para proteger correo electrónico. (SMTP & SMTPS)

La solución debe soportar redundancia.

La solución debe ofrecer una API basada en REST publicada en el mismo equipo , que permita la integración de aplicaciones inHouse con la tecnología de SandBoxing. La API debe utilizar JSON como formato de intercambio de mensajes.

La solución debe tener la capacidad de bloquear llamadas a servidores remotos (Callbacks). En el caso de ataques de Día Cero, el Sistema de Protección de Malware deberá bloquear la habilidad del Malware para realizar llamadas C&C (command & control).

La solución debe ser capaz de emular archivos ejecutables, documentos, java y flash. En específico:

2.8.3.1.1.7z
2.8.3.1.2.cab
2.8.3.1.3.csv
2.8.3.1.4.doc
2.8.3.1.5.docm
2.8.3.1.6.docx
2.8.3.1.7.dot
2.8.3.1.8.dotm
2.8.3.1.9.dotx
2.8.3.1.10.exe
2.8.3.1.11.jar
2.8.3.1.12.pdf
2.8.3.1.13.potx
2.8.3.1.14.pps
2.8.3.1.15.psm
2.8.3.1.16.ppsx
2.8.3.1.17.ppt
2.8.3.1.18.pptm
2.8.3.1.19.pptx
2.8.3.1.20.rar
2.8.3.1.21.rtf
2.8.3.1.22.scr
2.8.3.1.23.swf
2.8.3.1.24.tar
2.8.3.1.25.tgz
2.8.3.1.26.xla
2.8.3.1.27.xls
2.8.3.1.28.xlsb
2.8.3.1.29.xlsm
2.8.3.1.30.xlsx
2.8.3.1.31.xlt
2.8.3.1.32.xltm
2.8.3.1.33.xltx
2.8.3.1.34.xlw
2.8.3.1.35.zip

La solución debe permitir al usuario definir el TIEMPO en segundos que se dedicara en descomprimir archivos comprimidos anidados. Es decir que han sido comprimidos varias veces como medida de evasión y negación de servicio.

La solución debe ofrecer al menos los siguientes ambientes de virtualización, Windows XP32bit, Windows 7 32 y 64 bits, Windows 8.164 bits y Win1064 bits. Estos ambientes deben contar con diferentes versiones de Office, Adobe. Implementar la solución de SandBoxing no debe requerir la compra de licenciamiento extra para las instancias de Windows y Office que corren en los ambientes de emulación.

El motor de emulación debe ser capaz de inspeccionar, emular, prevenir y compartir los resultados de los eventos de sandboxing con la infraestructura anti malware.

La solución debe realizar una pre-emulación o validación a través de un filtrado estático, en donde se valide si es necesario enviar el archivo a emulación.

La solución debe ser capaz de emular archivos de más de 20 MB.

Detección y prevención inmediata. La solución debe detectar el ataque en la fase de exploit, por ejemplo, antes de que se ejecute el Shell code y antes de que el malware se descargue/ejecute.

La solución debe ser capaz de detectar la técnica de explotación ROP a través del monitoreo y análisis del flujo en el CPU real, y no en un CPU emulado.

La solución debe ser capaz de soportar el análisis de ligas dentro de los correos electrónicos, detectando de esta manera intentos de "Phishing" a los usuarios del corporativo.

La solución debe ofrecer la integración con el navegador (Al menos Chrome) mediante una extensión que permita la emulación de archivos descargados y la detección de sitios de "Phishing" cuando el usuario esté fuera del perímetro corporativo.

La solución debe poder ser administrada de forma centralizada en caso de necesitar múltiples equipos para la implementación.

Al detectar archivos maliciosos se debe generar un reporte detallado de las actividades que incluya: a) Captura de pantallas que muestre la ejecución del malware. B) Detalle de los procesos ejecutados, archivos y/o registros del sistema modificados o creados. c) Actividad a nivel de red.

La solución debe tener la capacidad de remover contenido activo o dinámico en documentos Office y PDF con el objetivo de eliminar la ejecución de código malicioso, de forma automática al ser recibidos por correo electrónico.

La solución debe ser capaz de reconstruir los documentos usando sus elementos seguros, entregando al usuario final un documento libre de riesgos en el mismo formato.

La solución debe ser capaz de convertir documentos a un formato PDF de forma automática al ser recibidos por correo electrónico.

La solución debe ofrecer una API basada en REST publicada en el mismo equipo, que permita la integración de aplicaciones inHouse con la tecnología de extracción y reconstrucción de documentos. La API debe utilizar JSON como formato de intercambio de mensajes.

La solución debe mantener flexibilidad con opciones de mantener el formato original del fichero y especificar el tipo de contenido a ser removido.

La solución debe permitir ejecutar de forma paralela en el mismo equipo las tecnologías de SandBoxing y Extracción/reconstrucción de documentos.

Debe ser capaz de soportar estas aplicaciones de seguridad de próxima generación en una plataforma unificada:
-stateful inspection firewall
-sistema de prevención de intrusos
-adquisición de identidad de usuario
-control de aplicación y filtrado de url
-antibot
-antimalware
-emulación de amenaza (sandboxing)
-extracción de amenaza (depuración)
-antispam y seguridad de correo electrónico
-vpn ipsec
-prevención de pérdida de datos
-acceso móvil
-gestión de políticas de seguridad
-registro y estado
-correlación de eventos e informes

El Gateway de seguridad debe usar Stateful Inspection basada en el análisis granular de la comunicación y el estado de la aplicación para rastrear y controlar el flujo de la red.

La solución debe admitir el control de acceso para al menos 150 servicios o protocolos predefinidos.

Debe proporcionar estadísticas de recuento de aciertos de reglas de seguridad a la Consola de administración.

Debe permitir que las reglas de seguridad se apliquen en intervalos de tiempo que se configurarán con una fecha / hora de caducidad.

La comunicación entre las consolas de administración y las Gateways de seguridad debe estar encriptada y autenticada con Certificados PKI.

Debe ser compatible con la integración de terceros (API pública).

Contar con un Motor de comparación de firmas que permita contrastar el contenido del tráfico de una sesión contra patrones de firmas de virus, ataques de intrusión, reconocimiento de aplicaciones u otros patrones sin comprometer el rendimiento de la red.

Debe soportar funcionalidad de alta disponibilidad activo-activo, activo-pasivo.

La GUI de la solución debe proporcionar una navegación fácil entre cientos de políticas, cada una con hasta 1 millón de reglas. Se deben proporcionar saltos entre sub-políticas y títulos de sección, así como una búsqueda exhaustiva

La solución debe admitir Alta disponibilidad de Gateways e intercambio de carga con sincronización de estado.

Debe soportar funcionalidad de balanceo de al menos dos Enlaces de Internet.

Soporte de protocolos: TCP, UDP, ARP, ICMP, IPv4, IPv6, OSPF, IPSec, RIP.

Debe poder ser administrado por una consola central

La consola de administración debe poder ser instalada en el mismo equipo

La solución debe admitir cifrado 3DES y AES-256 para IKE Phase I y II IKEv2 más "Suite-B-GCM-128" y "Suite-B-GCM-256" para Fase II.

La solución debe admitir al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 y Grupo 20

La solución debe ser compatible con la integridad de los datos con md5, sha1 SHA-256, SHA-384 y AES-XCBC.

Se debe admitir CA interna y CA externa de terceros.

La solución debe incluir soporte para VPN de sitio a sitio en las siguientes topologías:

Full Mesh (todo para todos),

Estrella (oficinas remotas al sitio central)

Hub and Spoke (sitio remoto a través del sitio central a otro sitio remoto)

La solución debe ser compatible con la configuración de VPN con una GUI mediante la adición de objetos de arrastrar y soltar a las comunidades de VPN

La solución debe admitir VPN SSL sin cliente para el acceso remoto.

La solución debe ser compatible con VPN L2TP, incluida la compatibilidad con el cliente de iPhone L2TP

La solución debe permitir que el administrador aplique reglas de seguridad para controlar el tráfico dentro de la VPN

La solución debe admitir redes privadas virtuales (VPN) basadas en dominio y VPN basadas en rutas que utilicen VTI y protocolos de enrutamiento dinámico.

La solución debe incluir la capacidad de establecer VPN con puertas de enlace con IP públicas dinámicas

La solución debe incluir compresión de IP para VPNs de cliente a sitio y de sitio a sitio.

Debe poder adquirir la identidad del usuario al consultar Microsoft Active Directory en función de los eventos de seguridad.

Debe tener un método de autenticación de identidad de usuario basado en el navegador para usuarios o activos que no sean de dominio

Debe proveer múltiples métodos de identificación de usuarios: Consulta de AD, basada en navegador o agentes de identidad, autenticación transparente de Kerberos, portal cautivo.

Debe soportar entornos de servidor de terminal.

La solución debe integrarse perfectamente con los servicios de directorio, IF-MAP y Radius.

El impacto en los controladores de dominio debe ser inferior al 3%.

La solución de identidad debe admitir servidores de terminal y Citrix.

La solución debería permitir la identificación a través de un proxy (por ejemplo: encabezados X-forward).

Debe poder adquirir la identidad del usuario de Microsoft Active Directory sin ningún tipo de agente instalado en los controladores de dominio.

Debe admitir la autenticación transparente de Kerberos para el inicio de sesión único.

Debe admitir el uso de grupos anidados LDAP.

Debe poder compartir o propagar identidades de usuario entre múltiples puertas de enlace de seguridad.

Debe poder crear roles de identidad para usar en todas las aplicaciones de seguridad.

Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;

Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios.

La solución ofrece soporte para la inspección / descifrado SSL con un rendimiento líder en todas las tecnologías de mitigación de amenazas.

La solución debe ser compatible con Perfect Forward Secrecy (PFS, ECDHE Cipher Suites).

La solución debe ser compatible con AES-NI, AES-GCM para mejorar el rendimiento

La solución debe aprovechar la base de datos de filtrado de URL para permitir al administrador crear una política de inspección https granular.

La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web;

Las características de VPN SSL se deben cumplir con o sin el uso de agentes;

Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy.

7.2 Firewalls y VPNs sitio alterno

17.55 Gbps de paquetes de UDP de 1518 byte firewall throughput

3.9 Gbps IPS de throughput

3.4 Gbps de throughput como NGFW

1.46 Gbps de throughput con "sandbox" activo

Con un throughput de 2.16 Gbps de VPN AES-128

Que soporte hasta 150,000 conexiones por segundo

3.2/6.4/12.8 Millones de conexiones concurrentes por segundo respectivamente para FW, IPS y NGFW

Deberá de contar con 8 interfaces en cobre 1000-T

Deberá contar con las capacidades de filtrado de puertos, previsor de intrusos, antibot, control de aplicaciones URL filtering y sandbox y VPNs de SSL para hasta 200 usuarios concurrentes

Debe poder adquirir la identidad del usuario al consultar Microsoft Active Directory en función de los eventos de seguridad.

Debe tener un método de autenticación de identidad de usuario basado en el navegador para usuarios o activos que no sean de dominio

Debe proveer múltiples métodos de identificación de usuarios: Consulta de AD, basada en navegador o agentes de identidad, autenticación transparente de Kerberos, portal captivo.

Debe soportar entornos de servidor de terminal.

La solución debe integrarse perfectamente con los servicios de directorio, IF-MAP y Radius.

El impacto en los controladores de dominio debe ser inferior al 3%.

La solución de identidad debe admitir servidores de terminal y Citrix.

La solución debería permitir la identificación a través de un proxy (por ejemplo: encabezados X-forward).

Debe poder adquirir la identidad del usuario de Microsoft Active Directory sin ningún tipo de agente instalado en los controladores de dominio.

Debe admitir la autenticación transparente de Kerberos para el inicio de sesión único.

Debe admitir el uso de grupos anidados LDAP.

Debe poder compartir o propagar identidades de usuario entre múltiples puertas de enlace de seguridad.

Debe poder crear roles de identidad para usar en todas las aplicaciones de seguridad.

Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;

Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios.

IPS

Se deberá suministrar el servicio de IPS pudiendo brindarse con el mismo Appliance, en una configuración de alta disponibilidad, para la protección de ataques orientados a conexiones internas y externas.

IPS debe basarse en los siguientes mecanismos de detección: firmas de explotación, anomalías de protocolo, controles de aplicaciones y detección basada en el comportamiento.

IPS y el módulo de firewall deben integrarse en una plataforma.

El administrador debe poder configurar la inspección para proteger únicamente los hosts internos.

IPS debe tener opciones para crear perfiles para las protecciones basadas en el cliente o servidor, o una combinación de ambos.

IPS debe proporcionar al menos tres perfiles o políticas predefinidos que se puedan usar de inmediato.

IPS debe tener un mecanismo de fail-open basado en software, configurable basado en umbrales de CPU de Gateways de seguridad y uso de memoria.

IPS debe proporcionar un mecanismo automático para activar o administrar nuevas firmas a partir de actualizaciones.

IPS debe admitir excepciones de red basadas en la fuente, el destino, el servicio o una combinación de los tres.

IPS debe incluir un modo de solución de problemas que establece el perfil en uso para detectar sólo, con un clic sin modificar las protecciones individuales.

La aplicación IPS debe tener un mecanismo centralizado de correlación e informe de eventos

El administrador debe poder activar automáticamente nuevas protecciones, en función de parámetros configurables (impacto en el rendimiento, gravedad de la amenaza, nivel de confianza, protecciones del cliente, protecciones del servidor).

IPS debe ser capaz de detectar y prevenir las siguientes amenazas: uso indebido de protocolos, comunicaciones de malware, intentos de tunelización y tipos de ataques genéricos sin firmas predefinidas.

Para cada protección, la solución debe incluir el tipo de protección (relacionada con el servidor o con el cliente), la gravedad de la amenaza, el impacto en el rendimiento, el nivel de confianza y la referencia de la industria.

IPS debe ser capaz de recopilar paquetes de captura para protecciones específicas.

IPS debe poder detectar y bloquear los ataques a la red y a la capa de aplicaciones, protegiendo al menos los siguientes servicios: servicios de correo electrónico, DNS, FTP, servicios de Windows (redes de Microsoft).

El proveedor debe proporcionar evidencia de liderazgo para proteger las vulnerabilidades de Microsoft.

IPS y/ o Application Control deben incluir la capacidad de detectar y bloquear aplicaciones P2P y evasivas.

El administrador debe ser capaz de definir exclusiones de red y host de la inspección de IPS.

La solución debe proteger contra el envenenamiento de caché de DNS e impide que los usuarios accedan a las direcciones de dominio bloqueadas.

La solución debe proporcionar protecciones de protocolos VOIP

IPS debe detectar y bloquear las aplicaciones de controles remotos, incluidas aquellas que son capaces de crear túneles a través del tráfico HTTP.

IPS debe tener protecciones SCADA.

IPS debe tener un mecanismo para convertir firmas SNORT.

La solución debe hacer cumplir la aplicación del protocolo Citrix.

La solución debe permitir al administrador bloquear fácilmente el tráfico entrante y / o saliente en función de los países, sin la necesidad de administrar manualmente los rangos de IP correspondientes al país.

Deberá contar como mínimo con los siguientes mecanismos de detección de ataques:

Detección de ataques de RPC (Remote procedure call).

Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, POP (Post Office Protocol).

Protección contra ataques DNS (Domain Name System).

Protección contra ataques a FTP, SSH, Telnet y Rlogin.

Protección contra ataques de ICMP (Internet Control Message Protocol).

Actualizaciones periódicas durante la vigencia del contrato de nuevas definiciones, las actualizaciones deberán realizarse de forma automática, programada por fecha y hora.

Debe integrarse protección basada en firmas contra ataques de inyección de SQL.

Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad;

CONTROL DE APLICACIONES Y FILTRADO DE URLS

La base de datos de control de aplicaciones debe contener más de 8,000 aplicaciones conocidas.

La solución debe tener una clasificación de URL que supere los 200 millones de URL y cubra más del 85% de los principales sitios de 1M de Alexa.

La solución debe ser capaz de crear una regla de filtrado con múltiples categorías.

La solución debe ser capaz de crear un filtro para un solo sitio que sea compatible con múltiples categorías.

La solución debe tener granularidad de usuarios y grupos con reglas de seguridad.

El caché local del Gateway de seguridad debe dar respuesta al 99% de las solicitudes de categorización de URL dentro de las 4 semanas de producción.

La solución debe tener una interfaz de búsqueda fácil de usar para aplicaciones y URL.

La solución debe clasificar las aplicaciones y las URL y las aplicaciones por Factor de riesgo.

El control de la aplicación y la política de seguridad URLF deben poder definirse por las identidades del usuario.

El control de la aplicación y la base de datos URLF deben ser actualizados por un servicio basado en la nube.

La solución debe tener un control de aplicación unificado y reglas de seguridad URLF.

La solución debe proporcionar un mecanismo para informar o solicitar a los usuarios en tiempo real que los eduquen o confirmen acciones basadas en la política de seguridad.

La solución debe proporcionar un mecanismo para limitar el uso de la aplicación en función del consumo de ancho de banda.

La solución debe permitir excepciones de red basadas en objetos de red definidos.

La solución debe proporcionar la opción de modificar la Notificación de bloqueo y redirigir al usuario a una página de corrección.

La solución debe incluir un mecanismo de listas en blanco y negro que permita al administrador denegar o permitir URL específicas independientemente de la categoría.

La solución debe tener un mecanismo de derivación configurable.

La solución debe proporcionar un mecanismo de anulación en la categorización de la base de datos de URL.

El control de la aplicación y la política de seguridad URLF deben informar sobre el conteo de aciertos de la regla.

Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);

Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad

Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory, y la base de datos local.

Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL

Permitir página de bloqueo personalizada.

Permitir el bloqueo y continuación (que permite al usuario acceder a un sitio bloqueado potencialmente informando en la pantalla de bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).

Debe tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo

Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos.

La solución debe admitir el control de acceso para al menos 150 servicios o protocolos predefinidos.

ANTI-BOT AND ANTIVIRUS

El proveedor debe tener una aplicación integrada Anti-Bot y Anti-Virus en el firewall de próxima generación.

La aplicación Anti-Bot debe ser capaz de detectar y detener el comportamiento anormal sospechoso de la red.

La aplicación Anti-Bot debe usar un motor de detección de niveles múltiples, que incluye la reputación de direcciones IP, URL y DNS, y detectar patrones de comunicaciones de bots.

Las protecciones anti-Bot deben poder escanear en busca de acciones de bots.

La solución debe ser compatible con la detección y prevención de virus y variantes de Cryptors y ransomware (por ejemplo, Wannacry, Cryptlocker, CryptoWall ...) mediante el uso de análisis estáticos y / o dinámicos.

La solución debe tener mecanismos para proteger contra los ataques de spear phishing.

Ataques basados en DNS:

La solución debe tener capacidades de detección y prevención para los escondites DNS de C & C:

Busque patrones de tráfico C & C, no solo en su destino DNS.

Invertir malware de ingeniería para descubrir su DGA (Generación de nombres de dominio).

Característica de captura de DNS como parte de nuestra prevención de amenazas, ayudando a descubrir hosts infectados generando comunicación C & C.

La solución debe tener capacidades de detección y prevención para los ataques de túnel DNS.

La política Anti-Bot y Antivirus debe administrarse desde una consola central.
La aplicación Anti-Bot y Antivirus debe tener un mecanismo centralizado de correlación e informe de eventos.
La aplicación de antivirus debe poder evitar el acceso a sitios web maliciosos.
La aplicación antivirus debe poder inspeccionar el tráfico cifrado SSL.
Anti-Bot y Antivirus deben tener actualizaciones en tiempo real de servicios de reputación basados en la nube.
Anti-Virus debe ser capaz de detener los archivos maliciosos entrantes.
Anti-Virus debe poder escanear archivos archivados.
Las políticas de antivirus y anti-Bot se deben administrar de forma centralizada con la configuración de políticas granulares y su aplicación.
El Antivirus debería admitir más de 50 motores AV basados en la nube.

El Antivirus debería ser compatible con el escaneo de enlaces dentro de los correos electrónicos.

El Antivirus debe escanear archivos que están pasando el protocolo CIFS.

INSPECCIÓN SSL (INBOUND / OUTBOUND)

La solución ofrece soporte para la inspección / descifrado SSL con un rendimiento líder en todas las tecnologías de mitigación de amenazas.

La solución debe ser compatible con Perfect Forward Secrecy (PFS, ECDHE Cipher Suites).

La solución debe ser compatible con AES-NI, AES-GCM para mejorar el rendimiento
La solución debe aprovechar la base de datos de filtrado de URL para permitir al administrador crear una política de inspección https granular.

La solución puede inspeccionar el filtrado de URL basado en HTTPS sin necesidad de descifrado SSL.

SANDBOX

La solución debe detectar y detener de forma inmediata contra ataques de día cero y malware desconocido antes de que una firma de protección estática sea creada. Las amenazas detectadas por la solución de SandBox no deben permitir ni siquiera el acceso de la primera muestra, evitando así la existencia del paciente cero.

La solución debe ser parte de una arquitectura de protección contra amenazas multicapa.

La solución debe poder implementarse de manera local e híbrida, permitiendo al usuario seleccionar la localización más adecuada para el análisis (local o en la nube) dependiendo de la naturaleza del archivo.

La solución debe soportar su implementación en modo puente (Layer 2) sin requerir cambios en la topología de la red a proteger.

La solución debe soportar la recepción de correo electrónico como un MTA (Mail Transfer Agent), después de obtener el veredicto del archivo analizada debe tener la capacidad de entregar los datos a un servidor de correo electrónico representado por una dirección IP o un nombre de dominio, permitiendo la redundancia mediante DNS.

La solución debe soportar su implementación en modo de detección conectado a un TAP o puerto espejo.

La solución no debe requerir equipos separados para proteger web (HTTP y HTTPs) y para proteger correo electrónico. (SMTP & SMTPS)

La solución debe soportar redundancia.

La solución debe ofrecer una API basada en REST publicada en el mismo equipo , que permita la integración de aplicaciones inHouse con la tecnología de SandBoxing. La API debe utilizar JSON como formato de intercambio de mensajes.

La solución debe tener la capacidad de bloquear llamadas a servidores remotos (Callbacks). En el caso de ataques de Día Cero, el Sistema de Protección de Malware deberá bloquear la habilidad del Malware para realizar llamadas C&C (command & control).

La solución debe ser capaz de emular archivos ejecutables, documentos, java y flash. En específico:

2.8.3.1.1.7z
2.8.3.1.2.cab
2.8.3.1.3.csv
2.8.3.1.4.doc
2.8.3.1.5.docm
2.8.3.1.6.docx
2.8.3.1.7.dot
2.8.3.1.8.dotm
2.8.3.1.9.dotx
2.8.3.1.10.exe
2.8.3.1.11.jar
2.8.3.1.12.pdf
2.8.3.1.13.potx
2.8.3.1.14.pps
2.8.3.1.15.psm
2.8.3.1.16.ppsx
2.8.3.1.17.ppt
2.8.3.1.18.pptm
2.8.3.1.19.pptx
2.8.3.1.20.rar

2.8.3.1.21.rtf
2.8.3.1.22.scr
2.8.3.1.23.swf
2.8.3.1.24.tar
2.8.3.1.25.tgz
2.8.3.1.26.xla
2.8.3.1.27.xls
2.8.3.1.28.xlsb
2.8.3.1.29.xlsm
2.8.3.1.30.xlsx
2.8.3.1.31.xlt
2.8.3.1.32.xltm
2.8.3.1.33.xltx
2.8.3.1.34.xlw
2.8.3.1.35.zip

La solución debe permitir al usuario definir el TIEMPO en segundos que se dedicara en descomprimir archivos comprimidos anidados. Es decir que han sido comprimidos varias veces como medida de evasión y negación de servicio.

La solución debe ofrecer al menos los siguientes ambientes de virtualización, Windows XP32bit, Windows 7 32 y 64 bits, Windows 8.164 bits y Win1064 bits. Estos ambientes deben contar con diferentes versiones de Office, Adobe. Implementar la solución de SandBoxing no debe requerir la compra de licenciamiento extra para las instancias de Windows y Office que corren en los ambientes de emulación.

El motor de emulación debe ser capaz de inspeccionar, emular, prevenir y compartir los resultados de los eventos de sandboxing con la infraestructura anti malware.

La solución debe realizar una pre-emulación o validación a través de un filtrado estático, en donde se valide si es necesario enviar el archivo a emulación.

La solución debe ser capaz de emular archivos de más de 20 MB.

Detección y prevención inmediata. La solución debe detectar el ataque en la fase de exploit, por ejemplo, antes de que se ejecute el Shell code y antes de que el malware se descargue/ejecute.

La solución debe ser capaz de detectar la técnica de explotación ROP a través del monitoreo y análisis del flujo en el CPU real, y no en un CPU emulado.

La solución debe ser capaz de soportar el análisis de ligas dentro de los correos electrónicos, detectando de esta manera intentos de "Phishing" a los usuarios del corporativo.

La solución debe ofrecer la integración con el navegador (Al menos Chrome) mediante una extensión que permita la emulación de archivos descargados y la detección de sitios de "Phishing" cuando el usuario esté fuera del perímetro corporativo.

La solución debe poder ser administrada de forma centralizada en caso de necesitar múltiples equipos para la implementación.

Al detectar archivos maliciosos se debe generar un reporte detallado de las actividades que incluya: a) Captura de pantallas que muestre la ejecución del malware. B) Detalle de los procesos ejecutados, archivos y/o registros del sistema modificados o creados. c) Actividad a nivel de red.

La solución debe tener la capacidad de remover contenido activo o dinámico en documentos Office y PDF con el objetivo de eliminar la ejecución de código malicioso, de forma automática al ser recibidos por correo electrónico.

La solución debe ser capaz de reconstruir los documentos usando sus elementos seguros, entregando al usuario final un documento libre de riesgos en el mismo formato.

La solución debe ser capaz de convertir documentos a un formato PDF de forma automática al ser recibidos por correo electrónico.

La solución debe ofrecer una API basada en REST publicada en el mismo equipo, que permita la integración de aplicaciones inHouse con la tecnología de extracción y reconstrucción de documentos. La API debe utilizar JSON como formato de intercambio de mensajes.

La solución debe mantener flexibilidad con opciones de mantener el formato original del fichero y especificar el tipo de contenido a ser removido.

La solución debe permitir ejecutar de forma paralela en el mismo equipo las tecnologías de SandBoxing y Extracción/reconstrucción de documentos.

El Gateway de seguridad debe usar Stateful Inspection basada en el análisis granular de la comunicación y el estado de la aplicación para rastrear y controlar el flujo de la red.

La solución debe admitir el control de acceso para al menos 150 servicios o protocolos predefinidos.

Debe proporcionar estadísticas de recuento de aciertos de reglas de seguridad a la Consola de administración.

Debe permitir que las reglas de seguridad se apliquen en intervalos de tiempo que se configurarán con una fecha / hora de caducidad.

La comunicación entre las consolas de administración y las Gateways de seguridad debe estar encriptada y autenticada con Certificados PKI.

Debe ser compatible con la integración de terceros (API pública).

Contar con un Motor de comparación de firmas que permita contrastar el contenido del tráfico de una sesión contra patrones de firmas de virus, ataques de intrusión, reconocimiento de aplicaciones u otros patrones sin comprometer el rendimiento de la red.

Debe soportar funcionalidad de alta disponibilidad activo-activo, activo-pasivo.

La solución debe admitir Alta disponibilidad de Gateways e intercambio de carga con sincronización de estado.

Debe soportar funcionalidad de balanceo de al menos dos enlaces de Internet.

Soporte de protocolos: TCP, UDP, ARP, ICMP, IPv4, IPv6, OSPF, IPSec, RIP.

Debe poder ser administrado por una consola central

La consola de administración debe poder ser instalada en el mismo equipo

La solución debe admitir cifrado 3DES y AES-256 para IKE Phase I y II IKEv2 más "Suite-B-GCM-128" y "Suite-B-GCM-256" para Fase II.

La solución debe admitir al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 y Grupo 20

La solución debe ser compatible con la integridad de los datos con md5, sha1 SHA-256, SHA-384 y AES-XCBC.

Se debe admitir CA interna y CA externa de terceros.

La solución debe incluir soporte para VPN de sitio a sitio en las siguientes topologías:

Full Mesh (todo para todos),

Estrella (oficinas remotas al sitio central)

Hub and Spoke (sitio remoto a través del sitio central a otro sitio remoto)

La solución debe ser compatible con la configuración de VPN con una GUI mediante la adición de objetos de arrastrar y soltar a las comunidades de VPN

La solución debe admitir VPN SSL sin cliente para el acceso remoto.

La solución debe ser compatible con VPN L2TP, incluida la compatibilidad con el cliente de iPhone L2TP

La solución debe permitir que el administrador aplique reglas de seguridad para controlar el tráfico dentro de la VPN

La solución debe admitir redes privadas virtuales (VPN) basadas en dominio y VPN basadas en rutas que utilicen VTI y protocolos de enrutamiento dinámico.

La solución debe incluir la capacidad de establecer VPN con puertas de enlace con IP públicas dinámicas

La solución debe incluir compresión de IP para VPNs de cliente a sitio y de sitio a sitio.

Debe poder adquirir la identidad del usuario al consultar Microsoft Active Directory en función de los eventos de seguridad.

Debe tener un método de autenticación de identidad de usuario basado en el navegador para usuarios o activos que no sean de dominio

Debe proveer múltiples métodos de identificación de usuarios: Consulta de AD, basada en navegador o agentes de identidad, autenticación transparente de Kerberos, portal captivo.

Debe soportar entornos de servidor de terminal.

La solución debe integrarse perfectamente con los servicios de directorio, IF-MAP y Radius.

El impacto en los controladores de dominio debe ser inferior al 3%.

La solución de identidad debe admitir servidores de terminal y Citrix.

La solución debería permitir la identificación a través de un proxy (por ejemplo: encabezados X-forward).

Debe poder adquirir la identidad del usuario de Microsoft Active Directory sin ningún tipo de agente instalado en los controladores de dominio.

Debe admitir la autenticación transparente de Kerberos para el inicio de sesión único.

Debe admitir el uso de grupos anidados LDAP.

Debe poder compartir o propagar identidades de usuario entre múltiples puertas de enlace de seguridad.

Debe poder crear roles de identidad para usar en todas las aplicaciones de seguridad.

Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;

Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios.

La solución ofrece soporte para la inspección / descifrado SSL con un rendimiento líder en todas las tecnologías de mitigación de amenazas.

La solución debe ser compatible con Perfect Forward Secrecy (PFS, ECDHE Cipher Suites).

La solución debe ser compatible con AES-NI, AES-GCM para mejorar el rendimiento

La solución debe aprovechar la base de datos de filtrado de URL para permitir al administrador crear una política de inspección https granular.

La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web;

Las características de VPN SSL se deben cumplir con o sin el uso de agentes;

Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy.

7.3 Firewalls localidades remotas

2 Gbps de paquetes de UDP de 1518 byte firewall throughput

670 Mbps IPS de throughput

600 Mbps de throughput como NGFW

Con un throughput de 970 Mbps de VPN AES-128

Que soporte hasta 10,500 conexiones por segundo

500,000 conexiones concurrentes por segundo

Debe poder integrarse a una consola centralizada para su administración

Deben contar con las capacidades de filtrado de puertos y previsión de intrusos.

El Gateway de seguridad debe usar Stateful Inspection basada en el análisis granular de la comunicación y el estado de la aplicación para rastrear y controlar el flujo de la red.

La solución debe admitir el control de acceso para al menos 150 servicios o protocolos predefinidos.

Debe proporcionar estadísticas de recuento de aciertos de reglas de seguridad a la Consola de administración.

Debe permitir que las reglas de seguridad se apliquen en intervalos de tiempo que se configurarán con una fecha / hora de caducidad.

La comunicación entre las consolas de administración y las Gateways de seguridad debe estar encriptada y autenticada con Certificados PKI.

Debe ser compatible con la integración de terceros (API pública).

Contar con un Motor de comparación de firmas que permita contrastar el contenido del tráfico de una sesión contra patrones de firmas de virus, ataques de intrusión, reconocimiento de aplicaciones u otros patrones sin comprometer el rendimiento de la red.

La solución debe admitir Alta disponibilidad de Gateways e intercambio de carga con sincronización de estado.

Debe soportar funcionalidad de balanceo de al menos dos enlaces de Internet.

Soporte de protocolos: TCP, UDP, ARP, ICMP, IPv4, IPv6, OSPF, IPSec, RIP.

Debe poder ser administrado por una consola central

La consola de administración debe poder ser instalada en el mismo equipo

La solución debe admitir cifrado 3DES y AES-256 para IKE Phase I y II IKEv2 más "Suite-B-GCM-128" y "Suite-B-GCM-256" para Fase II.

La solución debe admitir al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 y Grupo 20

La solución debe ser compatible con la integridad de los datos con md5, sha1 SHA-256, SHA-384 y AES-XCBC.

Se debe admitir CA interna y CA externa de terceros.

La solución debe incluir soporte para VPN de sitio a sitio en las siguientes topologías:

Full Mesh (todo para todos),

Estrella (oficinas remotas al sitio central)

Hub and Spoke (sitio remoto a través del sitio central a otro sitio remoto)

La solución debe ser compatible con la configuración de VPN con una GUI mediante la adición de objetos de arrastrar y soltar a las comunidades de VPN

La solución debe admitir VPN SSL sin cliente para el acceso remoto.

La solución debe ser compatible con VPN L2TP, incluida la compatibilidad con el cliente de iPhone L2TP

La solución debe permitir que el administrador aplique reglas de seguridad para controlar el tráfico dentro de la VPN

La solución debe admitir redes privadas virtuales (VPN) basadas en dominio y VPN basadas en rutas que utilicen VTI y protocolos de enrutamiento dinámico.

La solución debe incluir la capacidad de establecer VPN con puertas de enlace con IP públicas dinámicas

La solución debe incluir compresión de IP para VPNs de cliente a sitio y de sitio a sitio.

Debe poder adquirir la identidad del usuario al consultar Microsoft Active Directory en función de los eventos de seguridad.

Debe tener un método de autenticación de identidad de usuario basado en el navegador para usuarios o activos que no sean de dominio

Debe proveer múltiples métodos de identificación de usuarios: Consulta de AD, basada en navegador o agentes de identidad, autenticación transparente de Kerberos, portal captivo.

Debe soportar entornos de servidor de terminal.

La solución debe integrarse perfectamente con los servicios de directorio, IF-MAP y Radius.

El impacto en los controladores de dominio debe ser inferior al 3%.

La solución de identidad debe admitir servidores de terminal y Citrix.

La solución debería permitir la identificación a través de un proxy (por ejemplo: encabezados X-forward).

Debe poder adquirir la identidad del usuario de Microsoft Active Directory sin ningún tipo de agente instalado en los controladores de dominio.

Debe admitir la autenticación transparente de Kerberos para el inicio de sesión único.

Debe admitir el uso de grupos anidados LDAP.

Debe poder compartir o propagar identidades de usuario entre múltiples puertas de enlace de seguridad.

Debe poder crear roles de identidad para usar en todas las aplicaciones de seguridad.

Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;

Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios.

La solución ofrece soporte para la inspección / descifrado SSL con un rendimiento líder en todas las tecnologías de mitigación de amenazas.

La solución debe ser compatible con Perfect Forward Secrecy (PFS, ECDHE Cipher Suites).

La solución debe ser compatible con AES-NI, AES-GCM para mejorar el rendimiento

7.4 Consola de administración de firewalls

La consola de administración debe poder guardar la información de las bitácoras por al menos 1 año y/o tener un espacio para resguardarlas de 450GB

La aplicación de administración de seguridad debe admitir cuentas de administrador basadas en roles. Por ejemplo, roles para administración de políticas de firewall solamente o rol para visualización de registros solamente.

La solución debe incluir un canal de comunicaciones seguro cifrado basado en certificado entre todos los componentes distribuidos del proveedor que pertenecen a un único dominio de administración.

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 sitio principal
El servicio de WAF debe proteger un total de 100 aplicaciones web con un ancho de banda máximo de 500 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.
La solución debe incluir protección contra ataques en capa de aplicación WEB, WAF, y dicho WAF debe estar certificado por ICSA LABS
La solución propuesta debe proteger contra ataques conocidos y ataques de día cero, soportando modelos de seguridad positivos y modelos de seguridad negativos

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 Reporte - Modo Bloqueo - Modo bypass
Las protecciones individuales dentro de una política de seguridad deben soportar los siguientes modos operacionales: - Modo Reporte - 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 configurar el bloqueo de High ASCII Characters en cualquier parte del request o del response HTTP
La solución de WAF debe permitir la normalización a texto de la URL utilizando un codepage determinado
La solución debe permitir específica el esquema de codificación (codepage encoding Scheme)
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 TCP, definiendo para cada aplicación protegida el TCP Timeout de la sesión.
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 bloquear métodos que no estén en compliance con el RFC HTTP (rfc 2616)
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 evaluar parámetros dentro de una solicitud de usuario detectando y bloqueando aquellas que no sean válidas de acuerdo a los siguientes criterios que podrán ser configurados: - Tipo de parámetro: Long, Float, Número, Letra, Alfanumérico, Expresión, Cadena, Null Parameter. - Longitud mínima. - Longitud máxima. - Si permite o no valores nulos.
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.
8.2 Firewall de aplicaciones Web sitio alterno
El servicio de WAF debe proteger un total de 100 aplicaciones web con un ancho de banda máximo de 500 Mbps
Debe ser en la nube o en sitio 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.
La solución debe incluir protección contra ataques en capa de aplicación WEB, WAF, y dicho WAF debe estar certificado por ICSA LABS
La solución propuesta debe proteger contra ataques conocidos y ataques de día cero, soportando modelos de seguridad positivos y modelos de seguridad negativos
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 Reporte - Modo Bloqueo - Modo bypass
Las protecciones individuales dentro de una política de seguridad deben soportar los siguientes modos operacionales: - Modo Reporte - 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 configurar el bloqueo de High ASCII Characters en cualquier parte del request o del response HTTP
La solución de WAF debe permitir la normalización a texto de la URL utilizando un codepage determinado
La solución debe permitir específica el esquema de codificación (codepage encoding Scheme)
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 TCP, definiendo para cada aplicación protegida el TCP Timeout de la sesión.
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 bloquear métodos que no estén en compliance con el RFC HTTP (rfc 2616)
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 evaluar parámetros dentro de una solicitud de usuario detectando y bloqueando aquellas que no sean válidas de acuerdo a los siguientes criterios que podrán ser configurados: - Tipo de parámetro: Long, Float, Número, Letra, Alfanumérico, Expresión, Cadena, Null Parameter. - Longitud mínima. - Longitud máxima. - Si permite o no valores nulos.
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.
8.3 Consola de admon WAFs
La consola de gestión debe soportar la administración y monitoreo de 2 WAF el del sitio principal y el del sitio alterno
La consola de gestión deberá permitir asignar roles de administración y monitoreo de seguridad por cada uno de los equipos administrados.
La consola de gestión debe permitir el acceso a la interfaz gráfica a través del protocolo HTTPS.
La consola de gestión debe soportar autenticación remota a través de los protocolos de autenticación RADIUS, LDAP y TACACS+.
La consola de gestión debe permitir la configuración de NTP.
La consola de gestión deberá permitir el acceso por REST API. Todas las operaciones que puedan realizarse a través de esta API deben estar completamente documentadas.
La consola de gestión deberá permitir contar con un repositorio de logs que permitan visualizar todos los cambios de configuración que se realizan sobre los equipos.
La consola de gestión debe soportar alertas de auditoría
La consola de gestión debe permitir configuración de alertas a servidores de syslog y snmp externos
La consola de gestión debe permitir sincronización con un servidor NTP
La consola de gestión debe permitir visualizar la utilización de CPU de los dispositivos administrados
La consola de gestión debe contar con una funcionalidad que permita la captura de paquetes que ingresan y salen del equipo. Estos archivos deberán estar en formato CAP y deben poder descargarse.
La consola de gestión debe permitir creación de tareas calendarizadas de backup de los dispositivos administrados
La consola de gestión permitirá guardar los backups localmente o enviarlos a un repositorio externo a través de SCP, SFTP o SSH.
La consola de gestión debe permitir creación de tareas calendarizadas para las actualizaciones de seguridad del dispositivo
Desde la consola de gestión se podrá realizar la actualización de la versión principal de los dispositivos administrados.
Desde la consola de gestión se podrán administrar distintas versiones de dispositivos, teniendo la chance de un rollback de versión en caso de ser necesario
La consola de gestión debe permitir la administración de múltiples dispositivos, pudiendo realizar configuración simultánea en varios dispositivos.

La consola de gestión debe permitir la creación de scripts y flujos de trabajo para automatizar tareas de configuración recurrentes
La consola de gestión debe permitir la comparación de la configuración entre dos dispositivos.
La consola de gestión debe permitir la comparación de la configuración entre un dispositivo y un backup determinado
La consola de gestión centralizada debe contar con dashboards que resuman el estado de las aplicaciones balanceadas en caso de existir
Los dashboards debe mostrar el top de aplicaciones por Throughput y por Request por segundo
Los dashboards deben mostrar información de Throughput, Conexiones por Segundo, Conexiones concurrentes, Request por segundo para cada aplicación por separado.
Los dashboards debe mostrar información de Throughput, Conexiones por Segundo, Conexiones concurrentes para cada servidor real que hace parte de un grupo de balanceo
Para el tráfico SSL los dashboards deben mostrar las conexiones por segundo por cada aplicación, de acuerdo a la versión de TLS utilizada
Para el tráfico SSL los dashboards deben mostrar los algoritmos de intercambio de llaves por cada aplicación
Para el tráfico SSL los dashboards deben mostrar el TOP de los Ciphers utilizados por cada aplicación
Para el tráfico SSL los dashboards deben mostrar el porcentaje de handshakes rechazados por cada aplicación
Para el tráfico SSL los dashboards deben mostrar las conexiones por segundo SSL dando estadísticas gráficas de las nuevas conexiones, las conexiones reusadas y aquellas rechazadas
La consola de gestión debe incluir los logs de las transacciones que van a los sitios web publicados en los WAF.
La consola de gestión debe almacenar hasta 7 días de logs de transacciones que van a los sitios web publicados en en los balanceadores.
La consola de gestión debe permitir la navegación sobre los logs de transacciones, con al menos las siguientes características:
Modificar el rango de tiempo de búsqueda
Debe dar el número total de transacciones en un rango de tiempo seleccionado
Debe clasificar las conexiones en transacciones normales y transacciones fallidas, mostrando el número total para cada una de ellas
Por cada transacción debe entregar detalles de la petición, la respuesta, el tiempo de respuesta, los parámetros del cliente que realiza la conexión, detalles de SSL y los detalles del balanceo

Debe permitir búsquedas rápidas dentro del conjunto de logs transaccionales guardados, a través de criterios flexibles y personalizables.
La consola de gestión debe permitir generar reportes históricos de las aplicaciones
La consola de gestión debe permitir programar tareas de reportes y enviar los reportes vía correo electrónico.
La consola de gestión debe permitir configurar un rango de tiempo de hasta 3 meses para la generación de reportes históricos
Debe soportar formatos PDF, CSV y HTML para los reportes históricos
Debe permitir la personalización del logo de la entidad en los reportes
Debe permitir escoger las aplicaciones específicas sobre los cuales se ejecutará el reporte
La consola de gestión debe permitir personalizar el contenido de los reportes con mínimo las siguientes estadísticas:
Tiempo de Respuesta
Throughput
Conexiones Concurrentes
Conexiones por Segundo
Request por Segundo
MONITOREO Y REPORTES DE SEGURIDAD WEB
La consola de gestión debe contar con un dashboard que resuma los eventos de seguridad.
El dashboard debe permitir seleccionar la información a mostrar, las aplicaciones y el rango de tiempo.
El dashboard debe contener al menos los siguientes cuadros de información:
Top de Ataques por categoría
Top de Orígenes y Destinos
Ataques por acción
Top de Ataques por Severidad
Geolocalización de los ataques
La consola de gestión debe permitir generar reportes históricos de los ataques detectados y mitigados por la solución
La consola de gestión debe permitir programar tareas de reportes y enviar los reportes vía correo electrónico.
La consola de gestión debe permitir configurar un rango de tiempo de hasta 3 meses para la generación de reportes históricos
Debe soportar formatos PDF, CSV y HTML para los reportes históricos
Debe permitir la personalización del logo de la entidad en los reportes
Debe permitir escoger la o las aplicaciones que harán parte del reporte
La consola de gestión debe permitir búsquedas de eventos de seguridad a través de la definición de criterios de búsqueda. Como mínimo se deben incluir los siguientes criterios:
Nombre del Ataque
IP Origen e IP Destino

Nombre de la aplicación
Severidad
Tipo de amenaza
La consola de gestión debe permitir anidar múltiples criterios a través de expresiones regulares
Desde la consola de gestión se deben enviar alertas de ataques
Debe permitir escoger las aplicaciones específicas sobre los cuales se realizará la configuración de la alerta
Desde la consola de gestión se podrá personalizar el tipo de alertas que se enviarán a través de la creación de expresiones regulares con al menos los siguientes criterios:
Nombre del Ataque
IP Origen e IP Destino
Nombre de la aplicación
Severidad
Tipo de amenaza
Desde la consola de gestión se podrá configurar la severidad de la alerta
DASHBOARD DE IP DE MALA REPUTACIÓN
La consola de gestión debe incluir un dashboard en donde se muestre el impacto de las listas de mala reputación configuradas en la solución de mitigación de ataques DDoS.
El dashboard de IPs de mala reputación debe incluir el TOP de eventos, TOP de paquetes y TOP por volumen de tráfico, por al menos los siguientes criterios: - Geolocalización -Actividad Maliciosa -Direcciones IP Origen -Línea de tiempo
El dashboard de IPs de mala reputación debe permitir modificar el tiempo de muestra datos con una profundidad máxima de 3 meses.

9. ANALIZADOR EXPERTO DE PROTOCOLOS
9.1 Analizador experto de protocolos
Pueda instalarse en una PC portátil con Windows 7, Windows 8 y/o Windows 10

Que sobre los paquetes capturados pueda reportar: demanda de ancho de banda vs el tiempo, Permita el monitoreo y reporteo de demanda de puertos específicos vs el tiempo, demanda de grupos de puertos específicos vs el tiempo, uso de las aplicaciones vs el tiempo, las "pláticas" de estaciones, la distribución del tamaño de los paquetes, la distribución de protocolos, a nivel MAC pueda reportar el volumen de UNICAST, MULTICAST Y BROADCAST, y las estaciones más demandantes de los mismos, así como estadísticas y errores de VLANs, MPLS, ARP, ICMP, DHCP, DNS; VXLAN, LLDP, conversaciones a nivel IP, a nivel MAC, a nivel subnets, a nivel países. Estadísticas y errores a nivel web, comportamiento y estaciones, estadísticas y errores a nivel VoIP, estadísticas y errores del protocolo RIOS, estadísticas y errores del protocolo, estadísticas y errores a nivel SQL, estadísticas y errores a nivel CIFS, estadísticas y errores VXLAN, Códigos de error de los protocolos de red y de desempeño.

Permite el análisis de transacciones

Permite el análisis multisegmento

Permite el consumo de paquetes capturados en la herramienta Wireshark

Permite programar la captura de paquetes considerando criterios como tiempo, número de paquetes, la aparición de protocolos específicos

Que pueda identificar a nivel WiFi los canales utilizados

Que pueda a nivel WiFi descifrar la información si cuenta con la llave sobre los protocolos de WPA y WPA2

Que pueda conectarse a un elemento remoto, denominado PROBE para la captura remota de paquetes, siempre y cuando este sea compatible

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.

La plataforma que brinda los servicios debe contar con la autorización FedRAMP y auditorías para procedimientos de seguridad SSAE 18 SOC 2, así como ser una solución ASV (Approved Scanning Vendor) de PCI (Payment Card Industry).

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.

La solución se debe licenciar por IP o HOST y debe proveer capacidades de descubrimiento e inventario ilimitadas con acceso ilimitado a agentes y escáneres virtuales, así como contar con un sensor de descubrimiento pasivo sin licenciamientos o costos adicionales.
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 Contenedores: Debe permitir descubrir y tener visibilidad de la infraestructura de contenedores activos o inactivos brindando información de imágenes, registros, contenedores asociados o creados a partir de la misma imagen y hosts / pods donde se encuentran.

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
FQDN
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% (six sigma).
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 permitir la evaluación, informar y reportar problemas de configuración, en función de las referencias del estándar de industria Center of Internet Security (CIS).

El fabricante debe estar certificado por CIS de forma oficial para entregar este nivel de controles y los reportes deben incluir la leyenda de cumplimiento de CIS.

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.
La solución propuesta deberá:

Permitir enviar alertas en tiempo real acerca de las irregularidades en la red, identificar amenazas y supervisar los cambios inesperados que se produzcan en la misma.
Enviar notificaciones para usuarios específicos y grupos de usuarios para el perfil de monitoreo o múltiples perfiles de monitoreo.

Permitir personalizar el perfil de monitoreo asociado a una lista específica de criterios.

Permitir que las alertas se puedan personalizar para con una amplia variedad de condiciones que afectan a los sistemas, certificados, vulnerabilidades, puertos, servicios y software. Cada regla debe permitir configurarse para detectar cambios generales comunes o ajustarse a circunstancias muy específicas.
Permitir la asignación de diferentes destinatarios para cada alerta.

Enviar de alertas de monitoreo sobre vulnerabilidades, configuraciones incorrectas y otros parámetros definidos por el administrador de la solución, tales como:
Certificados expirados o por expirar
Puertos abiertos
Vulnerabilidades graves
Tickets de remediación abiertos, resueltos o cerrados
La solución propuesta deberá:

Proveer fuentes de inteligencia de amenazas en tiempo real y técnicas de aprendizaje automático, para brindar control al administrador sobre la evolución de las amenazas relacionadas con las vulnerabilidades halladas en los activos de la organización e identificar cuáles corregir primero.

Permitir realizar consultas ad hoc con múltiples variables y criterios, como clase de activo, tipo de vulnerabilidad, indicadores de amenazas en tiempo real, etiqueta del activo y sistema operativo, de modo que se pueda, por ejemplo, buscar todas las vulnerabilidades que tienen una clasificación de gravedad alta, son fáciles de explotar y fueron divulgadas en la última semana.
Hacer una correlación en tiempo real de amenazas activas contra las vulnerabilidades detectadas en los activos corporativos.
Incluir indicadores de amenazas en tiempo real que ayuden a evaluar y priorizar las vulnerabilidades detectadas, categorizados de la siguiente forma:
Dia cero: vulnerabilidades para las que no hay un parche disponible y para las que se ha observado un ataque activo.
Exploit público: Vulnerabilidades cuyo mecanismo de explotación es conocido, para las que existe un código de explotación y está disponible públicamente.
Ataques activos: Vulnerabilidades que están siendo atacadas activamente.
Movimiento lateral: Vulnerabilidades que permiten que el atacante propague el ataque ampliamente a través de la red violada.
Fácil explotación: Vulnerabilidades que se pueden explotar fácilmente, que requieren pocas habilidades y pocos conocimientos

Pérdida de datos: Vulnerabilidades cuyo exploit producirá una pérdida masiva de datos

Denegación de servicio: Vulnerabilidades cuyo payload podría sobrecargar o bloquear los sistemas comprometidos para que no estén disponibles de forma permanente o temporal.

Sin Parche: Vulnerabilidades para las que no hay una solución por parte del proveedor
Malware: Vulnerabilidades asociadas infecciones de malware
Kit de explotación: Vulnerabilidades para las que hay disponible un exploit kit
La solución propuesta deberá:

Proporcionar un flujo de trabajo de remediación basado en políticas de creación y asignación, reasignación de tickets de acuerdo a condiciones definidas por el administrador de la solución a través de políticas o también de forma manual.
Permitir la creación de tickets con estados abierto, cerrado, ignorado, basándose en los siguientes criterios:
Host/s a quien aplicar la regla
Vulnerabilidad/es a las cuales se aplica la regla
Usuario asignado
Fecha de creación o expiración
Cambio de estado
Crear tickets de remediación automáticamente a partir del resultado de un escaneo de vulnerabilidades o basándose en información de un host específico y también de forma manual por un administrador de la solución.
La solución propuesta deberá:
Correlacionar de forma automática vulnerabilidades y parches para los hosts (Windows) de la organización.

Mapear automáticamente los parches con los CVE asociados a las vulnerabilidades detectadas.
A través del agente en un servidor Windows, confirmar que parches considerados como críticos tiene instalados y cuales no tiene instalados
La solución propuesta deberá:

Permitir la administración centralizada vía interfaz gráfica WEB utilizando HTTPS.

Acceder a la consola de todos los componentes del servicio desde un único punto, incluso de forma remota desde cualquier parte del mundo sin conexiones hacia nuestra red.
Permitir definir diferentes perfiles y roles de usuario para su administración.

Proporcionar controles jerárquicos de acceso de usuarios basados en roles que permitan la delegación de responsabilidades para reflejar la estructura organizacional.
Permitir el acceso de un usuario autorizado desde cualquier ubicación.
Admitir una biblioteca de API XML extensible
La solución propuesta deberá:
Admitir la autenticación de dos factores para los usuarios y el inicio de sesión.
Admitir la configuración de seguridad de contraseñas y personalizar la política de seguridad para la configuración de administración de contraseñas:
Antigüedad y vencimiento de la contraseña.

Cuenta de usuario bloqueada después de un número de inicios de sesión fallidos.
Longitud mínima de la contraseña.
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.
La solución propuesta deberá:
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.
La solución propuesta deberá:
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.
Soportar escaneos programados de servicios API SOAP y REST.
Contar con una API e integración con Jenkins para automatizar el escaneo en un entorno de CI / CD.

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.
Admitir la capacidad de detección de malware de día cero.
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.

Resumen de servicios y/o funcionalidades requeridas

- Web Application Firewall (2)
- Consola de administración WAF (1)
- Licencias de Parcheo (1,200)
- Licencias de Firewall Personal (1,200)
- Anitvirus para móviles (opcional)
- Licencias de Cifrado (1,200)
- Sandbox para el endpoint (1)
- Previsor de Intrusos de Red (2)
- Scanner de vulnerabilidades (256)
- Scanner de vulnerabilidades web (25)
- Acceso a la red ZTNA (1,200)
- URL filtering (1,200)
- CASB (1,200)
- Data Loss Prevention (1,200)
- Packet Analyzer (1)
- IPS's virtuales (8)
- Consola de administración para IPS´s (2)
- Sandbox para los IPSs (1)
- Change Control para servers (70)
- Antivirus de nueva generación (1,200)
- Administrador de parcheo virtual (1,200)
- Seguridad en bases de datos (14)
- Correlacionador de eventos
- Privilege Access Manager (20)
- Next Generation Firewalls principales (4)
- Consola de administración para los Firewalls (2)
- EDR para PCs (1,200)
- EDR para Servers (70)
- Control de aplicaciones para pcs (1,200)
- Seguridad de prevención de fuga de información en dispositivos móviles con aplicaciones de Google Enterprise sin instalación de agentes.
- Instalación, soporte y servicios administrados por 3 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. Se espera que los IPS's y el firewall de seguridad perimetral no sean del mismo fabricante (esto como mejor práctica para asegurar que no existan las mismas vulnerabilidades en estos dispositivos).

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

El hardware que el proveedor requiera ubicar dentro de las instalaciones del municipio lo podrá retirar al término del contrato

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.

Es importante que los controles y herramientas tengan el menor número de
consolas con el objetivo de reducir el esfuerzo de monitoreo por parte del municipio.

El proveedor deberá contar con una certificación ISO/IEC 27001:2013

ATENTAMENTE

_____

Nombre y firma de la persona física o representante legal

MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN
Secretaría de Administración
Dirección de Adquisiciones

Concurso por Licitación Pública Nacional Presencial No. SA-DA-CL-26/2022
"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

Anexo 2. "Cotización"

Anexos	Conceptos	Precio Unitario
A	REQUERIMIENTOS DE PRODUCTOS	
B	REQUERIMIENTOS DE INSTALACIÓN Y CONFIGURACIÓN DE LOS PRODUCTOS	
C	REQUERIMIENTOS DE SOPORTE	
D	REQUERIMIENTOS DE SERVICIOS ADMINISTRADOS	
E	CARACTERÍSTICAS Y/O CAPACIDADES DE TODOS LOS PRODUCTOS	
	Subtotal.-	
	I.V.A.-	
	Total.-	

ATENTAMENTE

_____

Nombre y firma de la persona física o representante legal

Nota: Los modelos de carta que a continuación se presentan son un ejemplo que podrá utilizar el participante para la presentación de los documentos que se solicitan en las presentes bases, no será causa de descalificación el no utilizar estos ejemplos).

Modelo de Carta de Interés de Participar en el Concurso

_____ a ____ de _____ de 2022.

Municipio de San Pedro Garza García N.L.
Ing. Carlos Romanos Salazar
Director de Adquisiciones
Presente.-

Por medio de la presente y "Bajo protesta de decir verdad", manifiesto que los datos aquí asentados, son ciertos y han sido debidamente verificados, así como que cuento con facultades suficientes para **manifestar interés en participar** en el presente Concurso por Licitación Pública Nacional Presencial no. ___**,** relativo a "_____", a nombre y representación de la empresa (**participante**) por lo que solicito que se nos considere como participantes en la misma.

Registro Federal de Contribuyentes: _____

Domicilio: _____
(calle, número exterior y/o interior y colonia,)

_____
(municipio, entidad federativa y código postal)

Teléfonos: _____

Correo electrónico: _____
(de preferencia un correo institucional: ejemplo: ventas@sanpedro.gob.mx)

En caso de ser persona moral:

N° de la escritura pública en la que consta su acta constitutiva: _____

Fecha de la escritura pública: _____

_____
(Nombre, número y lugar del notario público ante el cual se dio fe de la misma)

Relación de accionistas:

Apellido paterno: Apellido materno Nombre (s):

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

Descripción del objeto social: _____

_____

_____

Reformas al acta constitutiva: _____

_____

_____

_____

Nombre del apoderado o representante legal: _____

Correo electrónico del representante legal : _____

(de preferencia un correo institucional del representante legal)

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 dio fe de la misma)

Protesto lo necesario.

_____

(nombre del representante legal de la concursante y firma autógrafa)

Modelo de Carta para presentar pregunta en la Junta de Aclaraciones

_____ a ____ de _____ de 2022.

Municipio de San Pedro Garza García N.L.
Ing. Carlos Romanos Salazar
Director de Adquisiciones
Presente.-

Por medio de la presente, y en representación de la empresa (nombre o razón social), me permito solicitar a la Dirección de Adquisiciones, la aclaración de las siguientes dudas a las bases del concurso por Licitación Pública Nacional Presencial no. _____.

1	Referencia	
	Pregunta	
	Respuesta	
2	Referencia	
	Pregunta	
	Respuesta	
3	Referencia	
	Pregunta	
	Respuesta	

A T E N T A M E N T E

_____

NOMBRE Y FIRMA DE LA PERSONA FÍSICA
O REPRESENTANTE LEGAL

Nota: Esta solicitud deberá presentarse en papel membretado de la concursante, acompañándola de la versión electrónica de la misma en formato Word en USB.

Modelo de Carta de cumplimiento a lo dispuesto en el artículo 49, fracción IX de la Ley de Responsabilidades Administrativas del Estado de Nuevo León, Persona Moral

AL MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN.
PRESENTE.-

En cumplimiento a lo dispuesto por el artículo 49, fracción IX de la Ley de Responsabilidades Administrativas del Estado de Nuevo León, el C. _____, acudo en mi carácter de Representante Legal de la persona moral denominada _____, para lo cual, manifiesto **Bajo Protesta De Decir Verdad,** que tanto el suscrito, la empresa que represento, así como sus socios y accionistas que la conforman, al participar en contrataciones públicas no se actualiza conflicto de interés con la administración pública de esta Municipalidad.

Asimismo, manifiesto que mi representada, sus socios y accionistas no mantenemos en la actualidad ningún procedimiento en nuestra contra vinculado con faltas administrativas o hecho de corrupción, ni existe sanción o medida cautelar dictada por autoridad administrativa, penal, mercantil, fiscal o de cualquier naturaleza que impida legalmente participar en contrataciones públicas.

Expreso igualmente, que mi representada no ha contratado a persona alguna que haya fungido como servidor público en este Municipio, durante el año previo a la firma de la presente constancia, que posea información privilegiada que directamente haya adquirido con motivo de su empleo, cargo o comisión en el servicio público, y directamente permita que mi representada se beneficie en el mercado o se coloque en situación de ventaja frente a sus competidores.

San Pedro Garza García Nuevo León, a los ___ días del mes de ____ 2022.

_____

Nombre y firma

Modelo de Carta de cumplimiento a lo dispuesto en el artículo 49, fracción IX de la Ley de Responsabilidades Administrativas del Estado de Nuevo León, Persona Física

AL MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN.
PRESENTE.-

En cumplimiento a lo dispuesto por el artículo 49, fracción IX de la Ley de Responsabilidades Administrativas del Estado de Nuevo León, el suscrito_____ manifiesto **Bajo Protesta De Decir Verdad** que con mi participación en contrataciones públicas con esta Municipalidad no se actualiza conflicto de interés.

Asimismo, manifiesto que actualmente no mantengo ningún procedimiento en mi contra vinculado con faltas administrativas o hecho de corrupción, tampoco existe sanción o medida cautelar dictada por autoridad administrativa, penal, mercantil, fiscal o de cualquier naturaleza que me impida legalmente participar en contrataciones públicas.

Expreso igualmente, que no he contratado a persona alguna que haya fungido como servidor público en este Municipio durante el año previo a la firma de la presente constancia, que posea información privilegiada que directamente haya adquirido con motivo de su empleo, cargo o comisión en el servicio público, y directamente me permita beneficiarme en el mercado o colocarme en situación de ventaja frente a mis competidores.

San Pedro Garza García Nuevo León, a los ___ días del mes de ____ 2022.

_____

Nombre y firma

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 LA C. LAURA LETICIA LOZANO VILLALOBOS, SECRETARIA DE ADMINISTRACIÓN, EN EJERCICIO DE LAS FACULTADES DELEGADAS POR EL C. PRESIDENTE MUNICIPAL Y EL C. SECRETARIO DEL REPUBLICANO AYUNTAMIENTO; Y POR OTRA PARTE, «ARTÍCULO» «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:

A) 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.

B) Que en la Primera Sesión Ordinaria del Republicano Ayuntamiento de San Pedro Garza García, Nuevo León, celebrada en fecha 10-diez de diciembre de 2019-dos mil diecinueve, se aprobó el Acuerdo Delegatorio del C. Presidente Municipal y el C. Secretario del Republicano Ayuntamiento, mediante el cual delegan en los Titulares de la Secretaría de Administración y de la Secretaría del Ramo correspondiente, la atribución de suscribir contratos o convenios relativos a adquisiciones, prestación de servicios o arrendamientos que se adjudiquen de conformidad con la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León y el Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León, lo anterior en términos del resolutivo Primero del Acuerdo; lo que es el caso en el presente Contrato. Dicho Acuerdo fue debidamente publicado en el Periódico Oficial del Estado de fecha 25-veinticinco de diciembre de 2019-dos mil diecinueve.

C) La C. LAURA LETICIA LOZANO VILLALOBOS, comparece a la celebración del presente acto jurídico en ejercicio de las facultades que le fueran delegadas por el C. Presidente Municipal y el C. Secretario del R. Ayuntamiento, así como en su carácter de Secretaria de Administración, manifestando que está facultada para dar seguimiento a los contratos de adquisiciones que requieran las distintas dependencias, órganos y unidades de la Administración Pública Municipal Centralizada, y participar en la

elaboración de los convenios o contratos que en esta materia comprometen financieramente al Municipio, llevar a cabo las adquisiciones, la contratación de arrendamientos de bienes muebles e inmuebles o la contratación de servicios que requiera la Administración Pública Municipal, de acuerdo con las necesidades descritas y limitadas por los presupuestos autorizados, aplicando las políticas y procedimientos vigentes, así como administrar y proveer los servicios de asistencia y atención médica a los trabajadores de la administración pública municipal centralizada y a sus familiares que tengan derecho, de conformidad a los convenios colectivos laborales vigentes o cualquier otra disposición legal, reglamentaria o administrativa que así lo determine. Lo anterior de conformidad con los artículos 86, 88, 89 y 91 de la Ley de Gobierno Municipal del Estado de Nuevo León vigente, y con los numerales 17, 18, 25, fracción I, 44 letra a, fracciones III y VI, y letra c, fracción I del Reglamento Orgánico de la Administración Pública Municipal de San Pedro Garza García, Nuevo León.

D) 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.

E) 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 _.

F) 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:

A) Que es «ESPECIALIDAD», lo que acredita con _», respectivamente, expedidas por _.

B) Que tiene los conocimientos, capacidad y experiencia necesaria para prestar el servicio que requiere “EL MUNICIPIO”.

C) 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.

NOVEVA: 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 2020-DOS

MIL VEINTE.

“EL MUNICIPIO”

C. LAURA LETICIA LOZANO VILLALOBOS

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

“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.

Ing. Carlos Romanos Salazar
Director de Adquisiciones
Rúbrica