CONTRATO DE ADQUISICIÓN DE LICENCIAS Y SUSCRIPCIONES DE SEGURIDAD INFORMÁTICA, SOPORTE DE INFRAESTRUCTURA INSTALADA Y SERVICIOS ADMINISTRADOS 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 EL **C. DANIEL ÓSCAR DARES DE LEÓN**, DIRECTOR GENERAL DE TECNOLOGÍAS, Y POR OTRA PARTE, LA SOCIEDAD DENOMINADA **"VDV NETWORKS", S.A. DE C.V.**, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ **"LA EMPRESA"**, REPRESENTADA EN ESTE ACTO POR EL **C. RENÉ FUENTES GARCÍA DE LEÓN**, EN SU CARÁCTER DE APODERADO GENERAL; MISMOS QUE SE SUJETAN AL TENOR DE LAS SIGUIENTES:

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

I.- DECLARA "EL MUNICIPIO", A TRAVÉS DE SUS REPRESENTANTES, LO SIGUIENTE:

a) Que de conformidad con lo dispuesto por el artículo 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.

9:31

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
RECIBIDO
26 OCT 2022
CONVENIOS Y CONTRATOS
SAN PEDRO GARZA GARCÍA, N.L.

b) Que en la Primera Sesión Ordinaria del Republicano Ayuntamiento de San Pedro Garza García, Nuevo León, celebrada en fecha 12-doce de octubre de 2021-dos mil veintiuno, 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 20-veinte de octubre de 2021-dos mil veintiuno; y además, en términos de los artículos Cuarto y Sexto

RECIBIDO
03:14
26 OCT 2022
SECRETARÍA DE FINANZAS Y TESORERÍA MUNICIPAL
SAN PEDRO GARZA GARCÍA, N. L.

Transitorios del Reglamento Orgánico de la Administración Pública Municipal de San Pedro Garza García, Nuevo León, vigente.

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, además de dictar las políticas, lineamientos y requerimientos técnicos para la sistematización, captura, control, seguimiento y resguardo de documentos digitales en poder de la Administración Pública Municipal Centralizada, así como también desarrollar y promover la generación y uso de sistemas de información para el establecimiento de gobierno electrónico en materia de trámites y servicios municipales; 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, 24, fracción III, 25, fracción I, 62, inciso a), fracciones III y VI, inciso e), fracciones IV y XIII, y 63, fracción IV del Reglamento Orgánico de la Administración Pública Municipal de San Pedro Garza García, Nuevo León.

d) El **C. DANIEL ÓSCAR DARES DE LEÓN**, comparece a la celebración del presente acto jurídico en su carácter de Director General de Tecnologías de la Secretaría de Administración, manifestando que está facultado para intervenir en el presente contrato en auxilio de la Secretaria de Administración en materia de tecnologías, en su facultad de dictar las políticas, lineamientos y requerimientos técnicos para la sistematización, captura, control, seguimiento y resguardo de documentos digitales en poder de la Administración Pública Municipal Centralizada, así como también desarrollar y promover la generación y uso de sistemas de información para el establecimiento de gobierno electrónico en materia de trámites y servicios municipales; 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 62, inciso e), fracciones IV y XIII, y 63, fracción IV del Reglamento

Orgánico de la Administración Pública Municipal de San Pedro Garza García, Nuevo León.

e) Que requiere la renovación de licencias y suscripciones de seguridad informática con soporte de fabricante, para la infraestructura actualmente instalada, así como los servicios administrados de dicha infraestructura, a fin de reducir riesgos a la seguridad en la red, navegación en internet, portales web, equipos de cómputo y bases de datos de sistemas municipales.

f) 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.

g) Que en virtud de que la vigencia del presente contrato excede el término de la actual Administración Municipal (2021-2024), en la Primera Sesión Ordinaria del Republicano Ayuntamiento de San Pedro Garza García Nuevo León, del mes de mayo, celebrada en fecha 10-diez de mayo de 2022-dos mil veintidós, se aprobó la celebración del presente contrato.

h) Por tal motivo, en fecha 13-trece de junio de 2022-dos mil veintidós, la Dirección de Adquisiciones de la Secretaría de Administración de este municipio, de conformidad con el procedimiento de Licitación Pública previsto en los artículos 1, fracción V, 2, 14, 16, fracciones II y 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 y 106 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León y artículos 36, fracciones VII, XII, XVIII, XXI y XXX, y 123, fracción I del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León lanzó la Convocatoria, en la que se contiene el Concurso por Licitación Pública Nacional Presencial número SA-DA-CL-26/2022, a las personas físicas y morales a participar en la "Adquisición de licencias y suscripciones de seguridad informática, soporte de infraestructura instalada y servicios administrados", objeto del presente instrumento. Dicha convocatoria fue debidamente publicada en el Periódico Oficial del Estado y en uno de los diarios de mayor circulación en la entidad.

i) En fecha 23-veintitrés de junio de 2022-dos mil veintidós, se suspendió la correspondiente Junta de Aclaraciones, con base en lo dispuesto en el artículo 167, fracción I, cuarto párrafo del Reglamento de Adquisiciones Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León, que a la letra dice: "*El servidor público que presida la junta de aclaraciones podrá suspender la sesión, en razón del número de solicitudes de aclaración recibidas o del tiempo que se emplearía en darles contestación*", por lo que se informó a los licitantes que se continuaría en la siguiente Junta, que se llevaría a cabo el día 28-veintiocho de junio de 2022-dos mil veintidós. En dicha fecha se reanudó la Junta de Aclaraciones en la que se hizo constar, que las empresas que manifestaron su intención de participar en la convocatoria de licitación fueron:

- Total Play Comunicaciones, S.A.P.I. de C.V.
- Seguridad Informática y de Telecomunicaciones, S.A. de C.V.
- Scitum, S.A. de C.V.
- VDV Networks S.A. de C.V. ("LA EMPRESA").
- CIH Telecomunicaciones de México, S.A. de C.V.
- Axtel, S.A.B. de C.V.
- Quanti Solutions S.A. de C.V.
- Corporativo Almaba S.A. de C.V.
- MIS Services, S.A. de C.V.
- DX International, S. de R.L. de C.V.
- IQSEC, S.A. de C.V.

Así mismo se menciona que dentro del plazo señalado en las Bases se recibieron en total 350-trescientas cincuenta preguntas que presentaron los participantes, las cuales se hizo constar que se respondieron todas ellas en dicho Acto. En ese mismo Acto se les hizo saber a los participantes que el Acto de Presentación de Propuesta Técnica y Económica y Apertura de Propuesta Técnica, se llevaría a cabo el día 5-cinco de julio de 2022-dos mil veintidós.

j) Que en fecha 5-cinco de julio de 2022-dos mil veintidós, en el Acto de Presentación de Propuesta Técnica y Económica y Apertura de Propuesta Técnica, las empresas: IQSEC, S.A. de C.V., Scitum, S.A. de C.V. y "LA EMPRESA", presentaron sus propuestas técnicas y económicas, procediéndose a revisar de manera cuantitativa las propuestas técnicas, cumpliendo todas las empresas participantes con los requisitos y especificaciones establecidos en las bases de este concurso, solicitados en el punto 8 inciso a). En ese mismo Acto se les hizo saber a los participantes

que el Acto de Fallo Técnico y Apertura de Propuesta Económica, se llevaría a cabo el día 11-once de julio de 2022-dos mil veintidós.

k) En fecha 11-once de julio de 2022-dos mil veintidós, en el acto de Fallo Técnico y Apertura de Propuesta Económica se hizo constar lo siguiente:

Que "LA EMPRESA", acreditó la etapa técnica en su revisión cualitativa cumpliendo con los requisitos y especificaciones establecidos en las bases del concurso en el punto 8), inciso a; por lo que se procedió a la apertura del sobre que contiene su propuesta económica, el cual se encontraba en custodia de la convocante, constatando que se mantenía cerrado, para lo cual la convocante empleó un formato de revisión (checklist), y a continuación se detalla el resultado de dicha revisión:

"LA EMPRESA" presentó su propuesta económica, la cual fue revisada de manera cuantitativa, cumpliendo con los requisitos establecidos en el punto 8), inciso b, siendo el importe para el Anexo número 2 Cotización, su oferta por la cantidad de $23'105,622.73 (Veintitrés millones ciento cinco mil seiscientos veintidós pesos 73/100 M.N.) I.V.A. incluido, entregando un cheque certificado en garantía por la oferta económica presentada, por un importe de $1'300,000.00 (Un millón trescientos mil pesos 00/100 M.N.) de BBVA México, S.A., con número 15259620.

Que la empresa IQSEC, S.A. de C.V., acreditó la etapa técnica en su revisión cualitativa cumpliendo con los requisitos y especificaciones establecidos en las bases del concurso en el punto 8) inciso a; por lo que se procedió a la apertura del sobre que contiene su propuesta económica, el cual se encontraba en custodia de la convocante constatando que se mantenía cerrado, para lo cual la convocante empleó un formato de revisión (checklist), y a continuación se detalla el resultado de dicha revisión:

La empresa IQSEC, S.A. de C.V., presentó su propuesta económica, la cual fue revisada de manera cuantitativa, cumpliendo con los requisitos establecidos en el punto 8), inciso b, siendo el importe para el Anexo número 2 Cotización, su oferta por la cantidad de $41'207,376.40 (Cuarenta y un millones doscientos siete mil trescientos setenta y seis pesos 40/100 M.N.) I.V.A. incluido, entregando una fianza en garantía por la oferta económica presentada, por un importe de $2'250,000.00 (Dos millones doscientos cincuenta mil pesos 00/100 M.N.) de Sofimex Institución de Garantías, S.A. con número 2684496.

Que la empresa Scitum, S.A. de C.V., acreditó la etapa técnica en su revisión cualitativa cumpliendo con los requisitos y especificaciones establecidos en las bases del presente concurso en el punto 8) inciso a; por lo que se procedió a la apertura del sobre que contiene su propuesta económica, el cual se encontraba en custodia de la convocante constatando que se mantenía cerrado, para lo cual la convocante empleó un formato de revisión (checklist), y a continuación se detalla el resultado de dicha revisión:

La empresa Scitum, S.A. de C.V., presentó su propuesta económica, la cual fue revisada de manera cuantitativa, cumpliendo con los requisitos establecidos en el punto 8), inciso b, siendo el importe para el Anexo número 2 Cotización, su oferta por la cantidad de $31'365,375.54 (Treinta y un millones trescientos sesenta y cinco mil trescientos setenta y cinco pesos 54/100 M.N.) I.V.A. incluido, entregando una fianza en garantía por la oferta económica presentada, por un importe de $2'030,000.00 (Dos millones treinta mil pesos 00/100 M.N.) de Inbursa Seguros de Caución y Fianzas, S.A., con número 20012148.

l) Una vez agotado el procedimiento establecido quedo asentado en el Acta de la Junta de Fallo, de fecha 13-trece de julio de 2022-dos mil veintidós, que las empresas IQSEC, S.A. de C.V., Scitum, S.A. de C.V. y "LA EMPRESA", cumplieron satisfactoriamente de manera cuantitativa y cualitativa con los requisitos establecidos en las bases del presente concurso por lo que, previa opinión del Comité de Adquisiciones, contenida en el Acta de la Octava Sesión Extraordinaria, de fecha 27-veintisiete de junio de 2022-dos mil veintidós, se dictó Fallo en el que se hace constar que se adjudica a "LA EMPRESA", la "Adquisición de licencias y suscripciones de seguridad informática, soporte de infraestructura instalada y servicios administrados", por un monto de $23'105,622.73 (Veintitrés millones ciento cinco mil seiscientos veintidós pesos 73/100 M.N.) I.V.A. incluido, con una vigencia a partir del día 13-trece de julio de 2022-dos mil veintidós, para concluir el día 6-seis de julio de 2025-dos mil veinticinco, toda vez que es la oferta más favorable y cumple con lo requerido por "EL MUNICIPIO".

m) Que su representada se encuentra inscrita en el Registro Federal de Contribuyentes del Servicio de Administración Tributaria de la Secretaría de Hacienda y Crédito Público con la clave MSP-821214-3G3.

n) "EL MUNICIPIO", por conducto de la Dirección de Adquisiciones de la Secretaría de Administración, otorgará a los Contralores Ciudadanos las facilidades que estén a su alcance, a fin de que éstos puedan realizar su

función de vigilancia, en términos de lo dispuesto por el Reglamento de la Contraloría Social del Municipio de San Pedro Garza García, Nuevo León.

o) Que para efectos de este contrato señala como domicilio para oír y recibir notificaciones el ubicado en la calle Libertad número 101, Colonia Centro en San Pedro Garza García, Nuevo León, C.P. 66200.

II.- MANIFIESTA "LA EMPRESA", POR CONDUCTO DE SU APODERADO GENERAL, LO SIGUIENTE:

a) Que su representada es una persona moral legalmente constituida conforme a las leyes de la materia, lo que acredita con la Escritura Pública número 69,770, de fecha 8-ocho de junio de 1999-mil novecientos noventa y nueve, otorgada ante la fe del Lic. José Visoso del Valle, Notario Titular número 92, con ejercicio en el entonces Distrito Federal, e inscrita en el Registro Público de Comercio del entonces Distrito Federal, bajo el Folio Mercantil Electrónico número 251458, de fecha 18-dieciocho de junio de 1999-mil novecientos noventa y nueve.

b) Que acredita la personalidad con que comparece, con el documento descrito en el inciso anterior, manifestando bajo protesta de decir verdad, que a la fecha no le ha sido revocado ni limitado el nombramiento en él consignado.

c) Que su representada tiene por objeto, la asesoría, diseño, administración, comercialización, servicio, compra y venta de equipos de cómputo, redes y sistemas de telecomunicación.

d) Que su representada se encuentra legalmente inscrita en el Servicio de Administración Tributaria de la Secretaría de Hacienda y Crédito Público, con la clave de Registro Federal de Contribuyente VNE990609282, manifestando que cumple con las obligaciones de acuerdo a lo dispuesto en el artículo 32-D del Código Fiscal de la Federación.

e) Que cuenta con la infraestructura, el equipo, el personal, las herramientas, capacidad y experiencia necesaria para proporcionar a "EL MUNICIPIO" el servicio requerido.

f) Que mediante escrito de fecha 11-once de marzo de 2022-dos mil veintidós, manifestó bajo protesta de decir verdad, que su representada cuenta con la Política de Integridad y acreditó ante la Dirección de Adquisiciones haber participado en el "Curso de Prevención de Corrupción

a Proveedores", según constancia de fecha 11-once de noviembre de 2021-dos mil veintiuno, suscrita por la Secretaria de la Contraloría y Transparencia; lo anterior conforme a lo establecido en el artículo 232, fracciones XXIV y XXV del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García Nuevo León.

g) Que los bienes y servicios ofrecidos cuentan por lo menos con un 50%-cincuenta por ciento de contenido nacional.

h) Que cuenta con los derechos para ejecutar la solución objeto de este contrato, ya que tiene la autorización para el uso de las licencias de los software y es proveedora de los siguientes fabricantes: McAfee, Forcepoint y Checkpoint, así mismo manifiesta que es distribuidor autorizado del fabricante de seguridad Web, de Previsión de Fuga de Información, de Firewall de bases de datos, de SIEM (correlacionador de eventos), del Previsor de intrusos de red, de Sandbox para endpoint y de antivirus y EDR.

i) Que para efectos de este contrato señala como domicilio para oír y recibir notificaciones el ubicado en la Avenida Real de Cumbres número 442, Colonia Real de Cumbres, Primer Sector, en Monterrey, Nuevo León.

III.- DECLARAN AMBAS PARTES:

a) Que cuentan con la capacidad legal necesaria, para contratar, obligarse y celebrar el presente contrato ajustándose al tenor de las siguientes:

C L Á U S U L A S

PRIMERA: OBJETO. "LA EMPRESA" se obliga con "EL MUNICIPIO" a llevar a cabo la renovación de licencias y suscripciones de seguridad informática con soporte de fabricante, para la infraestructura actualmente instalada, así como los servicios administrados de dicha infraestructura, a fin de reducir riesgos a la seguridad en la red, navegación en internet, portales web, equipos de cómputo y bases de datos de sistemas municipales, de igual forma a mantener las licencias y suscripciones vigentes, mantener las actualizaciones de nuevas firmas de seguridad de forma constante; los servicios deberán ser administrados y supervisados por personal de "LA EMPRESA", los cuales deberán trabajar en conjunto y bajo supervisión de la Dirección General de Tecnologías de "EL MUNICIPIO".

SEGUNDA: ESPECIFICACIONES TÉCNICAS. Los productos de seguridad de la información que "LA EMPRESA" suministrará a "EL MUNICIPIO", así como los servicios administrados, deberán cumplir con las especificaciones y cantidades descritas en los siguientes anexos

Anexo 1 "Especificaciones Técnicas".
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".

Los citados Anexos se adjuntan al presente contrato y forman parte integrante del mismo.

TERCERA: LUGAR Y FECHA DE ENTREGA DE LOS BIENES Y SERVICIOS. El tiempo total para la implementación y puesta en marcha de la solución será de 60-sesenta días naturales contados a partir del Fallo de Adjudicación, y el tiempo de operación de cada una de las Licencias será por 3-tres años a partir de la fecha de su vencimiento, la cobertura de los servicios será de conformidad con los citados Anexos.

La entrega de todos los bienes y servicios descritos en los Anexos citados, se realizará en la oficina de la Dirección General de Tecnologías, ubicada en Corregidora número 507, Palacio de Justicia, Segundo Piso, Centro de San Pedro Garza García, Nuevo León.

Al realizarse la entrega, deberá de levantarse un acta firmada por "LA EMPRESA" y el funcionario que designe "EL MUNICIPIO", a fin de dejar constancia de lo realizado.

Entregables:

- Servicios administrados de seguridad informática.

- Reporte mensual vía correo electrónico de los acontecimientos suscitados en 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.

"LA EMPRESA" deberá contar con un servicio de monitoreo 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, de igual forma, contar con al menos un Ingeniero en sitio, de lunes a viernes en horario de 8:00 a 16:00 horas.

"LA EMPRESA" deberá contar con una mesa de servicios que se encargará del registro, atención, solución y cierre de incidentes y requerimientos generados por parte de "EL MUNICIPIO". Dicha mesa operará resolviendo los temas que pueden atenderse de manera inmediata y que son concernientes a la implementación específica de "EL MUNICIPIO" y realizando las escalaciones necesarias para aquellas situaciones que requieran atención del especialista indicado; con ello se garantiza que "LA EMPRESA" tenga un canal de comunicación abierta con atención personalizada.

"LA EMPRESA" dentro del servicio administrado deberá realizar lo siguiente:

- 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.
- Planificación y recomendaciones para la optimización de arquitectura.
- Monitoreo continuo de servicios de seguridad y accesos.

CUARTA: VIGENCIA. La vigencia del presente contrato concluirá el día 6-seis de julio de 2025-dos mil veinticinco, en el entendido que el inicio de la misma fue a partir del día 13-trece de julio de 2022-dos mil veintidós.

La operatividad de las Licencias será por 3-tres años a partir de la fecha de vencimiento de cada una de ellas.

QUINTA: PRECIO Y FORMA DE PAGO. El precio total que pagará "EL MUNICIPIO" a "LA EMPRESA" por el suministro, instalación y configuración de los productos objeto del presente contrato, será la cantidad total de $23'105,622.73 (Veintitrés millones ciento cinco mil seiscientos veintidós pesos 73/100 M.N.) I.V.A. incluido, comprometiéndose "LA EMPRESA" a no realizar ninguna modificación a dicha cantidad durante la vigencia del presente contrato, ya que el mencionado precio es fijo y no se reconocerá incremento alguno.

Los precios unitarios de cada concepto, se citan en el Anexo 2 Cotización, el cual se agrega al presente contrato y forma parte integrante del mismo; los pagos se harán de forma mensual para el rubro de la operación de servicios administrados y en tres pagos anuales para la adquisición de licenciamientos y suscripciones, una vez

entregados, instalados y configurados en su totalidad los productos objeto del presente contrato y se hayan recibido a satisfacción de "EL MUNICIPIO", de conformidad al citado Anexo; y serán a los 8-ocho días hábiles posteriores al ingreso de cada factura ante la Secretaría de Finanzas y Tesorería municipal y conforme a la forma establecida por dicha Secretaría.

SEXTA: SUPERVISIÓN Y VERIFICACIÓN. "EL MUNICIPIO" tiene el derecho de verificar y supervisar la información del suministro e instalación de "LA EMPRESA", a través del Director General de Tecnologías de la Secretaría de Administración, la cual deberá estar en los términos que señala el objeto y características del presente contrato, para que cumpla con la calidad, cualidades y cantidades establecidas en el mismo. El Director General de Tecnologías de la Secretaría de Administración, es el responsable de verificar el exacto cumplimiento de las obligaciones estipuladas en el presente contrato hasta su conclusión. En caso de que durante el proceso de supervisión se observe algún incumplimiento por parte de "LA EMPRESA" deberá la Dirección General de Tecnologías comunicarlo por escrito, a la Dirección de Adquisiciones para que se proceda conforme a lo establecido en el Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León.

SÉPTIMA: 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 "LA EMPRESA" 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 "LA EMPRESA" será responsable del pago de los daños y perjuicios que se originen.

OCTAVA: CESIÓN DE DERECHOS. "LA EMPRESA" no podrá ceder en forma parcial ni total los derechos y obligaciones que se deriven del presente contrato, a favor de cualquiera otra persona.

NOVENA: RELACIÓN LABORAL. El presente contrato no podrá interpretarse de manera alguna como constitutivo de cualquier tipo de asociación o vínculo de carácter laboral entre "EL MUNICIPIO" y "LA EMPRESA", así como tampoco entre "EL MUNICIPIO" y los trabajadores o empleados que "LA EMPRESA" 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 contrato al trabajador de que se trate, asumir y cumplir 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 liberarla 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 individuales o colectivos provocados por personal de la primera, respondiendo de los daños y perjuicios que resultasen. "LA EMPRESA", se obliga a responder por cualquier demanda o reclamación que se promueva en contra de "EL MUNICIPIO" por parte de sus empleados, así como a pagarle el 100% de todos y cada uno de los gastos que hubiese efectuado con motivo o como consecuencia de la demanda o reclamación derivado de este contrato, ello sin perjuicio de las obligaciones y demás estipulaciones señaladas en el presente instrumento jurídico.

DÉCIMA: GARANTÍA DE CUMPLIMIENTO. "LA EMPRESA" deberá garantizar el debido cumplimiento de las obligaciones que se deriven del presente contrato, mediante póliza de fianza emitida por una institución de fianzas debidamente constituida en los términos de la Ley Federal de Instituciones de Fianzas. Dicha póliza deberá ser presentada a más tardar dentro de los 10-diez días naturales siguientes a la formalización del presente contrato, salvo que la entrega de los servicios 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 de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León.

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

a) Que se otorga a favor de "EL MUNICIPIO".
b) Que la fianza se otorga para garantizar todas y cada una de las estipulaciones contenidas en el presente contrato.

DÉCIMA PRIMERA: EFECTIVIDAD DE LA GARANTÍA. "EL MUNICIPIO" podrá hacer efectiva la garantía de cumplimiento de contrato cuando "LA EMPRESA":

a) No cumpla con el suministro, conforme a lo establecido en el presente contrato.
b) Incumpla con cualquiera de las obligaciones establecidas en el presente contrato.

c) Se rescinda administrativamente el contrato, considerando la parte proporcional al monto de las obligaciones incumplidas.

DÉCIMA SEGUNDA: DEVOLUCIÓN DE LA GARANTÍA. "EL MUNICIPIO" dará a "LA EMPRESA" su autorización por escrito, para que éste pueda cancelar la póliza de fianza correspondiente a la garantía de cumplimiento del contrato, previa solicitud por escrito en el momento que demuestre plenamente haber cumplido con la totalidad de las obligaciones establecidas en el contrato.

DÉCIMA TERCERA: DEFECTOS Y VICIOS OCULTOS. "LA EMPRESA" se obliga a responder, de cualquier otra responsabilidad derivada del servicio, de la misma manera se compromete a solucionar cualquier problema que se presente, con la colaboración de "EL MUNICIPIO".

DÉCIMA CUARTA: PATENTES Y MARCAS. "LA EMPRESA" será responsable, en el caso de que al suministrar las licencias y el equipo se infrinjan patentes y/o marcas registradas por terceros, quedando "EL MUNICIPIO" liberado de toda responsabilidad de carácter civil, penal, fiscal o de cualquier otra índole.

DÉCIMA QUINTA: PENA CONVENCIONAL. La penalización a la que se hará acreedora "LA EMPRESA" por el retraso en la entrega de los bienes y/o servicios a "EL MUNICIPIO" será de conformidad a lo siguiente:

Incidencias de no cumplimiento con los niveles de servicio especificados	**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

Las penalidades serán deducidas de las facturas pendientes por pagar a "LA EMPRESA", independientemente de que "EL MUNICIPIO" 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 se hace referencia en líneas anteriores, 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.

DÉCIMA SEXTA: RESPONSABILIDAD. "LA EMPRESA" asumirá la responsabilidad total para el caso de que, al cumplir con el objeto del presente contrato infrinja disposiciones referentes a regulaciones, permisos, normas, leyes, derechos de autor y de registro de marcas, quedando obligada a liberar a "EL MUNICIPIO" de toda

responsabilidad de carácter civil, penal, mercantil, fiscal o de cualquier otra índole. Así mismo se obliga a pasar por todos los gastos legales y sacar en buen término de cualquier conflicto a "EL MUNICIPIO" cubriendo para tal efecto el 100%-cien por ciento de todos y cada uno de los gastos, pago de sanciones, condenas, etcétera, que hubiese efectuado con motivo o consecuencia de la demanda o reclamación que en su caso se le haga a "EL MUNICIPIO".

DÉCIMA SÉPTIMA: RESCISIÓN ADMINISTRATIVA. El presente contrato podrá rescindirse por "EL MUNICIPIO" cuando "LA EMPRESA" incumpla con algunas de las obligaciones previstas en el presente instrumento. La Dirección de Adquisiciones rescindirá administrativamente siguiendo los lineamientos establecidos en el Artículo 111 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León.

DÉCIMA OCTAVA: TERMINACIÓN ANTICIPADA. "EL MUNICIPIO" por conducto de la Dirección de Adquisiciones podrá dar por terminado anticipadamente el presente contrato, de acuerdo a lo establecido en el Artículo 114 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León.

DÉCIMA NOVENA: SUSPENSIÓN POR CONTINGENCIA. Para el caso de que se presentara alguna disposición oficial emitida por autoridad competente en el sentido de declarar cualquier tipo de suspensión que afecte el cumplimiento del objeto del presente contrato, ésta se acatará y se suspenderá, hasta en tanto no se declare la terminación correspondiente.

VIGÉSIMA: OBLIGACIONES PREVISTAS EN LAS BASES. "LA EMPRESA" además de cumplir con todo lo previsto en el presente contrato tendrá la obligación de respetar y acatar el contenido y especificaciones de las bases que dieron origen al presente instrumento, es decir, para lo no estipulado en este contrato se atenderá a lo señalado en las Bases y en las Actas respectivas del proceso de licitación. Por otro lado, cualquier situación que no haya sido prevista en las presentes bases y sus anexos, será resuelta por la Dirección de Adquisiciones escuchando la opinión de las autoridades competentes, con base a las atribuciones establecidas en las disposiciones aplicables.

VIGÉSIMA PRIMERA: 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 SEGUNDA: COMPETENCIA. Para todo lo relativo a la interpretación y cumplimiento de este contrato, "LAS PARTES" se someten expresamente a los Tribunales competentes del Estado de Nuevo León, para conocer de cualquier juicio o reclamación derivado del mismo, renunciando a cualquier competencia o fuero que pudiera corresponderle por razón de su domicilio presente o futuro.

"LAS PARTES" MANIFIESTAN QUE SE ENCUENTRAN DE ACUERDO CON EL CONTENIDO DEL PRESENTE INSTRUMENTO MEDIANTE SU LECTURA, QUE SU TEXTO CONTIENE LA EXPRESIÓN EXACTA DE SU LIBRE VOLUNTAD, POR LO QUE NO EXISTEN ERROR, DOLO, VIOLENCIA, MALA FE, LESIÓN, ENRIQUECIMIENTO ILÍCITO, NI CUALQUIER VICIO DE LA VOLUNTAD QUE LO PUDIERAN INVALIDAR, Y EN CONSECUENCIA LO FIRMAN POR TRIPLICADO, EN LA CIUDAD DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN, EL DÍA 22-VEINTIDÓS DE JULIO DE 2022-DOS MIL VEINTIDÓS.

"EL MUNICIPIO"

C. LAURA LETICIA LOZANO VILLALOBOS
EN EJERCICIO DE LAS FACULTADES DELEGADAS POR EL C. PRESIDENTE MUNICIPAL Y EL C. SECRETARIO DE R. AYUNTAMIENTO
Y EN SU CARÁCTER DE SECRETARIA DE ADMINISTRACIÓN

C. DANIEL OSCAR DARES DE LEÓN
DIRECTOR GENERAL DE TECNOLOGÍAS

"LA EMPRESA"
"VDV NETWORKS", S.A. DE C.V.

C. RENÉ FUENTES GARCÍA DE LEÓN
APODERADO GENERAL

LAS PRESENTES FIRMAS FORMAN PARTE DEL CONTRATO DE ADQUISICIÓN CELEBRADO ENTRE EL MUNICIPIO DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN Y LA SOCIEDAD DENOMINADA "VDV NETWORKS", S.A. DE C.V./DGAJ/GMR/CJLG/RCCH/GATZ.

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

ANEXO 1

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
Jorge Velazquez	consultorvdv39@vdvnetworks.com.mx	8181295205
Antonio Barcenas	consultorvdv21@vdvnetworks.com.mx	8181295205

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

Rene Fuentes García de León
Representante Legal

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, prevision 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	**1200**

	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	
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	1200

	malware en el ambiente y que señale los mecanismos de afectación basados en el marco de Mitre	
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** Que cuente con el control de dispositivos periféricos en los sistemas operativos Windows y Mac, de tal modo que les detecte así 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	**1200**
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** Que cuente con un sandbox que se pueda integrar a la seguridad en el endpoint como una capa de protección adicional para identifica amenazas de día cero	**1**
2.12	**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 físicos y los previsores de intrusos virtuales, que pueda interactuar para ofrecer información, tomarlo o responder a una amenaza con la consola de antimalware. Que de preferencia no pueda consumirla	**CANTIDAD**

	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 clustar y la continuidad de la operación es prioridad.	
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 código maliciosos. Asimismo que tenga la capacidad de identificar y contener ataques de alto volumen de tráfico distribuido (DDoS)	1
3.3	**Previsores de Intrusos virtuales**	8

	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	
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	1

	retener la información al menos 1 año o contar con un espacio de 3TB de información	
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 las capacidades de correlacionar los eventos de todos los módulos, así como de reportear toda la actividad	**2**
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	**1**

	establecer mecanismos automáticos para identificar cuando los sitios cambian y adaptar las políticas de protección	
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** 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	**25**

ATENTAMENTE

Ing. Rene Fuentes García de León
Representante Legal

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.
  - Para PCs:
    - Habilitación de 10 estaciones (laboratorio)
    - Habilitación de 20 estaciones (prueba)
    - Habilitación de 40 estaciones (piloto)
    - La habilitación masiva en grupo de los parches críticos de Microsoft, asegurando la continuidad operativa y la resolución de problemas sin afectar de manera masiva a la operación de las PCs del municipio
  - Para los servidores:
    - Habilitación de 1 servers (laboratorio)
    - Habilitación de 3 servers (prueba)
    - Habilitación de 6 servers (piloto)
    - La habilitación de 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

René Fuentes García de León
Representante Legal

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

René Fuentes García de León
Representante Legal

Anexo C. Ingenieros Especialistas.

San Pedro Garza García N.L, a 1 de junio de 2022

Municipio de San Pedro Garza García N.L.
Atención. - Ing. Carlos Romanos Salazar
Director de Adquisiciones
Presente. -

Me refiero al Concurso por Licitación Pública Nacional Presencial **N°SA-DA-CL-26/2022 "Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"** en la que mi representada, la empresa VDV Networks S.A. de C.V. participa a través de la presente propuesta.

Sobre el particular, y "Bajo Protesta de Decir Verdad" Confirmo que mi representada VDV Networks SA de CV de acuerdo con lo indicado en el Anexo C, cuenta con ingenieros especialistas en:

- Seguridad web basada en proxy
- La tecnología de previsión de fuga de información en el endpoint
- La tecnología de Cloud Access Security Broker
- La tecnología de Control de Acceso con el mínimo privilegio
- La tecnología de identificación de vulnerabilidades
- La seguridad en los servidores y las PCs
- El cifrado de discos duros y files & folders
- El parcheo en los servidores y las PCs
- Los equipos de previsión de intrusos de red de propósito específico
- Sandbox de endpoint y de previsores de intrusos de propósito específico
- Seguridad de las bases de datos
- SIEM
- Firewalls y el Sandbox de los mismos
- La bóveda de contraseñas
- Web Application Firewal

ATENTAMENTE

Ing. Rene Fuentes García de León
Representante Legal

Anexo C. Carta de Certificaciones

San Pedro Garza García N.L., a 1 de julio de 2022

Municipio de San Pedro Garza García N.L.
Atención. - Ing. Carlos Romanos Salazar
Director de Adquisiciones
Presente. -

Me refiero al Concurso por Licitación Pública Nacional Presencial **N°SA-DA-CL-26/2022 "Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"**, en la que mi representada, la empresa VDV Networks S.A. de C.V. participa a través de la presente propuesta.

Sobre el particular, y "Bajo Protesta de Decir Verdad", Anexo los certificados solicitados en el Anexo C.

- Solución Perimetral (Firewalls): Check Point Certified Security Expert R80
- Sistema de Prevención de Intrusos: Virtual Network Security Platform Essentials y Network Security Platform
- Web Application Firewall: AppWall Certification (RCAScS)

Cabe aclarar lo siguiente:

- Radware es el OEM (Original Equipment Manufacturer) de Check Point para la tecnología WAF
- Trellix es la fusión de McAfee y FireEye quien es el fabricante de la tecnología de Previsión de Intrusos cotizada por mi representada en la presente licitación. Se anexa carta del fabricante describiendo la fusión.

ATENTAMENTE

Ing. Rene Fuentes García de León
Representante Legal

049

Trellix

Ciudad de México a 20 de junio de 2022.

MUNICIPIO DE SAN PEDRO GARZA GARCIA
P r e s e n t e-

Re. Carta Anuncio Trellix STG.

Le informamos que de acuerdo con información publicada el miércoles 19 de enero de 2022, **Symphony Technology Group (STG)** anunció el lanzamiento de **Trellix.**

Trellix surge de la fusión previamente anunciada de **McAfee Enterprise** y **FireEye** en octubre de 2021. Musarubra US LLC es el propietario de la marca Trellix.

Para mayores detalles de esta información puede ser revisado en el link público:

https://www.trellix.com/en-us/about/newsroom/news/news-detail.html?news_id=3e247ede-b638-4bb4-bd13-00b94a623e01

Para información sobre Trellix visite el sitio público:

https://www.trellix.com/es-es/index.html

Atentamente,

DocuSigned by:
miriam serrato
DCE07A866A86421...

Miriam Serrato
Channel Account Manager

Check Point Software Technologies Ltd.

This Certifies that

Jorge Velazquez ID#: CP0000115857

has demonstrated the knowledge to be a

Check Point Certified Security Expert R80

This 4 day of May , 2022

Expiration Date: May 4, 2024

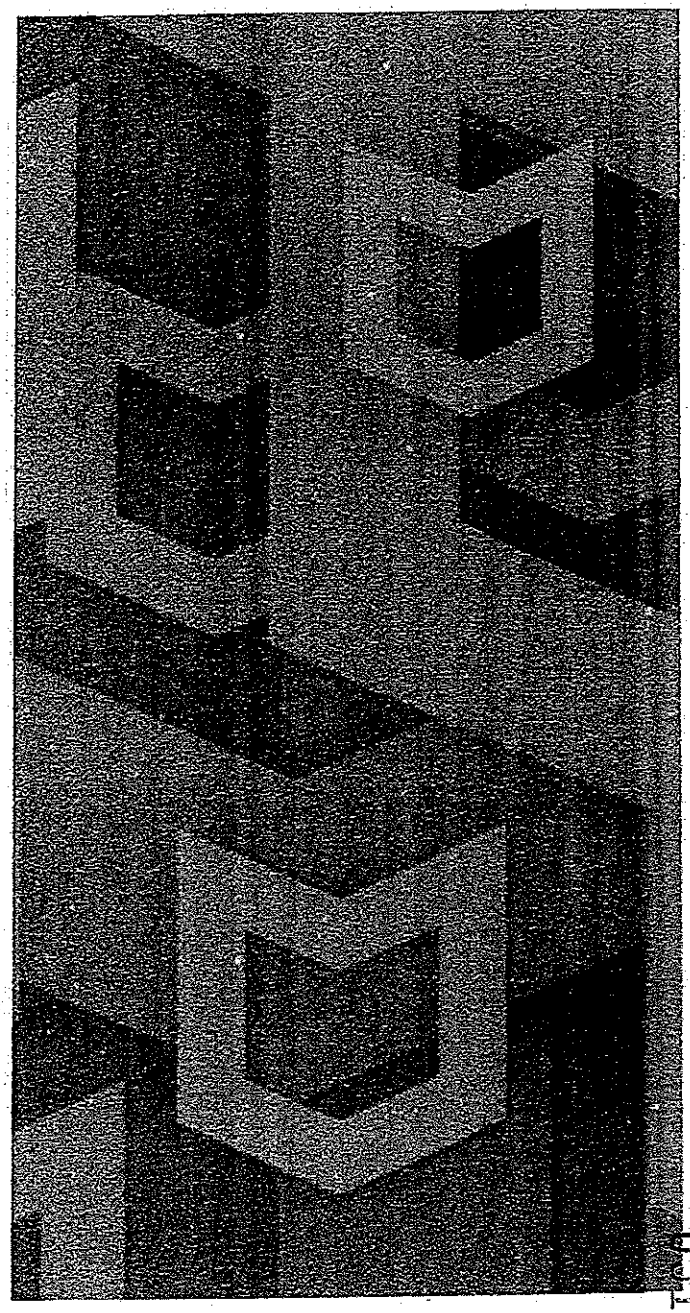
Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Shay Solomon - Head of Education Services

Check Point Certified
Check Point
Check Point Certified

McAfee
Together is power.

CERTIFICATE
OF COMPLETION



Edgar Antonio Beltrán Bocanegra

has successfully completed

Virtual Network Security Platform Essentials (Technical)

on *20-APR-2022*

Signature _____

Sr. Vice President, Customer Success Group

McAfee
together is power.

CERTIFICATE
OF COMPLETION

Roberto Medina

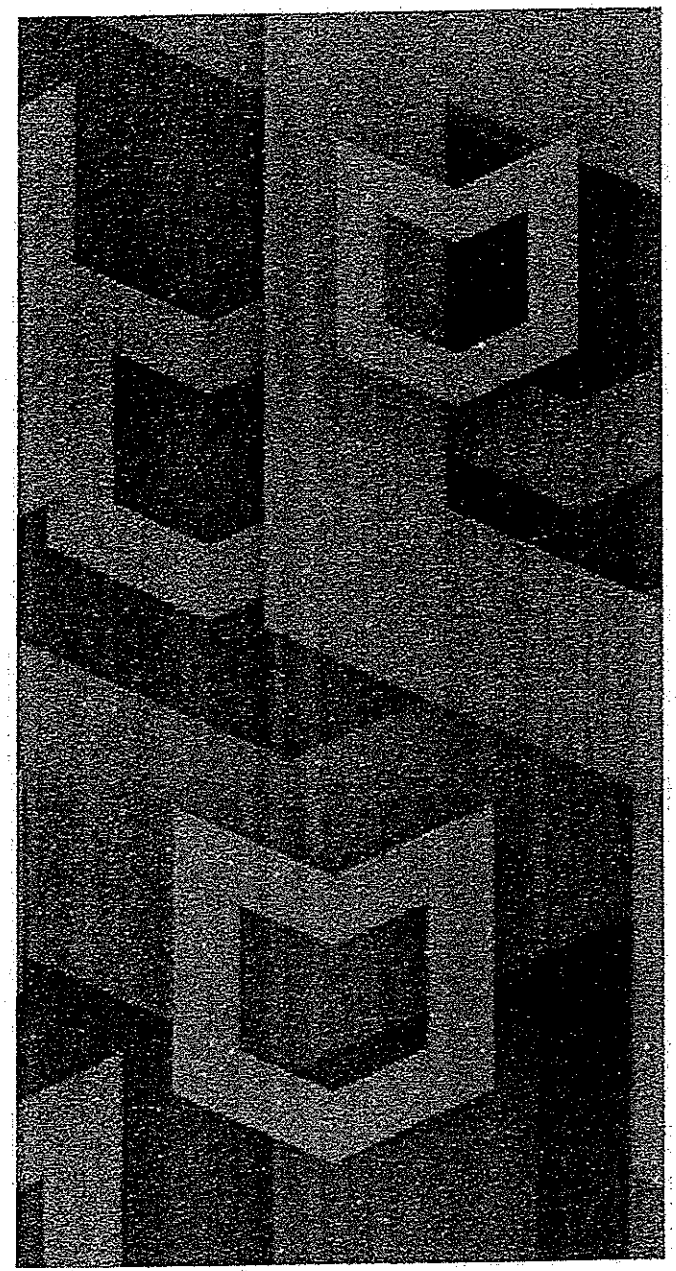
has successfully completed

Network Security Platform 10.1 Essentials Course

on *25-APR-2022*

Signature

Sr. Vice President, Customer Success Group



053

TRAINING CERTIFICATION

RADWARE HEREBY RECOGNIZES

yaritza arauza

RADWARE

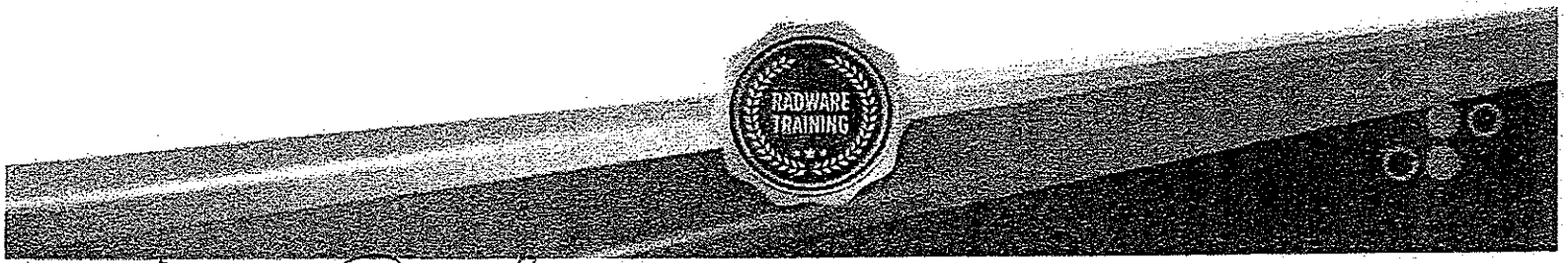
HAS COMPLETED ALL REQUIREMENTS AND IS HEREBY AWARDED

AppWall Certification (RCAScS)

This Certificate,issued on:May 20, 2022 and Bears the Signature of

AMIR PELES
VP, TECHNICAL SERVICES

radware



053

Anexo C. Carta Explicación ISO

San Pedro Garza García N.L a 1 de julio de 2022

Municipio de San Pedro Garza García N.L.
Atención. - Ing. Carlos Romanos Salazar
Director de Adquisiciones
Presente. -

Me refiero al Concurso por Licitación Pública Nacional Presencial **N° SA-DA-CL-26/2022 "Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"** en la que mi representada, la empresa VDV Networks S.A de C.V. participa a través de la presente propuesta.

Sobre el particular, y "Bajo protesta de decir verdad", Se anexa la carta generada por "Normalización y Certificación NYCE, SC", entidad certificadora acreditada en Mexico por la EMA. (Entidad Mexicana de Acreditación) donde señala que mi representada VDV Networks SA de CV se encuentra en proceso de certificación de la Norma ISO/IEC 27001:2013 solicitada en el Anexo E

ATENTAMENTE

Ing. Rene Fuentes García de León
Representante Legal

NYCE
A QIMA COMPANY

055

www.nyce.org.mx

Ciudad de México 30 de junio de 2022.

A QUIEN CORRESPONDA,

Estimados señores:

Por este medio, me es grato dirigirme a usted con el propósito de informarle respecto a las actividades que lleva a cabo Normalización y Certificación NYCE, S.C., organismo de certificación de Sistemas de Gestión que fue constituido legalmente el 22 febrero de 2011 y que pertenece a "Grupo NYCE", contamos con más de 25 años de experiencia y liderazgo en la normalización y evaluación de la conformidad, con presencia nacional e internacional.

Normalización y Certificación NYCE, S.C., hace constar que la organización:

VDV NETWORKS, S .A. DE C.V., ubicada en Av. Real de Cumbres 442. Col. Real de Cumbres Monterrey, N.L. CP 64346, N.L., México, se encuentra en proceso de certificación del Sistema de Gestión de Esquema bajo la norma: NMX-I-27001-NYCE-2015 / ISO/IEC 27001:2013, con número de expediente interno 202206SGSI245

Con el siguiente alcance:
Por definir

La presente tiene una vigencia de 30-días días y se extiende a petición de VDV NETWORKS, S.A. DE C.V. al 30 de julio de 2022.

Sin otro particular, le envió un saludo muy cordial.

Atentamente,

Ing. Martha Victoria CRUZ CORTÉS
Gerente Corporativo de Operaciones de Sistemas de Gestión

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 Broker	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 Validación del correcto funcionamient o	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 recomendacione s 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 requerimient o 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 funcionamient o	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 recomendacione s consolidadas al mes
Prevensión ante campañas de malware	Si 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 antiransomwar e y parcheo virtual	De la consola de administración De los repositorios distribuidos de productos y vacunas	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimient o del municipio	Validación del correcto funcionamient o Cobertura de producto y patrones (antimalware parcheo virtual)	La configuración La base de datos para la consola en sitio	Para revisión de eventos, incidentes, fallas	Coberturas Incidentes de Seguridad y/o Falla	El reporte debe incluir: - Cobertura de producto

			Identificación, resolución y reporteo de incidentes			Correcciones realizadas y/o recomendaciones	- 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 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
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 requerimient	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

		o del municipio					- 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	Si 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 Investigaciones de los eventos de seguridad	No Aplica	Para revisión de eventos, incidentes, fallas	Eventos de seguridad extraños o anómalos De las investigaciones realizadas	De eventos anómalos consolidades De acciones tomadas Las recomendaciones Las recomendaciones realizadas durante el mes
Cifrado para las computadoras	Si 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	Si 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	De la herramienta	Avance en la cobertura de	La configuración	Para revisión de eventos,	No Aplica	El reporte debe incluir:

	Salud de la herramienta de parcheo	de parcheo debe realizarse una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio	los parches de acuerdo a la métrica	Los eventos	incidentes, fallas		- Cobertura de parches vs las métrica - Eventos de falla - Acciones realizadas - 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 (Correlationador de eventos)	Sí de correcto funcionamiento	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimient	Alertamiento Modificación, adición a los dashboards sin límite de eventos Modificación adición a las Reglas de correlación sin	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

		o del municipio	límite de eventos				
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 infraestructura	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" con los responsables del equipo interno del municipio para solventarlas	No Aplica	Para la corrección de vulnerabilidades	No Aplica Sobre demanda para servidores y/o equipos activos a punto de ser liberados y/o mensual	De vulnerabilidades de los activos 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

René Fuentes García de León
Representante legal

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"

Partida	Conceptos	Precio Unitario	Cantidad	Importe
1	Operación de Servicios Administrados	$157,088.00	36	$5,655,168.00
2	Suscripciones, licencias, instalación y soportes	$4,754,490.76	3	$14,263,472.28
			Subtotal	$19,918,640.28
			IVA	$3,186,982.45
			Total	$23,105,622.73

ATENTAMENTE

Ing. Rene Fuentes García de León
Representante Legal