San Pedro Garza García
GOBIERNO MUNICIPAL

SA/DGAJ/CTODPRIV-ADQUISICIÓN/749/ADMÓN-18-21

DIRECCION DE ASUNTOS JURIDICOS
RECIBIDO
03 SEP 2020
SAN PEDRO GARZA GARCIA, N.L

1314

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 POR LOS **CC. MAURICIO SADA SANTOS**, SECRETARIO GENERAL, Y **LAURA LETICIA LOZANO VILLALOBOS**, SECRETARIA DE ADMINISTRACIÓN, AMBOS EN EJERCICIO DE LAS FACULTADES DELEGADAS POR EL C. PRESIDENTE MUNICIPAL Y EL C. SECRETARIO DEL REPUBLICANO AYUNTAMIENTO, Y POR OTRA PARTE, LA EMPRESA 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 los artículos 115, fracción II de la Constitución Política de los Estados Unidos Mexicanos, 120 de la Constitución Política del Estado de Nuevo León y 2 de la Ley de Gobierno Municipal del Estado de Nuevo León, tiene personalidad jurídica y capacidad legal para contratar y obligarse.

b) Que en la Primera Sesión Ordinaria del Republicano Ayuntamiento de San Pedro Garza García, Nuevo León, celebrada en fecha 10-diez de diciembre de 2019-dos mil diecinueve, se aprobó el Acuerdo Delegatorio del C. Presidente Municipal y el C. Secretario del Republicano Ayuntamiento, mediante el cual delegan en el Titular de la Secretaría General la atribución de suscribir aquellos documentos que contengan contratos y/o convenios para el despacho de los asuntos administrativos y la atención de los servicios públicos municipales, en términos de lo dispuesto en el resolutivo Sexto del Acuerdo; así como 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

RECIBIDO 13:17 03 SEP 2020
SECRETARÍA DE FINANZAS Y TESORERÍA MUNICIPAL SAN PEDRO GARZA GARCÍA, N.L.

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Aldama No. 403 Norte, esquina con Libertad, Centro
San Pedro Garza García, Nuevo León,
C.P. 66200 Tels: (81) 8400-4509 / 8400-4526
www.sanpedro.gob.mx

términos del resolutivo Primero del Acuerdo; lo que es el caso en el presente Contrato. Dicho Acuerdo fue debidamente publicado en el Periódico Oficial del Estado de fecha 25-veinticinco de diciembre de 2019-dos mil diecinueve.

c) El **C. MAURICIO SADA SANTOS**, 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 Republicano Ayuntamiento, así como en su carácter de Secretario General, por lo que está facultado para suscribir el presente instrumento jurídico, pues dentro de sus atribuciones se encuentra atender todas las solicitudes que le instruya el Presidente Municipal y el Republicano Ayuntamiento, así como ejercer todas aquellas facultades que se le asignen por Reglamento y Acuerdos del Republicano Ayuntamiento. 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 17, 18, 24 fracción III y 30 letra a, fracciones XIV y XV del Reglamento Orgánico de la Administración Pública Municipal de San Pedro Garza García, Nuevo León.

d) 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 y resguardo municipal, así como la de establecer medidas para salvaguardar la información electrónica en poder de la administración pública municipal centralizada y descentralizada y promover la actualización de los equipos, programas, sistemas y redes de voz, datos e imágenes, así como en materia de telefonía fija y acceso a Internet. Lo anterior de conformidad con los artículos 86, 88, 89 y 91 de la Ley de Gobierno Municipal del Estado de Nuevo León vigente, y con los numerales 17,18, 25, fracción I, 44 letra a,

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Aldama No. 403 Norte, esquina con Libertad, Centro
San Pedro Garza García, Nuevo León,
C.P. 66200 Tels: (81) 8400-4509 / 8400-4526
www.sanpedro.gob.mx

fracciones III y VI, y letra e, fracciones IV y XIII 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, 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) Por tal motivo en fecha 10-diez de junio de 2020-dos mil veinte, 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 fracción 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 Servicio del Estado de Nuevo León y artículo 36, fracciones VII, XII, XVIII, XXI y XXX, 123, fracción I del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios del Municipio de San Pedro Garza García, Nuevo León, lanzó la Convocatoria, en la que se contiene el Concurso por Licitación Pública Nacional Presencial N° SA-DA-CL-32/2020, 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.

h) En fecha 17-diecisiete de junio de 2020-dos mil veinte, se llevó a cabo 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:

- VDV Networks, S.A. de C.V. ("LA EMPRESA").
- Teléfonos de México, S.A.B. de C.V.

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Aldama No. 403 Norte, esquina con Libertad, Centro
San Pedro Garza García, Nuevo León,
C.P. 66200 Tels: (81) 8400-4509 / 8400-4526
www.sanpedro.gob.mx

En la que se presentaron diversas preguntas, las cuales fueron aclaradas, y que constan en Acta levantada en esta misma fecha, de conformidad a lo establecido en el artículo 34, párrafo 7° de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicio del Estado de Nuevo León.

i) En el Acto de Presentación de Propuesta Técnica y Económica y Apertura de Propuesta Técnica, de fecha 25-veinticino de junio de 2020-dos mil veinte, se contó únicamente con la participación de "LA EMPRESA", la cual presentó su propuesta técnica, la cual fue revisada de manera cuantitativa, cumpliendo con los requisitos y especificaciones establecidas en las Bases, específicamente en el punto 15, inciso a).

j) En el Acto de Fallo Técnico y Apertura de Propuesta Económica, de fecha 30-treinta de junio de 2020-dos mil veinte, se hizo constar que "LA EMPRESA" cumplió en la revisión cualitativa y cuantitativa de su propuesta técnica, en términos del punto 15, inciso a) de las Bases, por lo que se procedió a hacer la apertura de su propuesta económica respectiva:

"LA EMPRESA", presentó su propuesta económica la cual fue revisada de manera cuantitativa, cumpliendo con los requisitos y especificaciones establecidas en las Bases, específicamente en el punto 15, inciso b), siendo el importe para el Anexo No. 2 "Cotización" su oferta por la cantidad de $6'813,866.80 (Seis millones ochocientos trece mil ochocientos sesenta y seis pesos 80/100 M.N.) I.V.A. incluido, entregando además una fianza en garantía por la oferta económica presentada.

k) Una vez agotado el procedimiento establecido, quedó asentado en el Acto de Fallo, de fecha 6-seis de julio de 2020-dos mil veinte, previa opinión favorable del Comité de Adquisiciones, contenida en el Acta de la Octava Sesión Extraordinaria, de esta misma fecha, como concursante seleccionado a "LA EMPRESA" para la "Adquisición de licencias y suscripciones de seguridad informática, soporte de infraestructura instalada y servicios administrados", por un monto de $6'813,866.80 (Seis millones ochocientos trece mil ochocientos sesenta y seis pesos 80/100 M.N.) I.V.A. incluido, con una vigencia a partir del 7-siete de julio de 2020-dos mil veinte, al 6-seis de julio de 2021-dos mil veintiuno. La anterior adjudicación se realizó en virtud de que su propuesta cumple cabalmente con todos y cada uno de los requisitos establecidos en las Bases que dieron origen al presente contrato, así mismo por presentar excelentes condiciones de precio, ya que éste está dentro del presupuesto

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Aldama No. 403 Norte, esquina con Libertad, Centro
San Pedro Garza García, Nuevo León,
C.P. 66200 Tels: (81) 8400-4509 / 8400-4526
www.sanpedro.gob.mx

autorizado, presentando además buenas condiciones de calidad, oportunidad y demás circunstancias pertinentes.

l) Que para los efectos de este contrato señala como domicilio para oír y recibir notificaciones el ubicado en la calle Aldama número 403 norte, en el centro de San Pedro Garza García, Nuevo León.

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 Distrito Federal, e inscrita en el Registro Público de Comercio del Distrito Federal, bajo el Folio Mercantil número 251458, de fecha 18-dieciocho de junio de 1999-mil novecientos noventa y nueve. Sociedad que se encuentra inscrita ante el Registro Federal de Contribuyentes con la Clave VNE990609282.

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 cuenta con la infraestructura, el personal, las herramientas, capacidad y experiencia necesaria para proporcionar a "EL MUNICIPIO" el servicio requerido, 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 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, Checkpoint, Riverbed, Autonomic Software y Qualys.

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Aldama No. 403 Norte, esquina con Libertad, Centro
San Pedro Garza García, Nuevo León,
C.P. 66200 Tels: (81) 8400-4509 / 8400-4526
www.sanpedro.gob.mx

f) 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, 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 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 Anexos 1, A, B1 y B2 del presente contrato, los cuales se adjuntan 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 30-treinta días hábiles contados a partir del Fallo de Adjudicación, y el tiempo de operación de cada una de las Licencias será por 1-un año y al menos al día 6-seis de julio de 2021-dos mil veintiuno, 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 de Tecnologías, ubicada en Corregidora número 507, Palacio de Justicia Segundo Piso, Centro de San Pedro Garza García.

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.

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Aldama No. 403 Norte, esquina con Libertad, Centro
San Pedro Garza García, Nuevo León,
C.P. 66200 Tels: (81) 8400-4509 / 8400-4526
www.sanpedro.gob.mx

Entregables en caso de aplicar:

- 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 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 será a partir del día 7-siete de julio de 2020-dos mil veinte, para concluir el día 6-seis de julio de 2021-dos mil veintiuno.

La operatividad de las licencias será por un año 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 $6'813,866.80 (Seis millones ochocientos trece mil ochocientos sesenta y seis pesos 80/100 M.N.) I.V.A. incluido, comprometiéndose "LA EMPRESA" a no realizar ninguna modificación a

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Aldama No. 403 Norte, esquina con Libertad, Centro
San Pedro Garza García, Nuevo León,
C.P. 66200 Tels: (81) 8400-4509 / 8400-4526
www.sanpedro.gob.mx

dicha cantidad durante la vigencia del presente contrato, ya que el mencionado precio es fijo y no se reconocerá incremento alguno.

El pago correspondiente a las Licencias y Suscripciones de seguridad informática y soporte de infraestructura instalada será de $4'650,023.10 (Cuatro millones seiscientos cincuenta mil veintitrés pesos 10/100 M.N.) antes de impuestos, y se realizará una vez entregados, instalados y configurados en su totalidad los productos objeto del presente contrato y se hayan recibido a satisfacción de "EL MUNICIPIO", en una sola exhibición y a los 8-ocho días posteriores al ingreso de la factura ante la Secretaría de Finanzas y Tesorería municipal y conforme a la forma establecida por dicha Secretaría.

El pago correspondiente a los Servicios Administrados será de $1'224,000.00 (Un millón doscientos veinticuatro mil pesos 00/100 M.N.) antes de impuestos, y se realizará en pagos mensuales.

SEXTA.- SUPERVISIÓN Y REVISIÓN.- "EL MUNICIPIO" tendrá el derecho, en todo tiempo, de ejercer medidas de supervisión, por conducto del Director de Tecnologías de la Secretaría de Administración, o bien, de la persona designada por él mismo, a fin de comprobar la calidad de los bienes, así mismo "EL MUNICIPIO" se reserva el derecho de verificar toda la información proporcionada por "LA EMPRESA" en cualquier momento de la vigencia de este instrumento, sin que esto implique responsabilidad alguna para la misma, la falta de cumplimiento del servicio o las condiciones ofertadas será motivo de rescisión así como de la aplicación de las sanciones correspondientes.

SÉPTIMA.- IMPUESTOS Y DERECHOS.- Los impuestos y derechos federales o locales que se causen con motivo del objeto de este contrato, serán erogados por "LA EMPRESA", "EL MUNICIPIO" sólo cubrirá el Impuesto al Valor Agregado de acuerdo a lo establecido en las disposiciones legales vigentes en la materia.

OCTAVA.- GARANTÍA DE CUMPLIMIENTO.- "LA EMPRESA" deberá garantizar el debido cumplimiento de las obligaciones que se deriven del 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 contrato, salvo que la entrega de los bienes y 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. La póliza de fianza deberá contener, además de lo señalado en las cláusulas que la Ley Federal de Instituciones de Fianzas; las siguientes declaraciones:

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Aldama No. 403 Norte, esquina con Libertad, Centro
San Pedro Garza García, Nuevo León,
C.P. 66200 Tels: (81) 8400-4509 / 8400-4526
www.sanpedro.gob.mx

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

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

NOVENA.- EFECTIVIDAD DE LA GARANTÍA DE CUMPLIMIENTO.- Se hará efectiva la Garantía de Cumplimiento de contrato en los siguientes casos:

a) Cuando "LA EMPRESA" no cumpla con el suministro del servicio objeto del presente contrato.

b) Cuando "LA EMPRESA" no cumpla con cualquiera de las obligaciones establecidas en el presente contrato.

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

DÉCIMA.- CANCELACIÓN DE LA GARANTÍA DE CUMPLIMIENTO.- Para cancelar la fianza será requisito indispensable la voluntad expresa y por escrito de "EL MUNICIPIO", misma que se manifiesta únicamente cuando "LA EMPRESA" haya cumplido con todas y cada una de las obligaciones señaladas en el presente contrato.

DÉCIMA PRIMERA.- GARANTÍA POR DEFECTOS DE FABRICACIÓN Y VICIOS OCULTOS.- "LA EMPRESA" manifiesta que los bienes y servicios ofrecidos cuentan con las garantías de acuerdo a lo siguiente: "LA EMPRESA" se obliga a responder, de los defectos, vicios ocultos o cualquier otra responsabilidad derivada del suministro e instalación de los bienes y servicios; de la misma manera se compromete a solucionar cualquier problema que se presente, con la colaboración de "EL MUNICIPIO".

DÉCIMA SEGUNDA.- PENA CONVENCIONAL.- La penalización a la que se hará acreedora "LA EMPRESA" por el retraso en la entrega de productos 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	10% de penalidad del pago mensual
5-9 Incidencias	20% de penalidad del pago mensual
10 o más Incidencias	50% de penalidad del pago mensual

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Aldama No. 403 Norte, esquina con Libertad, Centro
San Pedro Garza García, Nuevo León,
C.P. 66200 Tels: (81) 8400-4509 / 8400-4526
www.sanpedro.gob.mx

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 TERCERA.- 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 CUARTA.- 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 QUINTA.- RESPONSABILIDAD.- "LA EMPRESA" asumirá la responsabilidad total para el caso de que, al proporcionar el servicio a "EL MUNICIPIO", infrinja disposiciones referentes a regulaciones, permisos, normas o leyes, quedando obligado a liberar a "EL MUNICIPIO" de toda responsabilidad de carácter civil, penal, mercantil, fiscal o de cualquier otra índole.

DÉCIMA SEXTA.- EQUIPO Y PERSONAL.- El equipo y personal que se requiere para cumplir con el objeto serán proporcionados por "LA EMPRESA".

DÉCIMA SÉPTIMA.- 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 OCTAVA.- CESIÓN DE DERECHOS.- Queda expresamente prohibido a "LA EMPRESA" ceder total o parcialmente a terceros, los derechos y obligaciones adquiridos por medio del presente contrato.

DÉCIMA NOVENA.- RESPONSABILIDAD 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",

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Aldama No. 403 Norte, esquina con Libertad, Centro
San Pedro Garza García, Nuevo León,
C.P. 66200 Tels: (81) 8400-4509 / 8400-4526
www.sanpedro.gob.mx

EN LA CIUDAD DE SAN PEDRO GARZA GARCÍA, NUEVO LEÓN, EL DÍA 7-SIETE DE JULIO DE 2020-DOS MIL VEINTE.

"EL MUNICIPIO"

C. MAURICIO SADA SANTOS
EN EJERCICIO DE LAS FACULTADES DELEGADAS POR LOS CC. PRESIDENTE MUNICIPAL Y SECRETARIO DEL REPUBLICANO AYUNTAMIENTO Y EN SU CARÁCTER DE SECRETARIO GENERAL

LIC. LAURA LETICIA LOZANO VILLALOBOS
EN EJERCICIO DE LAS FACULTADES DELEGADAS POR LOS CC. PRESIDENTE MUNICIPAL Y SECRETARIO DEL REPUBLICANO AYUNTAMIENTO Y EN SU CARÁCTER DE SECRETARIA DE ADMINISTRACIÓN

"EL PRESTADOR DE SERVICIOS"
"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/RCCH/GATZ/Ref. Contrato de Adquisición, "VDV NETWORKS", S.A. DE C.V. 2020.

DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Aldama No. 403 Norte, esquina con Libertad, Centro
San Pedro Garza García, Nuevo León,
C.P. 66200 Tels: (81) 8400-4509 / 8400-4526
www.sanpedro.gob.mx

Concurso por Licitación Pública Nacional Presencial No. SA-DA-CL-32/2020
"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

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

ALCANCE:
Mantener las licencias y suscripciones vigentes. Proveer los servicios administrados de seguridad informática 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 que proveen estos equipos 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.

LICENCIAS PARA EQUIPOS ACTUALES:

VER ANEXO A

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)

SERVICIOS ADMINISTRADOS:

VER ANEXO B1 Y B2

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.

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.

La Empresa debe ser distribuidor de los siguientes fabricantes y demostrarlo con una carta para efectos del presente proceso de adquisición:

- McAfee
- Forcepoint
- Checkpoint
- Riverbed
- Autonomic Software
- Qualys

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

CRONOGRAMA DE ACTIVIDADES Y FECHAS DE ENTREGA: El período del contrato es del 07 de julio del 2020 al 06 de julio del 2021.

ENTREGABLES:

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

- *Expectativa de servicio:*

- Deberá tener un compromiso de atención inmediato para situaciones de urgencia (30 Minutos)

- El tiempo para situaciones no urgentes será de 2 horas. Estas situaciones se llevarían registradas por medio de un sistema de tickets.

- La resolución del problema no deberá pasar de 4 horas desde que se reportó el evento, siempre y cuando este no sea una falla propia del software o equipo por defecto de fabricación y/o compatibilidad con las versiones nuevas de sistemas operativos, aplicaciones, bases de datos, hipervisores.

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:

- Habilitación de acuerdo a lo señalado en el anexo B1
- 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):**

Contacto	Correo	Teléfono
Ingeniero de soporte Jose Carlos Vega	consultorvdv31@vdvnetworks.com.mx	81295205
Ingeniero de escalación Antonio Barcenas	consultorvdv21@vdvnetworks.com.mx	8120108891

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

Se entiende que la resolución de una falla resultante de la fabricación del software o compatibilidad del mismo depende del fabricante, así como el tiempo para solventarla, sin embargo, se espera, que en dicho caso el proveedor le dé seguimiento con el fabricante y entregue reportes regulares del avance de la solución, hasta que quede resuelta.

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-32/2020
"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

Anexo A. Licencias y suscripciones de seguridad informática soporte de infraestructura instalada.

A continuación, se describen las herramientas actuales con las que cuenta el municipio.

El servicio otorgado deberá incluir la TRANSFERENCIA DE CONOCIMIENTO necesaria para todas y cada una de las herramientas en su instalación, administración y operación

Como parte de los servicios integrados deberá incluir al menos 1 ingeniero en sitio por parte del proveedor UN MINIMO DE 20 HORAS por semana durante el periodo del contrato.

TIEMPO DE ENTREGA 30 DIAS.

REQUERIMIENTOS DE PERSONAL
• El proveedor deberá proporcionar personal en sitio hasta que el evento quede resuelto en su totalidad de manera satisfactoria
REQUERIMIENTOS CARTAS DE FABRICANTES • Carta del fabricante Forcepoint señalando que el participante es distribuidor autorizado de la marca • Carta del fabricante Riverbed señalando que el participante es distribuidor autorizado • Carta del fabricante Checkpoint señalando que el participante es distribuidor autorizado • Carta del fabricante McAfee señalando que el participante es distribuidor autorizado • Carta del fabricante Qualys señalando que el participante es distribuidor autorizado • Carta del fabricante Autonomic señalando que el participante es distribuidor autorizado

Cantidad		Descripción
A) Filtrado de Contenido, Monitoreo de Infraestructura y Captura y análisis de Tráfico		
Licencias en modo de suscripción con vigencia de 1 año al menos al 6 de julio de 2021 para proveer seguridad en la navegación web a través de un proxy con las siguientes		

características (Se deberá incluir el Equipo (Appliance) sobre el cual se instalen las suscripciones para la provisión de la seguridad de navegación web, que soporte hasta 1200 usuarios concurrente): fabricante FORCEPOINT TRITON AP-WEB		
Licencias en modo de suscripción con vigencia de 1 año al menos al 6 de julio de 2021 para prever la Fuga de Información a través de un agente que pueda instalarse en computadoras personales con sistema operativo Windows, Macintosh o Linux, con la capacidad, en el mismo agente de cifrar la información. La solución debe poder ser administrada por la misma consola de administración que administra la seguridad de navegación web FACRICANTE FORCEPOINT LICENCIA TRITON AP-ENDPOINT DLP		
Mantenimiento de las licencias en suscripción de seguridad para la navegación web y las licencias en suscripción para la previsión de fuga de información por parte del fabricante con vigencia de 1 año al menos al 6 de julio de 2021, que permitan acceder a nuevas versiones, parches para mejorar las fallas, parches para eliminar las vulnerabilidades, que permita acceder al portal acceso a manuales, bases de datos de conocimientos, y poder registrar requerimientos de soporte de alta criticidad directo con el fabricante FABICANTE FORCEPOINT Premium Support AP-WEB Y AP-END POINT DLP		
1200	WSPA-X-CP12-R	TRITON AP-WEB (Forcepoint TRITON AP-Web)
1200	DLPEIP-0-CP12-PR	TRITON AP-ENDPOINT DLP (Forcepoint DLP Endpoint (IP Protection)
1	ESESPT-0-CP12-P-R	Premium Support AP-WEB Y AP-END POINT DLP (Essential Support forForcepoint TRITON AP-WEB y Essential Support forForcepoint DLP Endpoint (IPProtection)
Software de captura y análisis experto de paquetes de tráfico red que tenga las siguientes capacidades con vigencia de 1 año al menos al 6 de julio de 2021:		
1	MNT-CSP-LIC-USR-1	Support SteelCentral Packet Analyzer 1 User
B) Seguridad en las PCs, Servidores, la red interna y resguardo y registro de correlación de eventos		
licencias en modo suscripción para identificar vulnerabilidades con vigencia de 1 año al menos al 6 de julio de 2021, que tengan las siguientes capacidades:		
1	Q-XL-VS	Annual subscription for Qualys VM and 1 virtual scanner appliance, 256 Internal Ips fabricante qualys
Licencias para seguridad de los servidores WINDOWS con vigencia de 1 año al menos al 6 de julio de 2021, con las siguientes capacidades:		
50	CWAYFM-AB	McAfee Cloud Workload Security - Advanced McAfee Dynamic Application Containment y Real protect para 50 Servers en modo protección (con bloqueo y excepciones McAfee Change Control en 50 servers
Licencias de firewall/previsor de intrusos para las bases de datos con vigencia de 1 año al menos al 6 de julio de 2021,		
6	DCDYCM-AA	MFE Datacenter Security Suite f/Database1Yr Gold Support

Licencias en modo Suscripción de protección de seguridad en el endpoint con vigencia de 1 año al menos al 6 de julio de 2021, con al menos los siguientes controles: Antivirus basado en firmas y antivirus de nueva generación basado en inteligencia artificial para PCs y Servidores, Control de dispositivos periféricos, Previsor de intrusos de host, Firewall personal, Para control web, Control de aplicaciones en las PCs, Endpoint Detection and Response (EDR) y protección para los dispositivos móviles (Teléfonos inteligentes y tabletas) con al menos las siguientes capacidades por cada producto:		
1200	MV6ECE-AA	MVISION Protect Plus EDR for Endpoint
Cifrado de disco duro de fólders y archivos con vigencia de 1 año al menos al 6 de julio de 2021.		
1200	CDBYFM-AA	McAfee Complete Data Protection
Sistema de previciosn de intrusos El mantenimiento del equipo por 1 año que permita acceder a nuevas versiones de software a resolución de fixes y vulnerabilidades a la base de datos de conocimiento y a poner tickets de alta criticidad con el fabricate con vigencia de 1 año		
Previsor de intrusos de red de propósito específico que soporte un throughput de 300 Mbps y 80,000 conexiones concurrentes CON 8 INTEERFACES 100Mbps/1Gibabit por segundo "FAIL OPEN" , y que cuente con las siguientes características:		
1	IYVM15KADM	MFE Network Security M 1450 Sensor Appliance 1yr Gold Software Support & Advance RMA (same/next business day ship) Hardware Support - con vigencia de 1 año al menos al 6 de julio de 2021.
Previsor de intrusos de red de propósito específico tenga 8 INTEERFACES 100Mbps/1Gibabit por segundo "FAIL OPEN" y 12 INTERFACES SFP 100Mbps/1Gibabit por segundo, soporte un throughput de 1 Gbps y 750,000 conexiones concurrentes		
1	IYVM28KADMA	MFE Network Security M-2850 Sensor Appliance 1yr Gold Software Support & Advance RMA (same/next business day ship) Hardware Support - con vigencia de 1 año al menos al 6 de julio de 2021.
Previsor de intrusos de red para ambientes VMWare que pueda ser instalado en hasta 7 Hosts donde el throughput en total sea a lo mas de 500 Mbps con vigencia de 1 año al menos al 6 de julio de 2021.		
1	VC2YCM-AB	MFE vNSP Cloud Medium (500Mbps) 1Yr GL
Consola de administración de los Previsores de Intrusos de red físicos y virtuales con un año de mantenimiento con vigencia de 1 año al menos al 6 de julio de 2021.		
1	NMGECE-AA	McAfee Network Security Manager Software Subscription Global Edition

SIEM (Correlacionador de eventos) que soporte hasta 1000 eventos por segundo y tenga espacio para guardar bitácoras de 3 TB de información con vigencia de 1 año al menos al 6 de julio de 2021.		
1	ETM4600ELMNBD	MFE Enterprise Security, Enterprise Log Manager and Event Receiver 4600 Combination 1yr Gold Software Support & Onsite Next Business Day Hardware Support
Licencias para el parcheo de parches Microsoft con vigencia de 1 año al menos al 6 de julio de 2021.		
1200		Autonomic Patch Manager 1 Year manteinance
Licencia Sandbox para antivirus y los previsores de intrusos de red con vigencia de 1 año al menos al 6 de julio de 2021.		
1	AT1ECE-AB	McAfee Virtual Advanced Threat Defense Appliance - ATD-VM1008
C) FIREWALLS		
La suscripción con vigencia de 1 año al menos al 6 de julio de 2021 para que el firewall cuente con las capacidades de: Sandbox con capacidades de extracción de malware, Previsor de Intrusos Perimetral, Control de Aplicaciones en la navegación, Antivirus para el tráfico de red, Bloqueo de redes "Robot"		
1	CPEBP-NGTX	Enterprise Based Protection - Next Generation Threat Extraction Package kage Including IPS, APCL, URLF, AV, ABOT, ASPM, TX and TE for CPAP-SG5400-NGTX-SSD -
1	CPES-CO-Standard	Collaborative Standard Support 5400 Appliance NGTX 1y
Seguridad Perimetral (firewall) en alta disponibilidad con el mantenimiento con vigencia de 1 año al menos al 6 de julio de 2021		
1	CPEBP-NGTX	Enterprise Based Protection - Next Generation Threat Extraction Package kage Including IPS, APCL, URLF, AV, ABOT, ASPM, TX and TE for CPAP-SG5400-NGTX-SSD-HA -
1	CPES-CO-Standard	Collaborative Standard Support 5400 Appliance HA NGTX 1y -
La suscripción con vigencia de 1 año al menos al 6 de julio de 2021 para que los firewalls para oficinas pequeñas secundario (requerido para el cluster) cuente con las capacidades de: Sandbox con capacidades de extracción de malware, Previsor de Intrusos Perimetral, Control de Aplicaciones en la navegación, Antivirus para el tráfico de red, Bloqueo de redes "Robot", considerando las siguientes capacidades específicas:		
12	CPEBP-NGTX	Enterprise Based Protection - Next Generation Threat Prevention Package Including IPS, APCL, URLF, AV, ABOT and ASPM blades 1430 Next Generation Threat Prevention & SandBlast (NGTX) Appliance, Wired

12	CPES-CO-Standard	Collaborative Standard Support 1430 Appliance NGTX 1y
Módulo de acceso para VPNs de SSL para el firewall principal de 200 usuarios, con las siguientes capacidades:		
1	CPES-CO-Standard	Collaborative standard support 1y. CPSB-MOB-200 mobile access blade for to up 200 concurrent users
Módulo de acceso para VPNs de SSL para el firewall secundario (cluster) de 200 usuarios, con vigencia de 1 año al menos al 6 de julio de 2021 con las siguientes capacidades:		
1	CPES-CO-Standard	Collaborative standard support 1y. CPSB-MOB-200 HA mobile access blade for to up 200 concurrent users for availability
Mantenimiento de la consola de administración con vigencia de 1 año al menos al 6 de julio de 2021, que permite acceder a nuevas versiones y funcionalidades de la misma, así como a mejoras y parches del software		
1	CPSB-EVS-COMP-25-1Y	Next Generation Security Management Software for 25 gateways (SmartEvent & Compliance 1 year)
1	CPES-CO-Standard	Standard Collaborative Enterprise Support For 1 Year

ATENTAMENTE

Rene Fuentes García de León
Representante Legal

Concurso por Licitación Pública Nacional Presencial No. SA-DA-CL-32/2020
"Requerimiento de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

Anexo B1. Servicios Administrados
Habilitación

TIEMPOS DE IMPLEMENTACIÓN		
El tiempo total para la implementación y puesta en marcha de la solución será de 30 días hábiles		
SERVICIOS ADMINISTRADOS DE LOS CONTROLES DE SEGURIDAD INFORMÁTICA		
12 meses		La cobertura de los servicios administrados de seguridad informática para protección del Municipio debe ser 7x24x365, y se debe encargar de salvaguardar la seguridad a nivel informático con las herramientas y controles indicados; así como la visita en sitio por personal especializado en las herramientas instaladas cuando sea requerido y el tiempo que sea necesario.

REQUERIMIENTOS DE PERSONAL
• El proveedor deberá proporcionar personal en sitio hasta que las licencias queden instaladas en su totalidad de manera satisfactoria
Descripción
A) Filtrado de Contenido, Monitoreo de Infraestructura y Captura y análisis de Tráfico
Servicios de Habilitación licencias de seguridad en la navegación web (los días requeridos en sitio). Debe incluir al menos pero no está limitado a:
• La habilitación del equipo y el montado del mismo en el rack (de ser requerido) • La integración del equipo al dominio • La configuración de políticas de navegación web asociada los diferentes perfiles incluyendo el uso de cuotas de navegación basadas en tiempo o en volumen • La habilitación del filtrado de HTTPS, incluyendo la distribución del certificado en las estaciones (PCs) • La distribución automática del archivo .PAC • La integración con el firewall designado por el municipio para la redirección del tráfico HTTP y HTTPS adicional a la redirección vía el archivo .PAC • La estabilización de la operación, apoyada con personal en sitio por al menos 1 día posteriores a la finalización de la instalación y configuración
Servicios de afinación de reglas de -Previsión de Fuga de Información- (los días requeridos en sitio) a nivel agente de PCs validando su correcto funcionamiento y liberación. Debe incluir al menos pero no limitado a:
• El aseguramiento de la cobertura de agentes a los usuarios indicados y su habilitación silenciosa a las PCs licenciadas

• La afinación de la configuración reglas de notificación al usuario señaladas por el municipio minimizando falsos positivos • La configuración o reconfiguración de reglas de protección 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
Software de captura y análisis experto de paquetes de tráfico red que tenga las siguientes capacidades:
Proporcionar transferencia de conocimiento de las actualizaciones o nuevas caracteristicas de la aplicación

B) Seguridad en las PCs, Servidores, la red interna y resguardo y registro de correlación de eventos
Servicio para identificar vulnerabilidades, que tengan las siguientes capacidades:
Servicios de configuración de tareas de escaneo de vulnerabilidades para 10 grupos de activos (los días requeridos en sitio) Debe incluir al menos pero no limitado a:
• 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 • 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
Servicios de Instalación y configuración de Seguridad en 50 servers (los días requeridos en sitio). Debe incluir al menos pero no limitado a:
• La distribución en 50 servidores • El levantamiento del inventario de las aplicaciones • La configuración de listas "blancas" y listas "negras" • 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: o 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
Servicio de habilitación contra amenazas avanzadas para 50 Servers en modo protección, con bloqueo y excepciones (los días requeridos en sitio). Debe incluir al menos pero no limitado a:
• La distribución en 50 servidores • La habilitación progresiva de los módulos Machine Learning con las siguientes consideraciones: • La habilitación en modo monitoreo 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 protección de 4 servidores, asegurando la continuidad operativa y la resolución de problemas sin afectar la operación de los servidores y las aplicaciones del Municipio Habilitación del resto de servidores o En la instalación inicial deben considerarse las excepciones necesarias para evitar "falsos positivos"
Servicio para monitoreo de firewall/previsor de intrusos para las bases de datos 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 publicadas por el fabricante. 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
Licencias en modo Suscripción de protección de seguridad en el endpoint con al menos los siguientes controles: Antivirus basado en firmas y antivirus de nueva generación basado en inteligencia artificial para PCs y Servidores, Control de dispositivos periféricos, Previsor de intrusos de host, Firewall personal, Para control web, Control

de aplicaciones en las PCs, Endpoint Detection and Response (EDR) y protección para los dispositivos móviles (Teléfonos inteligentes y tabletas) con al menos las siguientes capacidades por cada producto:
Habilitación y configuración de seguridad en las PCs en sitio y la nube hasta 1200 PCs (los días requeridos en sitio). Al menos con el siguiente alcance pero no limitado a:
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 antivirus 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 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 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 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 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

Para el Endpoint Detection and Response Deberá distribuirse a todas las estaciones y 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 mas rápida 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
Cifrado de disco duro de folders y archivos
Instalación y configuración del cifrado de disco duro y de archivos y folders en 1200 PCs (los días requeridos en sitio), misma que debe incluir, pero no estar limitada a:
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 Excell, 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 para el Sistema de previsión de intrusos El mantenimiento del equipo por 1 año que permita acceder a nuevas versiones de software a resolución de fixes y vulnerabilidades a la base de datos de conocimiento y a poner tickets de alta criticidad con el fabricante con vigencia de 1 año
Previsor de intrusos de red de propósito específico que soporte un throughput de 300 Mbps y 80,000 conexiones concurrentes CON 8 INTEERFACES 100Mbps/1Gibabit por segundo "FAIL OPEN" , y que cuente con las siguientes características:
Previsor de intrusos de red de propósito específico tenga 8 INTEERFACES 100Mbps/1Gibabit por segundo "FAIL OPEN" y 12 INTERFACES SFP 100Mbps/1Gibabit por segundo, soporte un throughput de 1 Gbps y 750,000 conexiones concurrentes

Previsor de intrusos de red para ambientes VMWare que pueda ser instalado en hasta 7 Hosts donde el throughput en total sea a lo mas de 500 Mbps
Consola de administración de los Previsores de Intrusos de red físicos y virtuales con un año de mantenimiento Servicios instalación y afinación de previsores físicos en hasta 8 enlaces Gigabit Ethernet en cobre Y de previsores de intrusos virtuales en hasta 7 dominios de VMWare (los días requeridos en sitio). Debe de incluir al menos pero no limitado a:
• La instalación de la consola de administración, todos sus componentes incluyendo la conectividad a los equipos de previsión de intrusos físicos y virtuales • La instalación en modo transparente y configuración para proteger cada uno de los 8 enlaces Gigabit Ethernet, con al 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, tirado de paquetes o envío de reset, según sea el caso. • La habilitación por enlace, 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 instalación en modo transparente y configuración para proteger cada dominio de VMWare del resto de la red. Con las siguientes características: • 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"
SIEM (Correlacionador de eventos) que soporte hasta 1000 eventos por segundo y tenga espacio para guardar bitácoras de 3 TB de información: Servicios de Integración en el SIEM (Correlacionador de eventos) de 3 portales, 5 aplicaciones, 50 equipos de red que incluyan switches, call manager, routers, firewalls, 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, firewall de Base de datos y Configuración de 10 Tableros (dashboards) y 30 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 monitoreo y seguridad incluidas en el presente documento
- Eventos de malware o Eventos de actividad inusual
- Eventos de actividad maliciosa conocida como resultado de ejercicios de penetración
- Eventos bajo desempeño o falla en la infraestructura, las aplicaciones o la red
- 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
- 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 modificación a las políticas de previsores de intrusos de host
- La modificación a las políticas de los previsores de intrusos de red
- 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 o La fuga de información
- 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

Licencias para el parcheo de parches Microsoft

Servicios de Habilitación de control de parcheo para 1200 equipos (los días requeridos en sitio) Debe incluir al menos pero no limitado a:

- 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 servers, incluyendo parches de Microsoft, Adobe y JAVA
- La habilitación y el parcheo del mes en curso con los parches críticos de seguridad de Microsoft debe ser progresiva.

o Para PCs:

Habilitación de 10 estaciones (laboratorio)
Habilitación de 20 estaciones (prueba)
Habilitación de 40 estaciones (piloto)

• La habilitación masiva en grupo de los parches críticos de Microsoft, asegurando la continuidad operativa y la resolución de problemas sin afectar de manera masiva a la operación de las PCs del municipio o Para los servidores: Habilitación de 1 servers (laboratorio) Habilitación de 3 servers (prueba) Habilitación de 6 servers (piloto) • La habilitación de 40 servers restantes
Servicio Sandbox para antivirus y los previsores de intrusos de red Servicios de integración y estabilización de Sandbox con consola del antivirus y con consola del previsor de intrusos (los días requeridos en sitio). Debe incluir al menos, pero limitado a:
• La habilitación del Sandbox • La habilitación de al menos 2 estaciones tipo para el preanálisis • La integración con la consola de administración del antivirus • La integración con la consola de administración de los previsores de intrusos de red • La configuración para el envío de código o archivos con posible malware de día cero desde la consola del antivirus • La configuración para el envío de código o archivos con posible malware de día cero desde la consola de administración de los IPSs • Estabilización de la integración con la consola de antivirus y la consola de administración de los IPSs
C) FIREWALLS
La suscripción por 1 año para que el firewall cuente con las capacidades de: Sandbox con capacidades de extracción de malware, Previsor de Intrusos Perimetral, Control de Aplicaciones en la navegación, Antivirus para el tráfico de red, Bloqueo de redes "Robot"
Seguridad Perimetral (firewall) en alta disponibilidad con el mantenimiento por 1 año
La suscripción por 1 año para que los firewalls para oficinas pequeñas secundario (requerido para el cluster) cuente con las capacidades de: Sandbox con capacidades de extracción de malware, Previsor de Intrusos Perimetral, Control de Aplicaciones en la navegación, Antivirus para el tráfico de red, Bloqueo de redes "Robot", considerando las siguientes capacidades específicas:
Módulo de acceso para VPNs de SSL para el firewall principal de 200 usuarios, con las siguientes capacidades:
Módulo de acceso para VPNs de SSL para el firewall secundario (cluster) de 200 usuarios, con las siguientes capacidades:
Consola de administración, que permite acceder a nuevas versiones y funcionalidades de la misma, así como a mejoras y parches del software

Servicios de habilitación del firewall principal y su cluster, 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). Debe incluir, pero no estar limitado a la integración con la protección web de un proxy para el filtrado de contenido Web. Se deben considerar las excepciones de los 50 sitios más comunes, no "proxeables".
• 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 antiboot • 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 IPSec usuario a sitio con autenticación a través del directorio activo • La integración de cada equipo con la seguridad de navegación web de un tercero via proxy para el filtrado de contenido web • La habilitación del sandbox integrado en modo protección para la inspección del tráfico protegido a través del proxy • La estabilización de la operación de cada uno de los firewalls
Servicios de instalación y afinación de 12 equipos firewall para oficinas pequeñas y la consola de administración. Los equipos para oficinas pequeñas deberá instalarse en sitio con las capacidades de, Firewall, Antivirus, Antibot, una VPN IPS de sitio a sitio, IPS en modo bloqueo habilitado y la consola de administración (los días requeridos en sitio). Con al menos pero no limitado a:
• La instalación de conectividad en sitio en cada localidad • La integración a la consola de administración • La configuración de hasta 50 reglas de acceso incluyendo la traducción necesaria de IP (Network Address Translation) • La habilitación de los módulos de antivirus y antiboot • La habilitación del Blade de IPS inicialmente en modo monitoreo y posteriormente en modo protección o bloqueo • La habilitación de una VPN IPSec de sitio a sitio con certificado en cada localidad que permita el acceso a las aplicaciones corporativas • La integración de cada equipo con la seguridad de navegación web via proxy para el filtrado de contenido web • La estabilización de la operación de cada uno de los firewalls
D) TIEMPOS DE IMPLEMENTACIÓN

El tiempo total para la implementación y puesta en marcha de la solución será de 30 días hábiles
E) SOPORTE ESPECIALIZADO EN SITIO 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 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 y fólders - 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 sanbox de los mismos

ATENTAMENTE

Rene Fuentes García de León
Represéntate Legal

Concurso por Licitación Pública Nacional Presencial No. SA-DA-CL-32/2020
"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

Anexo B2. Servicios Administrados

SERVICIOS ADMINISTRADOS DE LOS CONTROLES DE SEGURIDAD INFORMÁTICA	
12 meses	La cobertura de los servicios administrados de seguridad informática para protección del Municipio debe ser 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. y se debe encargar de salvaguardar la seguridad a nivel informático con las herramientas y controles indicados; así como la visita en sitio por personal especializado en las herramientas instaladas cuando sea requerido y el tiempo que sea necesario.

SERVICIOS ADMINISTRADOS

	ACCIONES					REPORTES	
CONTROL	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 Del reporteador De la base de datos	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio	Modificación de políticas de navegación sin límite de modificaciones Reporteo de navegación de usuarios específicos como se requiera sin límite Validación del correcto funcionamiento	Debe respaldarse la configuración de la consola y de la base de datos de navegación	Para revisión de eventos, incidentes, fallas	De Salud de la herramienta, incluyendo la actualización de base de datos De evento 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 De la base de datos	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio	Modificación de políticas de protección sin límite de modificaciones Reporteo de incidentes de seguridad sin límite Validación del correcto funcionamiento	Debe respaldarse la configuración de la consola y de la base de datos de eventos	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

Monitoreo 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	Adición de elementos a monitorear su disponiblidad sin límite de eventos Adición de reportes de disponibilidad y desempeño sin límite de eventos	Debe respaldarse la configuración de la consola	Para revisión de eventos, incidentes, fallas	No Aplica	De disponibildiad de hasta 20 servicios De eventos de falla consolidados al mes De correcciones consolidadas al mes De recomendaciones consolidadas al mes
Administración de vulnerabilidades	De la herramienta	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio	Modificación direcciones IP a checar sus vulnerabilidades sin límite de eventos Reportes de vulnerabilidades sin límite de eventos	Debe respaldarse la configuración de la consola y el appliance físico o virtual	Para revisión de eventos, incidentes, fallas	No Aplica	De vulnerabilidades de los activos Del score de riesgo y su comportamiento vs el mes anterior
Antivirus de Nueva Generación	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 requerimiento del municipio	Validación del correcto funcionamiento Cobertura de producto y patrones Identificación, resolución y reporteo de incidents	La configuración La base de datos	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 de patrones o firmas - Eventos de seguridad - Eventos de falla - Acciones realizadas - Recomendaciones
Antivirus de Nueva Generación	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 requerimiento del municipio	Validación del correcto funcionamiento Cobertura de producto y patrones Identificación, resolución y reporteo de incidents	La configuración La base de datos	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 de patrones o firmas - Eventos de seguridad - Eventos de falla - Acciones realizadas - Recomendaciones
Control de aplicaciones/ Controles de cambios	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	De la cobertura de productos en modo bloqueo	La configuración El inventario	Para revisión de eventos,	Coberturas Incidentes de Seguridad y/o Falla	El reporte debe incluir: - Cobertura de producto - Cobertura modo de protección:

		del requerimiento del municipio			incidentes, fallas	Correcciones realizadas y/o recomendaciones	bloqueo o no bloqueo - Eventos de seguridad - Eventos de falla - Acciones realizadas - Recomendaciones
Parches	Cobertura de parches Salud de la herramienta de parcheo	De la herraienta de parcheo debe realizarse una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio	Avance en la cobertura de los parches de acuerdo a la métrica	La configuración Los eventos	Para revisión de eventos, incidentes, fallas	No Aplica	El reporte debe incluir: - Cobertura de parches vs las métrica - Eventos de falla - Acciones realizadas - Recomendaciones
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	No Aplica	De vulnerabilidades de los activos De los parches virtuales aplicaciones Las recomendaciones
Endpoint Detection & Response: EDR	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	No Aplica	Para revisión de eventos, incidentes, fallas	Eventos de seguridad extraños o anómalos	De eventos anómalos consolidades De acciones tomadas Las recomendaciones
Endpoint Detection & Response: EDR	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	No Aplica	Para revisión de eventos, incidentes, fallas	Eventos de seguridad extraños o anómalos	De eventos anómalos consolidades De acciones tomadas Las recomendaciones
Sandbox para PCs y previsores de intrusos de propósito específico	Sí de correcto funcionamiento	Sobre demanda, cuando aplique	Identificación del correcto funcionamiento	No Aplica	Para revisión de eventos, incidentes, fallas	Eventos de seguridad Fallas	Incluido en el reporto de antivirus de PCs, servidores y/o previsores de intrusos de propósito específico señalando el volumen de eventos administrados por el sandbox

SIEM (Correlacionador de eventos)	Sí de correcto funcionamiento	Debe realizarse al menos una vez al año como fundamento de una mejora o como resultado del requerimiento del municipio	Alertamiento Modificación, adición a los dashboards sin límite de eventos Modificación adición a las Reglas de correlación sin límite de eventos	La configuración	Para revisión de eventos, incidentes, fallas	Eventos de seguridad correlacionados extraños o anómalos	Sí de actividad anómala por mes. Incluida en los dashboards específicos
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
Firewalls s la 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	Modificación de reglas sin límite de eventos De configuración asociada a Sanbox 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

ATENTAMENTE

Rene Fuentes García de León
Representante Legal

PROPUESTA ECONÓMICA

Monterrey N.L a 25 de junio de 2020

Lic. Gloria Ma. Morales Martínez
Directora de Adquisiciones
Presente. -

Me refiero al Concurso por Licitación Pública Nacional Presencial **N°SA-DA-CL-32/2020 "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 propuesta económica, de acuerdo al formato requerido en el Anexo **N° 2 "Cotización", en Moneda Nacional (Pesos Mexicanos)**

Concurso por Licitación Pública Nacional Presencial No. SA-DA-CL-32/2020
"Adquisición de licencias y suscripciones de seguridad informática soporte de infraestructura instalada y servicios administrados"

Anexo 2 "Cotización"

Anexos	Conceptos	Precio Unitario
A	Licencias y suscripciones de seguridad informática soporte de infraestructura instalada	$4,650,023.10
B1 y B2	Servicios Administrados	$1,224,000.00
	Subtotal.-	$5,874,023.10
	I.V.A.-	$939,843.70
	Total.-	$6,813,866.80

ATENTAMENTE

Ing. Rene Fuentes García de León
Representante Legal