GOBIERNO DE
MONTERREY

SAD-563-2019

CONTRATO DE PRESTACIÓN DE SERVICIOS DE RENOVACIÓN DE LICENCIAS DE SEGURIDAD PARA LA PROTECCIÓN DE BIENES TECNOLÓGICOS INFORMÁTICOS, QUE CELEBRAN POR UNA PARTE EL MUNICIPIO DE MONTERREY, NUEVO LEÓN, A TRAVÉS DEL **C. HÉCTOR ANTONIO GALVÁN ANCIRA**, DIRECTOR JURÍDICO DE LA SECRETARÍA DEL AYUNTAMIENTO; **C. ALAN GERARDO GONZÁLEZ SALINAS**, DIRECTOR DE ADQUISICIONES DE LA SECRETARÍA DE ADMINISTRACIÓN; **C. JUAN CARLOS PASTRANA GARCÍA,** DIRECTOR DE EGRESOS DE LA TESORERÍA MUNICIPAL DE MONTERREY; **C. ELVIRA YAMILETH LOZANO GARZA,** SECRETARIA DE ADMINISTRACIÓN; Y EL **C. RAFAEL IVÁN RICO GARCÍA,** ENCARGADO DE LA DIRECCIÓN DE INFORMÁTICA DE LA SECRETARÍA DE ADMINISTRACIÓN, A QUIENES EN LO SUCESIVO SE LES DENOMINARÁ **"EL MUNICIPIO"** Y POR LA OTRA LA PERSONA MORAL DENOMINADA **MCS NETWORK SOLUTION, S.A. DE C.V.,** REPRESENTADA EN ESTE ACTO, POR EL **C. ELÍAS TREVIÑO BENAVIDES**, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ **"EL PRESTADOR DE SERVICIOS"**, AMBAS PARTES CON CAPACIDAD LEGAL PARA CONTRATAR Y OBLIGARSE, AL TENOR DE LAS SIGUIENTES:

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

1.- Declara **"EL MUNICIPIO":**

1.1.- Que es una entidad de carácter público, dotado de personalidad jurídica y patrimonio propio, autónomo en su régimen interior, con libertad para administrar su hacienda o gestión municipal conforme a lo establecido en los artículos 115 de la Constitución Política de los Estados Unidos Mexicanos, 118 y 120 de la Constitución Política del Estado de Nuevo León.

1.2.- Que de acuerdo con lo dispuesto por el acuerdo delegatorio de la representación legal en general de la Administración Pública Municipal del Ayuntamiento de Monterrey, aprobado en Sesión Ordinaria de fecha 31-treinta y uno de enero de 2019-dos mil diecinueve, en favor del Lic. Héctor Antonio Galván Ancira, y por los artículos 1, 2, 34, fracción II, 86, 88, 89, 91 y demás relativos de la Ley de Gobierno Municipal del Estado de Nuevo León; 3, 5, 11, 14, fracción IV, incisos c) y d), 16, fracciones II y VI, 31, 33 fracciones I, VIII, XI y XXX, 63, 64 fracciones X y XI, 65, 67, fracción I, 70 fracciones I, III, VII, XI, y demás aplicables del Reglamento de la Administración Pública del Municipio de Monterrey; 1, fracción V, 4, fracciones IV, XXV, XXVI, XXVII, XXVIII y 46, de la Ley de Adquisiciones, Arrendamientos y Contratación< de Servicios del Estado de Nuevo León; 89 y 90 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Contrataciones de Servicios del Estado de Nuevo León; 17, 37 y 38 del Reglamento de Adquisiciones, Arrendamientos y Servicios del Gobierno Municipal de Monterrey, los servidores públicos señalados en el proemio comparecen para la celebración del presente contrato en el ámbito y con estricto límite de sus competencias.

1.3.- Que, para los efectos del presente instrumento, señalan como domicilio para oír y recibir notificaciones y cumplimiento de obligaciones, la sede del mismo, ubicado en la calle Zaragoza Sur s/n, Zona Centro en la Ciudad de Monterrey, Nuevo León.

1.4.- Que los egresos originados con motivo de las obligaciones que se contraen en este contrato, serán cubiertos con Participaciones Federales 2019-dos mil diecinueve (Ramo 28), los cuales están debidamente autorizados por la Dirección de Planeación Presupuestal de la

GOBIERNO DE
MONTERREY

Tesorería Municipal, mediante Oficio PIM 19158024, de fecha 28-veintiocho de marzo de 2019-dos mil diecinueve, los cuales se distribuyen conforme a la siguiente estructura financiera:

EJERCICIO PRESUPUESTAL	MONTO AUTORIZADO
abril-diciembre 2019	$2´069,999.91
enero-diciembre 2020	$2´759,999.98
enero-septiembre 2021	$2´069,999.91
TOTAL	**$6´899,999.70**

1.5.- Que cuenta con el Registro Federal de Contribuyente MCM-610101-PT2, expedido por el Servicio de Administración Tributaria, Organismo Desconcentrado de la Secretaría de Hacienda y Crédito Público.

1.6.- Que para asegurar las mejores condiciones en cuanto a precio, calidad, financiamiento y oportunidad para los servicios renovación de Licencias de Seguridad para la protección de los bienes tecnológico informáticos del Municipio de Monterrey, se realizó el procedimiento de Adjudicación Directa, que se establece en los artículos 25 fracción III, 41, 42 fracciones II y V de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León, 81 fracción I del Reglamento de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León, así como los artículos 16 fracción II, 18 fracción I, 32 y 33 fracciones III y VIII del Reglamento de Adquisiciones, Arrendamientos y Servicios del Gobierno Municipal de Monterrey, contando con la opinión favorable del Comité de Adquisiciones, Arrendamientos y Servicios de la Administración Pública Municipal de Monterrey, según consta en el Acta de la Cuarta Sesión Extraordinaria, celebrada el día 01-uno de abril de 2019-dos mil diecinueve.

2.- Declara **"EL PRESTADOR DE SERVICIOS"**, a través de su Representante Legal y bajo protesta de decir verdad:

2.1.- Que su representada es una Sociedad Mercantil que se constituyó conforme a las Leyes Mexicanas, acreditando su existencia mediante Escritura Pública Número 8,778-ocho mil setecientos setenta y ocho, de fecha 19-diecinueve de marzo de 1999-mil novecientos noventa y nueve, pasada ante la fe del Notario Público Número 30-treinta, Lic. Enrique Martínez Morales, con ejercicio en la Ciudad de Monterrey, Nuevo León, documento que se encuentra debidamente inscrito en el Registro Público de la Propiedad y de Comercio del Estado de Nuevo León bajo el Número 1007, Volumen 431, Libro 3, Segundo Auxiliar Escrituras de Sociedades Mercantiles Sección Comercio, de fecha 13-trece de abril de 1999-mil novecientos noventa y nueve.

2.2.- Que se acredita la personalidad del Representante Legal mediante Escritura Pública Número 99,209-noventa y nueve mil doscientos nueve, de fecha 28-veintiocho de junio de 2013-dos mil trece, pasada ante la fe del Notario Público de la Notaría Pública Número 51-cincuenta y uno, Lic. Evaristo Ocañas Méndez, con ejercicio en la Ciudad de Monterrey, Nuevo León, documento que se encuentra debidamente inscrito en el Registro Público de la Propiedad y del Comercio bajo el Folio Mercantil Electrónico número 67143*9, de fecha 15-quince de enero de 2014-dos mil catorce, manifestando que a la fecha dichas facultades no le han sido revocadas, modificadas ni limitadas en forma alguna.

2.3.- Que para los efectos del presente Contrato señala como domicilio para el cumplimiento de las obligaciones contratadas en el mismo; así como para oír y recibir notificaciones el ubicado en Calle Distrito B3 No. 206, Colonia Leones, C.P. 64600, en Monterrey, Nuevo León.

2.4.- Que cuenta con el Registro Federal de Contribuyentes MNS990319C39, expedido por el Servicio de Administración Tributaria, Organismo Desconcentrado de la Secretaría de Hacienda y Crédito Público.

2.5.- Que, para los efectos legales correspondientes, el Representante Legal se identifica con credencial para votar con clave de elector número [redacted], expedida a su favor por el Instituto Federal Electoral, ahora Instituto Nacional Electoral, misma que contiene fotografía inserta cuyos rasgos fisonómicos coinciden con los del compareciente.

2.6.- Que cuenta con la organización, experiencia, capacidad técnica, financiera y legal necesarios para cumplir con los requerimientos objeto del presente Contrato, así mismo, ha llevado a cabo todos los actos corporativos, obtenido todas las autorizaciones corporativas o de otra naturaleza, y cumplido con todos los requerimientos legales aplicables para celebrar y cumplir el presente Contrato.

2.7.- Conoce el contenido y los requisitos que establecen la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León y su Reglamento; así como las demás normas que regulan la realización y/o adquisición de bienes y servicios, incluyendo las especificaciones generales y particulares objeto de este contrato y, en general, toda la información requerida para el bien y/o servicio materia del contrato.

2.8- Que su representada tiene por objeto, entre otros: la compra venta de equipo de cómputo, asesoría en instalación y diseño de redes, mantenimiento y reparación de equipo de cómputo, capacitación y desarrollo de sistemas.

Que expuesto lo anterior, las partes han revisado lo establecido en este Contrato, reconociendo la capacidad y personalidad jurídica con que se ostentan para obligarse mediante este acuerdo de voluntades, manifestando que previo a la celebración del mismo, han convenido libremente los términos establecidos en este, no existiendo dolo, mala fe, enriquecimiento ilegítimo, error, violencia ni vicios en el consentimiento, sujetándose a las siguientes:

C L Á U S U L A S:

PRIMERA.- (OBJETO) "EL PRESTADOR DE SERVICIOS" se obliga a la prestación de los servicios de renovación de Licencias de Seguridad para la protección de los bienes tecnológicos informáticos cuyas especificaciones y características se detallan conforme a las siguientes partidas:

PARTIDA 1
RENOVACIÓN DEL LICENCIAMIENTO DE EQUIPOS FIREWALL
EQUIPO MARCA FORTINET

Definición:

Sistema de Seguridad informática que sea del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés).

1.- Especificaciones del equipo:
Equipo FortiG ate Firewall 600

2.- Especificación de la actualización
1.a) Tamaño de licencia
1.a.1. El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de él.
1.b) Permitir conectarse en tiempo real a una base de datos centralizada en el fabricante para descargar actualizaciones de Antivirus, AntiSpam, IPS y URL Filtering.
1.c) Debe incluirse la capacidad de poder hacer actualizaciones de firmas Antivirus, AntiSpam, IPS y URL Filtering y cualquier otra actualización necesaria para la correcta operación de los equipos arriba descritos.

PARTIDA 2
RENOVACIÓN DEL LICENCIAMIENTO DE EQUIPOS ANTISPAM
EQUIPO MARCA FORTINET

Definición:
Sistema especializado de seguridad que sea capaz de proteger correo electrónico (E-mail contra SPAM, Virus, Spyware y Gusanos (Worms), instalación y puesta en marcha, deberá incluir los elementos necesarios para esta función.

1.- Especificaciones del equipo:
Equipo FortiMail Antispam FML 400BDL

2.- Especificaciones de la actualización
1.a) Tamaño de la licencia
1.a.1. No debe tener restricción por licencia en cuanto a usuarios o buzones de correo (mailboxes) a ser protegidos, debe apegarse a las especificaciones del modelo descrito.
1.b) Permitir conectarse en tiempo real a una base de datos centralizada en el fabricante para descargar actualizaciones antispam.
1.c) Soporte e inspección de contenido para cumplimiento de regulaciones mediante diccionarios personalizables. Los diccionarios personalizables pueden ser definidos en múltiples idiomas.
1.d) Debe incluirse la capacidad de poder hacer actualizaciones de firmas antispam, antivirus y cualquier otra actualización necesaria para la correcta operación del equipo arriba descrito.

PARTIDA 3
SOLUCION EN LA NUBE PARA FILTRADO WEB

WEB APPLICATION SECURITY

- El modelo positivo de seguridad deberá definir lo que está permitido y bloquear todo lo demás. Deberá incluir direcciones URL, directorios, cookies, campos, parámetros (identificando además el formato y tipo de estos), métodos HTTP.

- Para facilitar la configuración del modelo positivo de seguridad, el dispositivo deberá aprender automáticamente la estructura y los elementos de la aplicación de manera constante y sin intervención humana.
- La solución deberá contar con un modo aprendizaje para rastrear cambios continuos en las aplicaciones web, deberá reconocer los cambios en la aplicación y simultáneamente protegerlas. Deberá contar con las siguientes características:
  - ✓ Deberá aprender los valores aceptables para los campos de ingreso de datos con base en el registro de la actividad.
  - ✓ Los valores aprendidos podrán ser utilizados como la configuración inicial sobre la que se revisarán los datos ingresados en el modelo positivo de seguridad.
  - ✓ El modo aprendizaje deberá aprender la estructura y elementos de la aplicación (directorios, url´s, parámetros, cookies) y el comportamiento esperado del usuario (longitud del valor esperado, caracteres aceptados, si el parámetro es de sólo lectura o editable por el usuario) y esta información deberá estar disponible para automatizar la configuración del modelo positivo de seguridad.
  - ✓ La configuración aprendida deberá ser accesible y modificable para el administrador del dispositivo

- La solución deberá correlacionar múltiples eventos de seguridad para distinguir tráfico deseado del tráfico inadecuado.
- La solución deberá permitir la modificación de reglas de seguridad. Los administradores deberán poder definir reglas para el modelo de seguridad positivo o negativo y deberán crear reglas de correlación con múltiples criterios.
- Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación Web. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:
  - ✓ Estado de autenticación de la sesión web.
  - ✓ Por el URL de autenticación y el resultado del intento de autenticación.
  - ✓ Por URL, a través del prefijo, ruta o host.
  - ✓ Por la existencia o contenido de cualquier Header HTTP.
  - ✓ Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares), ya sea en el HTTP Request o el Response por parte del servidor Web.
  - ✓ Tipo de archivo siendo trasmitido en cualquier sentido.
  - ✓ Host o dominio accedido.
  - ✓ Métodos HTTP usados.
  - ✓ Número de ocurrencias en intervalos de tiempo definidos.
  - ✓ La existencia o contenido de cualquier Parámetro Web.
  - ✓ Por el protocolo usado, HTTP o HTTPS.
  - ✓ IPs de origen y destino.
  - ✓ Por la existencia o contenido de Cookies o el identificador de Sesión.
  - ✓ Response Code y Headers en el Response HTTP por parte del servidor Web.
  - ✓ Hora del día.
  - ✓ Por usuario firmado en el aplicativo web.
  - ✓ User-Agent.
  - ✓ Referer-URL
  - ✓ Tiempo de respuesta o tamaño de la respuesta HTTP.

- La solución deberá contar con el modo de instalación proxy transparente.
- La solución deberá cubrir con todas las vulnerabilidades expresadas en el OWASP Top Ten más reciente.
- La solución deberá cumplir con todos los criterios de evaluación del WAFEC definidos por el Web Application Security Consortium.
- La solución deberá soportar la integración con seguridad para base de datos, del mismo fabricante, para ofrecer seguridad de extremo a extremo; desde internet hasta la base de datos sin ningún cambio en la aplicación web. La seguridad integrada de la base de datos deberá proteger contra ataques conocidos a las bases de datos, deberá también tener capacidad de monitorear y controlar la actividad de la base de datos.
- La solución deberá proporcionar el bloqueo de direcciones IP, sesiones TCP o usuarios de la aplicación web.
- La solución deberá proteger tanto las aplicaciones Web HTTP, como las aplicaciones web SSL y HTTPS.
- La solución deberá tener la capacidad de recibir y utilizar los certificados y pares de llaves público / privadas para los servidores web protegidos.
- La solución deberá des encriptar el tráfico SSL, de las aplicaciones web, entre el cliente y el servidor y re-encriptarlo antes de su reenvío.
- En los modos puente (bridge)o sniffer, la solución deberá de poder des encriptar el tráfico SSL para inspección, sin terminar o cambiar la conexión HTTPS.
- La solución deberá tener la capacidad de proteger aplicaciones web que incluyan el contenido de servicios web (xml). La protección XML deberá contar con mecanismos automatizados de aprendizaje, similares a los de la protección de aplicaciones web.

- La solución deberá contar con funcionalidades que permitan:
  - ✓ Rastrear e identificar las fuentes de los ataques originadas desde proxies anónimos, direcciones ip maliciosas, botnets y sitios phishing.
  - ✓ Actualizar las fuentes de ataque para identificar y bloquear el tráfico malicioso.
  - ✓ Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.
  - ✓ Bloquear solicitudes de acceso basado en la reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por Botnet, DDoS, Phishing o redes de Anonimización (TOR y Proxies Anónimos).
  - ✓ Bloquear solicitudes de acceso basado en el país de origen de la conexión.
  - ✓ Realice un análisis automático de distribución de alertas en relación al país de origen, con opción a representar la información a través de un mapa mundial.
  - ✓ Detallar y analizar los eventos de seguridad ocurridos, orígenes y método del ataque, dirección IP y localización geográfica del ataque.
  - ✓ La solución solo soporta ataques simultáneos hasta 1GB.

- La solución deberá:
  - ✓ Inspeccionar y monitorear todos los datos http y la aplicación, incluyendo los encabezados http, campos de formularios y el cuerpo http.
  - ✓ Inspeccionar las peticiones y respuestas http.
  - ✓ Tener la habilidad de decodificar datos a su mínima expresión a partir de diferentes sistemas de enconding web y validarla.

- ✓ Validar todos los tipos de datos ingresados, incluyendo URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos http, elementos XML y acciones SOAP.
- ✓ La solución solo soporta ataques simultáneos hasta 1GB.

PARTIDA 4
Solución De Firewall para Bases de Datos.

El proveedor deberá ofrecer en su solución, el hardware y/o software necesario que cubra los siguientes requerimientos técnicos:

DATABASE SECURITY

- La solución deberá contar con tecnología de auto-aprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo schemas, objetos, tablas, sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un baseline de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.
- La solución deberá proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad de ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
- La solución deberá generar reportes y tendencias en tiempo real, así como permitir la modificación de los mismos.
- La solución deberá contar con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente.
- La solución no deberá requerir el instalar agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario.
- La solución deberá funcionar independiente a la activación de la auditoría nativa de la base de datos.
- La solución deberá ser transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
- El repositorio para el registro de la actividad en el appliance, no deberá ser accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante o por medios administrativos debidamente asegurados.
- La solución deberá ser capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.
- La solución deberá realizar una evaluación exhaustiva de los riesgos de la infraestructura objetivo a diferentes niveles/capas de la infraestructura de base de datos incluyendo:
    - Cuestiones de configuración de la base de datos tales como nivel de parcheo, configuración de las cuentas de usuario, evaluación de la fortaleza de las contraseñas, vigencia de las contraseñas.

GOBIERNO DE MONTERREY

- Cuestiones de configuración de plataforma, incluyendo configuración del sistema operativo de los servidores que soportan el software de base de datos.

- La solución deberá de poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.
- La solución deberá tener la capacidad de analizar y clasificar los tipos de datos entro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular.
- La solución deberá proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.
- La solución deberá apoyar en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y Control de cambios.
- La solución deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
- La solución deberá monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.
- La solución deberá hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
- La solución deberá tener la capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.
- La solución deberá proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.
- La solución deberá manejar reglas y políticas tan amplias o granulares como re requieran y deberán poder ser construidas automáticamente o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.
- Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos, Los criterios deberán de poder usarse en cualquier número y cualquier combinación:

  - Número de registros a regresar por la consulta (SQL Query).
  - Número de registros afectados.
  - Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada).
  - Acceso a datos marcados como sensibles.
  - Base de Datos, Schema, Instancia, Tabla y Columna accesada.
  - Estado de autenticación de la sesión.
  - Usuario y/o Grupo de Usuarios de Base de Datos conectado.
  - Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB.

- Por búsqueda en diccionario de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares).
- Logins, Logouts, Queries.
- IPs de origen y destino.
- Nombre del Host origen, Usuario firmado en el Host origen.
- Aplicación usada para la conexión a la base de datos.
- Tiempo de respuesta/procesamiento del Query.
- Errores en el manejador de SQL.
- Número de ocurrencias en intervalos de tiempo definidos.
- Por operaciones básicas (Select, Insert, Update, Delete).
- Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export).
- Por Stored Procedure o Function utilizada.
- Si existe ticket asignado de cambios.
- Hora del Día.

- La solución deberá identificar individualmente a los usuarios finales que realicen actividades mediante aplicaciones, aún si utilizan mecanismos comunes de comunicación entre la aplicación y la base de datos, ésta actividad no deberá implicar la modificación de la aplicación y/o de la base de datos.
- La solución debe posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
- La solución deberá asociar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son indicativos de una potencial violación de seguridad.
- La solución deberá proteger contra ataques SQL y no SQL (como buffer overflow).
- La solución deberá correlacionar actividad en base de datos con actividad de aplicaciones web para entender detalladamente como los usuarios están accesando datos privilegiados sin necesidad de alterar la aplicación web.
- La solución deberá contar con un mecanismo de actualización de la inteligencia interna de seguridad, que incluye las pruebas de las evaluaciones de vulnerabilidad, las firmas contra ataques, la granularidad de las políticas de seguridad y defensas contra comportamientos conocidos.
- Considerados de emergencia para potenciales violaciones de la información que incluyan, enunciativa mas no limitativamente:
  - Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
  - Acceso a datos inusuales para cierta hora del día.
  - Acceso a datos desde una ubicación (física) desconocida.
  - Acceso a datos utilizando aplicaciones/herramientas no autorizadas.
- L solución debe manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.
- La solución debe tener facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP).
- La solución deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.

- La solución deberá analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios:

    - Deberá mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos.
    - Deberá contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro de la organización hacia afuera de la misma o viceversa.
    - Deberá realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y base de datos.
    - Deberá ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas y determinadas actividades en bases de datos específicas sin necesidad de alterar aplicaciones o instalar API´s.
    - Deberá correlacionar eventos como número de errores inusuales de sentencias de SQL o al momento de hacer login a las bases de datos.

- La solución debe permitir el manejo de alarmas y notificaciones en tiempo real para los eventos de correlación mencionados anteriormente.
- La solución debe tener la capacidad de monitorear aplicaciones web en la misma solución, ofreciendo una visibilidad, seguridad y control desde el usuario web hasta la base de datos.
- La solución deberá contar con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.
- La solución deberá soportar y aplicar simultáneamente un modelo de seguridad positivo y negativo.
- El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:

    - Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
    - Deberá incluir una lista preconfigurada y detallada de las firmas de ataque.
    - Deberá permitir la modificación o adición de firmas por el administrador.
    - Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
    - Deberá detectar ataques conocidos en múltiples niveles, incluyendo, la red, sistemas operativos. Software del servidor web y ataques a nivel de aplicación.

PLATAFORMA

- Lo diferentes componentes de seguridad de los aplicativos Web y DB deberán de administrarse a través de una consola centralizada.
- Los equipos que realicen el monitoreo deben tener la capacidad de ejecutar simultáneamente los componentes de seguridad DB y Web dentro del mismo equipo.

GOBIERNO DE
MONTERREY

- La consola centralizada deberá ser el único punto de contacto, administración, control, análisis y reporteo para las diferentes soluciones e infraestructura de seguridad en aplicaciones Web y Bases de Datos.
- La solución deberá soportar ser desplegada o implementada en línea como un puente o bridge transparente (capa 2 del Modelo OSI, las interfaces no requieren de una dirección IP y debe soportar bypass/failopen/failclose configurable tanta para fallas de hardware como software), como un proxy transparente o un proxy inverso (según se requiera), o como un analizador no en línea o un non-inline sniffer /monitor, a través de puertos Mirror o SPAN. Deberá también:
    - En el modo monitoreo el administrador podrá visualizar alertas, ataques, errores de servidor y otra actividad no autorizada.
    - En el modo de cumplimiento de políticas, la solución deberá bloquear ataques proactivamente.
    - Respecto de algún ataque o alguna otra actividad no autorizada, la solución deberá ser capaz de tomar las acciones adecuadas. Las acciones deberán incluir la habilidad para terminar las solicitudes y respuestas, bloquear la sesión TCP, bloquear el usuario de la aplicación, o bloquear la dirección IP.
    - Respecto de ataques particularmente destructivos, la solución deberá ser capaz de enviar un paquete TCP RST a ambos extremos de la conexión. Alternativamente, si así se configura, la solución podrá reportar el comportamiento anómalo, pero no tomar acción alguna.

- La solución podrá ser desplegada dentro de ambientes virtuales VMWare como appliance virtual.

- La solución podrá ser desplegada dentro de ambientes virtuales Crossbeam como appliance virtual.
- La solución deberá soportar el volumen de tráfico y deberá tener una latencia sub-milisegundo (<5ms), para no impactar el desempeño de las aplicaciones.

- La solución deberá tener como límites operativos un throughput mínimo por appliance de 500/1000/2000 Mbps de tráfico inspeccionado.
- La solución deberá soportar opciones de conectividad física como 1Gb Ethernet en UTP o Fibra Óptica tipo SX, así como conectividad 10Gb en modos SR o LR.
- Las interfaces de conectividad a la red deberán de ser modulares para tener la posibilidad de hacer cambios de medio como por ejemplo Cobre UTP a Fibra Óptica y viceversa, sin necesidad de cambiar el appliance.
- La solución solo soporta ataques simultáneos hasta 1GB.

PARTIDA 5

FORTIANALYZER

- Debe soportar recibir logs de al menos 2,000 dispositivos
- Tener capacidad de recibir al menos 600 GBytes de logs diarios
- Soportar al menos 18,000 logs/segundo de forma continua

- Tener al menos 24 TB de espacio en disco
- Tener al menos 2 interfaces de 1Gbps RJ-45
- Debe soportar RAID0
- Debe soportar RAID1
- Debe soportar RAID5 y RAID10
- Debe soportar RAID6, RAID50 y RAID60
- Debe soportar acceso vía SSH, WEB (HTTPS) y Telnet para la gestión de la solución
- Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.
- Permitir acceso simultaneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
- Soporte SNMP versión 2 y 3
- Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
- Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
- Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH y Telnet.
- Autenticación de usuarios de acceso a la plataforma vía Radius
- Generación de informes en tiempo real de tráfico, ya sea en mapas geográficos y en tablas.
- Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
- Autenticación de usuarios de acceso a la plataforma vía Microsoft Active Directory
- Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
- Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
- Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado.
- Contar con mecanismos de borrado automático de logs antiguos.
- Permitir la importación y exportación de reportes
- Debe contar con la capacidad de crear informes en formato HTML
- Debe contar con la capacidad de crear informes en formato PDF
- Debe contar con la capacidad de crear informes en formato XML
- Debe contar con la capacidad de crear informes en formato CSV
- Debe permitir exportar los logs en formato CSV
- Generación de logs de auditoria, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
- Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la

posibilidad de utilizar un servidor externo de Syslog o similar.

- La solución debe contar con reportes predefinidos
- Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución
- Debe ser posible la duplicación de reportes existentes para su posterior edición.
- Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
- Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
- Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
- Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
- Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
- Debe permitir descargar de la plataforma los archivos de logs para uso externo.
- Tener la capacidad de generar y enviar reportes periódicos automáticamente.
- Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
- Permitir el envío por email de manera automática de reportes.
- Debe permitir que el reporte a enviar por email sea al destinatario especifico.
- Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
- Debe ser posible visualizar gráficamente en tiempo real el consumo de disco y la tasa de generación de logs por cada dispositivo gestionado.
- Debe permitir el uso de filtros en los reportes.
- Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
- Permitir que los reportes creados sean en idioma Español
- Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
- Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
- Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para su en gráficas y tablas en reportes.
- Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
- Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.
- Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
- Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
- La solución debe servir como un servidor Syslog y aceptar logs de diferentes fabricantes

- Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
- Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
- Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos
- Debe permitir visualizar en tiempo real los logs recibidos
- Debe permitir la creación de Dashboards personalizados para visualizar tráfico de aplicaciones, categorías de URL, amenazas, servicios, países, origen y destino.
- Debe contar con un Indicar de Comprometimiento (IoC), que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
- Debe contar con reporte de cumplimiento de PCI DSS
- Debe contar con reporte de utilización de aplicaciones SaaS
- Debe contar con reporte de prevención de perdida de datos (DLP)
- Debe contar con reporte de VPN
- Debe contar con reporte de Sistema de prevención de intrusos (IPS)
- Debe contar con reporte de reputación de cliente
- Debe contar con reporte de análisis de seguridad de usuario
- Debe contar con reporte de análisis de amenaza cibernética
- Debe contar con reporte de cumplimiento PCI de Wireless.
- Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WIFi
- Debe contar con reporte de vulnerabilidades de solución gestionada de seguridad de equipo terminal.
- Debe contar con reporte de aplicaciones web, si se cuenta con plataforma de seguridad web

PARTIDA 6
POLIZA DE SOPORTE

- Póliza de Soporte con cobertura local, Atención en Idioma español para Manejo de Tickets de Soporte Ilimitado (Llamadas Telefónica, Correo Electrónico, Messenger, Webex y/o Sitio) para 1er y 2º Nivel. 3er nivel escalación con el fabricante. (Incluye trámite de garantías con base al tiempo de respuesta del contrato de mantenimiento que el cliente tenga con el fabricante). Esta póliza deberá cubrir los equipos y licenciamiento que están definido en el alcance anterior (Partidas 1, 2, 3, 4 y 5).

PARTIDA 7
RENOVACION E INTEGRACION DE TECNOLOGIA

- Renovación de equipo Fortigate 600
- Renovación de equipo FortiMail 400
- Integración del equipo FortiAnalizer

GOBIERNO DE
MONTERREY

SEGUNDA.- (CONTRAPRESTACIÓN) "EL MUNICIPIO" se obliga a pagar, por concepto de la prestación de los servicios mencionados en la Cláusula Primera del presente instrumento jurídico a favor de **"EL PRESTADOR DE SERVICIOS",** la cantidad total de $6´899,999.96 (seis millones ochocientos noventa y nueve mil novecientos noventa y nueve pesos 96/100 M.N.), ya incluido el Impuesto al Valor Agregado, misma que será pagada en una modalidad de 03-tres pagos anuales, por el periodo de vigencia del presente instrumento legal (30-treinta meses).

Dentro de la cantidad mencionada en la presente Cláusula, se contempla cualquier provisión que se deba hacer para solventar los gastos necesarios a fin de poder realizar el objeto del presente Contrato, y se hace la mención de que el monto señalado como contraprestación no se considera anticipo y el pago será realizado en pesos mexicanos.

TERCERA.- (CONTRAPRESTACIÓN FIJA) La contraprestación que **"EL PRESTADOR DE SERVICIOS"** cobrará a **"EL MUNICIPIO"** por los servicios objeto del presente Contrato, se mantendrá fija durante toda la vigencia del presente instrumento. Todos los demás gastos que se generen, así como cualquier provisión que se deba realizar para cumplir con la totalidad de las obligaciones que mediante la firma de este instrumento jurídico adquiere **"EL PRESTADOR DE SERVICIOS"**, serán por cuenta del mismo.

CUARTA.- (VIGENCIA) Ambas partes acuerdan que el presente Contrato tendrá una vigencia a partir del día 01-uno de abril de 2019-dos mil diecinueve, para concluir el día 29-veintinueve de septiembre de 2021-dos mil veintiuno.

QUINTA.- (GARANTÍA DE CUMPLIMIENTO) A fin de garantizar el cumplimiento de todas y cada una de las obligaciones que se establecen en el presente Contrato, **"EL PRESTADOR DE SERVICIOS"** se obliga a otorgar a favor de la Tesorería Municipal de Monterrey, la siguiente Póliza de Fianza:

Una Póliza de Fianza que garantice el cumplimiento de Contrato, misma que deberá ser expedida por una Institución legalmente constituida en los términos de la Ley de Instituciones de Seguros y Fianzas, invariablemente a más tardar dentro de los 10-diez días hábiles siguientes a la formalización del o los Contratos respectivos, por un importe equivalente al 20%-veinte por ciento del monto total del Contrato, incluido el Impuesto al Valor Agregado.

La Póliza de Fianza deberá contener, además de lo señalado en la Ley de Instituciones de Seguros y Fianzas; las siguientes declaraciones:

a) Que se otorga a favor de la Tesorería Municipal de Monterrey;
b) Que la Fianza se otorga para garantizar todas y cada una de las estipulaciones contenidas en el Contrato;
c) Que la Fianza continuará vigente en caso de que se otorguen prórrogas al cumplimiento del Contrato;
d) Que la Fianza permanecerá vigente durante la substanciación de todos los recursos legales o Juicios que se interpongan, hasta que se dicte la Resolución definitiva por Autoridad competente;
e) Que para la liberación de la Fianza será requisito indispensable la manifestación expresa y por escrito del Municipio de Monterrey, a través de la Dirección de

Adquisiciones de la Secretaría de Administración, previa validación de cumplimiento total de la Dirección de Informática de la Secretaría de Administración;

f) Que la Afianzadora acepta expresamente someterse a los Procedimientos de ejecución previstos en la Ley de Instituciones de Seguros y Fianzas para la efectividad de la Fianza, aun para el caso de que procediera el cobro de intereses, con motivo del pago extemporáneo del importe de la Póliza de Fianza requerida.

A elección de **"EL MUNICIPIO"** podrá reclamarse el pago de la Fianza por cualquiera de los Procedimientos establecidos en los artículos 279, 280, 282, y 283 de la Ley de Instituciones de Seguros y Fianzas, asimismo, para que no se extinga la fianza, la Institución Afianzadora otorga su consentimiento en caso de prórroga o espera concedida por **"EL MUNICIPIO"** a **"EL PRESTADOR DE SERVICIOS"**, lo anterior de conformidad con el artículo 179 de la Ley de Instituciones de Seguros y Fianzas.

Las partes convienen en que la garantía tendrá vigencia hasta que se cumpla el término de vigencia del presente Contrato. Lo anterior en la inteligencia que para la cancelación y devolución de la misma deberá mediar autorización por escrito de la Dirección de Informática de la Secretaría de Administración, previa solicitud por escrito de **"EL PRESTADOR DE SERVICIOS"** en el momento que demuestre plenamente haber cumplido con la totalidad de las obligaciones establecidas en el presente Contrato.

SEXTA.- (EJECUCIÓN DE LA GARANTÍA) En caso de incumplimiento de la prestación de los servicios objeto de este Contrato, en los plazos establecidos u ofrecidos, o en caso de no prestarse los servicios a los cuales se comprometen, no se cumplan las especificaciones técnicas establecidas, o cualquier otra causa imputable a **"EL PRESTADOR DE SERVICIOS", "EL MUNICIPIO",** hará efectiva la garantía consignada a su favor dentro de la Cláusula que antecede, lo anterior sin demérito de la aplicación de la pena convencional que se fija dentro del presente Contrato.

La garantía se hará efectiva también, en caso de manifestación de defectos en la prestación de los servicios que se adquiere tales como calidad deficiente derivada de la falta de cumplimiento de las especificaciones o características técnicas establecidas en este Contrato.

SÉPTIMA.- (PLAZO, LUGAR Y CONDICIONES DE LA PRESTACIÓN DE LOS SERVICIOS) **"EL PRESTADOR DE SERVICIOS"** se obliga a llevar a cabo los servicios profesionales descritos en el presente Contrato, en un plazo contemplado a partir del día 01-uno de abril de 2019-dos mil diecinueve, para concluir los servicios el día 29-veintinueve de septiembre de 2021-dos mil veintiuno, cumpliendo con la totalidad de las características y especificaciones contenidas en el presente instrumento jurídico.

OCTAVA.- (ENTREGABLES) "EL PRESTADOR DE SERVICIOS" además de las obligaciones contenidas en el presente contrato, se obliga a:

- Entrega de Reporte en detalle de las actualizaciones y el soporte realizado al sistema, llevados a cabo en el mes inmediato anterior y deberá contener:
  - Detección y registro de incidentes
  - Investigación y diagnóstico de la problemática atendida
  - Resolución

- Cierre del incidente
- Encuesta de servicio

➢ La entrega se hará de manera mensual y de forma indubitable, a más tardar dentro de los primeros 10-diez días naturales de cada mes, en la Dirección de Informática de la Secretaría de Administración.

NOVENA.- (CASOS DE RECHAZO) Si durante la realización de los servicios se identifican defectos, daños u otros aspectos que afecten el funcionamiento y duración, así como el que los mismos no cumplan con las características especificadas en el presente contrato, **"EL MUNICIPIO"** procederá a no aceptar los servicios, obligándose **"EL PRESTADOR DE SERVICIOS"** a realizar y entregar nuevamente el 100%-cien por ciento de los servicios rechazados en un plazo no mayor a 05-cinco días naturales, con las características y especificaciones contenidas en el presente instrumento, sujetándose a la inspección y autorización de los servicios a realizar por parte de la Dirección de Informática de la Secretaría de Administración, por lo anterior, no se exime a **"EL PRESTADOR DE SERVICIOS"** de la sanción que resulte aplicable por retraso en la entrega.

DÉCIMA.- (PRÓRROGAS) "EL PRESTADOR DE SERVICIOS", podrá solicitar prórroga en la prestación de los servicios objeto del presente Contrato solamente en el siguiente supuesto:

a) Fuerza mayor o caso fortuito, entendiéndose como tal lo señalado en la legislación aplicable;

En el supuesto descrito en la presente Cláusula no procederá aplicar a **"EL PRESTADOR DE SERVICIOS",** penas convencionales por atraso.

DÉCIMA PRIMERA.- (RESCISIÓN) "EL MUNICIPIO" rescindirá administrativamente el Contrato cuando **"EL PRESTADOR DE SERVICIOS"** no cumpla con las condiciones establecidas en el mismo, sin necesidad de acudir a los Tribunales competentes en la materia, por lo que de manera enunciativa, mas no limitativa, se entenderá por incumplimiento: la no prestación de los servicios en las fechas establecidas en el presente instrumento jurídico, o en el plazo adicional que **"EL MUNICIPIO"** haya otorgado a **"EL PRESTADOR DE SERVICIOS"** para llevar a cabo el objeto del presente contrato.

Adicional a lo anterior, se podrá rescindir el Contrato por las siguientes causas:

a) No iniciar los trabajos objeto del Contrato dentro de los 15-quince días naturales siguientes a la fecha de la firma del Contrato;
b) Interrumpir injustificadamente la prestación de los servicios;
c) No prestar los servicios de conformidad con lo estipulado en el Contrato;
d) No hacer entrega sin justificación alguna de las garantías que al efecto se señalen en los Contratos derivados de los procedimientos de contratación regulados por la Ley y su Reglamento;
e) No dar cumplimiento a los programas pactados en el Contrato para la prestación del servicio de que se trate sin causa justificada;
f) No hacer del conocimiento de la Dirección de Adquisiciones de la Secretaría de Administración o de la Tesorería Municipal que fue declarado en concurso mercantil o alguna figura análoga;

g) Cuando **"EL PRESTADOR DE SERVICIOS"** ceda total o parcialmente, bajo cualquier título, los derechos y obligaciones a que se refiere el Contrato, con excepción de los derechos de cobro, en cuyo caso se debe contar con el consentimiento de **"EL MUNICIPIO"**;
h) No dar a la autoridad competente las facilidades y datos necesarios para la inspección, vigilancia y supervisión de los materiales y trabajos;
i) Cambiar su nacionalidad por otra, en el caso de que haya sido establecido como requisito tener una determinada nacionalidad;
j) Incumplir con el compromiso que, en su caso haya adquirido al momento de la suscripción del Contrato, relativo a la reserva y confidencialidad de la información y documentación proporcionada por el sujeto obligado para la ejecución de los trabajos.

Lo anterior, en la inteligencia de que **"EL PRESTADOR DE SERVICIOS"** tendrá la obligación de reparar los daños y perjuicios que se causen a **"EL MUNICIPIO"**, en caso de incurrir en cualquiera de los supuestos anteriormente mencionados, y a causa de ello, opere la rescisión de este Contrato.

La Dirección de Adquisiciones de la Secretaría de Administración, iniciará el Procedimiento de Rescisión, comunicando por escrito a **"EL PRESTADOR DE SERVICIOS"**, del incumplimiento en que haya incurrido, para que dentro de un término de 05-cinco días hábiles contados a partir del día hábil siguiente al en que se le entregó el escrito, exponga lo que a su derecho convenga y aporte, en su caso, las pruebas que estime pertinentes.

Transcurrido dicho plazo se resolverá en el término de 15-quince días hábiles, contados a partir de que **"EL PRESTADOR DE SERVICIOS"** haya expuesto lo que a su derecho convenga, considerando los argumentos y pruebas que se hubieren hecho valer, por parte de **"EL PRESTADOR DE SERVICIOS"**.

DÉCIMA SEGUNDA.- (LICENCIAS, AUTORIZACIONES Y PERMISOS) "EL PRESTADOR DE SERVICIOS" se obliga a asumir directamente la responsabilidad por el trámite y obtención de todos los permisos y licencias que resulten necesarios para llevar el debido cumplimiento de este Contrato y demás elementos necesarios cuando se trate de resarcir algún daño, liberando a **"EL MUNICIPIO"** de cualquier sanción económica o legal que pudiere darse por la carencia de dichas autorizaciones o irregularidades generadas.

DÉCIMA TERCERA.- (PENA CONVENCIONAL) En caso de que se incumpla cualquiera de los plazos establecidos en la prestación de los servicios objeto del presente instrumento por causas imputables a **"EL PRESTADOR DE SERVICIOS"**, debidamente probadas por **"EL MUNICIPIO"** y que se adquieren según lo estipulado dentro de las especificaciones y características técnicas y económicas ofertadas por **"EL PRESTADOR DE SERVICIOS"** deberá pagar como pena convencional a **"EL MUNICIPIO"**, la cantidad equivalente al 2%-dos por ciento, por cada día natural de mora, respecto de la entrega de los bienes o la prestación de los servicios contratados. Para dicho efecto se contabilizarán los días de retraso que hayan transcurrido en la entrega de los bienes y/o servicios.

a) Las penas se harán efectivas descontándose del pago que **"EL PRESTADOR DE SERVICIOS"** tenga pendiente en **"EL MUNICIPIO"**, independientemente que se hagan efectivas las garantías otorgadas.

DÉCIMA CUARTA.- (PROPIEDAD INTELECTUAL) Ambas partes acuerdan que **"EL PRESTADOR DE SERVICIOS",** es el único responsable en caso de violaciones en materia de derechos inherentes a la propiedad intelectual. Salvo que exista impedimento o así convengan a los intereses de **"EL MUNICIPIO",** la estipulación de que los derechos inherentes a la propiedad intelectual, que se deriven de los servicios de consultorías, asesorías, estudios e investigaciones contratados, invariablemente se constituirán a favor de **"EL MUNICIPIO",** en los términos de las disposiciones legales aplicables, obligándose **"EL PRESTADOR DE SERVICIOS"**, a llevar a cabo todos los procesos legales y administrativos necesarios para cumplir con dicha obligación.

DÉCIMA QUINTA.- (MODALIDAD DE PAGO) "EL PRESTADOR DE SERVICIOS", deberá de presentar la documentación completa y debidamente requisitada para realizar el pago correspondiente en:

a) Factura original a favor del Municipio de la Ciudad de Monterrey, en que deberá presentarse el Impuesto al Valor Agregado, dicho documento deberá ser validado por la Dirección de Informática de la Secretaría de Administración;
b) Copia del acuse de recibo de la garantía de cumplimiento del Contrato;
c) Los documentos que acrediten la prestación de servicios.

Dicha documentación deberá presentarse en la Dirección de Adquisiciones de la Secretaría de Administración, ubicada en el Segundo piso del Palacio Municipal de la Ciudad de Monterrey, sito en la calle Zaragoza Sur s/n, Zona Centro en la Ciudad de Monterrey, Nuevo León.

La fecha de pago no excederá de 45-cuarenta y cinco días naturales posteriores a la presentación de la documentación respectiva, previa validación de la factura y/o recibo de honorarios correspondiente por la Dirección de Informática de la Secretaría de Administración, la cual avala la comprobación de la prestación de los servicios contratados, siendo aceptada y autorizada por la Tesorería Municipal.

En caso de que **"EL PRESTADOR DE SERVICIOS"** no presente en tiempo y forma la documentación requerida, la fecha de pago se recorrerá el mismo número de días que dure el retraso.

El pago se efectuará por parte de la Dirección de Egresos de la Tesorería Municipal de Monterrey, previa entrega de la documentación correspondiente, para lo cual es necesario que la factura que presente **"EL PRESTADOR DE SERVICIOS"** reúna los requisitos fiscales que establece la Legislación vigente en la materia, en caso de no ser así, **"EL MUNICIPIO"** no gestionará el pago a **"EL PRESTADOR DE SERVICIOS",** hasta en tanto no se subsanen dichas omisiones.

DÉCIMA SEXTA.- (SUBCONTRATACIÓN) "EL PRESTADOR DE SERVICIOS" se obliga a prestar los servicios objeto del presente instrumento jurídico, por lo cual acepta que todos los derechos y obligaciones a su cargo, no podrán ser subcontratados, cedidos, vendidos o transmitidos a terceros en ninguna forma y bajo ninguna circunstancia, respondiendo en forma única y directa ante **"EL MUNICIPIO"** por todas y cada una de las obligaciones que se establecen en el presente Contrato.

GOBIERNO DE
MONTERREY

DÉCIMA SÉPTIMA.- (TERMINACIÓN ANTICIPADA) Ambas partes manifiestan estar de acuerdo en que **"EL MUNICIPIO"** podrá dar por terminado el presente Contrato en cualquier momento, dando aviso por escrito y de forma fehaciente, cuando menos con 15-quince días naturales de anticipación, sin que ello genere para ninguna de las partes contratantes obligación de satisfacer daños y perjuicios que pudiera causarse.

Adicional a lo señalado en el párrafo anterior y de manera enunciativa mas no limitativa, **"EL MUNICIPIO"** podrá dar por terminado anticipadamente el presente Contrato, en los siguientes casos:

a) Cuando concurran razones de interés general, o bien, cuando por causas justificadas se extinga la necesidad de requerir los servicios que se contratan y se demuestre que, de continuar con el cumplimiento del Contrato, se ocasionaría un daño o perjuicio a **"EL MUNICIPIO"**;
b) Por mutuo acuerdo de las partes;
c) Por el incumplimiento de las obligaciones contraídas por las partes;
d) Por rescisión.

DÉCIMA OCTAVA.- (NORMAS DE CALIDAD) "EL PRESTADOR DE SERVICIOS" se obliga al cumplimiento de las Normas Oficiales Mexicanas aplicables, Normas Mexicanas y a falta de estas, las Normas Internacionales o, en su caso, las normas de referencia o especificaciones, de acuerdo con las características y especificaciones técnicas de los servicios prestados objeto del presente Contrato.

DÉCIMA NOVENA.- (SUSPENSIÓN Y/O RENUNCIA DEL SERVICIO) Si **"EL PRESTADOR DE SERVICIOS"**, a su solo juicio y en cualquier momento, suspende la prestación de los servicios mediante los cuales fue adjudicado será sujeto a las siguientes condicionantes:

a) **"EL PRESTADOR DE SERVICIOS"** deberá cumplir plenamente con los requerimientos que le fueron solicitados antes de llevar a cabo la suspensión;
b) **"EL PRESTADOR DE SERVICIOS"** deberá pagar a **"EL MUNICIPIO"**, por la opción de suspensión y/o renuncia, los montos correspondientes al 100%-cien por ciento de la parte no ejercida del monto adjudicado o en su defecto, del monto de suficiencia presupuestal autorizado para el ejercicio fiscal según corresponda;
c) **"EL MUNICIPIO"** ejecutará las Garantías para cobrar los montos correspondientes al 100%-cien por ciento de la parte no ejercida del monto adjudicado o en su defecto, del monto de suficiencia presupuestal autorizado para el ejercicio fiscal según corresponda.

Ambas partes manifiestan que todas las obligaciones a cargo de **"EL PRESTADOR DE SERVICIOS"**, se encuentran insertas en el presente instrumento jurídico, por lo que deberán de ser cumplidas en la forma y términos previstos en el Contrato y la no realización de los mismos, hará incurrir a **"EL PRESTADOR DE SERVICIOS"** en incumplimiento del Contrato en forma automática y de pleno derecho, sin necesidad de notificación, requerimiento o interpelación de ninguna índole, y deberá de cubrir a **"EL MUNICIPIO"**, los gastos señalados en los inciso b) y c) del párrafo anterior de la presente Cláusula.

VIGÉSIMA.- (CONFIDENCIALIDAD) "EL MUNICIPIO" y **"EL PRESTADOR DE SERVICIOS"** son conscientes de que, en el presente Contrato, tanto los empleados de "**EL PRESTADOR DE SERVICIOS**" como asimismo los servidores públicos de "**EL MUNICIPIO**" podrán tener acceso a información en posesión, la cual a todo efecto deberá ser considerada como confidencial y/o reservada y en tal virtud no divulgable a ningún tercero (en adelante "**LA INFORMACIÓN"**).

En tal sentido, **"EL MUNICIPIO"** y **"EL PRESTADOR DE SERVICIOS"** convienen en no divulgar ni transferir a terceros, sin previa autorización por escrito del titular de **"LA INFORMACIÓN"**, cualquier información que se reciba, ya sea verbal, escrita, almacenada, en forma magnética o se genere con relación a las acciones y los trabajos que se desarrollen para alcanzar el objeto del presente Contrato.

"EL MUNICIPIO" y **"EL PRESTADOR DE SERVICIOS"** podrán divulgar **"LA INFORMACIÓN"**, total o parcialmente, sólo a aquellos empleados y funcionarios que tuvieren necesidad de conocerla exclusivamente a efecto de que puedan cumplir con sus obligaciones bajo este instrumento jurídico, comprometiéndose a tomar todas las medidas necesarias para que dichos empleados y funcionarios estén advertidos de la naturaleza confidencial de **"LA INFORMACIÓN"**. La divulgación a cualquier otra persona queda estrictamente prohibida salvo consentimiento por escrito de **"EL MUNICIPIO"**.

"EL MUNICIPIO" y **"EL PRESTADOR DE SERVICIOS"** se comprometen a que el manejo de **"LA INFORMACIÓN"** derivada del presente Contrato deberá de cumplir con lo señalado en la Ley de Transparencia y Acceso a la Información Pública del Estado de Nuevo León en materia de protección de datos de carácter personal, en particular, con las medidas de seguridad físicas, técnicas y administrativas de sus sistemas.

VIGÉSIMA PRIMERA.- (IMPUESTOS Y DERECHOS) Ambas partes acuerdan que los impuestos y derechos federales o locales que se causen, derivados de la realización del presente instrumento jurídico, serán erogados por **"EL PRESTADOR DE SERVICIOS"**, **"EL MUNICIPIO"** solo cubrirá el Impuesto al Valor Agregado, de conformidad con la Ley vigente en la materia.

VIGÉSIMA SEGUNDA.- (RESPONSABILIDAD TOTAL) "EL PRESTADOR DE SERVICIOS" asumirá la responsabilidad total para el caso de que, al suministrar los servicios 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.

VIGÉSIMA TERCERA.- (SUPERVISIÓN) "EL PRESTADOR DE SERVICIOS" acepta estar sujeto a la supervisión de la calidad de los servicios y a la inspección física de sus instalaciones que en todo tiempo se realice cada vez que **"EL MUNICIPIO"** lo estime necesario, a fin de verificar el debido cumplimiento de las normas oficiales que correspondan, licencias, autorizaciones y permisos a que deba sujetarse **"EL PRESTADOR DE SERVICIOS"**, dentro de su ámbito de acción comercial y profesional, sin que lo anterior implique responsabilidad alguna para la misma, la falta de cumplimiento del servicio o de las condiciones ofertadas será motivo de rescisión así como la aplicación de las sanciones correspondientes, lo anterior de conformidad con lo señalado en el artículo 78 de la Ley de Adquisiciones, Arrendamientos y Contratación de Servicios del Estado de Nuevo León y en el artículo 120 de su Reglamento.

VIGÉSIMA CUARTA.- (RELACIÓN LABORAL) Queda expresamente estipulado que el personal operativo que cada una de las partes asigne para llevar a cabo la prestación del servicio, estarán bajo la responsabilidad directa del que lo haya contratado, por lo que ninguna de las partes, serán considerados como patrón sustituto del personal de la otra.

En razón de lo anterior, **"EL MUNICIPIO"** no tendrá relación alguna de carácter laboral con dicho personal y por lo mismo, **"EL PRESTADOR DE SERVICIOS"** lo exime de toda responsabilidad o reclamación que pudiera presentarse en materia de trabajo y seguridad social.

VIGÉSIMA QUINTA.- (DEL PERSONAL) "EL PRESTADOR DE SERVICIOS" se compromete a que el personal a su cargo, designado para la prestación de servicios, los efectuará de manera eficiente y adecuada, mismos que deberán estar plenamente identificados para ello al encontrarse en las instalaciones de **"EL MUNICIPIO"**, además su personal será el único responsable de los daños y perjuicios que sean ocasionados al mismo, excluyendo de cualquier responsabilidad o riesgo a **"EL MUNICIPIO".**

VIGÉSIMA SEXTA.- (SUBSISTENCIA DEL CONTRATO) Los contratantes están de acuerdo en que, si durante la vigencia del Contrato **"EL PRESTADOR DE SERVICIOS"** por cualquier causa cambiara su domicilio o denominación social actual por alguna otra, el presente Contrato subsistirá en los términos establecidos, comprometiéndose **"EL PRESTADOR DE SERVICIOS"**, a notificar de inmediato tal circunstancia a **"EL MUNICIPIO"**.

VIGÉSIMA SÉPTIMA.- (MODIFICACIONES) Los actos y omisiones de las partes en relación al presente Contrato, no podrán en forma alguna interpretarse como una modificación al sentido o espíritu del mismo, es decir, para que el presente Contrato pueda ser modificado, será necesario e indispensable el acuerdo por escrito y firmado de ambas partes, siempre que el monto total de la modificación no rebase, en conjunto, el 20%-veinte por ciento de los conceptos y volúmenes establecidos originalmente en los mismos, y el precio de los servicios sea igual al originalmente pagado.

VIGÉSIMA OCTAVA.- (SUBTÍTULOS) Las partes acuerdan que los subtítulos en este Contrato son exclusivamente para referencia, por lo que no se considerarán para efectos de interpretación o cumplimiento del mismo.

VIGÉSIMA NOVENA.- (LEGISLACIÓN APLICABLE) En caso de suscitarse alguna controversia en relación a la interpretación o cumplimiento del presente Contrato, las partes están de acuerdo y convienen en sujetarse a los ordenamientos legales vigentes en el Estado de Nuevo León.

TRIGÉSIMA.- (TRIBUNALES COMPETENTES) Sin perjuicio de lo estipulado en la cláusula **DÉCIMA PRIMERA** de este Contrato, y sin renunciar **"EL MUNICIPIO"** al procedimiento administrativo de existir causa de rescisión ambas partes están de acuerdo en someterse y sujetarse a la competencia de los Tribunales de la Ciudad de Monterrey, Nuevo León, en caso de surgir alguna controversia relacionada con el cumplimiento o incumplimiento del presente Contrato, renunciando para ello a la competencia que por razón de su lugar, fuero o cualquier otro motivo pudiera corresponderles.

Enteradas las partes del contenido y alcance legal del presente Contrato, el cual consta de 23-veintitrés fojas, manifiestan que no existe impedimento legal o vicio alguno de voluntad o de consentimiento que pudiera invalidarlo, lo firman de conformidad el día 01-uno de abril de 2019-dos mil diecinueve, en la Ciudad de Monterrey, Nuevo León.

POR **"EL MUNICIPIO"**

C. HÉCTOR ANTONIO GALVÁN ANCIRA
DIRECTOR JURÍDICO
DE LA SECRETARÍA DEL AYUNTAMIENTO

C. ALAN GERARDO GONZÁLEZ SALINAS
DIRECTOR DE ADQUISICIONES
DE LA SECRETARÍA DE ADMINISTRACIÓN

C. JUAN CARLOS PASTRANA GARCÍA
DIRECTOR DE EGRESOS
DE LA TESORERÍA MUNICIPAL DE MONTERREY

C. ELVIRA YAMILETH LOZANO GARZA
SECRETARIA DE ADMINISTRACIÓN

C. RAFAEL IVÁN RICO GARCÍA
ENCARGADO DE LA DIRECCIÓN DE INFORMÁTICA
DE LA SECRETARÍA DE ADMINISTRACIÓN

POR **"EL PRESTADOR DE SERVICIOS"**

C. ELÍAS TREVIÑO BENAVIDES
REPRESENTANTE LEGAL
MCS NETWORK SOLUTION, S.A. DE C.V.

ÚLTIMA HOJA DE 23-VEINTITRÉS DEL **CONTRATO DE PRESTACIÓN DE SERVICIOS DE RENOVACIÓN DE LICENCIAS DE SEGURIDAD PARA LA PROTECCIÓN DE BIENES TECNOLÓGICOS INFORMÁTICOS**, QUE CELEBRAN POR UNA PARTE EL MUNICIPIO DE MONTERREY, NUEVO LEÓN Y LA PERSONA MORAL DENOMINADA **MCS NETWORK SOLUTION, S.A. DE C.V.**, EN FECHA DEL DÍA 01-UNO DE ABRIL DE 2019-DOS MIL DIECINUEVE.