Contrato de Adquisición de Equipo de Cómputo y Tecnología de la Información para la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Jalisco, que celebran por una parte, el Organismo Público Descentralizado denominado **Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Jalisco,** representado legalmente por su Titular la **Dra. Haimé Figueroa Neri,** asistida en este acto por la **Lic. Martha Iraí Arriola Flores Coordinadora Administrativa,** a quienes en conjunto y en representación del Organismo, en lo sucesivo se les denominará como **"LA SECRETARÍA"** y por la otra parte, la empresa denominada **SERVICIO DIVERGENTES EN TECNOLOGÍA, S.A. de C.V." representada en este acto por el C. Gustavo Soto Valencia,** a quien en lo sucesivo se le denominará como **"EL PROVEEDOR"**; y cuando se refiera a ambos contratantes se les denominará como **"LAS PARTES"**, los cuales se sujetan al tenor de las siguientes declaraciones y cláusulas:

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

I.- DECLARA "LA SECRETARÍA":

I.1.- Que es un organismo público descentralizado, no sectorizado, con personalidad jurídica y patrimonio propio, con autonomía técnica y de gestión, de conformidad con el artículo 24 de la Ley del Sistema Anticorrupción del Estado de Jalisco.

Que así mismo su representante cuenta con las facultades legales para suscribir el presente instrumento, de conformidad en los artículos 24 y 25 de Ley del Sistema Anticorrupción del Estado de Jalisco, artículos 78 punto 1 fracciones I, II inciso a), y III de la Ley Orgánica del Poder Ejecutivo del Estado de Jalisco, y artículos 18 fracción I y 30 fracción XIII del Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Jalisco.

I.2.- Que la **Dra. Haimé Figueroa Neri,** fue designada como Secretaria Técnica a partir del 01 de febrero de 2018, por lo que es la representante legal de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Jalisco.

I.3.- Que el Órgano de Gobierno del Organismo citado en su primera sesión de fecha 29 de enero del 2019, aprobó el Presupuesto de Egresos para el ejercicio 2019, por lo tanto, cuenta con los recursos suficientes para cubrir el importe del servicio contratado, conforme a la partida presupuestal **partida presupuestal 515 Equipo de cómputo y de tecnología de la información.**

I.4.- Que resulta procedente celebrar la presente contratación con **"EL PROVEEDOR"** de acuerdo a la Resolución de Adjudicación derivada del Proceso de Licitación Pública Local, **con concurrencia del Comité LSCC-10-SESEAJAL-DTP/2019, de fecha 16 dieciséis de agosto de 2019 dos mil diecinueve.**

I.5.- Que para efectos de este Contrato, señala como su domicilio el ubicado en **Av. de los Arcos, número 767, Colonia Jardines del Bosque, Guadalajara, Jalisco, México, Código Postal 44520.**

II.- DECLARA "EL PROVEEDOR", por medio de su apoderado legal por medio de su apoderado legal Gustavo Soto Valencia:

1 [redacted]

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

II.1.- Que acredita su existencia legal de la sociedad que representa, mediante la escritura pública número 3,153 tres mil ciento cincuenta y tres, de fecha 30 treinta de noviembre del 2015 dos mil quince, otorgada ante la fe del notario público número 132 ciento treinta y dos Lic. Ramiro Ruíz Casillas, de la Municipalidad de Guadalajara, Jalisco.

II.2.- Que tiene por objeto sustancial Diseño, desarrollo, aplicación, venta, distribución e instalación de sistemas de computación en general, así como la comercialización de paquetes computacionales, servicios de ingeniería, administración de proyectos, servicios de análisis y de investigación industrial, compraventa de todo tipo de maquinaria, herramienta, equipo, programas de computación (software), así como crear, otorgar, innovar, obtener, aprovechar, registrar y explotar por cualquier titulo legal toda clase de concesiones, permisos, licencias referentes a tecnología y asistencia técnica, patentes de invención, modelos de utilidad, diseños y secretos industriales, marcas, denominaciones de origen, avisos, nombres comerciales.

II.3.- Que es apoderado legal, de **"EL PROVEEDOR"**, el cual acredita su representación mediante escritura pública número 13,624 trece mil seiscientos veinticuatro, de fecha 16 dieciséis de octubre del 2018 dos mil dieciocho, otorgada ante la fe del Licenciado Ricardo Salvador Rodríguez Vera, Notario Público Titular de la Notaria número 34 treinta y cuatro de Zapopan, Jalisco, manifestando **"BAJO PROTESTA DE DECIR VERDAD"**, que las facultades conferidas no le han sido modificadas ni revocadas en forma alguna y lo dejan en capacidad legal para celebrar el presente contrato a través de su poderdante.

II.4.- Que cuenta con Registro Federal de Contribuyentes **SDT151203G75**, otorgado por el Servicio de Administración Tributaria de la Secretaría de Hacienda y Crédito Público, y bajo protesta de decir verdad manifiesta que no cuenta con contratos incumplidos y/o sanciones aplicadas a la misma.

II.5.- Se identifica con credencial para votar vigente con clave de elector número 2 [redacted] expedida por el Instituto Nacional Electoral, con fecha de vigencia hasta el año 2022.

II.6.- "EL PROVEEDOR", manifiesta bajo protesta de decir verdad que se encuentra al corriente de sus obligaciones fiscales.

II.7.- Para los efectos del presente contrato señala como su domicilio el ubicado en la **Calle Rio Tequila número 710, Colonia Las Águilas, Zapopan, Jalisco, México, Código Postal 45080.**

III.- LAS PARTES declaran que:

III.1.- Que en la prestación del servicio objeto del presente contrato, atenderá a las obligaciones que deriven de este instrumento, la propuesta de **"EL PROVEEDOR"** y las bases del procedimiento de licitación **LSCC-10-SESEAJAL-DTP/2019.**

III.2 El presente contrato se sustenta en los artículos 1850,1851, 1855 y 1863 y demás relativos del Código Civil del Estado de Jalisco, así como el numeral 17 y 18 fracción II, 19, 56 y 57 de las Políticas, bases y Lineamientos para la adquisición, enajenación, arrendamiento de bienes, contratación de servicios y manejo de almacenes de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Jalisco, por 1 [redacted]

Se eliminan los datos 1, (firma) 2 (clave de elector) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

no existe ninguna relación de subordinación entre las partes.

"LAS PARTES" acuerdan someterse a lo establecido en las siguientes:

C L Á U S U L A S.-

PRIMERA.- EI objeto del presente contrato lo constituye la Adquisición de Equipo de Sistema de Seguridad Perimetral (UTM) para la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Jalisco, por parte de **"EL PROVEEDOR"** en favor de **"LA SECRETARÍA",** conforme a la **partida 04 de las bases del** Proceso de Licitación Pública Local, **con concurrencia del Comité LSCC-10-SESEAJAL-DTP/2019, de fecha 16 dieciséis de agosto de 2019 dos mil diecinueve,** que a continuación se describen:
PARTIDA 4.

1 EQUIPO DE SISTEMA DE SEGURIDAD PERIMETRAL (UTM)

Sistema de control de seguridad perimetral con las siguientes características:

- El dispositivo debe ser un equipo (appliance) de propósito específico.
- Basado en tecnología de circuito integrado para aplicaciones específicas y que sea capaz de brindar una solución de "complete content protection". por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (pcs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, freebsd, sun solaris, apple os-x o gnu/linux, entre otros.
- Capacidad de incrementar el rendimiento de vpn a través de soluciones en hardware dentro del mismo dispositivo.
- Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware.
- El equipo deberá poder ser configurado en modo gateway) o en modo transparente en la red.
- El equipo debe contar con un throughput firewall de al menos 7 gbps aplica tanto para tráfico ipv4 como ipv6.
- El equipo debe contar con un throughput vpn ipsec de por lo menos 4 gbps.
- El equipo debe contar con un throughput vpn ssl de por lo menos 250 mbps.
- El equipo debe contar con un throughput ips de al menos 1.9 gbps.
- El equipo debe contar con un throughput de protección contra malware de al menos 250 mbps.
- El equipo debe contar con al menos 2 millones de sesiones concurrentes
- El equipo debe soportar 30,000 nuevas sesiones por segundo.
- El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 300 usuarios de vpn ssl.
- El equipo debe poder generar al menos 10,000 vpn's ipsec client to gateway y 2,000 vpn's ipsec gateway to gateway.
- El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 10 virtual firewalls.
- El equipo debe contar con al menos 14 interfaces gigaethernet rj45.
- El equipo debe contar con al menos 1 interfaz gigaethernet rj45 para administración.

1 [redacted]

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

- El equipo debe contar con al menos 2 interfaces gigaethernet rj45 para alta disponibilidad.
- El equipo debe contar con al menos 1 interfaz gigaethernet rj45 para dmz
- El equipo debe soportar al menos 64 access points físicos.
- El equipo deberá de soportar las funcionalidades siguientes firewall, ruteo, vpn, traffic shapping/QoS, IPS, DLP, control de aplicaciones, inspección de contenido SSL, antivirus, antispam, URL filtering.

Firewall

- Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o zonas) y vlans.
- Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
- Las reglas del firewall deberán tomar en cuenta dirección ip fuente (que puede ser un grupo de direcciones ip), dirección ip destino (que puede ser un grupo de direcciones ip) y servicio (o grupo de servicios) de la comunicación que se está analizando.
- Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación.
- Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones ip fuente, dirección ip destino.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año).
- Debe soportar la capacidad de definir nuevos servicios tcp y udp que no estén contemplados en los predefinidos.
- Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (tcp y udp).
- Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
- Capacidad de hacer traslación de direcciones dinámico, muchos a uno, pat.
- Deberá soportar reglas de firewall en ipv6 configurables tanto por cli (command line interface, interface de línea de comando) como por GUI (graphical user interface, interface gráfica de usuario).

Conectividad y sistema de ruteo

- Funcionalidad integrada de dhcp: como cliente dhcp, servidor dhcp y reenvío (relay) de solicitudes dhcp.
- Soporte a etiquetas de vlan (802.1q) y creación de zonas de seguridad en base a vlans.
- Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
- Soporte a políticas de ruteo (policy routing).
- El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace.
- Soporte a ruteo dinámico rip v1, v2, ospf, bgp y is-is.

1 [redacted]

- Soporte a ruteo dinámico ripng, ospfv3, bgp4+.
- Soporte a ruteo de multicast.

VPN IPSEC/L2TP/PPTP

- Soporte a certificados pki x.509 para construcción de vpns cliente a sitio (client-to-site).
- Soporte de vpns con algoritmos de cifrado: aes, des, 3des.
- Se debe soportar longitudes de llave para aes de 128, 192 y 256 bits.
- Se debe soportar al menos los grupos de diffie-hellman 1, 2, 5 y 14.
- Se debe soportar los siguientes algoritmos de integridad: md5, sha-1 y sha256.
- Posibilidad de crear vpn's entre gateways y clientes con ipsec. esto es, vpns ipsec site-to-site y vpns ipsec client-to-site.
- La vpn ipsec deberá poder ser configurada en modo interface (interface-mode vpn).
- En modo interface, la vpn ipsec deberá poder tener asignada una dirección ip, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.

VPN SSL

- Capacidad de realizar ssl vpns.
- Soporte a certificados pki x.509 para construcción de vpns ssl.
- Soporte de autenticación de dos factores. en este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de vpn.
- Soporte de renovación de contraseñas para ldap y radius.
- Soporte a asignación de aplicaciones permitidas por grupo de usuarios
- Soporte nativo para al menos http, ftp, smb/cifs, vnc, ssh, rdp y telnet.
- Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación vpn ssl.
- Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning).
- La vpn ssl integrada deberá soportar a través de algún plug-in activex y/o java, la capacidad de meter dentro del túnel ssl tráfico que no sea http/https
- Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la vpn ssl.
- Deberá soportar la redirección de página http a los usuarios que se registren en la vpn ssl, una vez que se hayan autenticado exitosamente.

Traffic shapping / QoS

- Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall.
- Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión.
- Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección ip en forma independiente, en contraste con la aplicación de las mismas para la regla en general.

1 [redacted]

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo

- Capacidad de poder definir ancho de banda garantizado en kilobytes por segundo.
- Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en kilobytes por segundo.
- Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.

Autenticación y certificación digital

- Capacidad de integrarse con servidores de autenticación radius.
- Capacidad nativa de integrarse con directorios ldap.
- Capacidad incluida, al integrarse con microsoft windows active directory o novell edirectory, de autenticar transparentemente usuarios sin preguntarles username o password. esto es, aprovechar las credenciales del dominio de windows bajo un concepto "single-sign-on".
- Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos tcp/udp/icmp. debe de mostrar solicitud de autenticación (prompt) al menos para web (http), ftp y telnet.
- Soporte a certificados pki x.509 para construcción de vpns cliente a sitio (client-to-site).

Protección contra intrusos (IPS)

- El detector y preventor de intrusos podrá implementarse en línea y fuera de línea en forma simultánea para distintos segmentos.
- Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico ipv6.
- Capacidad de detección de más de 4,000 ataques.
- Capacidad de actualización automática de firmas ips mediante tecnología de tipo "push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (consultar los centros de actualización por versiones nuevas).
- El detector y preventor de intrusos deberá de estar orientado para la protección de redes.
- El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". sin necesidad de instalar un servidor o "appliance" externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. la interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad "appliance", sin necesidad de integrar otro tipo de consola para poder administrar este servicio. esta deberá permitir la protección de este servicio por política de control de acceso.
- El detector y preventor de intrusos deberá soportar captar ataques por anomalía (anomaly detection) además de firmas (signature based / misuse detection).
- Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.
- Tecnología de detección tipo stateful basada en firmas (signatures).
- Actualización automática de firmas para el detector de intrusos.
- El detector de intrusos deberá mitigar los efectos de los ataques de negación de servicios.
- Mecanismos de detección de ataques:

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

1 [redacted]

- Reconocimiento de patrones y análisis de protocolos.
- Retección de anomalías.
- Detección de ataques de rpc (remote procedure call).
- Protección contra ataques de windows o netbios.
- Protección contra ataques de smtp (simple message transfer protocol) imap (internet message access protocol, sendmail o pop (post office protocol).
- Protección contra ataques dns (domain name system).
- Protección contra ataques a ftp, ssh , telnet y rlogin.
- Protección contra ataques de icmp (internet control message protocol).

➢ métodos de notificación:
- alarmas mostradas en la consola de administración del equipo (appliance).
- alertas vía correo electrónico.

➢ Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.

➢ La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. también podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto."

➢ Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. estos paquetes deben poder ser visualizados por una herramienta que soporte el formato pcap.

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

Prevención de fuga de información (DLP)

➢ La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.

➢ La funcionalidad debe soportar el análisis de archivos del tipo: ms-word, pdf, texto, archivos comprimidos.

➢ Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: http, pop3, smtp, imap, nntp y ftp.

➢ Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: bloquear el tráfico del usuario, bloquear el tráfico de la dirección ip de origen, registrar el evento.

➢ En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.

➢ La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. esta copia podría ser archivada localmente o en otro dispositivo.

➢ La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.

Control de aplicaciones

➢ La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.

➢ La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.

1 [redacted]

- La solución debe tener un listado de al menos 3,000 aplicaciones ya definidas por el fabricante.
- El listado de aplicaciones debe actualizarse periódicamente.
- Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
- Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en logs.
- Para aplicaciones de tipo p2p debe poder definirse adicionalmente políticas de traffic shaping.
- Preferentemente deben soportar mayor granularidad en las acciones.

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

Inspección de contenido SSL

- La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante tls al menos para los siguientes protocolos: https, imaps, smtps, pop3s.
- La inspección deberá realizarse mediante la técnica conocida como hombre en el medio (mitm – man in the middle).
- La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.
- Para el caso de url filtering, debe ser posible configurar excepciones de inspección de https. dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. las excepciones deben poder determinarse al menos por categoría de filtrado.

ANTIVIRUS

- Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer antivirus en tiempo real en al menos los siguientes protocolos aplicativos: http, smtp, imap, pop3, ftp.
- Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". sin necesidad de instalar un servidor o "appliance" externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
- El antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico ipv6.
- La configuración de antivirus en tiempo real sobre los protocolos http, smtp, imap, pop3 y ftp deberá estar completamente integrada a la administración del dispositivo equipo (appliance), que permita la aplicación de esta protección por política de control de acceso.
- El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.
- El equipo (appliance) deberá de manera opcional poder inspeccionar por todos los virus conocidos (zoo list).
- El antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos http, ftp, imap, pop3, smtp.
- El antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus

1 [redacted]

- El antivirus deberá incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.
- El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (instant messaging).
- El antivirus deberá ser capaz de filtrar archivos por extensión.
- El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo.
- Capacidad de actualización automática de firmas antivirus mediante tecnología de tipo "push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (consultar los centros de actualización por versiones nuevas).
- Las firmas de antivirus deberán ser del mismo fabricante que el "appliance".
- El sistema debe ser capaz de integrarse a futuro con una solución de sanboxing.

ANTISPAM

- La capacidad antispam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.
- La capacidad antispam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). las listas blancas y listas negras podrán ser por dirección ip o por dirección de correo electrónico (e-mail address).
- La capacidad antispam deberá poder consultar una base de datos donde se revise por lo menos dirección ip del emisor del mensaje, urls contenidos dentro del mensaje y "checksum" del mensaje, como mecanismos para detección de spam.
- En el caso de análisis de smtp, los mensajes encontrados como spam podrán ser etiquetados o rechazados (descartados). en el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado mime en el mensaje.

Filtrado de URLS (URL FILTERING)

- Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. por flexibilidad, el filtro de urls debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.
- Debe poder categorizar contenido web requerido mediante ipv6.
- Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". sin necesidad de instalar un servidor o "appliance" o dispositivo externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
- Configurable directamente desde la interfaz de administración del dispositivo "appliance". con capacidad para permitir esta protección por política de control de acceso.
- Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida.

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

1 [redacted]

- Los mensajes entregados al usuario por parte del url filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.
- Capacidad de filtrado de scripts en páginas web (java/active x).
- La solución de filtraje de contenido debe soportar el forzamiento de "safe search" o "búsqueda segura" independientemente de la configuración en el browser del usuario. esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. esta funcionalidad se soportará al menos para navegadores tales como google, yahoo! y bing.
- La solución deberá de ser capaz de poder bloquear el acceso cuentas de dominios específicos a servicios de google como por ejemplo gmail, gdocs.
- Será posible definir cuotas de tiempo para la navegación. dichas cuotas deben poder asignarse por cada categoría y por grupos.
- Será posible exceptuar la inspección de https por categoría.
- El equipo tendrá la capacidad para que automáticamente redirija el tráfico de www.youtube.com a http://www.youtube.com/education para que se acceda únicamente a contenido categorizado por el portal como contenido educativo.

Alta disponibilidad

- El dispositivo deberá soportar alta disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para ipv4 como para ipv6.
- Alta disponibilidad en modo activo-pasivo.
- Alta disponibilidad en modo activo-activo.
- Posibilidad de definir al menos dos interfaces para sincronía.
- El alta disponibilidad podrá hacerse de forma que el uso de multicast no sea necesario en la red.
- Será posible definir interfaces de gestión independientes para cada miembro en un clúster.

Características de administración

- Interface gráfica de usuario (GUI), vía web por http y https para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. por seguridad la interfase debe soportar ssl sobre http (https).
- La interface gráfica de usuario (GUI) vía web deberá poder estar en español y en inglés, configurable por el usuario.
- Interface basada en línea de comando (cli) para administración de la solución.
- Puerto serial dedicado para administración. este puerto debe estar etiquetado e identificado para tal efecto.
- Comunicación cifrada y autenticada con username y password, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (ssh o telnet).
- El administrador del sistema podrá tener las opciones incluidas de autenticarse vía password y vía certificados digitales.
- Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar

1 [redacted]

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

- El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones ip cuando se utilice ssh, telnet,http o https.
- El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a internet que tenga un browser (internet explorer, mozilla, firefox al menos) instalado sin necesidad de instalación de ningun software adicional.
- Soporte de snmp versión 2.
- Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de syslog remotos.
- Soporte de control de acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del firewall.
- Monitoreo de comportamiento del appliance mediante snmp, el dispositivo deberá ser capaz de enviar traps de snmp cuando ocurra un evento relevante para la correcta operación de la red.
- Debe ser posible definir la dirección ip que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. esto debe poder hacerse al menos para el tráfico de alertas, snmp, log y gestión.

Virtualización

- El dispositivo deberá poder virtualizar los servicios de seguridad mediante "virtual systems", "virtual firewalls" o "virtual domains".
- La instancia virtual debe soportar por lo menos funcionalidades de firewall, vpn, url filtering, ips y antivirus.
- Se debe incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer.
- Cada instancia virtual debe poder tener un administrador independiente.
- La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
- Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red.
- Debe ser posible la definición y asignación de recursos de forma Independiente para cada instancia virtual.
- Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
- Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.

Licenciamiento, soporte y actualizaciones

- El licenciamiento de todas las funcionalidades debe ser ilimitado en cuanto a usuarios y conexiones limitándola solamente por el desempeño del equipo.
- La vigencia de licencia de actualización debe incluir la capacidad de poder hacer actualizaciones de firmas ips, url, filtering, antispam, antivirus y cualquier otra actualización necesaria para la correcta operación del equipo con las características arriba descritas, por espacio mínimo de 1 año.
- La solución debe contar con un centro de investigación propio del mismo fabricante para la actualización de políticas.

[redacted]

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

- El equipo debe de incluir soporte telefónico, reemplazo de fábrica avanzado, actualizaciones de firmware por 1 año.

SEGUNDA.- "EL PROVEEDOR" además de lo descrito en la cláusula primera deberá:

- Llevar a cabo la instalación, configuración y puesta a punto del equipo de seguridad informática UTM.
- Realizar la configuración del equipo de seguridad UTM con base a los requerimientos de seguridad de **"LA SECRETARÍA".**
- Activar y configurar todos los servicios de seguridad.
- Realizar los registros de los equipos y garantías en el portal del fabricante.
- Llevar a cabo pruebas de funcionalidades y posibles fallas del equipo de seguridad UTM.
- Realizar la instalación física en los racks de **"LA SECRETARÍA"** y conexión a la energía eléctrica.
- Entregar la memoria técnica de las configuraciones realizadas al equipo de seguridad informática UTM.
- Incluir un total de 26 servicios del tipo ABC (alta, baja, cambios) para la administración del equipo; distribuidos a lo largo del año.

"EL PROVEEDOR" se compromete en caso de que el fabricante no cuente con un centro de atención al cliente (tac) basado en la ciudad de México con atención y soporte en lenguaje inglés y español, podrá estar con base en una ciudad extranjera, siempre y cuando la atención y soporte sea en español, además de un soporte mundial tipo "follow-the-sun".

"EL PROVEEDOR" deberá incluir los 26 tickets distribuidos a lo largo del año como parte del costo del equipo, esto es 26 servicios del tipo ABC (alta, baja, cambios) para la administración del equipo; distribuidos a lo largo del año, en un horario de 5x8, salvo si el reporte es de severidad 1 (pérdida total del servicio) a criterio de **"LA SECRETARÍA".**

Estos servicios deberán ser proporcionados en sitio o vía remota, según sea solicitado por **"LA SECRETARÍA".**

"EL PROVEEDOR" debe de llevar a cabo la capacitación necesaria y suficiente a por lo menos 3 personas de la Dirección de Tecnologías y Plataformas de **"LA SECRETARÍA"** para la administración del equipo, dentro de los dos días posteriores a su instalación, configuración y puesta a punto.

La capacitación deberá ser impartida por personal técnico por parte de **"EL PROVEEDOR"**, el cual deberá de contar por lo menos con el nivel de certificación NSE4, así mismo deberán de proporcionar un temario.

La capacitación deberá tener una duración mínima de 8 horas por tema, distribuidas de 2 a 3 horas máximo por día de lunes a viernes en un horario de 9:00 a 17:00 horas según las necesidades y disponibilidad de **"LA SECRETARÍA",** dicha capacitación deberá ser impartida de manera presencial, en las instalaciones de **"LA SECRETARIA".**

TERCERA.- El equipo del sistema de seguridad perimetral (UTM), objeto del presente contrato deberán ser entregados en la Dirección de Tecnologías y Plataformas en las

[redacted]

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

oficinas de **"LA SECRETARÍA"** ubicada en **la Avenida de los Arcos, Número 767, Colonia Jardines del Bosque, Guadalajara, Jalisco, México, Código Postal 44520**, de conformidad con las características y especificaciones establecidas en la cláusula primera de este instrumento.

"EL PROVEEDOR" se obliga a entregar dentro de un término de 45 días naturales a partir de la notificación de la Resolución de Adjudicación, el equipo de sistema de seguridad perimetral (UTM) descrito en la **CLÁUSULA PRIMERA** junto con la póliza de garantía, el plan de escalamiento para reportar fallas del equipo, niveles de servicio referente a revisión, reparación y entrega de este.

Así mismo se obliga a entregar a **"LA SECRETARÍA"** a partir de la instalación, configuración y puesta a punto del equipo de sistema de seguridad perimetral (UTM), la memoria técnica de las configuraciones realizadas al mismo, en formato digital y físico, en un término no mayor 10 días hábiles.

Así mismo **"EL PROVEEDOR"** se obliga a entregar a **"LA SECRETARÍA"** el equipo de sistema de seguridad perimetral (UTM), en una sola exhibición, es decir, solo se aceptará la totalidad del mismo, invariablemente para efecto de pago, la Dirección de Tecnologías y Plataformas deberá emitir una constancia firmada a **"EL PROVEEDOR"** que avale la entrega recepción del equipo mencionado a su entera satisfacción.

CUARTA.- "EL PROVEEDOR" realizará la instalación, configuración y puesta a punto del equipo de seguridad informática UTM así como los requerimientos de seguridad que le proporcione a **"LA SECRETARÍA",** a través de la Dirección de Tecnologías y Plataformas, lo anterior deberá ser ejecutado dentro del periodo establecido en la **CLÁUSULA TERCERA** del presente instrumento.

QUINTA.- "EL PROVEEDOR", se obliga a aplicar su capacidad y conocimientos especializados para cumplir satisfactoriamente con las actividades a realizar que solicita **"LA SECRETARÍA",** así mismo a responder de la calidad de los servicios, y de cualquier otra responsabilidad en la que incurra, igualmente de los daños y perjuicios que por inobservancia o negligencia de su parte le causaren a **"LA SECRETARÍA".**

En virtud de lo anterior, declara **"EL PROVEEDOR"** bajo protesta de decir verdad, que conoce cada una de las áreas de las instalaciones de **"LA SECRETARÍA"** en donde se llevará a cabo el proyecto descrito en la **CLÁUSULA PRIMERA**, así como los alcances y condiciones derivados del presente instrumento, y por tanto se obliga a cumplir en tiempo y forma con la totalidad de las obligaciones establecidas en este contrato.

SEXTA.- El presente servicio será supervisado y recibido por la Dirección de Tecnologías y Plataformas de **"LA SECRETARÍA".**

SÉPTIMA.- "EL PROVEEDOR" se obliga a proporcionar a **"LA SECRETARÍA",** equipo nuevo; ya que no aceptará equipos remanufacturados o usados.

OCTAVA.- "EL PROVEEDOR" deberá entregar por escrito las pólizas de garantía, cuya cobertura y vigencia afectarán la vigencia del contrato en cuanto a las obligaciones que derivan de la misma, independientemente del plazo de vigencia fijado por las partes en la **CLÁUSULA DÉCIMA.**

1 [redacted]

El equipo del sistema de seguridad perimetral (UTM), tendrá una garantía por escrito de mínimo 1 años en partes, refacciones y en sitio.

"EL PROVEEDOR" deberá sustituir el equipo del sistema de seguridad perimetral (UTM), por mala calidad, defecto o falla en un lapso no mayor de 24 horas, una vez realizado el reporte por parte de la **"LA SECRETARÍA",** de acuerdo al plan de escalamiento.

NOVENA.- "EL PROVEEDOR" deberá de entregar un plan de escalamiento para reportar fallas así como proporcionar los niveles de servicio (SLAs), referente a la revisión del equipo, reparación del equipo, entrega del equipo que aplique garantía por falla, en el momento en que entregue el equipo del sistema de seguridad perimetral (UTM), objeto de este contrato, el cual deberá describir y detallar como mínimo los datos de contacto de las personas a su cargo que deberán atender los requerimientos y necesidades de **"LA SECRETARÍA"** en atención a las obligaciones que derivan de las garantías otorgadas, en primer, segundo y tercer nivel de atención, sin que el tiempo de atención en el primer nivel rebase los 30 treinta minutos siguientes contados a partir de la recepción del reporte, y en cuanto al segundo nivel de atención no rebase una hora de atención a partir del momento en que se realice el reporte, y el tercer nivel no rebase las dos horas de atención a partir de que se realice el reporte.

Para el caso de que no exista atención por más de 3 tres ocasiones en las que no se atiendan los requerimientos y solicitudes de **"LA SECRETARIA"** por parte de **"EL PROVEEDOR"**, y por ello no se le dé solución a partir del segundo nivel de atención del plan de escalamiento, **"EL PROVEEDOR"** se obliga a pagar como pena convencional el 5% cinco por ciento del valor del presente contrato en favor de **"LA SECRETARÍA".**

DÉCIMA.- El presente contrato tendrá una vigencia comprendida del 30 de agosto del 2019 al 14 de octubre del 2019, sin desconocer lo pactado en la **CLÁUSULA OCTAVA.**

DÉCIMA PRIMERA.- "LA SECRETARÍA" se obliga a pagar como único pago a **"EL PROVEEDOR",** la cantidad total de **$126,191.12 (Ciento Veintiséis Mil Ciento Noventa y Un Pesos 12/100 M.N),** cantidad que incluye el impuesto al valor agregado.

"EL PROVEEDOR" deberá expedir la factura debidamente requisitada 3 tres días hábiles antes del pago correspondiente para que **"LA SECRETARÍA"** pueda iniciar con el tramite nominativo.

El pago se realizará en el primer viernes que suceda dentro los 08 ocho días hábiles posteriores a la recepción de la factura correspondiente, y una vez realizada la entrega total del equipo de cómputo, monitores y los escáner portátil, descritos en la cláusula primera de este instrumento y que la **Dirección de Tecnologías y Plataformas** de **"LA SECRETARÍA"** manifieste por escrito a la Coordinación administrativa, que el Equipo de Sistema de Seguridad Perimetral (UTM) para la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Jalisco, se encuentra debidamente instalados y funcionando a su entera satisfacción.

El pago será realizado mediante transferencia electrónica interbancaria, a la cuenta que **"EL PROVEEDOR"** proporcione a **"LA SECRETARÍA".**

Corresponderá a **"EL PROVEEDOR"** reportar a la Secretaría de Hacienda y Crédito

1 [redacted]

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

Público los impuestos y demás retenciones adicionales que le resulten aplicables con motivo de los pagos descritos en esta cláusula, deslindando desde luego a **"LA SECRETARÍA"** de cualquier responsabilidad que haya bajo este rubro.

DÉCIMA SEGUNDA.- "EL PROVEEDOR", se obliga a sostener el precio ofertado establecido en la cláusula anterior, por todo el tiempo de vigencia hasta la entrega total de los equipo de cómputo, monitores y los escáner portátil, objeto del presente contrato.

DÉCIMA TERCERA.- "EL PROVEEDOR" se obliga devolver las cantidades pagadas con los intereses correspondientes, aplicando una tasa equivalente al interés legal sobre el monto a devolver, y a recibir a su costa el Equipo de Sistema de Seguridad Perimetral (UTM) rechazado por **"LA SECRETARÍA"** por resultar defectuoso, falto de calidad en general o por ser de diferentes especificaciones a las solicitadas y descritas en la cláusula primera de este instrumento.

DÉCIMA CUARTA.- En caso que **"EL PROVEEDOR",** tenga atraso en la entrega del equipo del sistema de seguridad perimetral (UTM), por cualquier causa que no sea derivada de **"LA SECRETARÍA",** se le aplicará una pena convencional de conformidad a la siguiente tabla:

DÍAS DE ATRASO (NATURALES)	% DE LA SANCIÓN SOBRE EL MONTO TOTAL DEL CONTRATO
De 01 uno hasta 05 cinco	3% tres por ciento
De 06 seis hasta 10 diez	6% seis por ciento
De 11 once hasta 20 veinte	10% diez por ciento
De 21 veintiún días de atraso en adelante	Se rescindirá el contrato a criterio del ORGANISMO

DÉCIMA QUINTA.- "EL PROVEEDOR" queda obligado a responder por los defectos y/o vicios ocultos del equipo del sistema de seguridad perimetral (UTM), objeto del presente instrumento y a responder por los daños y perjuicios que se generen a **"LA SECRETARÍA".**

DÉCIMA SEXTA- Son causas enunciativas más no limitativas de rescisión del presente contrato sin que haya necesidad de declaración judicial, las siguientes:

1.- Por incumplir el objeto establecido en el presente instrumento.
2.- Ceder a terceras personas los derechos u obligaciones derivados del presente instrumento, en forma parcial o total.
3.- Que **"EL PROVEEDOR"** no entregue el equipo del sistema de seguridad perimetral (UTM) con las características, especificaciones de su propuesta técnica y en los plazos y formas convenidas.
4.- Por incluir equipos remanufacturados o usados o de mala calidad o defecto en el equipo del sistema de seguridad perimetral (UTM).
5.- Por común acuerdo de las partes.

DÉCIMA SÉPTIMA.- Para efectos del cumplimiento del objeto de este instrumento, **"LAS PARTES"** convienen que no habrá lugar a la sustitución de **"EL PROVEEDOR"**, por lo que no se podrá encomendar, delegar o subcontratar a otra persona física o jurídic

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

allá de sus trabajadores, por lo que no podrá ceder en forma parcial, ni total a favor de cualquier persona, los derechos y obligaciones derivados del presente instrumento, de, estableciéndose que de incurrir en dicha prohibición **"EL PROVEEDOR"** se le responsabilizará por su negligencia, impericia o dolo por su parte o cualquiera de las personas dependientes de este.

DÉCIMA OCTAVA.- "EL PROVEEDOR" será responsable de los actos realizados por su personal durante la entrega del equipo de cómputo, monitores y los escáner portátil, así como por los daños y perjuicios que se generen, por negligencia, descuido, falta de probidad u honradez en que incurra el personal del mismo.

DÉCIMA NOVENA.- "LAS PARTES" establecen, que no existe relación laboral alguna, derivada de las acciones del presente instrumento, ni sujeción a la relación obrero-patronal, incluyendo riesgos de trabajo o responsabilidad civil, por lo que le competerá únicamente a **"EL PROVEEDOR",** toda responsabilidad laboral, deslindando a **"LA SECRETARÍA"** de dichas obligaciones.

Por lo anterior, convienen **"LAS PARTES"** que el personal proporcionado por **"EL PROVEEDOR"** a **"LA SECRETARÍA",** estará subordinado y depende económica, administrativa y legalmente de **"EL PROVEEDOR"** bajo los términos establecidos en el artículo 20 de la Ley Federal del Trabajo, por lo que bajo ningún concepto podrá ser considerado como empleado o trabajador de **"LA SECRETARÍA"**, liberando a esta de cualquier reclamación de carácter laboral con dicho personal, sin que en ningún momento pueda considerarse a **"LA SECRETARÍA"** como patrón sustituto, o solidario, ni tendrá ninguna responsabilidad u obligación laboral, ni tampoco se le deberá considerar como intermediario de **"EL PROVEEDOR"**, ya que el personal recibirá ordenes directamente de **"EL PROVEEDOR"** y será el mismo el encargado de cubrir su salario y prestaciones legales correspondientes, por lo que desde este momento **"EL PROVEEDOR"** libera a **"LA SECRETARÍA"** de la responsabilidad solidaria que establecen los artículos 13 trece y 15 quince de la Ley Federal del Trabajo.

De igual forma **"EL PROVEEDOR"** será el único responsable de atender y pagar todos los gastos que se deriven por accidentes o riesgos de trabajo en que incurran los trabajadores que utilice, directa o indirectamente, para la realización del objeto del presente contrato, liberando desde este momento a **"LA SECRETARÍA"** de cualquier responsabilidad en ese sentido.

En el supuesto caso de que se llegasen a presentar demandas o reclamaciones laborales, de seguridad social, fiscales, o de cualquier otro tipo en contra de **"LA SECRETARÍA", "EL PROVEEDOR"** se obliga a liberar de toda responsabilidad jurídica y a cubrirle gastos, honorarios, o erogación que hubiese hecho **"LA SECRETARÍA"** con motivo de dar contestación y trámite a dichas demandas.

VIGÉSIMA.- La información que **"EL PROVEEDOR"** reciba por parte de **"LA SECRETARÍA"** derivado del presente contrato, será considerada en todo momento como "Información Confidencial", durante la vigencia del presente contrato y aun después de concluida la misma, de tal forma que **"EL PROVEEDOR"** se obliga a lo siguiente:

1.- A partir de la fecha de celebración del presente contrato, se obliga a no enajenarla, arrendarla, prestarla, grabarla, negociarla, revelarla, publicarla, darla a conocer

1 [redacted]

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

transmitirla o de alguna otra forma divulgarla o proporcionarla por cualquier medio, aun cuando se trate de incluirla o entregarla en otros documentos como estudios, reportes, propuestas u ofertas, ni en todo ni en parte, por ningún motivo a sociedades de las cuales **"EL PROVEEDOR"** sea accionista, asesor, apoderado, consejero, comisario, tenedor de acciones y, en general, tenga alguna relación de índole cualquiera por sí o por terceras personas, o proporcionar a cualquier persona física o moral, nacional o extranjera, pública o privada, presente o futura, por cualquier medio, extendiéndose a sus socios, consejeros, representantes legales, directivos, gerentes, asesores, dependientes y demás personas físicas o morales que guarden relación con **"EL PROVEEDOR"**, por lo que éste último se obliga a comprometer a las personas referidas en este párrafo al cumplimiento de este contrato.

2.- Adoptar precauciones razonables de seguridad para conservar en secreto la Información Confidencial que reciba de **"LA SECRETARÍA".**

3.- En caso de que **"EL PROVEEDOR"** incumpla con las obligaciones a su cargo, previstas en este instrumento, pagará a **"LA SECRETARÍA"** una indemnización correspondiente por los daños y perjuicios que por este concepto se generen, equivalente a un 10% del total de la cantidad pactada en el presente instrumento, además de las cantidades que se generen por concepto de gastos del procedimiento judicial.

VIGÉSIMA PRIMERA.- "EL PROVEEDOR", será la responsable por cualquier evento que le impida parcial o totalmente cumplir con las obligaciones contraídas en virtud del presente contrato, aún las de caso fortuito y fuerza mayor en cuanto estas hayan sido predecibles.

VIGÉSIMA SEGUNDA.- "LAS PARTES" aceptan que todo lo no previsto en el presente contrato se regirá por las disposiciones contenidas en el Código Civil del Estado de Jalisco, así como en las Políticas, Bases y Lineamientos para la Adquisición, Enajenación, Arrendamiento de Bienes, Contratación de Servicios y Manejo de Almacenes de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción del Estado de Jalisco, y en caso de controversia para su interpretación y cumplimiento, se someterán a la jurisdicción del Primer Partido Judicial del Estado de Jalisco, o en su caso a los medios alternativos de solución de controversias, renunciando al fuero que les pudiera corresponder en razón de su domicilio presente, futuro o por cualquier otra causa.

Leído que fue el presente documento por las partes contratantes, manifiestan su más entera conformidad firmando por duplicado al margen en cada una de sus fojas y al calce, en la Ciudad de Guadalajara, Jalisco a 30 treinta de agosto del año 2019 dos mil diecinueve.

"LA SECRETARÍA"

Dra. Haimé Figueroa Neri
Secretaria Técnica
de la Secretaría Ejecutiva del Sistema
Estatal Anticorrupción de Jalisco

1

Se eliminan los datos 1, (firma) Por ser considerados un dato personal identificable. Fundamento legal: Artículo 21.1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; Artículos 2 y 3 incisos IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; y de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como, para la Elaboración de Versiones Públicas emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso de la Información Pública y Protección de Datos Personales en su quincuagésimo sexto, quincuagésimo séptimo y quincuagésimo octavo, por tratarse de un dato personal identificativo.

Licda. Martha Iraí Arriola Flores
Coordinadora Administrativa
de la Secretaría Ejecutiva del Sistema
Estatal Anticorrupción de Jalisco

"EL PROVEEDOR"

1 [redacted]

C. Gustavo Soto Valencia
Apoderado Legal
Servicio Divergentes
en Tecnología, S.A. De C.V.

LA PRESENTE HOJA DE FIRMAS CORRESPONDE Y FORMA PARTE INTEGRANTE DEL CONTRATO DE ADQUISICIÓN DE EQUIPO DE CÓMPUTO Y TECNOLOGÍA DE LA INFORMACIÓN PARA LA SECRETARÍA EJECUTIVA DEL SISTEMA ESTATAL ANTICORRUPCIÓN DE JALISCO, QUE CELEBRAN, POR UNA PARTE, SECRETARÍA EJECUTIVA DEL SISTEMA ESTATAL ANTICORRUPCIÓN DE JALISCO Y POR LA OTRA PARTE EL C. GUSTAVO SOTO VALENCIA, APODERADO LEGAL DE SERVICIO DIVERGENTES EN TECNOLOGÍA, S.A. de C.V., DE FECHA 30 DE AGOSTO DEL 2019.