ANEXO TÉCNICO

SEGURIDAD EN TELECOMUNICACIONES

INDICE

1. Antecedentes

Se entenderá como **LA SECRETARÍA** para el efecto del presente procedimiento a la Secretaría de Medio Ambiente y Recursos Naturales.

LA SECRETARÍA es una Institución pública del Gobierno Federal, lo que la hace susceptible a ser blanco de diferentes tipos de ataques a través de Internet; por lo que se requiere de las soluciones y/o herramientas, así como su administración adecuada para que se puedan proteger los servicios de la Institución y los accesos a la red interna en el perímetro como un primer punto de protección contra ataques dirigidos, intentos de engaños a los usuarios y aplicaciones maliciosas, que en caso de ingresar a la red pondrían en riesgo la operación y continuidad de los servicios que se ofrecen a los usuarios internos y externos, también la protección de manera externa.

En años anteriores, **LA SECRETARÍA** ha contado con herramientas de seguridad perimetral con filtrado de contenido que han permitido mitigar y contener este tipo de ataques así como el robo de información, utilizando plataformas especializadas que han demostrado su eficacia. Dada la proliferación y la sofisticación en los métodos y herramientas utilizadas para ataques cibernéticos, hoy es necesario robustecer la infraestructura de red de **LA SECRETARÍA** no sólo a nivel perimetral sino también en sus capas internas.

2. Objetivo General

Proteger la red de **LA SECRETARÍA** ante intentos de acceso y vulneración del perímetro por parte de equipos y redes no autorizadas a trabajar en ella, lo anterior con la finalidad de preservar la información y contribuir a la continuidad y estabilidad de las plataformas informáticas que la almacenan, procesan y transforman. Para lograrlo, es necesario contar con el licenciamiento y los servicios de soporte en materia de seguridad informática que se describen a continuación:

- La renovación del licenciamiento de seguridad a nivel externo o perímetro (*Firewall*, software para protección de amenazas externas a la red de **LA SECRETARÍA**) para uso en los equipos PA-3250 y consola de administración M-200 (ambos propiedad de **LA SECRETARÍA**);

3. Objetivos específicos

- Contar con la continuidad en el licenciamiento del firewall permitirá a **LA SECRETARÍA** la protección de los servicios de Internet y la DMZ (este término se usa habitualmente para ubicar servidores a los cuales es necesario sean accedidos desde fuera, como servidores de: correo electrónico, aplicativos, filtrado de correo electrónico, DNS y bases de datos), para así obtener el mejor rendimiento e incrementar la eficiencia de operación para los usuarios y mitigar los riesgos de afectación para estos servicios, por la entrada y ejecución de código malicioso o *malware*.
- Continuar con la solución de Filtrado de Contenido Web dentro de los mismos *firewalls* de seguridad perimetral, que permita la administración y la protección de los servicios de internet para obtener el mejor rendimiento, incrementar la eficiencia de operación de los usuarios y mitigar los riesgos de afectación de estos servicios por la entrada y ejecución de código malicioso o *malware*.

- Creación de VPN para ofrecer una conexión remota y segura por WEB a **LA SECRETARÍA** desde cualquier proveedor de Internet, con el fin de poder hacer uso de los recursos internos de **LA SECRETARÍA**.

4. Descripción de los Servicios

Todos los servicios de los apartados que a continuación se enlistan serán asignados a un solo licitante mediante una partida única, la cual se describe a continuación.

Partida Única: Renovación del licenciamiento para los equipos PA-3250 y consola de administración M-200 propiedad de LA SECRETARÍA.

Esta renovación permitirá dar continuidad a la detección de posibles amenazas potenciales EXTERNAS (ataques, intrusión, robo y secuestro de información, entre otros) relacionadas con la seguridad de la información, a nivel de la infraestructura tecnológica de **LA SECRETARÍA** que pudieran impactar en la confidencialidad, integridad y disponibilidad de la información de manera preventiva, a fin de tomar acciones correctivas y de mejora, para lo cual se requiere de tecnología especializada y en apego a los procesos relacionados a la seguridad de la información establecidos en el Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI).

5. Alcance

Los servicios impactarán a 3500 usuarios a Nivel Nacional, así como los 5,300 dispositivos que operan en la red privada de **LA SECRETARÍA**. Esta red se compone de dos Data Center (Centro de Datos): en Ejército Nacional 223 y el que se encuentra en el site del Edificio de CONAGUA, así como las 31 delegaciones federales.

La renovación de licenciamiento, permitirá que **LA SECRETARÍA** obtenga la renovación de las licencias, el servicio de soporte y mantenimiento de la infraestructura de la plataforma de Palo Alto propiedad de **LA SECRETARÍA**.

El licitante deberá proporcionar el licenciamiento del firewall para seguridad perimetral a partir del día hábil siguiente de la notificación del fallo, así como el nivel de soporte técnico que está asociado al esquema de licenciamiento (soporte premium y póliza de mantenimiento).

6. Beneficios

Con la renovación del licenciamiento se alcanzarán los siguientes beneficios, que contribuirán a brindar mejores servicios a los ciudadanos:

- Permitirá contar con elementos de confidencialidad, protección de datos y análisis del tráfico en la infraestructura tecnológica de **LA SECRETARÍA**.
- Establecimiento de políticas de seguridad para la navegación segura en Internet.
- Aseguramiento para habilitar accesos a puertos seguros de nuestros aplicativos sustantivos e institucionales para navegar a Internet.
- Proteger los sitios de los ataques desde Internet.
- Permitirá a las aplicaciones y sistemas sustantivos y administrativos de **LA SECRETARÍA** mejorar los tiempos de respuesta.

- Permitirá contar con análisis del tráfico que genera la infraestructura tecnológica de **LA SECRETARÍA**.
- Asegurar el uso de los puertos seguros en los aplicativos sustantivos e institucionales para navegar a Internet.
- Proteger los dispositivos de ataques desde Internet.

7. Servicios solicitados por LA SECRETARÍA

7.1. Partida *Única.- Renovación del licenciamiento para los equipos PA-3250 y consola de administración M-200 propiedad de LA SECRETARÍA.*

La renovación del licenciamiento deberá contar con las siguientes características:

- Prevención de Amenazas (Threat prevention).
- Tecnología de detección y análisis de malware (Wildfire), ataques día cero.
- Filtrado de Contenido WEB (PANB URL Filtering).
- Global Protect.
- Consola de administración.
- Soporte Premium por el fabricante.
- Póliza de mantenimiento.

Lo cual involucrará actualizaciones para Filtrado de Contenido Web, Threat Prevention, Wildfire, Global Protect, y el software para la consola de administración.

Se requiere soporte del licitante 24x7 para apoyar en casos de fallas, configuraciones, contingencias con alguno de los equipos: dos PA-3250 y un M-200 de forma remota o en sitio conforme a las necesidades de **LA SECRETARÍA**.

El licitante adjudicado deberá contratar con el fabricante las pólizas de servicio, soporte y mantenimiento por el total de tiempo de la vigencia del soporte.
Las Pólizas que se mencionan en este apartado están vinculadas a la licencia del software de Palo Alto que se requiere para la operación de los equipos de seguridad perimetral PA-3250 y consola de administración M-200 propiedad de la Secretaría

7.1.1. Plazo de entrega

La renovación del licenciamiento debe activarse a partir del día hábil siguiente de la notificación del fallo. El licitante adjudicado deberá entregar al administrador del contrato la carta de activación **3 días hábiles** después de su activación.

El soporte de la solución iniciará a partir del día hábil siguiente de la notificación del fallo.

7.1.2. Características del servicio

Debe considerar la renovación de los siguientes equipos propiedad de **LA SECRETARÍA**:

- 2 equipos Next Generation Firewall PA-3250.
- 1 Consola de Administración M-200.

Especificaciones y Requerimientos Técnicos

- Que contemplen lo siguiente:
- Inspección de tráfico contra amenazas.
- Filtrado de navegación web y prevención de fuga de información.

- Póliza de servicios nivel 2 (soporte premium)
- Soporte por parte del licitante en caso de un incidente por personal con máximo nivel de certificación de la marca para análisis de la situación actual, recomendaciones de mejora, implementación de las mejoras, soporte de la solución.

Requerimientos del Servicio

El licitante adjudicado deberá proporcionar un soporte (póliza de mantenimiento) la cual debe entregar de forma electrónica a los **10 días hábiles** después de la notificación del fallo para garantizar el correcto funcionamiento de la solución, así como de los equipos o apliances, por lo que deberá considerar:

- El soporte deberá incluir sustitución de partes, así como del software y firmware para mantener la operación de los equipos con los que actualmente cuenta **LA SECRETARÍA**.
- El mantenimiento oportuno a los equipos propiedad de **LA SECRETARÍA** al menos **una vez** después de la firma del contrato, alineado al proceso de AOP (Proceso de Administración de la Operación del MAAGTICSI), para lo cual el licitante deberá considerar viáticos, materiales, papelería y demás gastos que se generen para la prestación del servicio sin costo alguno para **LA SECRETARÍA**.
- Reparar el equipo, en caso de que se presente una falla física o problema, deberá reemplazar el o los equipos por uno de al menos las mismas características o superiores al actual, en el plazo descrito en los niveles de servicio descritos en este Anexo Técnico, sin importar las causas que originaron la interrupción del servicio, siempre y cuando el servicio no sea interrumpido.
- Diagnosticar las fallas de hardware o software de los dispositivos que sean parte de la solución, así como generar y dar seguimiento a los reportes que deberán tener relación con el fabricante, mismas que deberán ser aplicados para garantizar la continuidad del servicio durante el periodo del soporte.

Requisitos funcionales

Características del Licenciamiento requerido:

Inspección de tráfico contra Amenazas

Integrar dentro de la misma plataforma licencias con características de inspección avanzada, identificación y bloqueo de tráfico originado por amenazas informáticas, orientado para la protección de los diferentes segmentos de red interna y comunicación hacia el exterior.

La función de protección contra amenazas se administrará completamente dentro de la misma interfaz de administración.

Funcionalidades de detección y bloqueo para:

- Anomalías de tráfico.
- Escaneo de puertos y barrido de hosts.

- Intentos de intrusión por fuerza bruta.
- Detección y bloqueo de intentos de intrusión por explotación de vulnerabilidades a nivel de capa aplicativa entre los diferentes segmentos internos de la institución.
- Protección contra amenazas de tipo spyware a nivel de capa aplicativa.
- Protección contra amenazas identificadas previamente y amenazas día cero, aun para aplicaciones permitidas, sin necesidad de bloquear dicha aplicación.
- 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 Botnets y amenazas "Command and Control"
- Protección contra ataques de tipo SYN Flood y UDP Flood.

- La solución incorpora licencias con capacidades para la detección de Amenazas Persistentes – APTs – de forma proactiva, y tomar acción para evitar su propagación y bloqueo de los canales de comunicación establecidos por dichas amenazas hacia el exterior, con un tiempo de respuesta de 1 hora máximo.
- En la protección contra botnets se implementará, en la detección y monitoreo por firmas y por comportamiento, a través de los siguientes criterios:

  - Visita a sitios con contenido malicioso y de propagación de malware en toda la infraestructura de red WAN.
  - Uso de sitios de DNS dinámicos y/o empleados por amenazas.
  - Visita de dominios de reciente registró.
  - Uso de aplicaciones desconocidas.
  - Presencia de tráfico de IRC (chat local).

- Capacidad de realizar la actualización automática de firmas, identificadores o patrones para las funciones de protección contra amenazas.
- La detección y protección contra ataques estará basada en análisis de firmas sobre el flujo de datos en la red.
- Capacidad de soportar la creación de firmas personalizadas de amenazas para cualquier protocolo, basado en patrones personalizados de tráfico a través de expresiones regulares.
- Capacidad de autogeneración de firmas de C2 (Command-and-Control) al momento de detectar tráfico de este tipo pasando por el dispositivo para su identificación y bloqueo.
- Contar con un ambiente de sandbox mejorado, permitiendo hacer análisis dinámico de malware en máquinas físicas (Bare-Metal) además de otros mecanismos para evitar que el malware reconozca que está en un ambiente virtual.
- Soporte ambientes virtualizados en la nube (sandboxing) para la ejecución de archivos para identificación de amenazas avanzadas persistentes, sobre archivos ejecutables y librerías de Windows tales como archivos exe, dll, pdf, archivos de Office y PE.

Filtrado de Navegación Web y prevención de Fuga de Información

Para el control de tráfico hacia redes externas, se requieren licencias con la capacidad de:

- Deberá soportar el volumen de usuarios de **LA SECRETARÍA** indicado en el presente anexo técnico.
- Proporcionar facilidades para incorporar el control de sitios en la navegación de los usuarios mediante categorías.

- El filtro de URLs tendrá por lo menos 60 categorías pre-definidas y cuando menos 2500 aplicaciones
- Soporte la creación de nuevas categorías de URL.
- Cuente la funcionalidad de permitir re categorización de sitios.
- Permita la creación de listas de bloqueo para URLs específicas, dominios y grupos de URLs a través de patrones y comodines.
- Los mensajes entregados al usuario por parte del filtrado de URL (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) serán personalizables.
- La solución de Filtrado de Contenido forzará la "Búsqueda Segura" (Safe Search) al menos para Google, Yahoo y Bing. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales.
- Capacidad de detectar y categorizar las URL's que el usuario pueda ingresar en herramientas de Google para evadir las políticas de filtrado de contenido implementadas, como por ejemplo Google Traslate.
- Cuente con capacidades para el análisis de archivos que se envíen a través de la red que pudieran contener información confidencial y sensible.
- La solución soportará análisis en archivos de formato MS-Word, texto/html, archivos comprimidos.
- La solución soportará el análisis de archivos en al menos los siguientes protocolos:

    - HTTP
    - POP3
    - SMTP
    - IMAP
    - FTP

- Capacidad de prevenir la transferencia de datos no autorizada correspondiente a patrones de números de tarjetas de crédito y de seguridad social, entre otras.
- Contar con un mecanismo de prevención de robo de credenciales, evitando que se ingresen credenciales válidas a sitios no autorizados.
- Permitirá el bloqueo de mensajería instantánea (IM).
- Permitirá el bloqueo de aplicaciones Peer-to-Peer.
- Permitirá el bloqueo de Streaming Media.
- Deberá poder catalogar las páginas por Dominio (o subdominio).
- Deberá permitir el bloqueo de las amenazas emergentes más comunes como: pop-ups, banners, spyware, adware, compartición de archivos punto a punto (P2P file sharing).
- Deberá soportar que la actualización de la base de datos para el filtrado de contenido se realice en tiempo real y de manera automática.
- Deberá permitir la personalización de políticas de control de acceso de forma visual en el equipo a través de diferentes parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, atributos, grupos y usuarios de directorio activo de Microsoft.
- Deberá permitir la creación y utilización de listas blancas y negras
- Deberá permitir el filtrado basado en reputación de los sitios web, para ello deberá contar con un sistema de reputación "en la nube" administrado y mantenido por el mismo fabricante que permita bloquear de forma dinámica contenido Web malicioso.
- Las actualizaciones de contenido para el filtrado de URL, deberán actualizarse como máximo cada 24 horas.

- Las actualizaciones de los filtros por reputación de URL, deben actualizarse en tiempo real continuamente, inmediatamente después que hayan sido descubiertas por el fabricante.

Control de Aplicaciones:

- Deberá permitir el Control de más de 1,000 Aplicaciones Web, permitiendo el control granular de características de aplicaciones tales como Facebook, Twitter, entre otras.
- Deberá tener la habilidad de remover de los sitios web contenido seleccionado por los administradores del sistema, eliminando o removiendo código del sitio, para que no sea presentado al usuario final.
- Deberá permitir el filtrado de tráfico no HTTP, como puede ser el de los programas P2P (eMule, etc.) o IM (mensajería instantánea).
- Deberá identificar el tipo de servicio o aplicación aprovechando la capacidad de realizar filtrados o análisis por cadenas o "body" dentro del código HTML de las páginas o sitios invocados.

Autenticación de los Usuarios:

Integración con un Directorio Activo de Microsoft el cual se encuentra implementado y configurado en Windows R2 2012 sin necesidad de instalar algún componente en los controladores de dominio. Esta integración permitirá que la administración de la solución se efectué por medio de cuentas de usuarios y grupos de administración basadas en el Directorio Activo.

Administración Basada en Roles: es requisito indispensable que se pueda segregar la administración de la seguridad diferenciando claramente los roles de Seguridad de Sistemas y de otras unidades definidas en el Directorio Activo.

Deberá permitir la segregación de funciones de forma granular, permitiendo así definir el alcance o posibilidades de gestión para cada administrador.

Tendrá la capacidad de presentar al usuario, una página web con mensajes modificables por los administradores del sistema, en caso de algún problema o infracción.

Deberá ofrecer mecanismos de autenticación tales como: autenticación local, NTLM, LDAP, RADIUS y certificados. Debe ser capaz de evitar la ejecución de códigos maliciosos, notificando al administrador.

Políticas de Protección y Accesos:

La renovación del licenciamiento debe:

1. Permitir el control de cuotas por tipo de tráfico o aplicación por ancho de banda.
2. Permitir el control de cuotas para los usuarios por tiempo consumido.
3. Permitir el control de cuotas de tamaños de los archivos.
4. Tener la capacidad de utilizar expresiones regulares como perfiles adicionales de seguridad dentro de las políticas.
5. Tener la capacidad de utilizar expresiones booleanas para la creación de políticas.
6. Tener la capacidad de utilizar las políticas en forma anidadas o encadenadas.
7. Estar basadas en:

- Dirección IP.
- Rango de Direcciones IP.
- Subredes y CIDR.
- Usuarios del Directorio Activo.
- Grupos de Usuarios del Directorio Activo.

Soportar la configuración de tiempos de conexión mediante la configuración de reglas específicas

VPN:

- Deberá brindar túneles IPSec que soporten algoritmos de cifrado AES con la capacidad de configurar longitudes de llave de 128 o 256 bits, permitiendo configurar al menos los grupos de Diffie-Hellman 1, 2, 5, 14 junto con la capacidad de configurar alguno de los siguientes algoritmos de integridad: MD5, SHA, SHA-1 y SHA256.
- Deberá brindar soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to- site) y soporte para SSL o IKEv2 o IKE main y agressive mode
- De manera opcional deberá poder ser configurada en modo interface, en esta funcionalidad deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interfaz.
- Se requiere contar con conexión a través de VPN client-to-site, aproximadamente para 100 usuarios (esto es usuarios que ingresan a los aplicativos y bases de datos para realizar cambios o configuraciones en los ambientes de producción o desarrollo).
- Se requiere contar con conexión a través de VPN site-to-site, aproximadamente 100, para realizar conexiones sitio a sitio.

Administración y Reportes

- La renovación del licenciamiento deberá permitir que la consola centralizada proporcione capacidades de administración y reporteo, incluyendo control de acceso discrecional, auditoría de usuario y sistema y utilerías de restauración de configuración.
- Actividad Web de: Spyware y Malware, uso de video, uso de aplicaciones Web, uso de términos para búsquedas, categorías filtradas, contenido Web, sesiones, perfiles de tráfico, usuarios y autentificación.
- Las cuentas de administrador proporcionaran los siguientes derechos de acceso configurables: negar, sólo lectura, lectura/escritura.
- Deberá ofrecer reportes preconfigurados y creación de reportes personalizados.
- Los reportes predefinidos deben proporcionar información tal como perfiles generales de tráfico, datos de rendimiento especifico de aplicaciones protocolos y usuarios, categorías de filtrado y sesiones

7.1.3. Servicios de ajustes y parametrización

Una vez actualizada la licencia, el licitante adjudicado deberá realizar un análisis de la situación actual de la configuración actual de los equipos o appliances propiedad de **LA SECRETARÍA**, mismo que deberá ser documentado, firmado, entregado en físico y electrónico al administrador del contrato, **5 días hábiles** después de la fecha de activación de la licencia.

Después de realizar el análisis, el licitante adjudicado deberá generar una propuesta de mejora de la situación actual, que deberá incluir:

1) Configurar las reglas de seguridad en los equipos, las cuales serán propuestas por el equipo de seguridad del "licitante" y validadas por el personal designado de acuerdo a los objetivos y lineamientos de normatividad bajo el cual se rige **LA SECRETARÍA**.
2) Cambios a políticas, requerimientos, generación de reportes para apoyo a auditorias y los solicitados como entregables por parte de **LA SECRETARÍA**.

El licitante adjudicado, deberá entregar el documento de propuesta de mejora firmado en físico y electrónico **10 días hábiles** posteriores de la entrega del análisis actual, esta propuesta será sometida al visto bueno del administrador del contrato

Una vez implementada la propuesta de mejora a su término, el licitante adjudicado deberá entregar al administrador del contrato una memoria técnica de los ajustes realizados a la solución, la cual deberá contener al menos lo siguiente:

I. Descripción del proyecto.
II. Cronograma del proyecto.
III. Diagrama Esquemático de conexiones y configuraciones.
IV. Documentación de rutas, políticas y configuraciones iniciales y realizadas a los equipos.
V. Memoria fotográfica y/o imágenes con detalle de lo realizados.
VI. Respaldo en medio magnético de todas las configuraciones.

Está memoria deberá ser entregada **10 días hábiles** después de su implementación.

Reportes por evento

Reporte de las fallas y/o incidentes presentados en donde se incluya la información siguiente:

- Tipos de fallas.
- Causas de las fallas y acciones preventivas y/o correctivas, tiempos promedio de respuesta y solución.
- Solución de la falla de forma detallada, causa origen y solución de raíz a la falla y/o incidente.

El formato del reporte de afectación se definirá de común acuerdo entre el licitante adjudicado y **LA SECRETARÍA**.

LA SECRETARÍA podrá solicitar cualquier otro reporte relacionado con los servicios cubiertos por la(s) póliza(s) durante la vigencia del contrato.

El licitante deberá alinear su documentación para dicho servicio en la parte de procesos en la implementación y operación conforme a lo definido en el MAAGTICSI (Manual Administrativo de Aplicación General en Materias de Tecnologías de Información y Comunicaciones y de la Seguridad de la Información). Por lo que deberá entregar el llenado de los formatos respectivos que son:

- Acta de Constitución del Proyecto, Formato ADP-F1 (UNICO, AL INICIO)

- Acta de Aceptación de Entregables. Formato ADP-F2 (CUANDO SEAN REQUERIDOS PARA PAGO)
- Acta de cierre de proyecto. Formato ADP F3 (UNICO, AL TÉRMINO)

Lo anterior, siendo enunciativo más no limitativo, por lo que **LA SECRETARÍA** en caso de requerir el llenado de algún o algunos otros formatos, podrá solicitarlo al licitante adjudicado.

Los reportes se deberá entregar los primeros **5 días hábiles** posteriores al evento.

7.1.4. Lugar, tiempo y Control de entrega de los Servicios.

La renovación del licenciamiento de la partida única del presente anexo técnico se debe activar en:
Para la Oficina Central de **LA SECRETARÍA**:

- El lugar de entrega de los servicios estará ubicado en el MDF de la Oficina Central con domicilio en Ejército Nacional 223, Planta Baja, Col. Anáhuac, C.P.11320, Alcaldía Miguel Hidalgo; o donde **LA SECRETARÍA** defina.

Para el Centro de Datos

El lugar de entrega de los servicios estará ubicado en las instalaciones de CONAGUA con domicilio en Av. Insurgente Sur, Col. Copilco el Bajo, Alcaldía Coyoacán, C.P. 04340 o donde **LA SECRETARÍA** defina.

7.1.5. Personal en sitio

Deberá designar el licitante adjudicado, un Coordinador de Seguridad durante la fase de Análisis de Situación Actual e implementación de mejoras, para la coordinación de los servicios durante su implementación y puesta en operación, considerando el liderazgo del diseño de arquitecturas de red para diferentes escenarios de seguridad perimetral, proporcionar soluciones que combinen tecnologías de diferentes propósitos, integrándolas bajo las mejores prácticas que se centran en el proceso de seguridad de redes e información, con el objetivo de mitigar los riesgos y alinear los esfuerzos a la normatividad aplicable en materia de seguridad de la información.

El licitante adjudicado proporcionará a su personal, los medios y herramientas tecnológicas de trabajo (equipos de cómputo, líneas telefónicas celulares y demás aplicables), requeridas para llevar a cabo sus funciones.

El personal designado por el licitante adjudicado, acudirá a las instalaciones de **LA SECRETARÍA** debidamente identificado y cumplirá con el código de Conducta de la institución.

Para la atención del soporte o mantenimiento a los equipos asignará a un Ingeniero para el soporte de los incidente que se susciten el cual tenga experiencia de al menos 2 años en Administración de firewalls especificados en la presente partida, el cual podrá atender de manera remota o en sitio de acuerdo a las necesidades de **LA SECRETARÍA**.

7.1.6. Monitoreo de la solución

El licitante adjudicado para dar atención a la renovación del licenciamiento y atender los incidentes, debe integrar una solución que le permita monitorear el servicio, este debe contar con las siguientes funcionalidades:

- Monitoreo de la disponibilidad de la infraestructura administrada y desempeño de la misma como:

  a) Utilización de los recursos (red, CPU, memoria, disco, etc.)
  b) Bitácoras de los diferentes componentes habilitados para proveer los servicios.

- **LA SECRETARÍA** una vez implementada la licencia y configurado el software, visitará las instalaciones del centro de monitoreo del licitante adjudicado cuando menos en una ocasión durante la vigencia del contrato para validar el monitoreo de la solución.
- La administración y monitoreo de seguridad deberá contar con las siguientes características mínimas:

  a. Atención y soporte de un equipo de personal con experiencia en las tecnologías propuestas, proveyendo un esquema continúo de operaciones y monitoreo 24x7.
  b. Los servicios de administración de seguridad deberán estar enlazados con la Mesa de Servicios del licitante, lo cual permita tener información de incidentes que potencialmente afectan a **LA SECRETARÍA**.
  c. El centro de monitoreo deberá contar con la infraestructura necesaria para albergar las consolas de administración y monitoreo de la solución propuesta.
  d. El centro de monitoreo del licitante deberá contar con acceso a Internet que permita la conectividad a través de VPN con **LA SECRETARÍA,** el cual garantice el monitoreo de los equipos y su administración.

7.1.7. Niveles de Servicio para los equipos

1. Atención de Reportes o Incidentes (soporte premium, póliza de mantenimiento)

Para todas las notificaciones hacia LA SECRETARÍA por motivo de algún incidente o evento identificado desde el centro de monitoreo, se deberán llevar a cabo mediante alguno de los siguientes medios en un lapso no mayor a 30 minutos después de ocurrido éste:

1. Teléfono
2. Correo electrónico

Notificación electrónica vía el Portal WEB de Mesa de Servicio

Con niveles de escalamiento de acuerdo a la severidad, definida a continuación:

Actividad	Severidad	Descripción
Incidente de Seguridad	Severidad 1	Afectación de Servicio. Eventos de alto riesgo, los cuales pueden ocasionar un daño severo en los activos de **LA SECRETARÍA**.
Incidente de Seguridad	Severidad 2	Degradación al Servicio. Eventos en donde se requiere que **LA SECRETARÍA** lleve a cabo una acción a partir de la notificación emitida por el Prestador de Servicios.
Incidente de Seguridad	Severidad 3	Intermitencia de Servicio.

Actividad	Severidad	Descripción
Solicitud de requerimiento	Severidad 4	Eventos de investigación, actualización de contenido de seguridad, cambios en configuraciones, Actualizaciones.

Mismos que serán definidos con **LA SECRETARÍA** para identificar cuáles serían incidentes o solicitudes.

1. **Administración de Incidentes o Reportes.**

El equipo de especialistas del licitante adjudicado deberá identificar los incidentes con severidad 1, 2, 3 y 4, que afecten la operación del servicio basado en la información recibida del Centro de Monitoreo y Operaciones y deberán ser atendidos de acuerdo a lo siguiente:

Actividad	Severidad	Detección / Notificación	Tiempo de Atención / Resolución
Afectación de servicio	Severidad 1	Incidentes con afectación al servicio (severidad 1) al responsable designado por **LA SECRETARÍA** en un lapso no mayor a 10 minutos de la afectación del servicio.	30 min / restablecimiento del servicio máximo 4 horas
Degradación del servicio	Severidad 2	Notificación de incidentes con degradación al servicio (severidad 2) al contacto de seguridad designado por **LA SECRETARÍA** en un lapso no mayor a 20 minutos de la afectación del servicio.	30 min / 6 horas
Intermitencia del Servicio	Severidad 3	Notificación de incidentes con intermitencia al servicio (severidad 3) al contacto de seguridad designado por **LA SECRETARÍA** en un lapso no mayor a 30 minutos de las intermitencias del servicio	30 min / 8 horas
Solicitud de requerimiento	Severidad 4	Incidente sin afectación de servicio, en esta severidad se consideran los tiempos determinados, para cambios de configuraciones urgentes.	30 min / 8 horas
		Respaldo de configuración	30 min / 8 horas
		Actualización de memoria técnica.	30 min / 3 días naturales
		Actualización de sistema operativo	30 min / 8 horas
		Ventanas de mantenimiento programadas y requeridas por el Prestador de Servicios (según él requerimiento)	30 min / hasta 12 hrs
		Cambio de equipos por daño en el propio equipo	1 día hábil / 10 días hábiles

7.1.8. Cartas y certificaciones para el servicio

El licitante deberá presentar carta o cartas membretadas que formen parte de su propuesta, la cual deberá venir dirigida a **LA SECRETARÍA**, donde especifique:

1. Carta expedida por el fabricante donde indique que el licitante es distribuidor autorizado para la actualización del licenciamiento.
2. Carta emitida por el fabricante de la solución propuesta, que acredite que el licitante cuenta con personal certificado en la operación y soporte de la solución (incluir certificados vigentes) y con al menos un ingeniero con la máxima certificación de seguridad del fabricante (incluir certificado vigente)

- El licitante adjudicado deberá entregar carta **3 días hábiles** después de la activación del licenciamiento, donde indique que el soporte y mantenimiento será de la vigencia del

licenciamiento (1 año) a partir de la activación de la renovación de licenciamiento, lo cual no implica el registro de plurianualidad toda vez que el tipo de contratación corresponderá a pago anticipado del servicio (tipo suscripción) en apego a la normatividad en materia de adquisiciones y a fin de garantizar la continuidad del servicio y operatividad de los procesos.

8. Estándares

Se requiere que con los servicios propuestos sea posible estructurar una primera línea de protección bajo un esquema de seguridad institucional. Por esto, **LA SECRETARÍA** requiere de una solución que opere acorde a los procesos de "Administración de Servicios "(ADS), "Administración de la Operación" (AOP), "Administración de la Seguridad de la Información" (ASI), "Operación de los Controles de la Información y del ERISC" (OPEC), "Administración de la Configuración" (ACNF) definidos en el MAAGTICSI.

Las características mínimas requeridas que deberán acompañar a esta solución:

1. Mejorar la administración de la seguridad implementada en **LA SECRETARÍA** en relación a la normatividad vigente del MAAGTICSI.
2. Mantenimiento y soporte operativo de la solución para cumplir con los niveles de servicio solicitados.
3. Realizar un análisis de la situación actual, en base a eso implementar, configurar las reglas de seguridad en los equipos, una vez validadas y aceptadas por **LA SECRETARÍA**.
4. Cambios a políticas y requerimientos de seguridad por parte de **LA SECRETARÍA** solicitados al licitante, que deberán estar alineados a los niveles de servicios y tiempos de respuesta establecidos por la Institución.
5. Administración y monitoreo de los servicios.

9. Transferencia de conocimiento

El licitante adjudicado para los servicios ofertados deberá realizar la transferencia de conocimientos para 6 personas de la solución ofertada sin tener algún costo adicional para **LA SECRETARÍA**.

Asimismo, deberá acordar con **LA SECRETARÍA** la programación para esta actividad una vez concluida la fase de implementación de mejoras, para lo cual se consideran sesiones de 3 horas diarias durante una semana.

Posterior de la transferencia de conocimiento, el licitante adjudicado deberá entregar al administrador del contrato, a más tardar **10 días hábiles** posteriores una vez que se concluya la implementación de mejoras, la o las listas de asistencia y una carta o documento comprobatorio debidamente firmado, de haber llevado a cabo la transferencia de conocimientos conforme a las especificaciones de este anexo técnico.

10. Entregables

La parte de reportes deberán permitir dar a conocer el funcionamiento y situaciones de la operación de los equipos de la solución. El licitante adjudicado deberá proporcionar los reportes solicitados, detallando los eventos más relevantes durante el mes, así como las situaciones más

importantes, tendencias en uso y desempeño (alienados a los procedimientos surgidos de MAAGTICSI).

Los entregables de los servicios durante la vigencia del contrato serán condicionantes para el pago de CFDI (Comprobante Fiscal Digital por Internet) y estos deberán de ser entregados a la Dirección General de Informática y Telecomunicaciones (DGIT) de **LA SECRETARÍA**.

Id. Entregable	Numeral Anexo Técnico	Nombre del entregable	Descripción	Tipo	Fecha de entrega	Periodicidad
1	1.1. Plazo de entrega	Carta de Activación – Renovación de licenciamiento	El licitante adjudicado deberá entregar al administrador del contrato. Carta de activación del Licenciamiento de la solución.	Físico y electrónico	**3 días hábiles** después de su activación.	1 vez (único)
2	1.3. Servicios de ajustes y parametrización	Análisis de la situación actual	Documento del análisis de la situación actual de la configuración actual de los equipos o appliances, firmado y entregado al administrador del contrato	Físico y electrónico	**5 días hábiles** después de la fecha de activación de la licencia	1 vez (único)
3	1.3. Servicios de ajustes y parametrización	Propuesta de mejora	Documento de propuesta de mejora, firmado y entregado al administrador del contrato	Físico y electrónico	**10 días hábiles** posteriores de la entrega del análisis actual	1 vez (único)
4	1.3. Servicios de ajustes y parametrización	Memoria Técnica	Memoria técnica de los ajustes realizados a la solución, la cual deberá contener al menos lo siguiente: I. Descripción del proyecto. II. Cronograma del proyecto III. Diagrama Esquemático de conexiones y configuraciones IV. Documentación de rutas, políticas y configuraciones iniciales y realizadas a los equipos. V. Memoria fotográfica y/o imágenes con	Físico y electrónico	**10 días hábiles** después de su implementación.	1 vez (único)

Id. Entregable	Numeral Anexo Técnico	Nombre del entregable	Descripción	Tipo	Fecha de entrega	Periodicidad
			detalle de lo realizados VI. Respaldo en medio magnético de todas las configuraciones.			
5	1.8. Cartas y certificaciones	Cartas y certificaciones	Cartas membretadas del fabricante	Físico y electrónico	En la propuesta técnica	1 vez (único)
6	1.8. Cartas y certificaciones	Cartas y certificaciones	Carta del soporte y mantenimiento	Físico y electrónico	**3 días hábiles** después de la activación del licenciamiento	1 vez (único)
7	1.3. Servicios de ajustes y parametrización	Reportes de los incidentes o fallas presentadas en el servicio	El licitante adjudicado deberá entregar al administrador los reportes de las fallas.	Físico y electrónico	Los reportes se deberá entregar los primeros **5 días hábiles** posteriores al evento	Por evento (incidente o falla)
8	10.Transferencia de conocimiento	Transferencia de conocimiento	Carta o documento probatorio de la transferencia de documento	Físico y electrónico	**10 días hábiles** posteriores una vez que se concluya la implementación de mejoras	1 vez (único)
9	21. Forma de pago, Administrador de Contrato y Facturación	Forma de pago	**CFDI** El licitante adjudicado deberá entregar el CFDI desglosada de los servicios de acuerdo a la propuesta económica	Físico y electrónico	**5 días hábiles** posteriores a la fecha de emisión con sus respectivos entregables	1 vez (único)

11. Cronograma de Trabajo

Para evaluar la contratación de este servicio, **LA SECRETARÍA** requiere de lo siguiente:

Actividad del Servicio	2020													
	Oct				Nov				Dic					
Activación de licenciamiento			■											
Carta del soporte y póliza de mantenimiento			■											
Análisis de la situación actual			■	■										
Propuesta de mejora					■	■								
Implementación de mejoras							■	■	■					
Memoria Técnica										■	■			
Transferencia de conocimiento										■	■			
MAAGTICSI:														

Acta de Constitución del Proyecto-ADP-F1					■								
Acta de aceptación de entregables. ADP-F2												■	
Reporte de avance sobre el cumplimiento de obligaciones. APRO-F1												■	
Acta de cierre de proyecto. ADP-F3												■	
Cierre del proyecto												■	

- La activación de la renovación de licenciamiento de los equipos propiedad de la Secretaría se realiza a partir del día hábil siguiente de la notificación de fallo, el soporte premium y póliza de mantenimiento estará vigente de acuerdo a los años de renovación del licenciamiento.
- La renovación de licenciamiento son requeridos por:
  1 año

12. Equipo de Trabajo requerido

Es importante señalar que el Licitante adjudicado deberá tener debidamente inscrito en el IMSS al 100% de la plantilla con que prestará el servicio para el área requirente, e igualmente deberá acreditar antes la Dirección General de Informática y Telecomunicaciones el cumplimiento de esta obligación, presentando durante los primeros veinte días naturales posteriores a **cada mes**, las Constancias de las aportaciones Obrero-Patronales al IMSS de cada bimestre, así como el listado del personal asignado en cada centro de trabajo de la SEMARNAT, durante la vigencia del contrato.

Perfil del personal requerido:

- Un Administrador de proyecto certificado como PMP, deseable (más no obligatoria) la certificación en ITIL; mismos que deberán estar vigentes al momento de presentar su propuesta y mantenerse vigentes durante la vigencia del contrato.
- Un Coordinador Experto en la solución que tenga el último nivel de certificación del fabricante de la solución ofertada; misma que deberá estar vigente al momento de presentar su propuesta y mantenerse vigentes durante la vigencia del contrato.

A continuación, se presentan de manera enunciativa más no limitativa, los lineamientos con los que deberá cumplir el licitante sobre la gestión del personal para el servicio de **LA SECRETARÍA**.

- Los licitantes deberán entregar las certificaciones que avalen el cumplimiento del personal requerido.
- Apoyo en actividades de operación del servicio de **LA SECRETARÍA**, independientemente del soporte del licitante adjudicado.
- El personal asignado por el licitante adjudicado, será responsable de la coordinación de actividades con el personal de **LA SECRETARÍA**.

Actividades de cada perfil

TABLA DE PERFILES ESPECIALIZADOS

Nivel de estudios: con estudios a nivel licenciatura en las áreas de Sistemas, Informática, Telecomunicaciones, Electrónica, Industrial, para lo cual deberá presentar en original para su cotejo, documento oficial mediante el cual se demuestre su nivel de estudios.	
Administrador de proyecto	**Experiencia:** 2 años (Demostrables mediante currículo y certificaciones vigentes especificadas en el presente apartado) mediante el cual se acredite que cuenta con dos años de experiencia en operación de similar. **RESPONSABILIDADES:** a) Dirigir y evaluar el proyecto; planear, proponer e implementar políticas de administración de proyectos, asegurar la finalización del proyecto conforme a los compromisos contractuales. b) Desarrollar y mantener los planes del proyecto, darle una calendarización, evaluar y reportar el avance. c) Debe resolver los problemas a través de decisiones orientadas al objetivo. d) Mantener informado al equipo de los eventos especiales, cambios y toda aquella actividad que afecte el servicio. e) Elaborar reportes e informes conforme lo solicite **LA SECRETARÍA**. f) Participar en las reuniones de trabajo que convoque **LA SECRETARÍA**. El personal asignado para las funciones de administrador del proyecto, no requiere estar asignado en las oficinas centrales de **LA SECRETARÍA**. Será el responsable de administrar las actividades del proyecto que se requieran
Coordinador Experto en la Solución	**Partida Única** Especialista en soluciones con experiencia de al menos 2 años, (demostrables mediante currículo y certificaciones vigentes especificadas en el presente apartado) en el diseño de arquitecturas de red para diferentes escenarios de seguridad perimetral, filtrado de contenido web, en proporcionar soluciones que combinen tecnologías de diferentes propósitos, integrándolas bajo las mejores prácticas que se centran en el proceso de seguridad de redes e información, con el objetivo de mitigar los riesgos y alinear los objetivos de la organización con la estrategia de seguridad. Para las actividades que forman parte del servicio, **LA SECRETARÍA** requiere por normatividad vigente, análisis de situación actual e Implementación de mejoras, el licitante cuente con un Coordinador Experto en la Solución que gestione las acciones de análisis, alineación y definición de políticas, procesos y mejores prácticas en la implementación de la solución; así como, asegurarse de la estabilización del servicio, establecer las directrices en materia de respuesta a incidentes de seguridad de la información, con base en la normatividad aplicable para **LA SECRETARÍA**

13. Sistema de administración de alertas

LA SECRETARÍA cuenta con una mesa de servicios basada en la metodología ITIL v3, la cual se encarga del registro y control de incidencias y requerimientos, así como seguimiento de eventos de manera telefónica (01 800 y local), por correo electrónico y/o en herramienta web. La Mesa de Servicios fungirá como único punto de contacto y coordinará de forma centralizada la recepción, distribución y seguimiento de solicitudes de incidentes y de servicio del usuario final, de acuerdo a los niveles de servicio que contemple cada servicio.

El licitante adjudicado deberá contar con un sistema de administración de alertas que genere de manera proactiva (automática) aviso a la mesa de servicio de **LA SECRETARÍA** con una disponibilidad de 7x24x365, con capacidad de recepción, atención y seguimiento de eventos de manera telefónica, por correo electrónico y en herramienta web, mediante una metodología de Punto Único de Contacto hacia la mesa de servicios de **LA SECRETARÍA**.

La mesa de servicios de **LA SECRETARÍA**, será el único punto de contacto para que los usuarios de los activos y servicios de TIC hagan llegar sus solicitudes de servicio. Por lo tanto, el sistema de administración de tickets del licitante adjudicado deberá ejecutar la integración pertinente y definir los mecanismos de comunicación, control y seguimiento hacia la misma, para la atención de los incidentes de servicio y solicitudes del Servicio, con base en los niveles de servicio acordados. El sistema de administración de tickets deberá de operar el primer día de la puesta en marcha de la fase de Operación del Servicio.

El licitante adjudicado deberá ejecutar procedimientos que permitan resolver con rapidez y eficiencia los requerimientos e incidentes que se presenten, así como la integración con la mesa de servicios de **LA SECRETARÍA**.

Con la finalidad de mantener la integridad, confidencialidad y disponibilidad de los activos claves de información relacionados al servicio, el licitante adjudicado podrá levantar de manera proactiva (automática) el ticket o solicitud correspondiente del producto de monitoreo, cuando se detecte la no disponibilidad, degradación o falla de los dispositivos o componentes que habilitan dicho servicio, manteniendo en todo momento la comunicación y seguimiento con la mesa de servicios de **LA SECRETARÍA**.

El licitante adjudicado deberá entregar su matriz de escalación de los servicios requeridos, tabla de incidentes para ser turnados a su mesa dentro de los **primeros 15 días después** de la notificación del fallo.

La fase de implementación del sistema de administración de alertas tendrá una duración máxima de 4 semanas.

14. Vigencia

El contrato del proyecto tendrá una vigencia a partir del día hábil siguiente de la notificación de fallo **y hasta el 31 de diciembre 2020.**

El periodo de la prestación del servicio (renovación del licenciamiento, soporte premium y póliza de mantenimiento de los equipos propiedad de la Secretaría) será establecido de acuerdo al periodo o períodos que establece el fabricante en sus modelos comerciales que, para el caso que nos ocupa, tiene duración de un año a partir de su contratación

Cabe mencionar que el tipo de contrato será cerrado

15. Normas aplicables para la prestación del Servicio

No aplica

16. Garantías

1. Garantía de Cumplimiento del Contrato

A fin de garantizar el debido cumplimiento de las obligaciones derivadas del contrato o los contratos en los términos señalados en el contrato, el licitante adjudicado deberá entregar dentro de los diez días naturales siguientes a la firmas del contrato, fianza indivisible expedida por una institución legalmente autorizada para ello a favor de la Tesorería de la Federación, en el formato autorizado por ésta Institución, por una cantidad equivalente al 10% del monto total del contrato antes del IVA, la cual deberá de mantener vigente hasta la terminación de la vigencia del contrato y en su caso convenio modificatorio.

La fianza deberá ser entregada en la Dirección de Adquisiciones y Contrataciones de **LA SECRETARÍA**, sita en Ejército Nacional 223, Col. Anáhuac, Delegación Miguel Hidalgo, C.P. 11320, México, CDMX piso 17, Ala B.

17. Póliza de Responsabilidad Civil

El licitante adjudicado, deberá mantener durante la vigencia del contrato o los contratos un seguro de responsabilidad civil, contratado con la empresa aseguradora legalmente autorizada, y entregar endoso de la póliza de responsabilidad civil del Prestador de Servicios ganador que ampare una cantidad equivalente al 10% (diez por ciento) del monto total del contrato a favor de **LA SECRETARÍA** por una compañía aseguradora debidamente autorizada, sin incluir el impuesto al valor agregado (IVA), a efecto de garantizar el pago de indemnización hasta por dicha cantidad, por los daños que se puedan ocasionar a los bienes muebles e inmuebles propiedad de **LA SECRETARÍA** a sus empleados o a terceras personas, o de cualquier causa imputable al prestador del servicio o a su personal.

El licitante adjudicado será responsable de la relación laboral de su personal, que esté involucrado en la prestación de los servicios objeto de la presente licitación, liberando de cualquier responsabilidad a **LA SECRETARÍA**.

Si ante cualquier evento o siniestro, esta cobertura resulta insuficiente, los gastos que queden sin cubrir serán por cuenta directamente de "licitante adjudicado".

En caso de que se presente un evento o siniestro y se dictamine la responsabilidad de "licitante adjudicado", éste tendrá un plazo máximo de **5 (cinco) días hábiles**, para realizar los pagos de los daños directamente a **LA SECRETARÍA** afectada y/o terceros implicados; o iniciar las gestiones correspondientes ante la aseguradora que corresponda, para que haga los pagos inmediatamente a dicha institución.

"El licitante adjudicado" deberá mantener durante la vigencia del contrato o contratos una póliza de responsabilidad civil y durante la substanciación de todos los recursos legales o juicios que se interpongan, hasta que se dicte resolución definitiva por autoridad competente, para lo cual, misma que deberá exhibir el original o por correo electrónico dentro de los primeros 15 días hábiles a partir de la notificación del fallo y copia para el expediente, debidamente pagada, documentos que entregará en la Dirección de Infraestructura Tecnológica, sita en Ejército Nacional 223, Col. Anáhuac, Alcaldía Miguel Hidalgo, C.P. 11320, México, CDMX. piso 17, Ala A. Dicha póliza deberá ser por un monto de 10% (diez por ciento) del monto total del contrato y cubrirá los

posibles daños causados a los equipos de seguridad, o bien por el personal que asigne para dar el servicio o atender los reportes (Energía, equipos de cómputo, red de datos).

En caso de que **LA SECRETARÍA** decida prorrogar el plazo por la prestación de los servicios, el "licitante adjudicado" se obliga a presentar una póliza de seguro de responsabilidad civil en los mismos términos señalados y por el período prorrogado.

18. Deducciones, Penalizaciones y Causales de Rescisión

1. Penas convencionales

LA SECRETARÍA considerará como penalizaciones lo siguiente:

Numeral del Anexo Técnico	ID	Descripción	Pena Convencional
7.1.3, 10	1	Analisis de la situación actual	0.2% del monto total del servicio mensual por cada día natural de atraso en la entrega del análisis de la situación actual.
7.1.3, 10	2	Propuesta de mejora	0.2% del monto total del servicio mensual por cada día natural de atraso en la entrega de la propuesta de mejora
7.1.3, 10	3	Memoria Técnica	0.2% del monto total del servicio mensual por cada día natural de atraso en la entrega de la memoria técnica.
7.1.3, 7.1.8, 10, 13	4	El licitante no haga entrega de cada uno de los entregables (únicos y por evento) en el plazo establecido en el Anexo Técnico. – Activación de licencia – Reporte de las fallas y/o incidentes – Carta del soporte y mantenimiento – Póliza del soporte y mantenimiento – Carta o documento probatorio de la transferencia de documento – Matriz de Escalación	0.2% del monto total del pago mensual referente al servicio por cada día natural de atraso en los entregables.

Si en un término de 10 (diez) días naturales persiste el atraso, **LA SECRETARÍA** podrá rescindir administrativamente el contrato y, en su caso, hará efectiva la fianza para el cumplimiento del contrato.

Por lo anterior, el pago del servicio quedará condicionado, proporcionalmente al pago que el prestador del servicio deba efectuar por concepto de penas convencionales por atraso, en el entendido de que, si el contrato es rescindido en términos de lo previsto en la Cláusula de Rescisión, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento del contrato.

Para efectuar este pago, el prestador contará con un plazo que no excederá de 5 (cinco) días hábiles contados a partir de la fecha de recepción de la notificación. En el supuesto de que el cálculo de la penalización contenga centavos, el monto se ajustará a pesos, de tal suerte que las que contengan cantidades que incluyan de 1 hasta 50 centavos, el importe de la penalización se

ajustará a pesos a la unidad inmediata anterior y las que contengan de 51 a 99 centavos, el importe de la penalización se ajustará a pesos a la unidad inmediata superior.

Ambas partes acuerdan que aquellas obligaciones que no tengan establecido en el contrato plazo determinado de cumplimiento no serán objeto de penalización alguna, pero su incumplimiento parcial o deficiente dará lugar a que **LA SECRETARÍA** deduzca su costo del importe correspondiente.

La notificación y cálculo de la pena convencional, corresponde a la Dirección General de Informática y Telecomunicaciones.

2. Deducciones

La aplicación de las deducciones será del 1% por cada día natural sobre el importe de los servicios prestados en forma parcial o deficientemente.

LA SECRETARÍA considerará como deductiva lo siguiente:

Numeral del Anexo Técnico	Obligación	Cálculo para la aplicación de la deducción		Tipo de falta por evento	Límite de eventos permitidos
		% deducción a aplicarse	Aplicación		
7.1.7	Incidentes con afectación de severidad 1	1% (Uno por ciento)	Calculado sobre sobre el importe de los servicios prestados en forma parcial o deficientemente.	Muy Alta	No atender este requerimiento hasta 3 veces en el mismo mes calendario para esta deductiva.
7.1.7	Incidentes con afectación de severidad 2	1% (Uno por ciento)		Alta	No atender este requerimiento hasta 3 veces en el mismo mes calendario para esta deductiva
7.1.7	Incidentes con afectación de severidad 3	1% (Uno por ciento)		Media	No atender este requerimiento hasta 3 veces en el mismo mes calendario para esta deductiva
7.1.7	Solicitud de requerimiento con afectación de severidad 4	1% (Uno por ciento)		Baja	No atender este requerimiento hasta 3 veces en el mismo mes calendario para esta deductiva

En caso de no existir pagos pendientes, la deducción se aplicará sobre la garantía de cumplimiento del contrato y solo para el caso de que la garantía no sea suficiente para cubrir la deducción correspondiente, "EL PRESTADOR DEL SERVICIO" realizará el pago de la deductiva a través esquema E5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA's),

ante alguna de las instituciones bancarias autorizadas, acreditando dicho pago con la entrega del recibo bancario al administrador del contrato.

Lo anterior, en el entendido de que de forma inmediata se cumpla con el objeto del contrato, conforme a lo acordado, en caso contrario **LA SECRETARÍA** podrá iniciar en cualquier momento posterior al incumplimiento el procedimiento de rescisión del contrato, considerando la gravedad del incumplimiento, daños y perjuicios que el mismo pudiera ocasionar a los intereses del Estado, representados por **LA SECRETARÍA**.

Las deducciones económicas se aplicarán sobre la cantidad indicada sin incluir el Impuesto al Valor Agregado, que corresponde al importe de la garantía de cumplimiento.

La notificación y cálculo de las deducciones correspondientes la realizará la Dirección General de Informática y Telecomunicaciones.

3. Causales de Rescisión

Los causales de rescisión establecidos conforme a la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento una vez que se formalice el contrato podrá en cualquier momento rescindir administrativamente el mismo por:

a) Si transfiere en todo o en parte las obligaciones que deriven del contrato a un tercero ajeno a la relación actual.
a) Si cede los derechos de cobro derivados del contrato, sin contar con la conformidad previa por escrito de **LA SECRETARÍA**.
b) Si suspende sin causa justificada la prestación del servicio objeto del Contrato o no le otorgue la debida atención conforme a las instrucciones de **LA SECRETARÍA**.
c) Si cambia de nacionalidad e invoca la protección de su gobierno contra reclamaciones y ordenes de **LA SECRETARÍA**.
d) Si es declarado en concurso mercantil por autoridad competente o por cualquier otra causa distinta o análoga que afecte su patrimonio.
e) Si divulga, transfiere o utiliza la información que conozca en el desarrollo del servicio contratado, sin contar con la autorización expresa de **LA SECRETARÍA**.
f) Si no acepta pagar penalizaciones o no repara los daños o perdidas, por argumentar que no le es directamente imputable, sino a uno de sus asociados o filiales o a cualquier otra causa que no sea de fuerza mayor o caso fortuito.
g) Si transcurrido el tiempo señalado para el inicio de la prestación del servicio, este no se efectúe.
h) Cuando "EL PRESTADOR DEL SERVICIO" y/o su personal, impidan el desempeño normal de labores de **LA SECRETARÍA**, durante la prestación del servicio, por causas distintas a la naturaleza de la prestación del mismo.
i) Cuando exista conocimiento y se corrobore mediante resolución definitiva de autoridad competente que "EL PRESTADOR DEL SERVICIO" incurrió en violaciones en materia penal, civil, fiscal, mercantil o administrativa que redunde en perjuicio de los intereses de **LA SECRETARÍA** en cuanto al cumplimiento oportuno y eficaz en la prestación de los servicios objeto del presente Contrato.

LA SECRETARÍA podrá en cualquier momento rescindir administrativamente el mismo, en caso de cualquier incumplimiento a las obligaciones a cargo del prestador de servicios, sin necesidad de acudir a los tribunales competentes en la materia. Si previamente a la determinación de dar por rescindido el contrato se prestaren los servicios, el procedimiento iniciado quedará sin efecto,

previa aceptación y verificación de **LA SECRETARÍA** de que continúa vigente la necesidad de la prestación del servicio, aplicando, en su caso, las penas convencionales correspondientes.

1. Que el licitante adjudicado no cumpla con los requerimientos establecidos conforme al Anexo Técnico.
2. El licitante adjudicado tenga fallas por evento denominada **Muy alta** de hasta 3 veces en el mismo mes calendario.

19. Forma de pago, Administrador de Contrato y Facturación

NO HABRÁ ANTICIPO ALGUNO y **LA SECRETARÍA** efectuará **UN SOLO PAGO** en pesos mexicanos de acuerdo con lo siguiente:

- El pago por el concepto de renovación de licenciamiento, soporte premium y póliza de mantenimiento será cubierto en su totalidad una vez entregados y a entera satisfacción de **LA SECRETARÍA**:

100 % del total del servicio conforme a la siguiente tabla de entregables, para aplicar el PAGO ÚNICO considerando I.V.A.

Nombre del entregable	Fecha de entrega
Carta de Activación – Renovación de licenciamiento	**3 días hábiles** después de su activación.
Análisis de la situación actual	**5 días hábiles** después de la fecha de activación de la licencia
Propuesta de mejora	**10 días hábiles** posteriores de la entrega del análisis actual
Memoria Técnica	**10 días hábiles** después de su implementación.
Carta del soporte y mantenimiento	**3 días hábiles** después de la activación del licenciamiento
Carta o documento probatorio de la transferencia de documento	**10 días hábiles** posteriores una vez que se concluya la implementación de mejoras

Para ello la propuesta y la CFDI deberán venir desglosadas en costos unitarios de cada uno de los puntos de la TABLA PROPUESTA ECONÓMICA.

El administrador del contrato y responsable de verificar la correcta prestación del servicio será el Ing. Juan Francisco Ferráez Mena, Director de Infraestructura Tecnológica o quien lo sustituya en el cargo, adscrita a la Dirección General de Informática y Telecomunicaciones.

El licitante deberá enviar el CFDI, desglosando el Impuesto al Valor Agregado.

El o los CDFI deberán enviarse a la siguiente dirección de correo electrónico:

INSTITUCIÓN	CORREO PARA RECEPCIÓN DE FACTURACIÓN
LA SECRETARÍA	francisco.ferraez@semarnat.gob.mx

20. Propuesta Económica

Para evaluar la contratación de estos servicios

La propuesta de cotización debe venir desglosada en costos unitarios de cada uno de los servicios descritos en el presente anexo y de acuerdo con la tabla siguiente:

No. Partida	DESCRIPCIÓN DEL SERVICIO	COSTO SIN I.V.A DEL SERVICIO (LICENCIAMIENTO)
Única	Renovación del Licenciamiento de: - Prevención de Amenazas - Tecnología de detección y análisis de malware, ataques día cero - Filtrado de Contenido WEB - Global Protect - Soporte Premium por el fabricante - Póliza de mantenimiento Para Oficina Central de la SECRETARÍA	
	Renovación del Licenciamiento de: - Prevención de Amenazas - Tecnología de detección y análisis de malware, ataques día cero - Filtrado de Contenido WEB - Global Protect - Soporte Premium por el fabricante - Póliza de mantenimiento Para el Centro de Datos	
	Renovación del licenciamiento de: - Consola de administración	
SUBTOTAL		
IVA		
TOTAL		

- Se evaluará el precio aceptable de cada cotización.
- Los precios del servicio solicitado deberán ser fijos durante la vigencia del contrato y/o hasta concluir con la prestación de los servicios ofertados a satisfacción de **LA SECRETARÍA**.
- Los precios del servicio solicitado deberá estar expresado en Moneda Nacional, a dos decimales de acuerdo con la Ley Monetaria en vigor y desglosando el Impuesto al Valor Agregado
- Los precios incluye los costos de implementación, mantenimiento, soporte y operación que impliquen la contratación (recursos materiales, humanos y financieros)

21. Derechos de autor

El licitante adjudicado aceptará que todos los productos incluyendo especificaciones, informes, diseños, desarrollos adicionales, personalizaciones e insumos para el proceso y lo que se obtenga como resultado de la ejecución de este proyecto serán confidenciales y propiedad de **LA SECRETARÍA** con los derechos de autor y en su caso, de propiedad industrial. En su caso, sólo

podrá hacerla del conocimiento de terceros previa autorización del servidor público de **LA SECRETARÍA** facultado para ello. Esto excluye los procesos, metodologías, herramientas, documentos y artefactos propiedad del Prestador de Servicios, previamente informado y demostrado a **LA SECRETARÍA**.

22. Glosario de términos

- **Activo de Información.** Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.
- **Activo clave**. El activo de información que resulta esencial o estratégico para la operación y/o el control de una(s) infraestructura(s) de información esenciales y/o críticas, o incluso de una que no tenga este carácter, pero cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura o en los servicios que soporta.
- **Adware.** Un programa de clase adware es cualquier programa que automáticamente muestra publicidad web al usuario durante su instalación o durante su uso para generar lucro a sus autores. 'Ad' en la palabra 'adware' se refiere a 'advertisement' (anuncios) en idioma inglés.
- **AES.** Advance Encryption Standard, esquema o algoritmo de cifrado por bloques.
- **Antibot.** Mecanismo que permite detectar actividades maliciosas de un atacante en los equipos de punto final.
- **Appliance.** Término en el idioma inglés con significado en castellano como aparato, accesorio, artefacto, etc. En informática, este término se refiere a un aparato o dispositivo electrónico (hardware) provisto de un software embebido (firmware) con la función del sistema operativo, que se utiliza para realizar funciones específicas de la aplicación y enorme complejo de software, por lo que a menudo se utilizan en las grandes redes de ordenadores o la granja de servidores de negocio.
- **CDN.** Content delivery network, es una red de computadoras que contienen copias de datos, colocados en varios puntos de una red con el fin de maximizar el ancho de banda para el acceso a los datos de clientes por la red.
- **DMZ.** Zona desmilitarizada, es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red.
- **ERISC.** Equipo de respuesta a incidentes de seguridad en TIC de la SECRETARÍA.
- **GUI.** Graphical user interface, o interfaz gráfica de usuario es un programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz.
- **Malware.** (del inglés malicious software), también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.[1] El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.
- **Spam.** Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se

denomina spamming. La palabra spam proviene de la segunda guerra mundial, cuando los familiares de los soldados en guerra les enviaban comida enlatada; entre estas comidas enlatadas estaba una carne enlatada llamada spam, que en los Estados Unidos era y sigue siendo muy común.

- **Phishing.** Conocido también como suplantación de identidad, es un término informático que denomina un tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).
- **RFC´s**. Request for Comments, publicaciones que describen los aspectos principales del funcionamiento del Internet, protocolos y procedimientos.
- **RMA.** Return Merchandise Authorization (autorización de devolución de mercancía) usado por distribuidores o corporaciones, para la transacción por el retorno de un producto por defectos para luego repararlo o reemplazarlo o hacer una nota de crédito para la compra de otro producto.
- **Spyware**. El spyware o programa espía es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas.
- Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.
- **SLAs.** Un acuerdo de nivel de servicio o Service Level Agreement, también conocido por las siglas ANS o SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. SGSI
- **SGSI.** El sistema de gestión de seguridad de la información que, por medio del análisis de riesgos y de la definición de controles, define las guías para la implementación, operación, monitoreo, revisión y mejora de la seguridad de la información.
- **TIC.** Las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

Ciudad de México, a 17 de septiembre de 2020

Elaboró

Ing. Paula Ramona Hernández Álvarez
Subdirectora de Atención a Usuarios
paular.hernandez@semarnat.gob.mx

Revisó

Ing. Juan Francisco Ferráez Mena
Director de Infraestructura Tecnológica
francisco.ferraez@semarnat.gob.mx

TITULAR DE LA DIRECCIÓN GENERAL DE INFORMÁTICA Y TELECOMUNICACIONES La presente hoja de firmas corresponde al Proyecto denominado **Seguridad en Telecomunicaciones**

Dr. Enrique Scheinvar Gottdiener enrique.s@semarnat.gob.mx

PROPUESTA TÉCNICA

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

PROPUESTA TÉCNICA

Lugar y fecha de expedición: Ciudad de México a 21 de octubre de 2020.
LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA No. LA-016000997-E72-2020
PARA LA CONTRATACIÓN DEL SERVICIO DE SEGURIDAD EN TELECOMUNICACIONES

SECRETARÍA DE MEDIO AMBIENTE Y
RECURSOS NATURALES
DIRECCIÓN GENERAL DE RECURSOS MATERIALES,
INMUEBLES Y SERVICIOS
DIRECCIÓN DE ADQUISICIONES Y CONTRATOS
P R E S E N T E.-

Yo, **Nancy Grisell Ponce Zúñiga**, como Apoderada Legal de la empresa **B DRIVE IT, S.A. de C.V.**, manifiesto **BAJO PROTESTA DE DECIR VERDAD**, que para el "SERVICIO DE SEGURIDAD EN TELECOMUNICACIONES" ofertado para la LICITACIÓN PÚBLICA NACIONAL ELECTRONICA No. LA-016000997-E72-2020 se presenta la propuesta técnica en el presente documento.

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante preciso lo siguiente:

III. PRECISIONES DE LA CONVOCANTE.

1. Se modifica el Anexo 7 "Cumplimiento de Normas" en su texto.

DICE:
(Nombre representante legal), manifiesto:
Que mí representada, la empresa_____, cumple con las siguientes Normas (las señaladas en el Anexo 1 "Especificaciones Técnicas) para la prestación de los servicios que oferta:

NORMA		ESTABLECE

DEBE DECIR:
(Nombre representante legal), manifiesto:
Que mi representada, la persona_____, que para el servicio que oferta no existen normas de referencia, por lo tanto la prestación del servicio se llevará a cabo conforme a las especificaciones establecidas en el Anexo 1 "Especificaciones Técnicas (Anexo Técnico)".

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 5
e) Idioma
El Idioma será en español.
El contrato derivado de este procedimiento y las proposiciones que prepare la persona licitante, así como toda la correspondencia y documentos relativos a ella, que intercambie con la Convocante, deberán de redactarse en el idioma español, con excepción de los acrónimos que son propios del uso de la adquisición objeto del presente

procedimiento o catálogos que se presente en otro idioma los cuales deberán ir acompañados de su traducción simple al español.
Se le solicita a la convocante aclarar si es correcto entender que para la presentación de la propuesta técnica se deberá de agregar los manuales y folletos de la solución, así como su referenciación con traducción simple al español. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación, la convocante aclara que se podrán presentar solo las hojas de los catálogos, folletos, manuales con su traducción simple al español de las especificaciones solicitadas. En caso de que algunos de estos elementos sólo estén disponibles en otro idioma, el licitante deberá traducir al español todos los elementos sustantivos que permitan a la Convocante evaluar el cumplimiento de su propuesta.

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

1. Antecedentes

Se entenderá como **LA SECRETARÍA** para el efecto del presente procedimiento a **LA SECRETARÍA** de Medio Ambiente y Recursos Naturales.

LA SECRETARÍA es una Institución pública del Gobierno Federal, lo que la hace susceptible a ser blanco de diferentes tipos de ataques a través de Internet; por lo que se requiere de las soluciones y/o herramientas, así como su administración adecuada para que se puedan proteger los servicios de la Institución y los accesos a la red interna en el perímetro como un primer punto de protección contra ataques dirigidos, intentos de engaños a los usuarios y aplicaciones maliciosas, que en caso de ingresar a la red pondrían en riesgo la operación y continuidad de los servicios que se ofrecen a los usuarios internos y externos, también la protección de manera externa.

En años anteriores, **LA SECRETARÍA** ha contado con herramientas de seguridad perimetral con filtrado de contenido que han permitido mitigar y contener este tipo de ataques así como el robo de información, utilizando plataformas especializadas que han demostrado su eficacia. Dada la proliferación y la sofisticación en los métodos y herramientas utilizadas para ataques cibernéticos, hoy es necesario robustecer la infraestructura de red de **LA SECRETARÍA** no sólo a nivel perimetral sino también en sus capas internas.

2. Objetivo General

Proteger la red de **LA SECRETARÍA** ante intentos de acceso y vulneración del perímetro por parte de equipos y redes no autorizadas a trabajar en ella, lo anterior con la finalidad de preservar la información y contribuir a la continuidad y estabilidad de las plataformas informáticas que la almacenan, procesan y transforman. Para lograrlo, es necesario contar con el licenciamiento y los servicios de soporte en materia de seguridad informática que se describen a continuación:

- **B-Drive IT**, proporcionará la renovación del licenciamiento de seguridad a nivel externo o perímetro (Firewall, software para protección de amenazas externas a la red de **LA SECRETARÍA**) para uso en los equipos PA-3250 y consola de administración M-200 (ambos propiedad de **LA SECRETARÍA**);

3. Objetivos específicos

B-Drive IT considera como parte de su propuesta una solución tecnológica que cubre las especificaciones técnicas indicadas en el presente documento.

- Contar con la continuidad en el licenciamiento del firewall permitirá a **LA SECRETARÍA** la protección de los servicios de Internet y la DMZ (este término se usa habitualmente para ubicar servidores a los cuales es necesario sean accedidos desde fuera, como servidores de: correo electrónico, aplicativos, filtrado de correo electrónico, DNS y bases de datos), para así obtener el mejor rendimiento e incrementar la eficiencia de operación para los usuarios y mitigar los riesgos de afectación para estos servicios, por la entrada y ejecución de código malicioso o malware.
- Continuar con la solución de Filtrado de Contenido Web dentro de los mismos firewalls de seguridad perimetral, que permita la administración y la protección de los servicios de internet para obtener el mejor rendimiento, incrementar la eficiencia de operación de los usuarios y mitigar los riesgos de afectación de estos servicios por la entrada y ejecución de código malicioso o malware.

- Creación de VPN para ofrecer una conexión remota y segura por WEB a **LA SECRETARÍA** desde cualquier proveedor de Internet, con el fin de poder hacer uso de los recursos internos de **LA SECRETARÍA**.

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 9
3. Objetivos específicos
• Creación de VPN para ofrecer una conexión remota y segura por WEB a LA SECRETARÍA desde cualquier proveedor de Internet, con el fin de poder hacer uso de los recursos internos de LA SECRETARÍA.
Es correcto entender que la convocante ya cuenta con la conectividad a internet requerida para la creación de VPN, por lo cual no es parte del alcance de esta presente convocatoria. Favor de pronunciarse al respecto

Respuesta
Es correcta su apreciación, se cuenta con los enlaces de internet .

4. Descripción de los Servicios

Todos los servicios de los apartados que a continuación se enlistan serán asignados a un solo licitante mediante una partida única, la cual se describe a continuación.

Partida Única: Renovación del licenciamiento para los equipos PA-3250 y consola de administración M-200 propiedad de LA SECRETARÍA.

Esta renovación permitirá dar continuidad a la detección de posibles amenazas potenciales EXTERNAS (ataques, intrusión, robo y secuestro de información, entre otros) relacionadas con la seguridad de la información, a nivel de la infraestructura tecnológica de **LA SECRETARÍA** que pudieran impactar en la confidencialidad, integridad y disponibilidad de la información de manera preventiva, a fin de tomar acciones correctivas y de mejora, para lo cual se requiere de tecnología especializada y en apego a los procesos relacionados a la seguridad de la información establecidos en el Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI).

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 10
Partida Única: Renovación del licenciamiento para los equipos PA-3250 y consola de administración M-200 propiedad de LA SECRETARÍA.

Esta renovación permitirá dar continuidad a la detección de posibles amenazas potenciales EXTERNAS (ataques, intrusión, robo y secuestro de información, entre otros) relacionadas con la seguridad de la información, a nivel de la infraestructura tecnológica de LA SECRETARÍA que pudieran impactar en la confidencialidad, integridad y disponibilidad de la información de manera preventiva, a fin de tomar acciones correctivas y de mejora, para lo cual se requiere de tecnología especializada y en apego a los procesos relacionados a la seguridad de la información establecidos en el Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI).

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

Se solicita a la convocante indicar si es correcto entender que el proveedor deberá de contar con la experiencia para el soporte y mantenimiento de la solución requerida en el presente Anexo Técnico y para asegurar esto, se deberá integrar como parte de la propuesta carta expedida por el fabricante que avale que el Licitante cuenta con la experiencia y certificaciones solicitadas en el nivel máximo que serán utilizadas para cumplimiento de soporte y mantenimiento de la solución requerida. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación

5. Alcance

Los servicios impactarán a 3500 usuarios a Nivel Nacional, así como los 5,300 dispositivos que operan en la red privada de **LA SECRETARÍA**. Esta red se compone de dos Data Center (Centro de Datos): en Ejército Nacional 223 y el que se encuentra en el site del Edificio de CONAGUA, así como las 31 delegaciones federales.

La renovación de licenciamiento, permitirá que **LA SECRETARÍA** obtenga la renovación de las licencias, el servicio de soporte y mantenimiento de la infraestructura de la plataforma de Palo Alto propiedad de **LA SECRETARÍA**.

B-Drive IT proporcionará el licenciamiento del firewall para seguridad perimetral a partir del inicio del contrato, así como el nivel de soporte técnico que está asociado al esquema de licenciamiento (soporte premium y póliza de mantenimiento).

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 12

5. Alcance

La renovación de licenciamiento, permitirá que LA SECRETARÍA obtenga la renovación de las licencias, el servicio de soporte y mantenimiento de la infraestructura de la plataforma de Palo Alto propiedad de LA SECRETARÍA.

Es correcto entender que adicional a la renovación de las licencias el licitante deberá de considerar el soporte del equipamiento, así como del licenciamiento por parte del fabricante correspondiente por un periodo de un año. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación, deben ser consideradas por 12 meses equivalentes a un año.

6. Beneficios

Con la renovación del licenciamiento se alcanzarán los siguientes beneficios, que contribuirán a brindar mejores servicios a los ciudadanos:

- Permitirá contar con elementos de confidencialidad, protección de datos y análisis del tráfico en la infraestructura tecnológica de **LA SECRETARÍA**.
- Establecimiento de políticas de seguridad para la navegación segura en Internet.
- Aseguramiento para habilitar accesos a puertos seguros de nuestros aplicativos sustantivos e institucionales para navegar a Internet.
- Proteger los sitios de los ataques desde Internet.
- Permitirá a las aplicaciones y sistemas sustantivos y administrativos de **LA SECRETARÍA** mejorar los tiempos de respuesta.

Se solicita a la convocante indicar si es correcto entender que el proveedor deberá de contar con la experiencia para el soporte y mantenimiento de la solución requerida en el presente Anexo Técnico y para asegurar esto, se deberá integrar como parte de la propuesta carta expedida por el fabricante que avale que el Licitante cuenta con la experiencia y certificaciones solicitadas en el nivel máximo que serán utilizadas para cumplimiento de soporte y mantenimiento de la solución requerida. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación

5. Alcance

Los servicios impactarán a 3500 usuarios a Nivel Nacional, así como los 5,300 dispositivos que operan en la red privada de **LA SECRETARÍA**. Esta red se compone de dos Data Center (Centro de Datos): en Ejército Nacional 223 y el que se encuentra en el site del Edificio de CONAGUA, así como las 31 delegaciones federales.

La renovación de licenciamiento, permitirá que **LA SECRETARÍA** obtenga la renovación de las licencias, el servicio de soporte y mantenimiento de la infraestructura de la plataforma de Palo Alto propiedad de **LA SECRETARÍA**.

B-Drive IT proporcionará el licenciamiento del firewall para seguridad perimetral a partir del inicio del contrato, así como el nivel de soporte técnico que está asociado al esquema de licenciamiento (soporte premium y póliza de mantenimiento).

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 12

5. Alcance

La renovación de licenciamiento, permitirá que LA SECRETARÍA obtenga la renovación de las licencias, el servicio de soporte y mantenimiento de la infraestructura de la plataforma de Palo Alto propiedad de LA SECRETARÍA.

Es correcto entender que adicional a la renovación de las licencias el licitante deberá de considerar el soporte del equipamiento, así como del licenciamiento por parte del fabricante correspondiente por un periodo de un año. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación, deben ser consideradas por 12 meses equivalentes a un año.

6. Beneficios

Con la renovación del licenciamiento se alcanzarán los siguientes beneficios, que contribuirán a brindar mejores servicios a los ciudadanos:

- Permitirá contar con elementos de confidencialidad, protección de datos y análisis del tráfico en la infraestructura tecnológica de **LA SECRETARÍA**.
- Establecimiento de políticas de seguridad para la navegación segura en Internet.
- Aseguramiento para habilitar accesos a puertos seguros de nuestros aplicativos sustantivos e institucionales para navegar a Internet.
- Proteger los sitios de los ataques desde Internet.
- Permitirá a las aplicaciones y sistemas sustantivos y administrativos de **LA SECRETARÍA** mejorar los tiempos de respuesta.

- Permitirá contar con análisis del tráfico que genera la infraestructura tecnológica de **LA SECRETARÍA**.
- Asegurar el uso de los puertos seguros en los aplicativos sustantivos e institucionales para navegar a Internet.
- Proteger los dispositivos de ataques desde Internet.

7. Servicios solicitados por LA SECRETARÍA

7.1. Partida Única.- Renovación del licenciamiento para los equipos PA-3250 y consola de administración M-200

B-Drive IT considera como parte de su propuesta una solución tecnológica que cubre las especificaciones técnicas indicadas en el presente documento.

B-Drive IT proporcionará la renovación del licenciamiento que contará con las siguientes características:

- Prevención de Amenazas (Threat prevention).
- Tecnología de detección y análisis de malware (Wildfire), ataques día cero.
- Filtrado de Contenido WEB (PANB URL Filtering).
- Global Protect.
- Consola de administración.
- Soporte Premium por el fabricante.
- Póliza de mantenimiento.

Lo cual involucrará actualizaciones para Filtrado de Contenido Web, Threat Prevention, Wildfire, Global Protect, y el software para la consola de administración.

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 14
7. Servicios solicitados por LA SECRETARÍA
7.1. Partida Única. - Renovación del licenciamiento para los equipos PA-3250 y consola de administración M-200 propiedad de LA SECRETARÍA.
Lo cual involucrará actualizaciones para Filtrado de Contenido Web, Threat Prevention, Wildfire, Global Protect, y el software para la consola de administración.
Es correcto entender que las actualizaciones requeridas serán sobre la última versión soportada por el equipamiento. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación, debe actualizarse a la última versión estable y soportada por el equipamiento.

B-Drive IT proporcionará el soporte 24x7 para apoyar en casos de fallas, configuraciones, contingencias con alguno de los equipos: dos PA-3250 Y un M-200 de forma remota o en sitio conforme a las necesidades de **LA SECRETARÍA**.

B-Drive IT en caso de resultar adjudicado contratará con el fabricante las pólizas de servicio, soporte y mantenimiento por el total de tiempo de la vigencia del soporte.

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

Las Pólizas que se mencionan en este apartado están vinculadas a la licencia del software de Palo Alto que se requiere para la operación de los equipos de seguridad perimetral PA-3250 y consola de administración M-200 propiedad de la Secretaría

7.1.1. Plazo de entrega

B-Drive IT considerará que la renovación del licenciamiento se activará a partir del día hábil siguiente de la notificación del fallo. **B-Drive IT** entregará al administrador del contrato la carta de activación 3 días hábiles después de su activación.

El soporte de la solución iniciará a partir del día hábil siguiente de la notificación del fallo.

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 16
Soporte por parte del licitante en caso de un incidente por personal con máximo nivel de certificación de la marca para análisis de la situación actual, recomendaciones de mejora, implementación de las mejoras, soporte de la solución.
¿Es correcto entender que el personal mencionado hace referencia al coordinador de seguridad para el análisis en la situación actual?

Respuesta
Es correcta su apreciación, se refiere al Coordinador de Seguridad

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 19
Reparar el equipo, en caso de que se presente una falla física o problema, deberá reemplazar el o los equipos por uno de al menos las mismas características o superiores al actual, en el plazo descrito en los niveles de servicio descritos en este Anexo Técnico, sin importar las causas que originaron la interrupción del servicio, siempre y cuando el servicio no sea interrumpido.
Es correcto entender que la convocante permitirá colocar un equipo temporal mientras se realiza el análisis de la falla física o problema en caso de ser requerido. Y deberá tramitar el RMA correspondiente. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación; se aceptaría proporcionar un equipo temporal (puede ser un equipo "demo" o "muestra") realizando el trámite correspondiente mientras se envía a revisión el que sufrió daño, y deberá mantenerse el equipo temporal hasta que el equipo original sea reparado o reacondicionado. De no conseguir la reparación del equipo original antes de quince días hábiles, se documentará formalmente esta situación y se acordará con el administrador del proyecto la permanencia definitiva del equipo temporal o los términos para llevar a cabo una sustitución por un equipo nuevo con las mismas características o superiores al original.

7.1.2. Características del servicio

B-Drive IT considerará la renovación de los siguientes equipos propiedad de **LA SECRETARÍA**:

- 2 equipos Next Generation Firewall PA-3250.
- 1 consola de Administración M-200.

Especificaciones y Requerimientos Técnicos

- Que contemplen lo siguiente:
  - Inspección de tráfico contra amenazas.
  - Filtrado de navegación web y prevención de fuga de información.
- Póliza de servicios nivel 2 (soporte premium)
- Soporte por parte de **B-Drive IT** en caso de un incidente por personal con máximo nivel de certificación de la marca para análisis de la situación actual, recomendaciones de mejora, implementación de las mejoras, soporte de la solución.

Requerimientos del Servicio

B-Drive IT proporcionará un soporte (póliza de mantenimiento) la cual entregará de forma electrónica a los 10 días hábiles después de la notificación del fallo para garantizar el correcto funcionamiento de la solución, así como de los equipos o apliances, por lo que considerará:

- El soporte incluirá sustitución de partes, así como del software y firmware para mantener la operación de los equipos con los que actualmente cuenta **LA SECRETARÍA**.
- El mantenimiento oportuno a los equipos propiedad de **LA SECRETARÍA** al menos una vez después de la firma del contrato, alineado al proceso de AOP (Proceso de Administración de la Operación del MAAGTICSI), para lo cual **B-Drive IT** considerará viáticos, materiales, papelería y demás gastos que se generen para la prestación del servicio sin costo alguno para **LA SECRETARÍA**.
- Reparar el equipo, en caso de que se presente una falla física o problema, reemplazará el o los equipos por uno de al menos las mismas características o superiores al actual, en el plazo descrito en los niveles de servicio descritos en este documento, sin importar las causas que originaron la interrupción del servicio, siempre y cuando el servicio no sea interrumpido.
- Diagnosticar las fallas de hardware o software de los dispositivos que sean parte de la solución, así como generar y dar seguimiento a los reportes que tendrá relación con el fabricante, mismas que serán aplicados para garantizar la continuidad del servicio durante el periodo del soporte.

Requisitos funcionales

B-Drive IT considera como parte de su propuesta una solución tecnológica que cubre las especificaciones técnicas indicadas en el presente documento.

Características del Licenciamiento requerido:

Inspección de tráfico contra Amenazas

Integrar dentro de la misma plataforma licencias con características de inspección avanzada, identificación y bloqueo de tráfico originado por amenazas informáticas, orientado para la protección de los diferentes segmentos de red interna y comunicación hacia el exterior.

La función de protección contra amenazas se administrará completamente dentro de la misma interfaz de administración.

Funcionalidades de detección y bloqueo para:

- Anomalías de tráfico.
- Escaneo de puertos y barrido de hosts.
- Intentos de intrusión por fuerza bruta.
- Detección y bloqueo de intentos de intrusión por explotación de vulnerabilidades a nivel de capa aplicativa entre los diferentes segmentos internos de la institución.
- Protección contra amenazas de tipo spyware a nivel de capa aplicativa.

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

- Protección contra amenazas identificadas previamente y amenazas día cero, aun para aplicaciones permitidas, sin necesidad de bloquear dicha aplicación.
- 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 Botnets y amenazas “Command and Control”
- Protección contra ataques de tipo SYN Flood y UDP Flood.

- La solución incorpora licencias con capacidades para la detección de Amenazas Persistentes – APTs – de forma proactiva, y tomar acción para evitar su propagación y bloqueo de los canales de comunicación establecidos por dichas amenazas hacia el exterior, con un tiempo de respuesta de 1 hora máximo.
- En la protección contra botnets se implementará, en la detección y monitoreo por firmas y por comportamiento, a través de los siguientes criterios:
  - Visita a sitios con contenido malicioso y de propagación de malware en toda la infraestructura de red WAN.
  - Uso de sitios de DNS dinámicos y/o empleados por amenazas.
  - Visita de dominios de reciente registró.
  - Uso de aplicaciones desconocidas.
  - Presencia de tráfico de IRC (chat local).

- Capacidad de realizar la actualización automática de firmas, identificadores o patrones para las funciones de protección contra amenazas.
- La detección y protección contra ataques estará basada en análisis de firmas sobre el flujo de datos en la red.
- Capacidad de soportar la creación de firmas personalizadas de amenazas para cualquier protocolo, basado en patrones personalizados de tráfico a través de expresiones regulares.
- Capacidad de autogeneración de firmas de C2 (Command-and-Control) al momento de detectar tráfico de este tipo pasando por el dispositivo para su identificación y bloqueo.
- Contar con un ambiente de sandbox mejorado, permitiendo hacer análisis dinámico de malware en máquinas físicas (Bare-Metal) además de otros mecanismos para evitar que el malware reconozca que está en un ambiente virtual.
- Soporte ambientes virtualizados en la nube (sandboxing) para la ejecución de archivos para identificación de amenazas avanzadas persistentes, sobre archivos ejecutables y librerías de Windows tales como archivos exe, dll, pdf, archivos de Office y PE.

Filtrado de Navegación Web y prevención de Fuga de Información

Para el control de tráfico hacia redes externas, se requieren licencias con la capacidad de:

- Soportará el volumen de usuarios de **LA SECRETARÍA** indicado en el presente documento.
- Proporcionar facilidades para incorporar el control de sitios en la navegación de los usuarios mediante categorías.
- El filtro de URLs tendrá por lo menos 60 categorías pre-definidas y cuando menos 2500 aplicaciones
- Soporte la creación de nuevas categorías de URL.
- Cuente la funcionalidad de permitir re categorización de sitios.
- Permita la creación de listas de bloqueo para URLs específicas, dominios y grupos de URLs a través de patrones y comodines.
- Los mensajes entregados al usuario por parte del filtrado de URL (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) serán personalizables.
- La solución de Filtrado de Contenido forzará la “Búsqueda Segura” (Safe Search) al menos para

Google, Yahoo y Bing. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales.

- Capacidad de detectar y categorizar las URL's que el usuario pueda ingresar en herramientas de Google para evadir las políticas de filtrado de contenido implementadas, como por ejemplo Google Traslate.
- Cuente con capacidades para el análisis de archivos que se envíen a través de la red que pudieran contener información confidencial y sensible.
- La solución soportará análisis en archivos de formato MS-Word, texto/html, archivos comprimidos.
- La solución soportará el análisis de archivos en al menos los siguientes protocolos:
  - HTTP.
  - POP3.
  - SMTP.
  - IMAP.
  - FTP.
- Capacidad de prevenir la transferencia de datos no autorizada correspondiente a patrones de números de tarjetas de crédito y de seguridad social, entre otras.
- Contar con un mecanismo de prevención de robo de credenciales, evitando que se ingresen credenciales válidas a sitios no autorizados.
- Permitirá el bloqueo de mensajería instantánea (IM).
- Permitirá el bloqueo de aplicaciones Peer-to-Peer.
- Permitirá el bloqueo de Streaming Media.
- Podrá catalogar las páginas por Dominio (o subdominio).
- Permitirá el bloqueo de las amenazas emergentes más comunes como: pop-ups, banners, spyware, adware, compartición de archivos punto a punto (P2P file sharing).
- Soportará que la actualización de la base de datos para el filtrado de contenido se realice en tiempo real y de manera automática.
- Permitirá la personalización de políticas de control de acceso de forma visual en el equipo a través de diferentes parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, atributos, grupos y usuarios de directorio activo de Microsoft.
- Permitirá la creación y utilización de listas blancas y negras
- Permitirá el filtrado basado en reputación de los sitios web, para ello contará con un sistema de reputación "en la nube" administrado y mantenido por el mismo fabricante que permita bloquear de forma dinámica contenido Web malicioso.
- Las actualizaciones de contenido para el filtrado de URL, se actualizará como máximo cada 24 horas.
- Las actualizaciones de los filtros por reputación de URL se actualizarán en tiempo real continuamente, inmediatamente después que hayan sido descubiertas por el fabricante.

Control de Aplicaciones:

- Permitirá el Control de más de 1,000 Aplicaciones Web, permitiendo el control granular de características de aplicaciones tales como Facebook, Twitter, entre otras.
- Tendrá la habilidad de remover de los sitios web contenido seleccionado por los administradores del sistema, eliminando o removiendo código del sitio, para que no sea presentado al usuario final.
- Permitirá el filtrado de tráfico no HTTP, como puede ser el de los programas P2P (eMule, etc.) o IM (mensajería instantánea).
- Identificará el tipo de servicio o aplicación aprovechando la capacidad de realizar filtrados o análisis por cadenas o "body" dentro del código HTML de las páginas o sitios invocados.

Autenticación de los Usuarios:

Integración con un Directorio Activo de Microsoft el cual se encuentra implementado y configurado en Windows R2 2012 sin necesidad de instalar algún componente en los controladores de dominio. Esta integración permitirá que la administración de la solución se efectué por medio de cuentas de usuarios y grupos de administración basadas en el Directorio Activo.

Administración Basada en Roles: es requisito indispensable que se pueda segregar la administración de la seguridad diferenciando claramente los roles de Seguridad de Sistemas y de otras unidades definidas en el Directorio Activo.

Permitirá la segregación de funciones de forma granular, permitiendo así definir el alcance o posibilidades de gestión para cada administrador.

Tendrá la capacidad de presentar al usuario, una página web con mensajes modificables por los administradores del sistema, en caso de algún problema o infracción.

Ofrecerá mecanismos de autenticación tales como: autenticación local, NTLM, LDAP, RADIUS y certificados. Será capaz de evitar la ejecución de códigos maliciosos, notificando al administrador.

Políticas de Protección y Accesos:

La renovación del licenciamiento:

1. Permitir el control de cuotas por tipo de tráfico o aplicación por ancho de banda.
2. Permitir el control de cuotas para los usuarios por tiempo consumido.
3. Permitir el control de cuotas de tamaños de los archivos.
4. Tener la capacidad de utilizar expresiones regulares como perfiles adicionales de seguridad dentro de las políticas.
5. Tener la capacidad de utilizar expresiones booleanas para la creación de políticas.
6. Tener la capacidad de utilizar las políticas en forma anidadas o encadenadas.
7. Estar basadas en:
   - Dirección IP.
   - Rango de Direcciones IP.
   - Subredes y CIDR.
   - Usuarios del Directorio Activo.
   - Grupos de Usuarios del Directorio Activo.

Soportar la configuración de tiempos de conexión mediante la configuración de reglas específicas

VPN:

- Brindará túneles IPSec que soporten algoritmos de cifrado AES con la capacidad de configurar longitudes de llave de 128 o 256 bits, permitiendo configurar al menos los grupos de Diffie-Hellman 1, 2, 5, 14 junto con la capacidad de configurar alguno de los siguientes algoritmos de integridad: MD5, SHA, SHA-1 y SHA256.
- Brindará soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) y soporte para SSL o IKEv2 o IKE main y agressive mode
- De manera opcional podrá ser configurada en modo interface, en esta funcionalidad podrá tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interfaz.
- Se requiere contar con conexión a través de VPN client-to-site, aproximadamente para 100 usuarios (esto es usuarios que ingresan a los aplicativos y bases de datos para realizar cambios o configuraciones en los ambientes de producción o desarrollo).
- Se requiere contar con conexión a través de VPN site-to-site, aproximadamente 100, para realizar conexiones sitio a sitio.

Administración y Reportes

- La renovación del licenciamiento permitirá que la consola centralizada proporcione capacidades de administración y reporteo, incluyendo control de acceso discrecional, auditoría de usuario y sistema y utilerías de restauración de configuración.

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 20
La renovación del licenciamiento deberá permitir que la consola centralizada proporcione capacidades de administración y reporteo, incluyendo control de acceso discrecional, auditoría de usuario y sistema y utilerías de restauración de configuración.
Es correcto entender que la consola de administración está en las instalaciones de la convocante. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación.

- Actividad Web de: Spyware y Malware, uso de video, uso de aplicaciones Web, uso de términos para búsquedas, categorías filtradas, contenido Web, sesiones, perfiles de tráfico, usuarios y autentificación.
- Las cuentas de administrador proporcionaran los siguientes derechos de acceso configurables: negar, sólo lectura, lectura/escritura.
- Ofrecerá reportes preconfigurados y creación de reportes personalizados.
- Los reportes predefinidos proporcionarán información tal como perfiles generales de tráfico, datos de rendimiento especifico de aplicaciones protocolos y usuarios, categorías de filtrado y sesiones

7.1.3. Servicios de ajustes y parametrización

Una vez actualizada la licencia, **B-Drive IT** realizará un análisis de la situación actual de la configuración actual de los equipos o appliances propiedad de **LA SECRETARÍA**, mismo que será documentado, firmado, entregado en físico y electrónico al administrador del contrato, **5 días hábiles** después de la fecha de activación de la licencia.

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 21
7.1.3. Servicios de ajustes y parametrización
Una vez actualizada la licencia, el licitante ganador deberá realizar un análisis de la situación actual de la configuración actual de los equipos o appliances propiedad de LA SECRETARÍA, mismo que deberá ser documentado, firmado, entregado en físico y electrónico al administrador del contrato, 5 días hábiles después de la fecha de activación de la licencia.
¿Es correcto entender que, una vez realizado el análisis de la situación actual, el proveedor adjudicado deberá de implementar y realizar los debidos cambios para una correcta operación de los servicios? Favor de pronunciarse al respecto.

Respuesta
Despúes de realizar un analisis de la situación actual, el proveedor adjudicado entregará una propuesta de mejora, estará será revisada y aprobada por el administrador del contrato, una vez aprobada se implementaran estos cambios para la operación correcta de los servicios.

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

Después de realizar el análisis, **B-Drive IT** generará una propuesta de mejora de la situación actual, que incluirá:

1) Configurar las reglas de seguridad en los equipos, las cuales serán propuestas por el equipo de seguridad de **B-Drive IT** y validadas por el personal designado de acuerdo a los objetivos y lineamientos de normatividad bajo el cual se rige **LA SECRETARÍA**.
2) Cambios a políticas, requerimientos, generación de reportes para apoyo a auditorias y los solicitados como entregables por parte de **LA SECRETARÍA**.

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 22
Después de realizar el análisis, el licitante ganador deberá generar una propuesta de mejora de la situación actual, que deberá incluir:
1) Configurar las reglas de seguridad en los equipos, las cuales serán propuestas por el equipo de seguridad del "licitante" y validadas por el personal designado de acuerdo a los objetivos y lineamientos de normatividad bajo el cual se rige LA SECRETARÍA.
2) Cambios a políticas, requerimientos, generación de reportes para apoyo a auditorias y los solicitados como entregables por parte de LA SECRETARÍA.
Es correcto entender que la implementación de las reglas de seguridad solo aplicará a los equipos mencionados en la presente convocatoria. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación

B-Drive IT, entregará el documento de propuesta de mejora firmado en físico y electrónico **10 días hábiles** posteriores de la entrega del análisis actual, esta propuesta será sometida al visto bueno del administrador del contrato.

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 23
El licitante ganador, deberá entregar el documento de propuesta de mejora firmado en físico y electrónico 10 días hábiles posteriores de la entrega del análisis actual, esta propuesta será sometida al visto bueno del administrador del contrato
En caso de que la propuesta de mejora sea entregada en tiempo y forma y el visto bueno tenga algún contratiempo imputable a la convocante, es correcto entender que el cronograma de actividades deberá de ser actualizado una vez liberada y aceptada la propuesta de mejoras para su ejecución. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación siempre y cuando el contratiempo resulte imputable a la convocante.

Una vez implementada la propuesta de mejora a su término, **B-Drive IT** entregará al administrador del contrato una memoria técnica de los ajustes realizados a la solución, la cual contendrá al menos lo siguiente:

I. Descripción del proyecto.
II. Cronograma del proyecto.
III. Diagrama Esquemático de conexiones y configuraciones.
IV. Documentación de rutas, políticas y configuraciones iniciales y realizadas a los equipos.

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

V. Memoria fotográfica y/o imágenes con detalle de lo realizados.
VI. Respaldo en medio magnético de todas las configuraciones.

Está memoria será entregada **10 días hábiles** después de su implementación.

Reportes por evento

Reporte de las fallas y/o incidentes presentados en donde se incluya la información siguiente:

- Tipos de fallas.
- Causas de las fallas y acciones preventivas y/o correctivas, tiempos promedio de respuesta y solución.
- Solución de la falla de forma detallada, causa origen y solución de raíz a la falla y/o incidente.

El formato del reporte de afectación se definirá de común acuerdo entre **B-Drive IT** y **LA SECRETARÍA**.

LA SECRETARÍA podrá solicitar cualquier otro reporte relacionado con los servicios cubiertos por la(s) póliza(s) durante la vigencia del contrato.

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 24
LA SECRETARÍA podrá solicitar cualquier otro reporte de los servicios contratados y en los tiempos.
Es correcto entender que cualquier reporte adicional solicitado a los descritos en la convocatoria, será realizado con la información que entreguen los equipos propiedad de la convocante. Favor de pronunciarse al respecto.

Respuesta
Se podrán solicitar reportes o informes ejecutivos con información que proporcionan los equipos (por ejemplo; un análisis de tráfico a servidores) siempre y cuando resulten legibles a personas no técnicas.

B-Drive IT alineará su documentación para dicho servicio en la parte de procesos en la implementación y operación conforme a lo definido en el MAAGTICSI (Manual Administrativo de Aplicación General en Materias de Tecnologías de Información y Comunicaciones y de la Seguridad de la Información). Por lo que entregará el llenado de los formatos respectivos que son:

- Acta de Constitución del Proyecto, Formato ADP-F1 (UNICO, AL INICIO)
- Acta de Aceptación de Entregables. Formato ADP-F2 (CUANDO SEAN REQUERIDOS PARA PAGO)
- Acta de cierre de proyecto. Formato ADP F3 (UNICO, AL TÉRMINO)

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 25
El licitante deberá alinear su documentación para dicho servicio en la parte de procesos en la implementación y operación conforme a lo definido en el MAAGTICSI (Manual Administrativo de Aplicación General en Materias de Tecnologías de Información y Comunicaciones y de la Seguridad de la Información). Por lo que deberá entregar el llenado de los formatos respectivos que son:
• Acta de Constitución del Proyecto, Formato ADP-F1 (UNICO, AL INICIO)

• Acta de Aceptación de Entregables. Formato ADP-F2 (CUANDO SEAN REQUERIDOS PARA PAGO)
• Acta de cierre de proyecto. Formato ADP F3 (UNICO, AL TÉRMINO) 12
¿Es correcto entender que los formatos mencionados deberán ser entregados únicamente por el licitante ganador y no son requisito de evaluación y presentación en la propuesta técnica? Favor de pronunciarse al respecto.

Lo anterior, siendo enunciativo más no limitativo, por lo que **LA SECRETARÍA** en caso de requerir el llenado de algún o algunos otros formatos, podrá solicitarlo a **B-Drive IT**.

Los reportes se entregarán los primeros **5 días hábiles** posteriores al evento.

7.1.4. Lugar, tiempo y Control de entrega de los Servicios.

La renovación del licenciamiento de la partida única del presente documento se activar en: Para la Oficina Central de **LA SECRETARÍA**:

- El lugar de entrega de los servicios estará ubicado en el MDF de la Oficina Central con domicilio en Ejército Nacional 223, Planta Baja, Col. Anáhuac, C.P.11320, Alcaldía Miguel Hidalgo; o donde **LA SECRETARÍA** defina.

Para el Centro de Datos

- El lugar de entrega de los servicios estará ubicado en las instalaciones de CONAGUA con domicilio en Av. Insurgente Sur, Col. Copilco el Bajo, Alcaldía Coyoacán, C.P. 04340 o donde **LA SECRETARÍA** defina.

7.1.5. Personal en sitio

B-Drive IT designará, un Coordinador de Seguridad durante la fase de Análisis de Situación Actual e implementación de mejoras, para la coordinación de los servicios durante su implementación y puesta en operación, considerando el liderazgo del diseño de arquitecturas de red para diferentes escenarios de seguridad perimetral, proporcionar soluciones que combinen tecnologías de diferentes propósitos, integrándolas bajo las mejores prácticas que se centran en el proceso de seguridad de redes e información, con el objetivo de mitigar los riesgos y alinear los esfuerzos a la normatividad aplicable en materia de seguridad de la información.

B-Drive IT proporcionará a su personal, los medios y herramientas tecnológicas de trabajo (equipos de cómputo, líneas telefónicas celulares y demás aplicables), requeridas para llevar a cabo sus funciones.

El personal designado por **B-Drive IT**, acudirá a las instalaciones de **LA SECRETARÍA** debidamente identificado y cumplirá con el código de Conducta de la institución.

Para la atención del soporte o mantenimiento a los equipos asignará a un Ingeniero para el soporte de los incidentes que se susciten el cual tenga experiencia de al menos 2 años en Administración de firewalls especificados en la presente partida, el cual podrá atender de manera remota o en sitio de acuerdo a las necesidades de **LA SECRETARÍA**.

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 26
7.1.5. Personal en sitio
Deberá designar el licitante ganador, un Coordinador de Seguridad durante la fase de Análisis de Situación Actual e implementación de mejoras, para la coordinación de los servicios durante su implementación y puesta en operación, considerando el liderazgo del diseño de arquitecturas de red para diferentes escenarios de seguridad perimetral, proporcionar soluciones que combinen tecnologías de diferentes propósitos, integrándolas bajo las mejores prácticas que se centran en el proceso de seguridad de redes e información, con el objetivo de mitigar los riesgos y alinear los esfuerzos a la normatividad aplicable en materia de seguridad de la información.
Es correcto entender que el coordinador de seguridad deberá de estar en sitio y de manera dedicado durante la vigencia del contrato. Favor de pronunciarse al respecto.

Respuesta
El coordinador de Seguridad debe realizar en sitio la fase de análisis e implementación; los tiempos que permanezca en la SEMARNAT dependerán de la duración establecida en el contrato y/o el anexo técnico para esta actividad, debiendo de estar presente en la reunión de entrega de los documentos de estas fases. Se entiende que en el supuesto de un retraso en la entrega de los entregables y servicios correspondientes a estas fases, la convocante aplicará las deductivas y/o penalizaciones que correspondan.

7.1.6. Monitoreo de la solución

B-Drive IT para dar atención a la renovación del licenciamiento y atender los incidentes, integrará una solución que le permita monitorear el servicio, este contará con las siguientes funcionalidades:

- Monitoreo de la disponibilidad de la infraestructura administrada y desempeño de la misma como:
  a) Utilización de los recursos (red, CPU, memoria, disco, etc.)
  b) Bitácoras de los diferentes componentes habilitados para proveer los servicios.

- **LA SECRETARÍA** una vez implementada la licencia y configurado el software, se reserva el derecho de visitar las instalaciones del centro de monitoreo de **B-Drive IT** de manera periódica para validar el monitoreo de la solución.
- La administración y monitoreo de seguridad contará con las siguientes características mínimas:

  a. Atención y soporte de un equipo de personal con experiencia en las tecnologías propuestas, proveyendo un esquema continúo de operaciones y monitoreo 24x7.
  b. Los servicios de administración de seguridad estarán enlazados con la Mesa de Servicios de **B-Drive IT**, lo cual permita tener información de incidentes que potencialmente afectan a **LA SECRETARÍA**.
  c. El centro de monitoreo contará con la infraestructura necesaria para albergar las consolas de administración y monitoreo de la solución propuesta.
  d. El centro de monitoreo de **B-Drive IT** contará con acceso a Internet que permita la conectividad a través de VPN con **LA SECRETARÍA**, el cual garantice el monitoreo de los equipos y su administración.

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 29
c. El centro de monitoreo deberá contar con la infraestructura necesaria para albergar las consolas de administración y monitoreo de la solución propuesta.
¿Es correcto entender que las consolas de administración deberán estar dentro de las instalaciones de la convocante y se le proporcionará permisos al licitante a través de VPN con LA SECRETARIA para garantizar el monitoreo de los equipos y administración desde las instalaciones del licitante? Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación; el equipamiento que el licitante tenga a bien instalar como su centro de monitoreo para entregar los servicios solicitados por la convocante, podrán acceder a la red de LA SECRETARÍA a través de una VPN.

7.1.7. Niveles de Servicio para los equipos

1. Atención de Reportes o Incidentes (soporte premium, póliza de mantenimiento)

Para todas las notificaciones hacia **LA SECRETARÍA** por motivo de algún incidente o evento identificado desde el centro de monitoreo, se llevará a cabo mediante alguno de los siguientes medios en un lapso no mayor a 30 minutos después de ocurrido éste:

1. Teléfono
2. Correo electrónico

Notificación electrónica vía el Portal WEB de Mesa de Servicio

Con niveles de escalamiento de acuerdo a la severidad, definida a continuación:

Actividad	Severidad	Descripción
Incidente de Seguridad	Severidad 1	Afectación de Servicio. Eventos de alto riesgo, los cuales pueden ocasionar un daño severo en los activos de **LA SECRETARÍA**.
Incidente de Seguridad	Severidad 2	Degradación al Servicio. Eventos en donde se requiere que **LA SECRETARÍA** lleve a cabo una acción a partir de la notificación emitida por el Prestador de Servicios.
Incidente de Seguridad	Severidad 3	Intermitencia de Servicio.
Solicitud de requerimiento	Severidad 4	Eventos de investigación, actualización de contenido de seguridad, cambios en configuraciones, Actualizaciones.

Mismos que serán definidos con **LA SECRETARÍA** para identificar cuáles serían incidentes o solicitudes.

1. Administración de Incidentes o Reportes.

El equipo de especialistas de **B-Drive IT** identificará los incidentes con severidad 1, 2, 3 y 4, que afecten la operación del servicio basado en la información recibida del Centro de Monitoreo y Operaciones y deberán ser atendidos de acuerdo a lo siguiente:

Actividad	Severidad	Detección / Notificación	Tiempo de Atención / Resolución
Afectación de servicio	Severidad 1	Incidentes con afectación al servicio (severidad 1) al responsable designado por **LA SECRETARÍA** en un lapso no mayor a 10 minutos de la afectación del servicio.	30 min / restablecimiento del servicio máximo 4 horas
Degradación del servicio	Severidad 2	Notificación de incidentes con degradación al servicio (severidad 2) al contacto de seguridad designado por **LA SECRETARÍA** en un lapso no mayor a 20 minutos de la afectación del servicio.	30 min / 6 horas
Intermitencia del Servicio	Severidad 3	Notificación de incidentes con intermitencia al servicio (severidad 3) al contacto de seguridad designado por **LA SECRETARÍA** en un lapso no mayor a 30 minutos de las intermitencias del servicio	30 min / 8 horas
Solicitud de requerimiento	Severidad 4	Incidente sin afectación de servicio, en esta severidad se consideran los tiempos determinados, para cambios de configuraciones urgentes.	30 min / 8 horas
		Respaldo de configuración	30 min / 8 horas
		Actualización de memoria técnica.	30 min / 3 días naturales
		Actualización de sistema operativo	30 min / 8 horas
		Ventanas de mantenimiento programadas y requeridas por el Prestador de Servicios (según él requerimiento)	30 min / hasta 12 hrs
		Cambio de equipos por daño en el propio equipo	1 día hábil / 10 días hábiles

7.1.8. Cartas y certificaciones para el servicio

B-Drive IT presenta carta o cartas membretadas que formen parte de su propuesta, la cual vendrá dirigida a **LA SECRETARÍA**, donde especifique:

1. Carta expedida por el fabricante donde indique que **B-Drive IT** es distribuidor autorizado para la actualización del licenciamiento.
2. Carta emitida por el fabricante de la solución propuesta, que acredite que **B-Drive IT** cuenta con personal certificado en la operación y soporte de la solución (incluir certificados vigentes) y con al menos un ingeniero con la máxima certificación de seguridad del fabricante (incluir certificado vigente)

Favor de dirigirse al Apartado de Cartas

- **B-Drive IT** entregará carta **3 días hábiles** después de la activación del licenciamiento, donde indique que el soporte y mantenimiento será de la vigencia del licenciamiento (1 año) a partir de la activación de la renovación de licenciamiento, lo cual no implica el registro de plurianualidad toda vez que el tipo de contratación corresponderá a pago anticipado del servicio (tipo suscripción) en apego a la normatividad en materia de adquisiciones y a fin de garantizar la continuidad del servicio y operatividad de los procesos.

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 31
El licitante deberá presentar carta o cartas membretadas que formen parte de su propuesta, la cual deberá venir dirigida a LA SECRETARÍA, donde especifique:
Carta expedida por el fabricante donde indique que el licitante es distribuidor autorizado para la actualización del licenciamiento.
Carta emitida por el fabricante de la solución propuesta, que acredite que el licitante cuenta con personal certificado en la operación y soporte de la solución (incluir certificados vigentes) y con al menos un ingeniero con la máxima certificación de seguridad de fabricante (incluir certificado vigente)
Es correcto entender que las cartas y certificaciones para el servicio deberán ser presentadas en la propuesta técnica y la omisión de alguna de estas será causa de desechamiento. Favor de pronunciarse al respecto
Respuesta
La convocante aclara que estas cartas deben ser presentadas como parte de su propuesta técnica, al no presentarlas no se le otorgaran los puntos en el mecanismo de evaluación y serán causal de desechamiento para el cumplimiento del anexo técnico.

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 32
El licitante deberá presentar carta o cartas membretadas que formen parte de su propuesta, la cual deberá venir dirigida a LA SECRETARÍA, donde especifique:

Carta expedida por el fabricante donde indique que el licitante es distribuidor autorizado para la actualización del licenciamiento.
Carta emitida por el fabricante de la solución propuesta, que acredite que el licitante cuenta con personal certificado en la operación y soporte de la solución (incluir certificados vigentes) y con al menos un ingeniero con la máxima certificación de seguridad de fabricante (incluir certificado vigente)
Es correcto entender que se deberá presentar carta expedida por el fabricante donde indique que el licitante es distribuidor autorizado para distribuir y comercializar la marca solicitada. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación. Se debe entender que la carta que se solicita expedida por el fabricante debe indicar que el licitante es distribuidor autorizado para la actualización del licenciamiento o bien que el licitante es distribuidor autorizado para distribuir y comercializar la marca solicitada.

De acuerdo a la Última Junta de Aclaraciones celebrada el día 14 de octubre de 2020 a las 17:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 38 de B-DRIVE IT, SA. DE C.V. El periodo de la prestación del servicio (renovación del licenciamiento, soporte premium y póliza de mantenimiento de los equipos propiedad de la Secretaría) será establecido de acuerdo al periodo o períodos que establece el fabricante en sus modelos comerciales que, para el caso que nos ocupa, tiene duración de un año a partir de su contratación Se solicita a la convocante aclare si es correcto entender que el licitante deberá entregar como parte de su propuesta una carta del fabricante donde se exprese que el Licitante adquirirá el soporte para el equipo y licenciamiento por un año, favor de pronunciarse al respecto. **Respuesta** Su apreciación no es del todo correcta, las cartas deberán ser presentadas únicamente por el licitante adjudicado durante la fase inicial del proyecto.	Las cartas de Fabricante, al ser un requerimiento de evaluación para la tabla de puntos y porcentajes, es correcto entender que las cartas de fabricante y certificaciones requeridas en la convocatoria y junta de aclaraciones se deberán de presentar como parte de la propuesta técnica del licitante. Favor de pronunciarse al respecto. RESPUESTA ES CORRECTA SU APRECIACIÓN EN CUANTO A LA PRESENTACIÓN DE CARTAS DEL FABRICANTE Y CERTIFICACIONES REQUERIDAS EN LA CONVOCATORIA Y JUNTA DE ACLARACIONES QUE SE ESPECIFICAN COMO PARTE DE LA PROPUESTA TÉCNICA DEL LICITANTE Y/O PARA EL OTORGAMIENTO DE PUNTOS DEL MECANISMO DE EVALUACIÓN; NO OBSTANTE ES CONVENIENTE ACLARAR QUE HAY DOCUMENTACIÓN Y/O REQUISITOS QUE SOLO CORRESPONDE PRESENTAR AL LICITANTE ADJUDICADO DURANTE LA FASE DE ANÁLISIS E IMPLEMENTACIÓN.

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

8. Estándares

Se requiere que con los servicios propuestos sea posible estructurar una primera línea de protección bajo un esquema de seguridad institucional. Por esto, **LA SECRETARÍA** requiere de una solución que opere acorde a los procesos de "Administración de Servicios "(ADS), "Administración de la Operación" (AOP), "Administración de la Seguridad de la Información" (ASI), "Operación de los Controles de la Información y del ERISC" (OPEC), "Administración de la Configuración" (ACNF) definidos en el MAAGTICSI.

Las características mínimas requeridas que acompañará a esta solución:

1. Mejorar la administración de la seguridad implementada en **LA SECRETARÍA** en relación a la normatividad vigente del MAAGTICSI.
2. Mantenimiento y soporte operativo de la solución para cumplir con los niveles de servicio solicitados.
3. Realizar un análisis de la situación actual, en base a eso implementar, configurar las reglas de seguridad en los equipos, una vez validadas y aceptadas por **LA SECRETARÍA**.
4. Cambios a políticas y requerimientos de seguridad por parte de **LA SECRETARÍA** solicitados a **B-Drive IT**, que estarán alineados a los niveles de servicios y tiempos de respuesta establecidos por la Institución.
5. Administración y monitoreo de los servicios.

9. Transferencia de conocimiento

B-Drive IT para los servicios ofertados realizará la transferencia de conocimientos para 6 personas de la solución ofertada sin tener algún costo adicional para **LA SECRETARÍA**.

Asimismo, acordará con **LA SECRETARÍA** la programación para esta actividad una vez concluida la fase de implementación de mejoras, para lo cual se consideran sesiones de 3 horas diarias durante una semana.

Posterior de la transferencia de conocimiento, **B-Drive IT** entregará al administrador del contrato, a más tardar **10 días hábiles** posteriores una vez que se concluya la implementación de mejoras, la o las listas de asistencia y una carta o documento comprobatorio debidamente firmado, de haber llevado a cabo la transferencia de conocimientos conforme a las especificaciones de este documento.

10. Entregables

La parte de reportes permitirá dar a conocer el funcionamiento y situaciones de la operación de los equipos de la solución. **B-Drive IT** proporcionará los reportes solicitados, detallando los eventos más relevantes durante el mes, así como las situaciones más importantes, tendencias en uso y desempeño (alienados a los procedimientos surgidos de MAAGTICSI).

Los entregables de los servicios durante la vigencia del contrato serán condicionantes para el pago de CFDI (Comprobante Fiscal Digital por Internet) y estos serán entregados a la Dirección General de Informática y Telecomunicaciones (DGIT) de **LA SECRETARÍA**.

Id. Entregable	Numeral documento	Nombre del entregable	Descripción	Tipo	Fecha de entrega	Periodicidad
1	1.1. Plazo de entrega	Carta de Activación – Renovación de licenciamiento	**B-Drive IT** entregará al administrador del contrato. Carta de activación del Licenciamiento de la solución.	Físico y electrónico	**3 días hábiles** después de su activación.	1 vez (único)
2	1.3. Servicios de ajustes y parametrización	Análisis de la situación actual	Documento del análisis de la situación actual de la configuración actual de los equipos o appliances, firmado y entregado al administrador del contrato	Físico y electrónico	**5 días hábiles** después de la fecha de activación de la licencia	1 vez (único)
3	1.3. Servicios de ajustes y parametrización	Propuesta de mejora	Documento de propuesta de mejora, firmado y entregado al administrador del contrato	Físico y electrónico	**10 días hábiles** posteriores de la entrega del análisis actual	1 vez (único)
4	1.3. Servicios de ajustes y parametrización	Memoria Técnica	Memoria técnica de los ajustes realizados a la solución, la cual contendrá al menos lo siguiente: I. Descripción del proyecto. II. Cronograma del proyecto III. Diagrama Esquemático de conexiones y configuraciones IV. Documentación de rutas, políticas y configuraciones iniciales y realizadas a los equipos. V. Memoria fotográfica y/o imágenes con detalle de lo realizados VI. Respaldo en medio magnético de todas las configuraciones.	Físico y electrónico	**10 días hábiles** después de su implementación.	1 vez (único)
5	1.8. Cartas y certificaciones	Cartas y certificaciones	Cartas membretadas del fabricante	Físico y electrónico	En la propuesta técnica	1 vez (único)
6	1.8. Cartas y certificaciones	Cartas y certificaciones	Carta del soporte y mantenimiento	Físico y electrónico	3 días hábiles después de la activación del licenciamiento	1 vez (único)

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

7	1.3. Servicios de ajustes y parametrización	Reportes de los incidentes o fallas presentadas en el servicio	**B-Drive IT** entregará al administrador los reportes de las fallas.	Físico y electrónico	Los reportes se entregarán los primeros 5 días hábiles posteriores al evento	Por evento (incidente o falla)
8	10.Transferencia de conocimiento	Transferencia de conocimiento	Carta o documento probatorio de la transferencia de documento	Físico y electrónico	10 días hábiles posteriores una vez que se concluya la implementación de mejoras	1 vez (único)
9	21. Forma de pago, Administrador de Contrato y Facturación	Forma de pago	**CFDI** **B-Drive IT** entregará el CFDI desglosada de los servicios de acuerdo a la propuesta económica	Físico y electrónico	5 días hábiles posteriores a la fecha de emisión con sus respectivos entregables	1 vez (único)

11. Cronograma de Trabajo

Para evaluar la contratación de este servicio, **LA SECRETARÍA** requiere de lo siguiente:

Actividad del Servicio	2020												
	Oct				Nov				Dic				
Activación de licenciamiento			■										
Carta del soporte y póliza de mantenimiento			■										
Análisis de la situación actual			■	■									
Propuesta de mejora					■	■							
Implementación de mejoras							■	■	■				
Memoria Técnica										■	■		
Transferencia de conocimiento										■	■		
MAAGTICSI:													
Acta de Constitución del Proyecto- ADP-F1					■								
Acta de aceptación de entregables. ADP-F2												■	
Reporte de avance sobre el cumplimiento de obligaciones. APRO-F1												■	
Acta de cierre de proyecto. ADP-F3												■	
												■	
Cierre del proyecto												■	

- La activación de la renovación de licenciamiento de los equipos propiedad de **LA SECRETARÍA** a partir del día hábil siguiente de la notificación de fallo, el soporte premium y póliza de mantenimiento estará vigente de acuerdo a los años de renovación del licenciamiento.
- La renovación de licenciamiento son requeridos por:
  1 año

Favor de dirigirse al Apartado de PLAN DE TRABAJO

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 42
1. Cronograma de Trabajo

Para evaluar la contratación de este servicio, LA SECRETARÍA requiere de lo siguiente:

Es correcto entender y considerando de acuerdo a la fecha de fallo siendo esta el 27 de octubre del 2020, y con base al cronograma de actividades incluido en el anexo técnico por la convocante, que el licitante deberá considerar en el cronograma de trabajo las fechas que corresponden a la fecha del fallo hasta el 31 de diciembre del 2020. ¿Es correcta nuestra apreciación?

Respuesta
ara fines de evaluación conforme los numerales: 10 "Entregables" del Anexo Técnico y alineado a los tiempos establecidos en el numeral 11 "Cronograma de Trabajo" del Anexo Técnico.

12. Equipo de Trabajo requerido

Es importante señalar que **B-Drive IT** tendrá debidamente inscrito en el IMSS al 100% de la plantilla con que prestará el servicio para el área requirente, e igualmente acreditará antes la Dirección General de Informática y Telecomunicaciones el cumplimiento de esta obligación, presentando durante los primeros veinte días naturales posteriores a cada mes, las Constancias de las aportaciones Obrero-Patronales al IMSS de cada bimestre, así como el listado del personal asignado en cada centro de trabajo de la SEMARNAT, durante la vigencia del contrato.

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 33
Es importante señalar que el Licitante adjudicado deberá tener debidamente inscrito en el IMSS al 100% de la plantilla con que prestará el servicio para el área requirente, e igualmente deberá acreditar antes la Dirección General de Informática y Telecomunicaciones el cumplimiento de esta obligación, presentando durante los primeros veinte días naturales posteriores a cada mes, las Constancias de las aportaciones Obrero-Patronales al IMSS de cada bimestre, así como el listado del personal asignado en cada centro de trabajo de la SEMARNAT, durante la vigencia del contrato.
Se le solicita a la convocante aclarar si es correcto entender que el personal solicitado deberá de estar de manera dedicada para la prestación de los servicios y estos deberán de tener al menos una antigüedad de 6 Meses de relación laboral con el licitante, lo cual debe ser demostrado con su correspondiente alta al IMSS esto con el fin de garantizar la correcta soporte y mantenimiento. Favor de pronunciarse al respecto.

Respuesta
Por lo que respecta a su pregunta de que el personal deberá estar dedicado al servicio objeto del presente procedimiento me permito aclararle que se debe realizar en sitio la fase de análisis e implementación; los tiempos que permanezca en la SEMARNAT dependerán de la duración establecida en el contrato y/o el anexo técnico para esta actividad. Y para la atención de incidentes el licitante deberá presentarse en sitio para resolver cualquier presunto incidente imputable al producto, como lo estipula la póliza de soporte

Y por lo que al alta del IMSS, es obligación del licitante mantener asegurados a su personal, durante la vigencia del servicio objeto de la presente licitación

De acuerdo a la Última Junta de Aclaraciones celebrada el día 14 de octubre de 2020 a las 17:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 33 Es importante señalar que el Licitante adjudicado deberá tener debidamente inscrito en el IMSS al 100% de la plantilla con que prestará el servicio para el área requirente, e igualmente deberá acreditar antes la Dirección General de Informática y Telecomunicaciones el cumplimiento de esta obligación, presentando durante los primeros veinte días naturales posteriores a cada mes, las Constancias de las aportaciones Obrero-Patronales al IMSS de cada bimestre, así como el listado del personal asignado en cada centro de trabajo de la SEMARNAT, durante la vigencia del contrato. Se le solicita a la convocante aclarar si es correcto entender que el personal solicitado deberá de estar de manera dedicada para la prestación de los servicios y estos deberán de tener al menos una antigüedad de 6 Meses de relación laboral con el licitante, lo cual debe ser demostrado con su correspondiente alta al IMSS esto con el fin de garantizar la correcta soporte y mantenimiento. Favor de pronunciarse al respecto. **Respuesta** Por lo que respecta a su pregunta de que el personal deberá estar dedicado al servicio objeto del presente procedimiento me permito aclararle que se debe realizar en sitio la fase de análisis e implementación; los tiempos que permanezca en la SEMARNAT dependerán de la duración establecida en el	Es correcto entender que, para acreditar la relación laboral entre el personal requerido y el licitante, las constancias de aportaciones al IMSS deberán mostrar la razón social de quien realiza las aportaciones, siendo este el licitante. Favor de pronunciarse al respecto. **RESPUESTA** **ES CORRECTA SU APRECIACIÓN O EN EL CASO DE QUE EL LICITANTE NO TENGA PERSONAL DIRECTO PODRA PRESENTAR EL CONTRATO CORRESPONDIENTE ENTRE EL LICITANTE Y EL TERCERO, E INCLUIR LAS APORTACIONES CORRESPONDIENTES.**
contrato y/o el anexo técnico para esta actividad. Y para la atención de incidentes el licitante deberá presentarse en sitio para resolver cualquier presunto incidente imputable al producto, como lo estipula la póliza de soporte Y por lo que al alta del IMSS, es obligación del licitante mantener asegurados a su personal, durante la vigencia del servicio objeto de la presente licitación	

Perfil del personal requerido:

- Un Administrador de proyecto certificado como PMP, deseable (más no obligatoria) la certificación en ITIL; mismos que estarán vigentes al momento de presentar su propuesta y mantenerse vigentes durante la vigencia del contrato.
- Un Coordinador Experto en la solución que tenga el último nivel de certificación del fabricante de la solución ofertada; misma que estarán vigente al momento de presentar su propuesta y mantenerse vigentes durante la vigencia del contrato.
  Favor de dirigirse al Apartado de CERTIFICACIONES

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 35
Perfil del personal requerido:
Un Coordinador Experto en la solución que tenga el último nivel de certificación del fabricante de la solución ofertada; misma que deberá estar vigente al momento de presentar su propuesta y mantenerse vigentes durante la vigencia del contrato.
Es correcto entender que se deberá de agregar en la propuesta técnica el certificado con el máximo nivel de certificación de la solución. Favor de pronunciarse al respecto.

Respuesta
Es correcta su apreciación.

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

A continuación, se presentan de manera enunciativa más no limitativa, los lineamientos con los que cumplirá **B-Drive IT** sobre la gestión del personal para el servicio de **LA SECRETARÍA**.

- **B-Drive IT** entregará las certificaciones que avalen el cumplimiento del personal requerido.
- Apoyo en actividades de operación del servicio de **LA SECRETARÍA**, independientemente del soporte de **B-Drive IT**.
- El personal asignado por **B-Drive IT**, será responsable de la coordinación de actividades con el personal de **LA SECRETARÍA**.

De acuerdo a la Última Junta de Aclaraciones celebrada el día 14 de octubre de 2020 a las 17:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 34 de B-DRIVE IT, SA. DE C.V. **Perfil del personal requerido:** Un Administrador de proyecto certificado como PMP, deseable (más no obligatoria) la certificación en ITIL; mismos que deberán estar vigentes al momento de presentar su propuesta y mantenerse vigentes durante la vigencia del contrato. Es correcto entender que; para asegurar el correcto soporte y mantenimiento, el administrador de proyecto deberá de presentar como obligatorio la certificación de PMP e ITIL. Favor de pronunciarse al respecto. **Respuesta** No es correcta su apreciación, la de PMP es obligatoria, la certificación ITIL es deseable más no obligatoria; no obstante, dicha certificación será considerada en el otorgamiento de puntos asentado en el mecanismo de evaluación.	Es correcto entender que las certificaciones ITIL y PMP deberán ser incluidas como parte de la propuesta técnica del licitante para el otorgamiento de puntos asentados en el mecanismo de evaluación. Favor de pronunciarse al respecto. **RESPUESTA** **ES CORRECTA SU APRECIACIÓN, DEBERÁN SER INCLUIDAS TALES CERTIFICACIONES PARA QUE PUEDAN SER CONSIDERADAS EN EL OTORGAMIENTO DE PUNTOS ASENTADOS EN EL MECANISMO DE EVALUACIÓN.**

Actividades de cada perfil

TABLA DE PERFILES ESPECIALIZADOS

Nivel de estudios: con estudios a nivel licenciatura en las áreas de Sistemas, Informática, Telecomunicaciones, Electrónica, Industrial, para lo cual presentará en original para su cotejo, documento oficial mediante el cual se demuestre su nivel de estudios.	
Administrador de proyecto	**Experiencia:** 2 años (Demostrables mediante currículo y certificaciones vigentes especificadas en el presente apartado) mediante el cual se acredite que cuenta con dos años de experiencia en operación de similar. **RESPONSABILIDADES:** a) Dirigir y evaluar el proyecto; planear, proponer e implementar políticas de administración de proyectos, asegurar la finalización del proyecto conforme a los compromisos contractuales. b) Desarrollar y mantener los planes del proyecto, darle una calendarización, evaluar y reportar el avance. c) Resolverá los problemas a través de decisiones orientadas al objetivo. d) Mantener informado al equipo de los eventos especiales, cambios y toda aquella actividad que afecte el servicio. e) Elaborar reportes e informes conforme lo solicite **LA SECRETARÍA**. f) Participar en las reuniones de trabajo que convoque **LA SECRETARÍA**. El personal asignado para las funciones de administrador del proyecto, no requiere estar asignado en las oficinas centrales de **LA SECRETARÍA**. Será el responsable de administrar las actividades del proyecto que se requieran

Coordinador Experto en la Solución	**Partida Única** Especialista en soluciones con experiencia de al menos 2 años, (demostrables mediante currículo y certificaciones vigentes especificadas en el presente apartado) en el diseño de arquitecturas de red para diferentes escenarios de seguridad perimetral, filtrado de contenido web, en proporcionar soluciones que combinen tecnologías de diferentes propósitos, integrándolas bajo las mejores prácticas que se centran en el proceso de seguridad de redes e información, con el objetivo de mitigar los riesgos y alinear los objetivos de la organización con la estrategia de seguridad. Para las actividades que forman parte del servicio, **LA SECRETARÍA** requiere por normatividad vigente, análisis de situación actual e Implementación de mejoras, **B-Drive IT** cuente con un Coordinador Experto en la Solución que gestione las acciones de análisis, alineación y definición de políticas, procesos y mejores prácticas en la implementación de la solución; así como, asegurarse de la estabilización del servicio, establecer las directrices en materia de respuesta a incidentes de seguridad de la información, con base en la normatividad aplicable para **LA SECRETARÍA**

13. Sistema de administración de alertas

LA SECRETARÍA cuenta con una mesa de servicios basada en la metodología ITIL v3, la cual se encarga del registro y control de incidencias y requerimientos, así como seguimiento de eventos de manera telefónica (01 800 y local), por correo electrónico y/o en herramienta web. La Mesa de Servicios fungirá como único punto de contacto y coordinará de forma centralizada la recepción, distribución y seguimiento de solicitudes de incidentes y de servicio del usuario final, de acuerdo a los niveles de servicio que contemple cada servicio.

B-Drive IT contará con un sistema de administración de alertas que genere de manera proactiva (automática) aviso a la mesa de servicio de **LA SECRETARÍA** con una disponibilidad de 7x24x365, con capacidad de recepción, atención y seguimiento de eventos de manera telefónica, por correo electrónico y en herramienta web, mediante una metodología de Punto Único de Contacto hacia la mesa de servicios de **LA SECRETARÍA**.

La mesa de servicios de **LA SECRETARÍA**, será el único punto de contacto para que los usuarios de los activos y servicios de TIC hagan llegar sus solicitudes de servicio. Por lo tanto, el sistema de administración de tickets de **B-Drive IT** ejecutará la integración pertinente y definir los mecanismos de comunicación, control y seguimiento hacia la misma, para la atención de los incidentes de servicio y solicitudes del Servicio, con base en los niveles de servicio acordados. El sistema de administración de tickets operará el primer día de la puesta en marcha de la fase de Operación del Servicio.

B-Drive IT ejecutará procedimientos que permitan resolver con rapidez y eficiencia los requerimientos e incidentes que se presenten, así como la integración con la mesa de servicios de **LA SECRETARÍA**.

Con la finalidad de mantener la integridad, confidencialidad y disponibilidad de los activos claves de información relacionados al servicio, **B-Drive IT** podrá levantar de manera proactiva (automática) el ticket o solicitud correspondiente del producto de monitoreo, cuando se detecte la no disponibilidad, degradación o falla de los dispositivos o componentes que habilitan dicho servicio, manteniendo en todo momento la comunicación y seguimiento con la mesa de servicios de **LA SECRETARÍA**.

B-Drive IT entregará su matriz de escalación de los servicios requeridos, tabla de incidentes para ser turnados a su mesa dentro de los primeros 15 días después de la notificación del fallo.

La fase de implementación del sistema de administración de alertas tendrá una duración máxima de 4 semanas.

14. Vigencia

El contrato del proyecto tendrá una vigencia a partir del día hábil siguiente de la notificación de fallo y hasta el **31 de diciembre.**

El periodo de la prestación del servicio (renovación del licenciamiento, soporte premium y póliza de mantenimiento de los equipos propiedad de **LA SECRETARÍA**) será establecido de acuerdo al periodo o periodos que establece el fabricante en sus modelos comerciales que, para el caso que nos ocupa, tiene duración de un año a partir de su contratación.

Cabe mencionar que el tipo de contrato será cerrado

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 36
El contrato del proyecto tendrá una vigencia a partir del día hábil siguiente de la notificación de fallo y hasta el 31 de diciembre 2020.
Se le solicita amablemente a la convocante aclare el periodo de la contratación de los servicios para "La renovación del licenciamiento de seguridad a nivel externo o perímetro (Firewall, software para protección de amenazas externas a la red de LA SECRETARÍA" para uso en los equipos PA-3250 y consola de administración M-200 (ambos propiedad de LA SECRETARÍA)". Favor de pronunciarse al respecto.
Respuesta
Conforme a los numerales del Anexo Técnico:

"7.1.1. Plazo de entrega
La renovación del licenciamiento debe activarse a partir del día hábil siguiente de la notificación del fallo....
El soporte de la solución iniciará a partir del día hábil siguiente de la notificación del fallo.

14. vigencia
...
El periodo de la prestación del servicio (renovación del licenciamiento, soporte premium y póliza de mantenimiento de los equipos propiedad de la Secretaría) será establecido de acuerdo al periodo o períodos que establece el fabricante en sus modelos comerciales que, para el caso que nos ocupa, tiene duración de un año a partir de su contratación.
..."

De acuerdo a la Junta de Aclaraciones celebrada el día 13 de octubre de 2020 a las 10:00 horas la convocante respondió lo siguiente:

PREGUNTA No. 37
El periodo de la prestación del servicio (renovación del licenciamiento, soporte premium y póliza de mantenimiento de los equipos propiedad de la Secretaría) será establecido de acuerdo al periodo o períodos que establece el fabricante en sus modelos comerciales que, para el caso que nos ocupa, tiene duración de un año a partir de su contratación
Es correcto entender que el periodo de licenciamiento con el fabricante deberá de ser de 1 año. Favor de pronunciarse al respecto.
Respuesta
Es correcta su apreciación.

15. Normas aplicables para la prestación del Servicio

No aplica

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

16. Garantías

1. Garantía de Cumplimiento del Contrato

A fin de garantizar el debido cumplimiento de las obligaciones derivadas del contrato o los contratos en los términos señalados en el contrato, **B-Drive IT** entregará dentro de los diez días naturales siguientes a la firmas del contrato, fianza divisible expedida por una institución legalmente autorizada para ello a favor de la Tesorería de la Federación, en el formato autorizado por ésta Institución, por una cantidad equivalente al 10% del monto total del contrato antes del IVA, la cual mantendrá vigente hasta la terminación de la vigencia del contrato y en su caso convenio modificatorio.

La fianza será entregada en la Dirección de Adquisiciones y Contrataciones de **LA SECRETARÍA**, sita en Ejército Nacional 223, Col. Anáhuac, Delegación Miguel Hidalgo, C.P. 11320, México, CDMX piso 17, Ala B.

17. Póliza de Responsabilidad Civil

B-Drive IT, mantendrá durante la vigencia del contrato o los contratos un seguro de responsabilidad civil, contratado con la empresa aseguradora legalmente autorizada, y entregar endoso de la póliza de responsabilidad civil del Prestador de Servicios ganador que ampare una cantidad equivalente al 10% (diez por ciento) del monto total del contrato a favor de la convocante por una compañía aseguradora debidamente autorizada, sin incluir el impuesto al valor agregado (IVA), a efecto de garantizar el pago de indemnización hasta por dicha cantidad, por los daños que se puedan ocasionar a los bienes muebles e inmuebles propiedad de **LA SECRETARÍA** a sus empleados o a terceras personas, o de cualquier causa imputable al prestador del servicio o a su personal.

B-Drive IT será responsable de la relación laboral de su personal, que esté involucrado en la prestación de los servicios objeto de la presente licitación, liberando de cualquier responsabilidad a **LA SECRETARÍA**.

Si ante cualquier evento o siniestro, esta cobertura resulta insuficiente, los gastos que queden sin cubrir serán por cuenta directamente de **B-Drive IT,**

En caso de que se presente un evento o siniestro y se dictamine la responsabilidad de **B-Drive IT**, éste tendrá un plazo máximo de 5 (cinco) días hábiles, para realizar los pagos de los daños directamente a la Institución afectada y/o terceros implicados; o iniciar las gestiones correspondientes ante la aseguradora que corresponda, para que haga los pagos inmediatamente a dicha institución.

B-Drive IT, mantendrá durante la vigencia del contrato o contratos una póliza de responsabilidad civil y durante la substanciación de todos los recursos legales o juicios que se interpongan, hasta que se dicte resolución definitiva por autoridad competente, para lo cual, misma que exhibirá el original al día siguiente a la notificación del fallo y copia para el expediente, debidamente pagada, documentos que entregará en la Dirección de Infraestructura Tecnológica, sita en Ejército Nacional 223, Col. Anáhuac, Alcaldía Miguel Hidalgo, C.P. 11320, México, CDMX. piso 17, Ala A. Dicha póliza será por un monto de 10% (diez por ciento) del monto total del contrato y cubrirá los posibles daños causados a los equipos de seguridad, o bien por el personal que asigne para dar el servicio o atender los reportes (Energía, equipos de cómputo, red de datos).

En caso de que **LA SECRETARÍA** decida prorrogar el plazo por la prestación de los servicios, el **B-Drive IT** se obliga a presentar una póliza de seguro de responsabilidad civil en los mismos términos señalados y por el período prorrogado.

18. Deducciones, Penalizaciones y Causales de Rescisión

1. Penas convencionales

LA SECRETARÍA considerará como penalizaciones lo siguiente:

Numeral del documento	ID	Descripción	Pena Convencional
7.1.3, 10	1	Analisis de la situación actual	0.2% del monto total del servicio mensual por cada día natural de atraso en la entrega del análisis de la situación actual.
7.1.3, 10	2	Propuesta de mejora	0.2% del monto total del servicio mensual por cada día natural de atraso en la entrega de la propuesta de mejora
7.1.3, 10	3	Memoria Técnica	0.2% del monto total del servicio mensual por cada día natural de atraso en la entrega de la memoria técnica.
7.1.3, 7.1.8, 10, 13	4	El licitante no haga entrega de cada uno de los entregables (únicos y por evento) en el plazo establecido en el presente documento. – Activación de licencia – Reporte de las fallas y/o incidentes – Carta del soporte y mantenimiento – Póliza del soporte y mantenimiento – Carta o documento probatorio de la transferencia de documento – Matriz de Escalación	0.2% del monto total del pago mensual referente al servicio por cada día natural de atraso en los entregables.

Si en un término de 10 (diez) días naturales persiste el atraso, **LA SECRETARÍA** podrá rescindir administrativamente el contrato y, en su caso, hará efectiva la fianza para el cumplimiento del contrato.

Por lo anterior, el pago del servicio quedará condicionado, proporcionalmente al pago que el prestador del servicio deba efectuar por concepto de penas convencionales por atraso, en el entendido de que, si el contrato es rescindido en términos de lo previsto en la Cláusula de Rescisión, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento del contrato.

Para efectuar este pago, el prestador contará con un plazo que no excederá de 5 (cinco) días hábiles contados a partir de la fecha de recepción de la notificación. En el supuesto de que el cálculo de la penalización contenga centavos, el monto se ajustará a pesos, de tal suerte que las que contengan cantidades que incluyan de 1 hasta 50 centavos, el importe de la penalización se ajustará a pesos a

la unidad inmediata anterior y las que contengan de 51 a 99 centavos, el importe de la penalización se ajustará a pesos a la unidad inmediata superior.

Ambas partes acuerdan que aquellas obligaciones que no tengan establecido en el contrato plazo determinado de cumplimiento no serán objeto de penalización alguna, pero su incumplimiento parcial o deficiente dará lugar a que **LA SECRETARÍA** deduzca su costo del importe correspondiente.

La notificación y cálculo de la pena convencional, corresponde a la Dirección General de Informática y Telecomunicaciones.

2. Deducciones

La aplicación de las deducciones será del 1% por cada día natural sobre el importe de los servicios prestados en forma parcial o deficientemente.

LA SECRETARÍA considerará como deductiva lo siguiente:

Numeral del documento	Obligación	Cálculo para la aplicación de la deducción		Tipo de falta por evento	Límite de eventos permitidos
		% deducción a aplicarse	Aplicación		
7.1.7	Incidentes con afectación de severidad 1	1% (Uno por ciento)	Calculado sobre sobre el importe de los servicios prestados en forma parcial o deficientemente.	Muy Alta	No atender este requerimiento hasta 3 veces en el mismo mes calendario para esta deductiva.
7.1.7	Incidentes con afectación de severidad 2	1% (Uno por ciento)		Alta	No atender este requerimiento hasta 3 veces en el mismo mes calendario para esta deductiva
7.1.7	Incidentes con afectación de severidad 3	1% (Uno por ciento)		Media	No atender este requerimiento hasta 3 veces en el mismo mes calendario para esta deductiva
7.1.7	Solicitud de requerimiento con afectación de severidad 4	1% (Uno por ciento)		Baja	No atender este requerimiento hasta 3 veces en el mismo mes calendario para esta deductiva

En caso de no existir pagos pendientes, la deducción se aplicará sobre la garantía de cumplimiento del contrato y solo para el caso de que la garantía no sea suficiente para cubrir la deducción correspondiente, "EL PRESTADOR DEL SERVICIO" realizará el pago de la deductiva a través esquema E5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA's), ante alguna de las instituciones bancarias autorizadas, acreditando dicho pago con la entrega del recibo bancario al administrador del contrato.

Lo anterior, en el entendido de que de forma inmediata se cumpla con el objeto del contrato, conforme a lo acordado, en caso contrario **LA SECRETARÍA** podrá iniciar en cualquier momento posterior al incumplimiento el procedimiento de rescisión del contrato, considerando la gravedad del incumplimiento, daños y perjuicios que el mismo pudiera ocasionar a los intereses del Estado, representados por **LA SECRETARÍA**.

Las deducciones económicas se aplicarán sobre la cantidad indicada sin incluir el Impuesto al Valor Agregado, que corresponde al importe de la garantía de cumplimiento.

La notificación y cálculo de las deducciones correspondientes la realizará la Dirección General de Informática y Telecomunicaciones.

3. Causales de Rescisión

Los causales de rescisión establecidos conforme a la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento una vez que se formalice el contrato podrá en cualquier momento rescindir administrativamente el mismo por:

a) Si transfiere en todo o en parte las obligaciones que deriven del contrato a un tercero ajeno a la relación actual.
a) Si cede los derechos de cobro derivados del contrato, sin contar con la conformidad previa por escrito de **LA SECRETARÍA**.
b) Si suspende sin causa justificada la prestación del servicio objeto del Contrato o no le otorgue la debida atención conforme a las instrucciones de **LA SECRETARÍA**.
c) Si cambia de nacionalidad e invoca la protección de su gobierno contra reclamaciones y ordenes de **LA SECRETARÍA**.
d) Si es declarado en concurso mercantil por autoridad competente o por cualquier otra causa distinta o análoga que afecte su patrimonio.
e) Si divulga, transfiere o utiliza la información que conozca en el desarrollo del servicio contratado, sin contar con la autorización expresa de **LA SECRETARÍA**.
f) Si no acepta pagar penalizaciones o no repara los daños o perdidas, por argumentar que no le es directamente imputable, sino a uno de sus asociados o filiales o a cualquier otra causa que no sea de fuerza mayor o caso fortuito.
g) Si transcurrido el tiempo señalado para el inicio de la prestación del servicio, este no se efectúe.
h) Cuando "EL PRESTADOR DEL SERVICIO" y/o su personal, impidan el desempeño normal de labores de **LA SECRETARÍA**, durante la prestación del servicio, por causas distintas a la naturaleza de la prestación del mismo.
i) Cuando exista conocimiento y se corrobore mediante resolución definitiva de autoridad competente que "EL PRESTADOR DEL SERVICIO" incurrió en violaciones en materia penal, civil, fiscal, mercantil o administrativa que redunde en perjuicio de los intereses de **LA SECRETARÍA** en cuanto al cumplimiento oportuno y eficaz en la prestación de los servicios objeto del presente Contrato.

LA SECRETARÍA podrá en cualquier momento rescindir administrativamente el mismo, en caso de cualquier incumplimiento a las obligaciones a cargo del prestador de servicios, sin necesidad de acudir a los tribunales competentes en la materia. Si previamente a la determinación de dar por

rescindido el contrato se prestaren los servicios, el procedimiento iniciado quedará sin efecto, previa aceptación y verificación de **LA SECRETARÍA** de que continúa vigente la necesidad de la prestación del servicio, aplicando, en su caso, las penas convencionales correspondientes.

1. Que **B-Drive IT** no cumpla con los requerimientos establecidos conforme al presente documento.
2. Si **B-Drive IT** tiene un tipo de falta por evento denominada Muy Alta de hasta 3 veces en el mismo mes calendario.

19. Forma de pago, Administrador de Contrato y Facturación

NO HABRÁ ANTICIPO ALGUNO y **LA SECRETARÍA** efectuará **UN SOLO PAGO** en pesos mexicanos de acuerdo con lo siguiente:

- El pago por el concepto de renovación de licenciamiento, soporte premium y póliza de mantenimiento será cubierto en su totalidad una vez entregados y a entera satisfacción de **LA SECRETARÍA**.

  100 % del total del servicio conforme a la siguiente tabla de entregables, para aplicar el PAGO ÚNICO considerando I.V.A.

Nombre del entregable	Fecha de entrega
Carta de Activación – Renovación de licenciamiento	**3 días hábiles** después de su activación.
Análisis de la situación actual	**5 días hábiles** después de la fecha de activación de la licencia
Propuesta de mejora	**10 días hábiles** posteriores de la entrega del análisis actual
Memoria Técnica	**10 días hábiles** después de su implementación.
Carta del soporte y mantenimiento	**3 días hábiles** después de la activación del licenciamiento
Carta o documento probatorio de la transferencia de documento	**10 días hábiles** posteriores una vez que se concluya la implementación de mejoras

Para ello la propuesta y la factura vendrá desglosadas en costos unitarios de cada uno de los puntos de la TABLA PROPUESTA ECONÓMICA.

El administrador del contrato y responsable de verificar la correcta prestación del servicio será el Ing. Juan Francisco Ferráez Mena, Director de Infraestructura Tecnológica o quien lo sustituya en el cargo, adscrita a la Dirección General de Informática y Telecomunicaciones.

B-Drive IT enviará el CFDI, desglosando el Impuesto al Valor Agregado.

El o los CDFI se enviará a la siguiente dirección de correo electrónico:

INSTITUCIÓN	CORREO PARA RECEPCIÓN DE FACTURACIÓN
LA SECRETARÍA	francisco.ferraez@semarnat.gob.mx

21. Derechos de autor

B-Drive IT aceptará que todos los productos incluyendo especificaciones, informes, diseños, desarrollos adicionales, personalizaciones e insumos para el proceso y lo que se obtenga como resultado de la ejecución de este proyecto serán confidenciales y propiedad de **LA SECRETARÍA** con los derechos de autor y en su caso, de propiedad industrial. En su caso, sólo podrá hacerla del conocimiento de terceros previa autorización del servidor público de **LA SECRETARÍA** facultado para ello. Esto excluye los procesos, metodologías, herramientas, documentos y artefactos propiedad del Prestador de Servicios, previamente informado y demostrado a **LA SECRETARÍA**.

23. Glosario de términos

- Activo de Información. Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, será protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.
- Activo clave. El activo de información que resulta esencial o estratégico para la operación y/o el control de una(s) infraestructura(s) de información esenciales y/o críticas, o incluso de una que no tenga este carácter, pero cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura o en los servicios que soporta.
- Adware. Un programa de clase adware es cualquier programa que automáticamente muestra publicidad web al usuario durante su instalación o durante su uso para generar lucro a sus autores. 'Ad' en la palabra 'adware' se refiere a 'advertisement' (anuncios) en idioma inglés.
- AES. Advance Encryption Standard, esquema o algoritmo de cifrado por bloques.
- Antibot. Mecanismo que permite detectar actividades maliciosas de un atacante en los equipos de punto final.
- Appliance. Término en el idioma inglés con significado en castellano como aparato, accesorio, artefacto, etc. En informática, este término se refiere a un aparato o dispositivo electrónico (hardware) provisto de un software embebido (firmware) con la función del sistema operativo, que se utiliza para realizar funciones específicas de la aplicación y enorme complejo de software, por lo que a menudo se utilizan en las grandes redes de ordenadores o la granja de servidores de negocio.
- CDN. Content delivery network, es una red de computadoras que contienen copias de datos, colocados en varios puntos de una red con el fin de maximizar el ancho de banda para el acceso a los datos de clientes por la red.
- DMZ. Zona desmilitarizada, es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red.
- ERISC. Equipo de respuesta a incidentes de seguridad en TIC de **LA SECRETARÍA**.
- GUI. Graphical user interface, o interfaz gráfica de usuario es un programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz.
- Malware. (del inglés malicious software), también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.[1] El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.
- Spam. Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La palabra spam proviene de la segunda guerra mundial, cuando los familiares de los soldados en guerra les enviaban comida enlatada; entre estas comidas enlatadas estaba una carne enlatada llamada spam, que en los Estados Unidos era y sigue siendo muy común.
- Phishing. Conocido también como suplantación de identidad, es un término informático que denomina un tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).
- RFC´s. Request for Comments, publicaciones que describen los aspectos principales del funcionamiento del Internet, protocolos y procedimientos.
- RMA. Return Merchandise Authorization (autorización de devolución de mercancía) usado por distribuidores o corporaciones, para la transacción por el retorno de un producto por defectos para luego repararlo o reemplazarlo o hacer una nota de crédito para la compra de otro producto.

- Spyware. El spyware o programa espía es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas.
- Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.
- SLAs. Un acuerdo de nivel de servicio o Service Level Agreement, también conocido por las siglas ANS o SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. SGSI
- SGSI. El sistema de gestión de seguridad de la información que, por medio del análisis de riesgos y de la definición de controles, define las guías para la implementación, operación, monitoreo, revisión y mejora de la seguridad de la información.
- TIC. Las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

ATENTAMENTE

Nancy Grisell Ponce Zuñiga
Apoderada Legal de
“B DRIVE IT, S.A. de C.V.”

B DRIVE IT S.A. DE C.V. R.F.C. BDI-161222-Q43 Miguel Laurent 15bis, 503,504 , Col. Tlacoquemecatl, Benito Juárez CDMX C.P. 03200
Tel. +52 55 8438 3450 Correo electrónico: contacto@b-drive.com.mx

ANEXO 2

"POPUESTA ECONOMICA"

Lugar y fecha de expedición: Ciudad de México a 21 de octubre de 2020.
LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA No. LA-016000997-E72-2020
PARA LA CONTRATACIÓN DEL SERVICIO DE SEGURIDAD EN TELECOMUNICACIONES

SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES
DIRECCIÓN GENERAL DE RECURSOS MATERIALES, INMUEBLES Y SERVICIOS
DIRECCIÓN DE ADQUISICIONES Y CONTRATOS
P R E S E N T E.-

Yo, **Nancy Grisell Ponce Zúñiga**, como Apoderada Legal de la empresa **B DRIVE IT, S.A. de C.V.**, manifiesto **BAJO PROTESTA DE DECIR VERDAD**, que para el "SERVICIO DE SEGURIDAD EN TELECOMUNICACIONES" ofertado para La LICITACIÓN PÚBLICA NACIONAL ELECTRONICA No. LA-016000997-E72-2020 se presenta la propuesta económica desglosada en costos unitarios de cada uno de los servicios descritos en la propuesta técnica "ANEXO 1" y de acuerdo con la tabla siguiente:

No. Partida	Descripción del Servicio	Costo sin I.V.A. del servicio (Licenciamiento)
Única	Renovación del Licenciamiento de: - Prevención de Amenazas - Tecnología de detección y análisis de malware, ataques día cero - Filtrado de Contenido WEB - Global Protect - Soporte Premium por el fabricante - Póliza de mantenimiento Para Oficina Central de la Secretaría	$ 1,370,260.05
	Renovación del Licenciamiento de: - Prevención de Amenazas - Tecnología de detección y análisis de malware, ataques día cero - Filtrado de Contenido WEB - Global Protect - Soporte Premium por el fabricante - Póliza de mantenimiento Para Centro de Datos	$ 1,370,260.05
	Renovación del Licenciamiento de: Consola de administración	$ 613,758.58
	Sub Total	$ 3,354,278.68
	I.V.A.	$ 536,684.58
	Total	$ 3,890,963.26

SON TRES MILLONES TRES CIENTOS CINCUENTA Y CUATRO MIL DOS CIENTOS SETENTA Y OCHO PESOS (68/100) M.N. SIN IVA, SON TRES MILLONES OCHO CIENTOS NOVENTA MIL NOVECIENTOS SESENTA Y TRES PESOS (26/100) M.N. CON IVA

- **LOS PRECIOS SON EN MONEDA NACIONAL**
- **LOS PRECIOS SON FIJOS DURANTE LA VIGENCIA DEL CONTRATO Y/O HASTA CONCLUIR CON LA PRESENTACIÓN DE LOS SERVICIOS OFERTADOS A SATISFACCIÓN DE LA SECRETARÍA**
- **LOS PRECIOS DEL SERVICIO SOLICITADO ESTAN EXPRESADOS EN MONEDA NACIONAL, A DOS DECIMALES DE ACUERDO CON LA LEY MONETARIA EN VIGOR Y DESGLOSADO EL IMPUESTO AL VALOR AGREGADO.**
- **LOS PRECIOS INCLUYEN LOS COSTOS DE IMPLEMENTACIÓN, MANTENIMIENTO, SOPORTE Y OPERACIÓN QUE IMPLIQUE LA CONTRATACIÓN (RECURSOS, MATERIALES, HUMANOS Y FINANCIEROS).**
- **LOS PRECIOS OFERTADOS YA CONSIDERAN TODOS LOS COSTOS HASTA LA PRESENTACIÓN TOTAL DE LOS SERVICIOS.**
- **LA PROPUESTA ECONÓMICA ESTA VIGENTE DENTRO DEL PROCEDIMIENTO DE LICITACIÓN Y HASTA SU CONCLUSIÓN.**
- **INCLUYEN EL IVA DESGLOSADO.**

A T E N T A M E N T E

Nancy Grisell Ponce Zúñiga
Apoderada Legal de
“B DRIVE IT, S.A. de C.V.”