LICITACIÓN PÚBLICA NACIONAL PRESENCIAL

FORMATO DE COTIZACIÓN

SERVICIOS ADMINISTRADOS DE SEGURIDAD PERIMETRAL Y SERVICIOS ESPECIALIZADOS PARA LA RED DE INFORMATICA"

PARTIDA	SERVICIO	IMPORTE MENSUAL
1	SERVICIOS ADMINISTRADOS DE SEGURIDAD PERIMETRAL Y SERVICIOS ESPECIALIZADOS PARA LA RED DE INFORMATICA"	
	SUBTOTAL	
	IVA	
	TOTAL	

_____

Nombre y Firma del Representante Legal

Monterrey, N. L. a _____ de _____ del 2021

FICHA TÉCNICA
REQUISICION NO.227308

SERVICIOS ADMINISTRADOS DE SEGURIDAD PERIMETRAL Y SERVICIOS ESPECIALIZADOS PARA LA RED INFORMÁTICA DEL GOBIERNO DEL ESTADO DE NUEVO LEÓN.

Cantidad: 01 servicio

COMPONENTE	DESCRIPCIÓN
Servicios Administrados solicitados	Servicios administrados de seguridad perimetral de la Red Informática, además de otros servicios especializados, la cual ayude a proteger los bienes, procesos y servicios basados en el uso de las tecnologías de información y comunicaciones, e información que obre en medios electrónicos, a través de una solución integral de tecnología de alta especialidad y servicios de acuerdo a las siguientes características: • Implementación de una solución integral de tecnología de alta especialidad para proveer servicios administrados de seguridad perimetral de la red informática del Gobierno del Estado de Nuevo León, diseñada especialmente para la protección de los activos tecnológicos que operan en la red y en los sitios principales. • Servicio de protección de seguridad de la red para los servicios de Internet, servicios inherentes a la zona desmilitarizada como aplicativos, sistemas, servicios en línea 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, de la actividad de software mal intencionado, que podría causar pérdida de información, robo de información, o suspensión de procesos de gobierno. • Servicio mensual de revisión y ajustes de la configuración de la tecnología de protección perimetral que pudieran impactar en la confidencialidad, integridad y disponibilidad de la información de manera preventiva, a fin de tomar acciones correctivas y estar alineadas con las mejores prácticas del fabricante y los estándares de seguridad • Servicio de Seguridad para protección del Correo institucional entrante y saliente, se deberá considerar una solución de servicio adaptable en sitio y/o en la nube, considerar 9000 buzones de correo electrónico, que ayude a la prevención de correo no deseado, virus, gusanos, phishing y ataques de denegación de servicio. • Servicio de protección para Aplicaciones y Portales web especializados la solución deberá soportar al menos 50 sitios sin importar la plataforma o tamaño del sitio, lenguaje o escenario de implementación. • Servicio de capacitación continua especializada para el personal a cargo de los Servicios que integran los diferentes elementos de la Seguridad Informática. • Servicio de Mesa de Ayuda 7x24x365, Servicio de Monitoreo y Servicio de Operación de Seguridad (SOC) para proporcionar asistencia y soporte técnico sobre cualquier funcionalidad de la solución propuesta, a través del esquema de servicios administrados en forma compartida.

COMPONENTE	DESCRIPCIÓN
Servicio basado en clusters de alta disponibilidad	Se requiere que el servicio de Seguridad Perimetral esté basado en una solución de al menos una infraestructura configurada en 2 (dos) Clusters físicos de alta disponibilidad en Modo Activo-Pasivo y una Consola de Administración. Los cuales deben ser instalados en 2 Centros de Datos con diferente ubicación. Se requiere la migración de la configuración de la infraestructura actual a la nueva infraestructura, que contemple todo lo necesario, incluyendo Objetos de red, NAT, Políticas, Reglas, e Interfaces, así como elaborar una matriz de validación de servicios. La solución propuesta deberá contar al menos con el siguiente Equipo Requerido: Considerar al menos 2 (dos) Clusters Físicos, cada cluster constituido por 2 (dos) Firewalls de siguiente generación Modo Alta Disponibilidad (HA) Activo-Pasivo o Activo-Activo, los cuales deberán cumplir con al menos las siguientes características: • El equipo deberá proveer los servicios de: Firewall, VPN y Prevención de Amenazas • Ser una solución en hardware (dispositivo o "*appliance*"). • Contar con la Consola de Administración Centralizada • Desempeño de firewall con control de aplicaciones: al menos 17 Gbps • Desempeño de Prevención de Amenazas (IPS, Antivirus, Antispyware, Protección de Malware día cero habilitados simultáneamente): al menos 8 Gbps • Desempeño de VPN: al menos 3 Gbps • Sesiones soportadas al menos: al menos 4,000,000 • Túneles IPSec VPN Soportados: al menos 1,000 • Ruteadores virtuales soportados: al menos 20 • Zonas de seguridad soportadas: al menos 500 • Puertos de Red: al menos 4 x 100/1000/10000, 4 x 1 GbE en Cobre y 4 x 10 GbE en SFP+ en SR. • Deberá de contar con servicios para VPN client to site para al menos 600 usuarios móviles con soporte de Windows 10, Windows 8, MacOS 10 en adelante, Android 5.0 en adelante y IOS 10.0 en adelante. • Capacidad de generar al menos 1,000 VPN Site to Site. • Interfaz de administración fuera de línea adicionales a las solicitadas a la inspección. • Al menos dos interfaces predefinidas para la funcionalidad de alta disponibilidad adicionales a las solicitadas a la inspección. • La solución deberá contar con certificación ICSA Labs y Nist USG v6 tipo NPD para modulo Firewall e IPS. Se requiere que cumpla con las siguientes funcionalidades y características para análisis de amenazas y protección tipo Firewall de siguiente generación integrado:

COMPONENTE	DESCRIPCIÓN
	• Capacidad de identificar y controlar aplicaciones independientemente del puerto, protocolo, cifrado SSL o SSH, o táctica evasiva. • Deberá permitir políticas de uso positivo de aplicaciones, es decir, permitir, negar, habilitar políticas por horario. • Deberá incluir la capacidad de actualización para identificar nuevas aplicaciones. • Deberá incluir la capacidad de creación de políticas basadas en el control por aplicación, por categoría de aplicación, subcategoría de aplicación, tecnología y factor de riesgo. • Deberá incluir la capacidad de creación de políticas basadas en nombre de usuario, grupo de usuario o dirección IP. • Deberá permitir definir instancias virtuales dentro del firewall físico (firewalls virtuales). • La tecnología de identificación de aplicaciones deberá estar habilitada por default (motor de inspección base) sin necesidad de habilitar funcionalidades adicionales. • Deberá incluir herramientas gráficas que permitan tener la vista de aplicaciones que fluyen a través del firewall. • Deberá identificar usuarios a través de integración con Active Directory, LDAP, eDirectory, Syslog Listener y XML-API. • Deberá realizar políticas que permitan el control de aplicaciones, usuarios y contenido mediante una sola política. • Deberá incluir mecanismos de protección contra paquetes fragmentados. • Deberá incluir mecanismos de protección contra ataques de reconocimiento (escaneo). • La identificación de aplicaciones deberá realizarse tan pronto la información llegue al Firewall, sin depender de tecnología de Firewall de estado. • Deberá permitir el manejo de aplicaciones no identificadas, ya sea creando políticas para su inspección y control, además de permitir, desarrollar firmas para la identificación de aplicaciones desconocidas. • Para garantizar el acceso de la plataforma de seguridad, incluso en períodos de alta cantidad de tráfico, la solución deberá contar con procesadores y memorias dedicados a un plano de control (administración del equipo) y deberá integrar procesadores y memorias separados y dedicados específicamente al plano de datos (inspección de usuarios) dentro del mismo dispositivo. • Para aquellos usuarios que no estén integrados al directorio activo del Gobierno del Estado de Nuevo León, por ejemplo, red invitados, deberá permitir la integración con soluciones de autenticación a través de un XML-API configurable. Para esto, deberá incluir el soporte de identificación de usuarios que utilicen direcciones IPv4 e IPv6. • Deberá considerar tecnología que permita descifrar el tráfico SSL y SSH. Deberá permitir lo siguiente: Bloqueo de sesiones SSL con certificados expirados,

COMPONENTE	DESCRIPCIÓN
	Bloqueo de sesiones SSL con certificados no confiables, y Bloqueo de sesiones SSL y SSH para mecanismos de cifrado no soportados. • Deberá incluir la capacidad de limitar la transferencia de archivos no autorizados. • Deberá permitir el control de trasferencia de archivos por aplicación, identificando más de 30 tipos de archivos (DLL, ZIP, EXE, etc.) • Deberá incluir tecnología de identificación de malware moderno contando con la detección de comportamientos maliciosos, detección de tácticas de evasión y aprendizaje de máquina (machine learning). • Deberá incluir la capacidad de análisis malware día cero de archivos ejecutando archivos desconocidos en un SandBox virtualizado. • Deberá incluir la inspección de malware en día cero para documentos del tipo: Ejecutables (EXE), DLL, Office (Word, Excel, Powerpoint) , VBS, Linux ELF, Powershell script, RAR, BAT, 7-zip, PDF, APK, JAR (Java), MacOS y Adobe Flash. • Deberá incluir mecanismos para establecer redes privadas virtuales (VPN) IPsec Site to Site con las siguientes características: Cifrado 3DES, AES 128, 192 y 256 bits, Autenticación MD5, SHA1, SHA256, SHA384, SHA512. • El firewall deberá tener la capacidad de operar en los siguientes modos de manera simultánea mediante el uso de sus interfaces físicas modo sniffer (monitoreo y análisis del tráfico de la red), capa 2 (L2) y Capa 3 (L3): Modo sniffer: Para inspección vía un puerto espejo del tráfico de datos de la red, Modo Capa-2 (L2): Para inspección de datos en línea y tener visibilidad y control del tráfico a nivel aplicación, Modo Capa-3 (L3): Para inspección de datos en línea y tener visibilidad y control del tráfico a nivel aplicación. • Con capacidad de generar ruteo virtual para al menos 100 ruteadores virtuales y manejo de tráfico entre diferentes zonas de seguridad y sub-redes, soportando al menos 500 zonas de seguridad. • Deberá contar con soporte para los siguientes servicios: Soporte de al menos 4,000 redes virtuales VLANs 802.1q, Traducción de direcciones de red (NAT) por fuente y destino, por direcciones IP dinámicas y pool de puertos, Traducción de direcciones IPv6 NAT64, Al menos 10,000 direcciones en tabla de ruteo en IPv4 y al menos 10,000 direcciones en tabla de ruteo en IPv6, PPPoE, Enrutamiento BGP, OSPFv3 y RIP2, Soporte de enrutamiento con base en políticas, Soporte de enrutamiento multicast PIM-SM o PIM-SSM, IGMP v1, v2, v3, BFD (Bidirectional Forwarding Detection), DHCP server y DHCP Relay. • Deberá incluir fuentes de poder redundantes. • En caso de aplicaciones desconocidas, deberá contar con un editor de firmas. • Deberá incluir control de tráfico IPv4 e IPv6, este último también incluye visibilidad e inspección de amenazas en aplicaciones y control de contenido IPv6, debe ser soportado en interfaces trabajando en Capa 2 (L2) y Capa 3 (L3). • Deberá soportar SLAAC en interfaces de IPv6. • Deberá soportar alta disponibilidad en esquemas activo-activo y activo-pasivo.

COMPONENTE	DESCRIPCIÓN
	• Activar alta disponibilidad con base en el estado de interfaz o Monitoreo de conectividad para activar alta disponibilidad. • Deberá soportar geo localización para la creación de políticas con base en la región/país o zona geográfica. • Deberá incluir características para la definición de criterios y complejidad mínima para contraseña y soportar al menos los siguientes criterios: Longitud mínima de contraseña, Número mínimo de mayúsculas, Número mínimo de minúsculas, Número mínimo de caracteres numéricos, Número mínimo de caracteres no alfanuméricos, Prevenir el uso de contraseñas previas, Prevenir el uso de nombre de usuario como contraseña, Advertencia de expiración de contraseña, Forzar el cambio de contraseña en un periodo específico. • Capacidad para crear listas dinámicas a partir del registro de algún evento en el log de seguridad, obteniendo leer de forma dinámica el origen y/o destino IP para asociarlo a una etiqueta dinámica, por ejemplo, a partir del registro de un evento tipo malware asociará a la dirección IP víctima de forma automática a una etiqueta dinámica de direcciones IPs, donde se asociarán a una política restrictiva de seguridad para impedir conexiones subsecuentes a dicho evento. • Soporte a la creación de políticas de autenticación cuando el destino sea de altamente restringido sin la necesidad de instalar algún cliente en el endpoint, es decir de forma transparente, solicitará automáticamente al usuario final autenticación tipo Multifactor (MFA), evitando el acceso a servidores únicamente por usuario y contraseña. Este módulo deberá ser compatible al menos con PingID, Duo y Okta. Deberá incluir las siguientes funcionalidades y características para la Prevención de Amenazas: • El equipamiento deberá tener un rendimiento mínimo de 9 Gbps en modo de IPS. • La licencia de IPS deberá permitir la protección contra amenazas de virus, spyware y otras clases de malware sin costo adicional. • Deberá incluir también, dentro del mismo equipo, el control de transferencia de archivos y bloqueo de archivos por tipo. • Deberá incluir la capacidad de creación de políticas de inspección basadas en nombre de aplicación, categoría de aplicación y tipo de tecnología. • Deberá incluir la capacidad de creación de políticas de inspección basadas en nombre de usuario, grupos de usuarios o Dirección IP. • Deberá permitir crear firmas para identificar las aplicaciones desarrolladas por la entidad. • Deberá permitir la personalización de firmas "phone home" de spyware. • La solución deberá permitir el diseño de firmas de vulnerabilidades. • La solución deberá permitir la detección y bloqueo de amenazas sobre puertos no estándares, tomando como criterio la política de seguridad definida con base en aplicaciones. • Deberá realizar análisis bidireccionales de paquetes SSL/TLS/SSH e identificación de aplicaciones que viajen en el túnel SSL para detener el empleo

COMPONENTE	DESCRIPCIÓN
	de aplicaciones que utilizan tácticas evasivas para viajar de modo cifrado, tales como: PROXIES-SSL, ULTRASURF, SKYPE, y ataques mediante el puerto 443. Este análisis deberá poderse realizar, aunque la sesión SSL no utilice el puerto 443. • Deberá incluir la funcionalidad de protección contra amenazas de red, bloqueo de virus, spyware, control de transferencia de archivos, control de la navegación en Internet y bloqueo de archivos por tipo. • Deberá permitir la protección contra descargas involuntarias de archivos ejecutables maliciosos al usar el protocolo HTTP. • Deberá permitir la inspección en archivos comprimidos que usan algoritmo deflate (zip, gzip, etc.) • La actualización de firmas de ataques deberá poder realizarse de manera diaria y semanal. • Los dispositivos deberán tener los siguientes mecanismos, realizar la detección y protección de ataques de Red como: Análisis basado en protocolo, Protección contra anomalías basadas en protocolo para detectar uso de protocolos sin cumplimento de RFC, Identificación de patrones que detecte ataques a través de más de un paquete, tomando en cuenta elementos como el orden y secuencia de arribo, Análisis heurísticos que detecten paquetes anómalos y patrones de tráfico como escaneo de puertos y Host Sweeps, Bloqueo de paquetes malformados o inválidos, defragmentación IP, reensamble TCP para protección contra métodos de ofuscación y evasión, Protección contra malformación de paquetes, Análisis heurístico. • Deberá permitir el diseño de firmas de vulnerabilidades. • Deberá tener capacidad de firmas basadas en DNS para detectar búsquedas específicas de DNS hacia nombres de equipo que han sido asociados con malware. La solución deberá permitir habilitar/deshabilitar las firmas de DNS para crear excepciones. • Deberá tener la capacidad de un módulo de protección a ataques DNS del tipo DGA, DNS tunneling y machine learning, basado en nube consiguiendo tener predictibilidad de posible nuevos ataques. • Deberá contar con la funcionalidad de DNS Sinkhole para la reescritura de resoluciones de nombres maliciosas. Se requiere que incluya las siguientes funcionalidades y características para el Filtrado de Contenido: • Deberá poder ofrecer la opción de usar ya sea una base de datos de URLs de terceros o la desarrollada por el fabricante. • La plataforma propuesta deberá incluir la funcionalidad de Filtrado de Contenido sin necesidad de añadir hardware, procesadores ni memoria extra. • Deberá contar con al menos 60 categorías predefinidas. • La plataforma propuesta deberá soportar la funcionalidad de desencripción SSL sin necesidad de añadir hardware, procesadores ni memoria extra.

COMPONENTE	DESCRIPCIÓN
	• La solución de filtrado de contenido deberá incluir la capacidad de creación de políticas de filtrado con base al nombre de usuario o grupo de usuarios definidos en el directorio de la convocante. • Deberá permitir configurar acciones como: Permitir, el acceso a la página web, • Bloquear, el acceso a una página web, continuar, cuando un usuario acceda a una página que no cumpla con las políticas definidas, mostrando una página de advertencia y mostrando un botón para continuar, Opción de override: para solicitarle al usuario una contraseña que le permita continuar navegando. • Deberá bloquear el uso de aplicaciones tipo Proxy, ToR y Ultrasurf. • Además de las funciones de bloqueo, el motor de URL deberá permitir usar las categorías identificadas para definir criterios de desencripción de SSL. • Deberá permitir prevenir la carga/descarga de archivos para categorías que representen alto riesgo. Deberá permitir a los administradores del sistema, crear categorías personalizadas • Deberá permitir obtener reportes de uso de actividad por usuario, que muestren las aplicaciones utilizadas, las categorías URL visitadas, y un reporte detallado de los URL´s visitados en un periodo de tiempo específico. • Deberá contar con una variedad de al menos 30 reportes que desplieguen las categorías URL visitadas, los sitios web visitados, los usuarios que fueron bloqueados, los sitios que fueron bloqueados, etc. • Deberá permitir la creación de búsquedas en los logs a través de expresiones regulares. El resultado de la búsqueda de registros deberá poder guardarse y exportarse. • Los registros de los accesos a las páginas deberán poder enviarse a un servidor de logs. Se requiere que incluya las siguientes funcionalidades y características de VPN (Red Privada Virtual): • La solución deberá contar con capacidades la Red Privada Virtual (por sus siglas en Ingles VPNs) para el envío y recepción de información de forma cifrada, basada en el estándar IPSec. • Deberá contar con la funcionalidad de establecer túneles seguros sitio a sitio con funcionalidades mínimas de cifrado AES 256, AES 192, AES 128, 3DES y DES. • Los túneles de VPN deberán contar con soporte de llaves Diffie Hellman mínimos de grupos 1,2,5, 14, 19 y 20. Y métodos de autenticación MD5, SHA1, SHA256, SHA384 y SHA512. • Soporte de distribución de ruteo dinámico y estático en túneles de VPN, para la conectividad de sitios remotos. • Soporte de IKEv1 y IKEv2 • Soporte de DPD (Dead Peer Detection) • Soporte de VPNs en modo Main Mode, aggressive Mode y auto-detección.

COMPONENTE	DESCRIPCIÓN
	• La solución deberá contar con túneles cliente a sitio con funcionalidad de completar la VPN via IPSec en dado caso que no sea posible se auto-conectará vía SSL. • La solución deberá contar al menos con 1,000 túneles simultáneos sitio a sito y al menos 600 túneles cliente a sitio soportando Windows y MacOS • Deberá contar con la capacidad de VPNs cliente a sitio con la funcionalidad de revisar el estado del host, es decir, si el Firewall personal se encuentra activo, el estado de la solución de antimalware, parches del sistema operativo y algunas condiciones como entradas en el registry, para permitir no el acceso de uso en políticas de aplicaciones a través del Firewall de siguiente generación. Se requiere que cumpla con las siguientes funcionalidades y características para la administración del equipo y reporteo: • La administración de políticas y objetos deberá realizarse a través de interface gráfica embebida en el equipo Firewall basada en Web y Administración del equipo a través de CLI (ssh y puerto consola) y adicionalmente va una consola de administración centralizada basada en un appliance con capacidad de almacenamiento de al menos 16 TB en disco en RAID1. • Deberá soportar Syslog y SNMPv3. • Deberá desplegar un resumen gráfico de aplicaciones y amenazas. • Deberá desplegar las aplicaciones con el mayor número de sesiones o Deberá desplegar las aplicaciones con el mayor factor de riesgo. • Deberá permitir crear de manera automática búsquedas a la base de datos de registros a partir de la navegación de uso principal de aplicaciones. • Deberá permitir la generación de reportes de actividad de usuarios, con base en el tiempo, los cuales deberán incluir listado de aplicaciones utilizadas, categoría y subcategoría de aplicaciones utilizadas. • Envío de reportes por correo de manera automática. • Generación de reportes personalizados permitiendo seleccionar la base de datos de registro a utilizar, así como el periodo de tiempo a emplear en el reporte incluyendo la capacidad de proporcionar un resumen gráfico. • Deberá contar con la funcionalidad para exportar logs de tráfico y amenazas. • Deberá permitir la creación de reportes personalizados. • Deberá contar con herramientas para crear filtros de monitoreo de las sesiones en el Firewall, por aplicación y por origen y/o destino. • Deberá proporcionar como mínimo los siguientes tipos de reportes: Utilización en bytes por aplicación, Número de sesiones por aplicación, Comparativo de utilización de aplicaciones (por consumo o por sesiones) con respecto a periodos anteriores, considerando al menos 24 horas antes y hasta 30 días, Principales aplicaciones circulando a través del Firewall, Principales direcciones IP (origen o destino) por aplicación, Reporte de actividades específicas por usuario, Origen o destino del tráfico por aplicación-usuario.

COMPONENTE	DESCRIPCIÓN
	• Deberá permitir la creación de expresiones regulares para hacer búsquedas o queries. • Deberá permitir la muestra de los registros del Firewall y amenazas del IPS con base en la información de contexto que se esté mostrando en ese momento en la herramienta de monitoreo. • Deberá permitir generar reportes de aplicaciones tipo SaaS. • Deberá incluir funcionalidades de prevención de robo de credenciales, detectando el momento en que los usuarios envían credenciales corporativas válidas a un sitio. Este procedimiento puede realizarse de acuerdo a un grupo de usuarios de LDAP e identificación de usuarios activos en la red.
Entregable	Informe mensual impreso y en versión electrónica acerca del servicio de solicitado y asistencia técnica proporcionado en forma mensual.
Experiencia del Licitante para esta solución propuesta.	• El licitante deberá comprobar experiencia de al menos 3 años en proyectos directamente relacionados con la solución propuesta. • Lo anterior deberá acreditarse mediante copias simples de al menos 3 contratos debidamente firmados, ya sea con el sector público o iniciativa privada. • Deberá presentarse por cada contrato, al menos un CFDI (Comprobante Fiscal Digital) de algún pago de los servicios. • Deberá comprobar al menos ser Canal Autorizado con un nivel Platinum o equivalente de la solución propuesta. • Deberá comprobar al menos ser Canal autorizado como Socio de Servicios Profesionales de la solución propuesta (Professional Services Provider) • Deberá comprobar al menos 3 ingenieros con certificados vigentes que demuestren conocimientos y habilidades avanzadas para instalar, configurar, diseñar, mantener y solucionar problemas en las diferentes implementaciones de la plataforma de seguridad perimetral propuesta.
Cartas para esta solución propuesta.	El licitante deberá presentar carta de Distribuidor Autorizado por el fabricante de la marca de la solución propuesta, la cual deberá ser en papelería membretada del fabricante, contener la firma autógrafa del representante legal del fabricante, hacer referencia al número de licitación pública, mencionar que el licitante es distribuidor autorizado de la marca, y contener los datos del emisor, tales como nombre, correo electrónico y teléfono, para validación de la emisión de la carta. El licitante deberá presentar carta de Personal Capacitado y Especializado por el fabricante de la marca de la solución propuesta, la cual deberá ser en papelería membretada del fabricante, contener la firma autógrafa del representante legal del fabricante, hacer referencia al número de licitación pública, mencionar en forma explícita que el licitante cuenta con personal capacitado y especializado para la instalación, configuración y operación de los bienes y las soluciones ofertadas, requeridas en el presente procedimiento, y contener los datos del emisor, tales como nombre, correo electrónico y teléfono, para validación de la emisión de la carta. El licitante deberá presentar carta de que el equipo ofertado para la solución, no se encuentra con anuncio de fin de venta, la cual deberá ser en papelería membretada del fabricante, contener la firma autógrafa del representante legal del fabricante, hacer referencia al número de licitación pública, mencionar en forma explícita que el

COMPONENTE	DESCRIPCIÓN
	fabricante manifiesta que el equipamiento ofertado para la solución, no se encuentra con anuncio de fin de venta, y contener los datos del emisor, tales como nombre, correo electrónico y teléfono, para validación de la emisión de la carta. El licitante deberá presentar carta donde los equipos ofertados para esta solución, una vez que se haya celebrado este contrato de 12 meses la infraestructura propuesta para este servicio Administrado, pasa a ser propiedad de Gobierno del Estado de Nuevo Leon.
Servicio de Seguridad para protección del Correo institucional entrante y saliente.	Se requiere la migración de la configuración de la infraestructura actual a la nueva infraestructura, que contemple todo lo necesario, incluyendo Políticas, Reglas, e Interfaces, así como elaborar una matriz de validación de servicios. **Características Específicas que se ofrecen con esta herramienta:** • La solución debe poder escanear correo por SMTP/S entrante y saliente. • Protección contra Amenazas Avanzadas y de día Cero. • Mostrar de forma gráfica el número de amenazas desconocidas que han sido analizadas y diagnosticadas • Actualización programada y automática de firmas de malware, spam y phising. • Soportar Autenticación por SPF • Soportar Autenticación por DKIM • Soportar Autenticación por DMARC • Contar con un motor de detección de amenazas avanzadas y de día cero Cloud (Sandboxing) y de día cero que esté basado en tecnología de Deep Learning • Soportar anti suplantación de SPF y DKIM. • Protección contra URLs maliciosas al realizar click sobre ellas • Soportar TLS • Tener la capacidad de Habilitar enrutamiento por SmartHost • Métodos de detección avanzada en numerosos idiomas. • Bloquear más del 99% del correo spam. • Contar con validación de reputación de genotipo de Sender • Contar con Filtros de reputación de IP • Administrar listas Blancas/Negras

COMPONENTE	DESCRIPCIÓN
	• Poder habilitar validación de recipiente • Detección de URLs incluidas en correo. • Establecer el umbral de filtrado de contenido antispam fácilmente. • Habilitar protección de Harvesting • Garantizar la continuidad del correo electrónico con spool de correo y bandeja de entrada de emergencia. • Tener la capacidad de habilitar filtrado por Bulk Mail • Permite el respaldo de su configuración a carpetas compartidas en un servidor, ftp. • Tener la capacidad de validar encabezados de correo • Tener la capacidad de validar contenido activo. • Tener la capacidad de limitar el tamaño de los correos y los adjuntos. • Poder validar a nivel de Anti Spam tanto correo entrante como saliente • Controlar la información confidencial que sale del correo corporativo mediante el escaneo de todos los correos electrónicos en busca de palabras clave y tipos de archivos. • Permitir a las organizaciones cifrar todos los mensajes salientes enviados a una lista establecida de dominios y direcciones de destinatarios. • Respuesta de forma segura para obtener correo electrónico seguras, incluidos los archivos adjuntos. • Filtro para leguaje o palabras ofensivas • Tener la capacidad de Descartar Correos • Tener la capacidad de Enviar a cuarentena Correos • Bloqueo de IP, dominios o cuentas de correo remitentes. • Exención de IP, dominios o cuentas de correo. • Agregar disclaimer o pie de correo • Procesar a una siguiente regla • Entregar correo después de aplicar una regla especifica en caso de estar en cuarentena.

COMPONENTE	DESCRIPCIÓN
	• Re-enrutar el mensaje hacia otro servidor de correo. • Re-enrutar el mensaje hacia buzón, copiar a diferente servidor de correo. • Poder integrarse a un Active Directory, SNMP, Syslog • Compatible con todos los servidores de correo electrónico.
Entregables	Informe mensual impreso y en versión electrónica acerca del servicio de solicitado y asistencia técnica proporcionado en forma mensual.
Servicio de protección para Aplicaciones y Portales web especializados para protección de Ciberseguridad.	Se requiere la migración de la configuración de la infraestructura actual a la nueva infraestructura, que contemple todo lo necesario, incluyendo Políticas, Reglas, e Interfaces, así como elaborar una matriz de validación de servicios. Deberá cumplir con las siguientes Características: La solución deberá soportar por lo menos 80 aplicaciones y un ancho de banda de al menos 50 Mbps. • La implementación de la solución deberá requerir únicamente cambiar la configuración de DNS para los Dominios web que apuntan a los Aplicativos Web. Es decir, no requiere la instalación de hardware o software adicional o hacer cambios en la programación de las aplicaciones. • La solución deberá soportar cualquier aplicación web, sin importar la plataforma, tamaño del sitio, lenguaje o escenario de implementación. • La solución deberá ofrecer los siguientes servicios en una única plataforma integrada 1. Web Application Firewall WAF 2. Servicio de Proteccion de APIs 3. Protección contra Bots 4. Detección de Backdoors en aplicativos Web 5. CDN con failover y redundancia 6. Servicio de Balanceo Global Aplicativo 7. Almacenamiento en Cache 8. Optimización de Contenido 9. Servicio de Mitigación de ataques DDoS L3/L4/L7 10. Servicio de Mitigación de ataques DDoS al servicio DNS 11. Herramientas de monitoreo en tiempo real de conexiones, ancho de banda y ataques. 12. Capacidad de exportar los eventos de seguridad a una herramienta tipo SIEM • Una vez configurada, la solución tendrá la opción de deshabilitarse/habilitarse sin tener que hacer cambios en la Aplicación o DNS. Sin afectar el servicio a los usuarios. • La solución deberá garantizar un SLA del 99.999% • La solución deberá contar con la Certificación de Proveedor PCI Nivel 1 • La solucion debera contar con la certificacion "SOC 2" tipo "I y II", con los cuales garantice que los sistemas utlizados, su diseño y su efectividad operacional, son adecuados para cumplir con los principios de confianza definidos por la AICPA • El proveedor deberá contar con una capacidad de red global de al menos 6 Tbps

COMPONENTE	DESCRIPCIÓN
	• Como respuesta a un ataque, deberá ofrecer la opción de únicamente alertar o de bloquear al usuario o la dirección IP origen por un periodo de tiempo • Deberá permitir la creación de reglas personalizadas basadas en al menos URL, tasa de peticiones, existencia de algún parámetro o header HTTP, si el cliente es humano o bot, y el contenido del header REFERER. • Web Application Firewall (WAF) • La solución deberá permitir la creación de políticas de seguridad personalizadas, mediante la configuración de una variedad de factores que las desencadenen, además de tener múltiples acciones como bloquear Usuario, Bloquear petición, Bloquear Usuario o poner en cuarenta la URL. • • La solución deberá entregar un análisis detallado de las amenazas, incluyendo: 1. Dirección IP 2. User Agent 3. Locación geográfica 4. Información relevante de la sesión • La solución deberá contar con un mecanismo de perfilado, dicho mecanismo debe diferenciar entre usuarios humanos, bots legítimos (google, bing) y robots maliciosos como gusanos. • La solución deberá proteger tanto las aplicaciones Web HTTP, como las aplicaciones web SSL y HTTPS. • La solución deberá contar con una clasificación de bots basada en reputación para la distinción de Bots buenos, malos y sospechosos. Permitiendo el bloqueo de ataques como comment spam, scraping y escaneo de vulnerabilidades, y asegurando el acceso de bots como Google, Facebook y Pingdom. • La solución deberá detectar y bloquear los intentos de instalar y/o operar backdoors en los Aplicativos Web. • La solución deberá hacer bloqueos a partir del País de Origen (GeoBlocking) • La solución deberá contar con un sistema de Seguridad Colaborativa para evitar ataques que han sufrido otros sitios web. (Crowdsourcing) • La solución deberá incluir un servicio de Inteligencia Artificial y Machine Learning para la investigación, correlación de eventos de seguridad y alertas originados por el firewall de aplicaciones web independientemente donde resida ya sea en sitio, en la nube o hibrido. • La solución deberá permitir la creación de reglas personalizadas para reescribir peticiones (URL Rewrite) • La solución deberá permitir crear reglas personalizadas para agregar/quitar encabezados en los paquetes HTTP, como, por ejemplo, X-Forward-For, País, Ciudad, Coordenadas de geolocalización y contar con una mayor visibilidad del origen de las conexiones. • La solución deberá proteger servicios APIs aplicando un modelo positivo de seguridad automáticamente y permitir la integración con plataformas de administración de APIs. **Protección DDoS** • La solución deberá proporcionar los mecanismos necesarios para la mitigación de todos los tipos de ataques DDoS, ya sean basados en la Red (Capa 3, 4) o ataques de nivel aplicativo (Capa 7). Teniendo en cuenta la siguiente lista:

COMPONENTE	DESCRIPCIÓN
	1. TCP SYN+ACK 2. TCP FIN 3. TCP RESET 4. TCP ACK 5. TCP ACK+PSH 6. TCP Fragment 7. UDP 8. ICMP 9. IGMP 10. HTTP Flood 11. Brute Force 12. Connection Flood 13. Slowloris 14. Spoofing 15. DNS Flood 16. Mixed SYN+UDP or ICMP+UDP Flood 17. TCP SYN+ACK 18. Ping Of Death 19. Smurf 20. Reflected ICMP and UDP 21. Teardrop 22. Zero-day DDoS attacks 23. Ataques comunes a plataformas Web (Apache, IIS) • La solución deberá proporcionar conocimiento de la situación en tiempo real para la detección temprana de ataques de DDoS para que el tiempo entre el ataque y la mitigación sea reducido. • Para la mitigación de ataques DDoS al servicio DNS, la plataforma de nube deberá tomar el rol de NS (Nameserver), designado a través del sistema DNS gobal, para que sea la primera instancia que reciba peticiones de DNS provenientes de Internet y destinadas a la infraestructura; y las reenvíe después de la inspección de seguridad. • Deberá de tener la capacidad de definir los queries de DNS válidos, en cuanto a tipo y dominio, que habrá de dejar pasar a los servidores DNS reales, bloqueando el resto de las peticiones. • La solución deberá ofrecer un SLA de 3 segundos para la mitigación de ataques de DDoS **Optimización y Disponibilidad** • La solución deberá contar con la capacidad de hacer Balanceo Aplicativo (Capa 7) y/o failover entre múltiples servidores y múltiples datacenters. • La solución deberá contar con un mecanismo de monitoreo de salud de los servidores, para asegurar la máxima disponibilidad y utilización de tráfico del sitio a proteger. Haciendo un ruteo de las peticiones de los clientes en caso de que un servidor falle. • La solución deberá contar con una consola en tiempo real en la cual se podrá monitorear y verificar que el tráfico se está optimizando de forma correcta. • La solución deberá ser capaz de proveer la capacidad de hacer compresión y almacenamiento en cache. • La solución deberá soportar las siguientes capacidades para el almacenamiento en cache

COMPONENTE	DESCRIPCIÓN
	• Contenido Estático • Contenido Dinámico • Servir Paginas desde Memoria • Almacenamiento cache desde el lado del Usuario • La solución deberá tener la opción de generar reglas personalizadas para el almacenamiento en cache • Servicio de DNS • La solución deberá contar con la capacidad de proteger el servicio de DNS contra ataques, y a su vez realizar la optimización del servicio de DNS. • La solución deberá ser capaz de funcionar como DNS Proxy. • La solución deberá ser capaz de funcionar como Managed DNS. •
Entregables	Informe mensual impreso y en versión electrónica acerca del servicio de solicitado y asistencia técnica proporcionado en forma mensual.
Servicio de Capacitación especializada continua	• Se deberá considerar a 1 personas para el Curso de preparación y Examen de Certificación CISM (Certified Information Security Manager) • Se deberá considerar a 2 personas para el Curso de preparación y Examen de Certificación C|EH (Certified Ethical Hacker) • Se deberá considerar al menos 1 personas para el Curso de CISSP (Certified Information Systems Security Professional) • Se deberá considerar al menos 1 personas para el Curso de CCISO (Certified Chief Information Security Officer) Estos cursos se deberán ofrecer en el Área Metropolitana del Estado de Nuevo León y deberán de agendarse durante el año vigente de servicio solicitado.
Entregable	Voucher de entrenamiento y examen valido con fechas definidas previamente con el equipo a cargo en Gobierno del Estado.
Servicio de Mesa de Ayuda	El licitante deberá proveer de un Sistema de Mesa de Servicios fuera de las instalaciones del Gobierno del Estado de Nuevo León, que sea la que utilice para la administración del servicio y la atención de reportes de falla, con las siguientes características: • El servicio debe considerar el soporte de la solución a incidentes y solicitudes de servicio de primer y segundo nivel. • El servicio de primer nivel: refiere a agentes telefónicos que generarán el registro de los incidentes y las solicitudes, y brindarán asistencia remota para los reportes (tickets) que puedan ser solucionados mediante las consolas de administración o configuración. • El servicio de segundo Nivel: refiere a especialistas técnicos, ya sea para atención remota o en sitio, que deberán atender aquellos incidentes que requieran de un mayor grado de especialización. Los reportes que atienda este grupo, serán escalados desde la atención del Primer Nivel de acuerdo al tipo de incidente.

COMPONENTE	DESCRIPCIÓN
	• El licitante deberá proveer de un canal de comunicación telefónico 7x24x365 que fungirá como punto único de contacto para el servicio. • El licitante deberá proporcionar un correo electrónico de contacto como medio alterno de comunicación. • El licitante deberá contar con un Sistema de Mesa de Servicios fuera de las instalaciones de la convocante y que sea la que utilice para la administración del servicio y la atención de reportes de falla. • El licitante deberá contar con personal especializado en la administración, gestión y soporte en herramientas de gestión de incidentes. • El licitante deberá contar con el conocimiento en mejores prácticas como ITIL. • Monitoreo de disponibilidad, desempeño y salud de los equipos. • Modificación de reglas sobre demanda con al menos 10 cambios al mes. • Respaldo mensual de la configuración. • Recuperación de equipo en caso de una falla mayor. • Póliza de reemplazo con fabricante, así como actualizaciones de versión, parches/fixes críticos de seguridad. • Reporte ejecutivo mensual, así como top 25 de eventos críticos, aplicaciones, utilización, amenazas, ataques, disponibilidad, desempeño y efectividad del bloqueo señalando las estadísticas de los accesos y los bloqueos de puertos y direcciones.
Entregables	Informe mensual impreso y en versión electrónica acerca del servicio de solicitado y asistencia técnica proporcionado en forma mensual.
Cartas de la solución para todos los Servicios solicitados	• El licitante deberá entregar una carta firmada por su representante legal y haciendo referencia al número de convocatoria de garantía que especifique que, durante la vigencia del contrato de servicios administrados, el licitante será responsable de las garantías relacionadas con todos los componentes de la solución, tanto de hardware como de software, así como de las posibles actualizaciones que con motivo de la mejora continua de funcionalidades por parte del fabricante • El licitante deberá entregar una carta firmada por su representante legal y haciendo referencia al número de convocatoria donde se manifieste bajo protesta de decir verdad donde indique que cuenta con un centro de capacitación para las soluciones propuestas y además que cuentan con oficinas locales en el Área Metropolitana de donde celebra esta licitación. • El licitante deberá entregar una carta firmada por su representante legal y haciendo referencia al número de convocatoria donde se manifieste bajo

COMPONENTE	DESCRIPCIÓN
	protesta de decir verdad donde indique que cuenta con un centro de soporte para las soluciones propuestas y además que cuentan con oficinas locales en el Área Metropolitana de donde celebra esta licitación. • El licitante deberá entregar una carta firmada por su representante legal y haciendo referencia al número de convocatoria, en la que manifieste bajo protesta de decir verdad, su compromiso de atención a los lineamientos de operación, seguridad y confidencialidad de la información. • El licitante deberá entregar una carta firmada por su representante legal y haciendo referencia al número de convocatoria donde se manifieste bajo protesta de decir verdad indique que acepta y cumplirá todas las solicitudes para esta licitación definidas en esta ficha Técnica del Gobierno de Estado de Nuevo Leon.
Garantía de la solución para todos los Servicios solicitados	• Durante la vigencia del contrato de servicios administrados, el licitante será responsable de las garantías relacionadas con todos los componentes de la solución, tanto de hardware como de software, así como de las posibles actualizaciones que con motivo de la mejora continua de funcionalidades por parte del fabricante.
Transferencia de Conocimiento para todos los Servicios solicitados	El licitante será responsable de ejecutar la transferencia de conocimientos al personal indicado por el usuario y se realizará sobre el diseño, implementación y configuración de la infraestructura y/o soluciones propuestas bajo el siguiente esquema: • La transferencia de conocimientos se impartirá después de que se hayan concluido las pruebas de verificación de funcionalidad. • La transferencia de conocimientos será impartida dentro de las instalaciones del usuario o bien, en el lugar que éste designe. • Se determinará de común acuerdo con el usuario el programa para la capacitación corresponiente. • Se elaborará un acta de cierre de la transferencia de conocimientos, la cual será validada y aceptada por el personal designado por el usuario. • Como parte de la transferencia de conocimientos, el licitante entregará a quien designe el usuario, la memoria técnica de la instalación, configuración y operación de la solución implementada.
Entregables para todos los Servicios solicitados	• El proveedor ganador deberá entregar un documento, tanto en versión impresa como en electrónica, que contenga la descripción de cada una de las etapas del Plan de Trabajo rector del proceso de migración a la nueva plataforma de servicios administrados. Dicho documento deberá contener al menos los siguientes apartados: Planeación, Diseño, Implementación, Verificación, validación y pruebas, Puesta en Marcha. • El proveedor ganador deberá entregar un documento, tanto en versión impresa como en electrónica, que contenga previo acuerdo con el usuario, en donde se detalle los procedimientos a seguir para establecer el programa de ventanas de mantenimiento, y procurando la interrupción del servicio. • El proveedor ganador deberá entregar la documentación, tanto en versión impresa como en electrónica, correspondiente a las memorias técnicas de todos

COMPONENTE	DESCRIPCIÓN
	y cada uno de los detalles de la solución implementada, que sirva como referencia para posibles ajustes y/o actualizaciones. • El proveedor ganador deberá entregar una carta en papelería membretada, en la que se especifique que todos los Entregables fueron entregados a entera satisfacción del Gobierno del Estado de Nuevo León, firmada de conformidad por el usuario funcional del Gobierno del Estado de Nuevo León.
Vigencia	15 meses de servicio.
Tiempo de entrega	04 semanas después de la firma del contrato.
Forma de pago	40% de anticipo posterior a entrega de orden de compra y el 60% restante dividido en 15 pagos mensuales a entera satisfacción del solicitante.