SUBASTA ELECTRÓNICA INVERSA NACIONAL NO. DGAS-DC-SEI-035/2024 RELATIVA A LOS SERVICIOS ADMINISTRADOS DE SEGURIDAD PERIMETRAL Y SERVICIOS ESPECIALIZADOS DE SEGURIDAD INFORMÁTICA, SOLICITADO POR LA SUBSECRETARÍA DE TECNOLOGÍAS DE LA SECRETARÍA DE ADMINISTRACIÓN.

FICHA TÉCNICA

Equipo/Servicio:	Servicios Administrados De Seguridad Perimetral, Filtrado De Correo Electronico, Concentrador De VPN Site To Site, Evaluacion De Controles De Riesgos Tecnologicos De Ciberseguridad, Seguridad De Las Aplicaciones, Firewall De Aplicaciones Web, Mesa De Ayuda Y Servicios Especializados De Seguridad Informatica Para El Gobierno Del Estado De Nuevo León.	**Cantidad:**	**1**
Vigencia	36 meses		

Componente	Características
Servicios Administrados solicitados	Los servicios administrados de seguridad para la red Informática del Gobierno del Central del Estado de Nuevo León junto con otros servicios de Ciberseguridad especializados, protegen los bienes, procesos, datos y servicios basados en el uso de las tecnologías de información y comunicaciones, y la información misma que reside en activos electrónicos, a través de una solución integral de tecnología de alta especialidad y servicios de acuerdo con las siguientes características: ● El servicio dará protección a la red de seguridad 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 malintencionado, que podrían causar daño, pérdida, robo de información, o suspensión de procesos de gobierno. ● El servicio realizará revisiones y ajustes de las configuraciones en la tecnología, procesos y procedimientos operativos en la protección perimetral que pudieran impactar la confidencialidad, integridad y disponibilidad de la información de manera proactiva, a fin de tomar acciones correctivas y estar alineadas con las mejores prácticas y estándares de ciberseguridad ● El servicio de seguridad para protección del Correo Electrónico entrante y saliente deberá considerar una solución de servicio adaptable en sitio y/o en la nube, hasta para 15,000 buzones de correo electrónico, que ayude a la prevención de correo no deseado, virus, gusanos, phishing, malware y ataques de denegación de servicio. ● El servicio de concentrador de VPN Site to Site para la conectividad de los sitios, se deberá considerar una solución de servicio adaptable en sitio. ● Servicio de plataforma que permita una gestión de los activos y de software, así como la identificación de vulnerabilidades, forzado de políticas en el sistema operativo y las remediaciones mediante la actualización de parches para el sistema operativo y las aplicaciones de software. ● El servicio para el análisis y evaluación de controles para la gestión de riesgos que permita mejorar la seguridad de la información, mediante la identificación del nivel de riesgo tecnológico existente en la plataforma y el desarrollo de un plan de tratamiento de los riesgos identificados incluyendo priorización y tiempos estimados de mitigación o eliminación. ● El servicio de protección para Aplicaciones Web especializados deberá soportar al menos 80 sitios sin importar la plataforma o tamaño del sitio, lenguaje o escenario de implementación. ● Servicio de Mesa de Ayuda 7x24, Servicio de Monitoreo y Servicio de

	Operación de los dispositivos de Seguridad en el alcance para proporcionar asistencia y soporte técnico sobre cualquier propuesta para mejorar la seguridad a través de modificación a la funcionalidad a través del esquema de servicios administrados en forma compartida. ● El Licitante deberá considerar al inicio de los servicios mesas de trabajo técnicas en conjunto con la unidad requirente para la revisión de las configuraciones de seguridad actuales con el fin de realizar las reconfiguraciones que sean necesarias. ● El Licitante deberá proporcionar las recomendaciones que sean necesarias para modificar las configuraciones de los equipos propiedad del Gobierno del Estado de Nuevo León, lo anterior con el fin de garantizar una correcta operación de la infraestructura y servicios apegados a las mejores prácticas de seguridad. Por ejemplo: emitir recomendaciones para los switches Core, routers de publicación o navegación, direccionamientos públicos o privados, DNS, VLANs, ruteo dinámico o estático, configuraciones de alta disponibilidad, configuraciones de red o ruteo para la infraestructura de servidores virtualizados, al menos. La responsabilidad de la reconfiguración de dichos servicios será de la Dirección de Infraestructura Tecnológica de la Subsecretaría de Tecnologías. ● El Licitante deberá considerar como parte del servicio todas las configuraciones en las Soluciones de Seguridad que sean necesarias para la correcta operación de la infraestructura y servicios en el alcance, incluyendo funcionalidades como ruteo, segmentación de red VLAN, protección de la DMZ, protección de navegación, inspección de tráfico IPS, protección de tráfico, monitoreo de tráfico, protección de correo electrónico, protección de la publicación de servicios Web, al menos. ● Al termino de los 36 meses de la vigencia del servicio a contratar la propiedad de los equipos y software suministrados para el servicio contratado será transferida al Gobierno del Estado de Nuevo León
Servicio de seguridad perimetral	El servicio de seguridad perimetral deberá considerar la implementación y actualización de software y hardware, según corresponda, para protección de amenazas para dar continuidad a la infraestructura ~~existente~~ de seguridad perimetral de firewalls. Se requiere la revisión del sistema productivo para la migración de la configuración de la infraestructura lógica de red actual a la nueva infraestructura, que contemple todo lo necesario, incluyendo Políticas, Reglas, e Interfaces, así como elaborar una matriz de validación de servicios. Podrá ser entregada conforme a que se encuentre disponible en el mercado. Las especificaciones de hardware mínimas para los 2 equipos de seguridad perimetral son las siguientes por cada equipo: ● Storage: 2 x 240 GB SSD ● FW Throughput (64 bytes) [Gbps]: 137.5 ● Concurrent Sessions (TCP): 8000000 ● New Sessions/Second (TCP): 550000 ● IPsec VPN Throughput (512 byte) [Gbps]: 55 ● Gateway-to-Gateway IPsec VPN Tunnels: 2000 ● Client-to-Gateway IPsec VPN Tunnels: 50000 ● SSL-VPN Throughput [Gbps]: 9 ● Concurrent SSL-VPN Users: 10000 ● IPS Throughput (Enterprise Mix) [Gbps]: 14 ● SSL Inspection Throughput (IPS, avg. HTTPS) [Gbps]: 9 ● Application Control Throughput (HTTP 64K) [Gbps]: 32 ● NGFW Throughput [Gbps]: 11.5 ● Threat Protection Throughput [Gbps]: 10.5 ● GE RJ45 MGMT/HA Ports 2 ● 10GE Interfaces: 4 ● 25GE Interfaces: 4

	● Deberá contar con los siguientes transceptores requeridos mínimos para aprovisionamiento:
	  • 8 x Transceptor de media distancia para fibra óptica Multi-Modo SFP28 SR, 25 /10 GE, hasta 100 mts.
	  • 10 x Transceptor de media distancia para fibra óptica Multi-Modo QSFP28 SR, 10 GE, hasta 100 mts.
	● Deberá contar con los siguientes cables requeridos mínimos para aprovisionamiento:
	  • 9 x fibra LC to LC 30 mts OM3/OM4 Multimodo en color celeste
	● Deberá contar con capacidades de aceleración de tráfico de red e inspección de tráfico encriptado mediante el uso de procesadores de seguridad ASICs.
	● Deberá ser compatible con NAT estática y dinámica (varios-a-1).
	● Deberá ser compatible con NAT estática y dinámica (muchos-a-muchos).
	● Deberá ser compatible con NAT estático bidireccional 1-a-1.
	● Deberá ser compatible con la traducción de puertos (PAT).
	● Deberá ser compatible con NAT Origen.
	● Deberá ser compatible con NAT de destino.
	● Deberá soportar NAT de origen y NAT de destino de forma simultánea.
	● Deberá soportar NAT de origen y NAT de destino en la misma política.
	● Deberá implementar el protocolo ECMP, para balanceo de tráfico con ruteo, sin creación de interfaz virtual.
	● Deberá soportar SD-WAN de forma nativa.
	● Deberá soportar el balanceo de enlace hash por IP de origen.
	● Deberá soportar el balanceo de enlace por hash de IP de origen y destino.
	● Deberá soportar balanceo de enlace por peso. En esta opción Deberá ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Deberá ser compatible con el balanceo en al menos tres enlaces.
	● Debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.
	● Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;
	● El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;
	● Deberá tener capacidad de firmas basadas en DNS para detectar búsquedas específicas de DNS hacia nombres de equipo que han sido asociados con malware. Además, deberá permitir habilitar o deshabilitar estas firmas de DNS para crear excepciones cuando sea necesario.
	● Deberá contar con un módulo de protección contra ataques DNS del tipo DGA y DNS tunneling, así como con capacidades de machine learning basadas en la nube, logrando predecir posibles nuevos ataques.
	● Deberá ser capaz de identificar aplicaciones independientemente del puerto o protocolo que usen, permitiendo así conocer, permitir o denegar sus dependencias y limitar las aplicaciones a sus puertos estándar.
	● Deberá poder crear políticas basadas en el control por aplicación, por categoría (cuando menos 24 categorías y la capacidad de crear categorías personalizadas), subcategorías, tecnología, factor de riesgo y características
	● Deberá poder tener la capacidad de creación de políticas basadas en

	nombre de usuario, grupo de usuario y dirección IP. ● Deberá incluir las siguientes funcionalidades y características para el Filtrado de Contenido. ● 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 contar con una variedad de al menos 30 reportes locales o en plataforma central que desplieguen las categorías URL visitadas, los sitios web visitados, los usuarios que fueron bloqueados, los sitios que fueron bloqueados, etc. ● Los registros de los accesos a las páginas deberán poder enviarse a un servidor de logs. Deberá incluir las siguientes funcionalidades y características de VPN (Red Privada Virtual): ● Deberá contar con capacidades de Red Privada Virtual (por sus siglas en inglés 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. ● 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 autodetección. ● Deberá contar con túneles cliente a sitio con funcionalidad de completar la VPN vía IPSec en dado caso que no sea posible se auto-conectará vía SSL. ● Deberá tener capacidad de VPNs cliente a sitio que revise el estado del host, verificando si el Firewall personal está activo, el estado de antimalware, los parches del sistema operativo y condiciones del registry, para permitir o denegar el acceso según las políticas del Firewall de siguiente generación ● Deberá prevenir el uso de herramientas de elusión y evasión ● Deberá contar con acceso seguro a las aplicaciones SaaS y bloquear las aplicaciones no autorizadas en las políticas asignadas al dispositivo. El servicio deberá cumplir con las siguientes funcionalidades y características enfocado a dar continuidad a la administración de los equipos y reporteo: ● Consola de administración centralizada para la gestión de los equipos de seguridad perimetral, en formato Appliance físico o VM máquina virtual. ● Consola de analíticos que permita la visibilidad del uso de la red, aplicaciones, amenazas e indicadores de compromiso, en formato Appliance físico o VM máquina virtual. ● Deberá soportar Syslog y SNMPv3. ● Deberá desplegar un resumen gráfico de aplicaciones y amenazas. ● 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. ● 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 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 soportará por lo menos las técnicas para la distribución inteligente del tráfico. El servicio deberá incluir las siguientes funcionalidades y características de protección de tráfico contra ataques que usan el servicio de DNS y dominios maliciosos: ● Capacidad de detección y prevención del mal uso de los servicios de resolución de nombre de dominios para detener ataques conocidos y no conocidos. Con capacidad de aislar equipos de manera automática para contener un ataque, con capacidad de inferencia para detección automática del mal uso de un DNS y categorización automática. Los equipos proporcionados deberán contar con licencia de exportación de equipos de alto nivel de encriptación para uso gubernamental emitida desde el país de origen. Todas las soluciones de tipo software propuestas deberán ser registradas en el portal de soporte del fabricante bajo la cuenta de Gobierno del Estado de Nuevo León, la cual será proporcionada al LICITANTE ADJUDICADO posterior al fallo
Entregables para el Servicio para seguridad perimetral	• El Informe para entregar será en formato tipo checklist con evidencia de la configuración de hardware, software y vigencia de los soportes correspondientes para el servicio a administrar. • La Dirección de Infraestructura Tecnológica de la Subsecretaria de Tecnologías validará el entregable y dará su visto bueno para la aceptación del servicio.
Experiencia del Licitante para su propuesta	● El licitante deberá comprobar experiencia de 36 meses en proyectos directamente relacionados con la propuesta. ● Lo anterior deberá acreditarse mediante copias simples de al menos 3 contratos debidamente firmados, ya sea con el sector público o iniciativa privada.
Los requisitos nombrados en esta sección deberán presentarse como parte de la propuesta del licitante	• El Licitante deberá asegurar que los equipos y el licenciamiento de software a suministrar seram originales, nuevos, que su vida comercial sea de al menos 3 años y que estén cubiertos por garantía o contrato de soporte vigente con el fabricante durante la duración del servicio.
Servicio de Seguridad para protección del Correo Electrónico	El servicio para la protección del correo electrónico requiere la renovación del licenciamiento de la plataforma de seguridad de correo electrónico. El servicio deberá constar de una evaluación inicial y configuraciones requeridas para la protección de correo entrante y saliente, debe contemplar todo lo necesario, incluyendo Políticas, Reglas, e Interfaces, así como elaborar una matriz de validación de servicios. La matriz podrá ser entregada conforme a lo que se encuentre disponible en la Instalación del Gobierno del estado de Nuevo León en la máquina virtual.

	Todo el licenciamiento de software del servicio deberán registrarse en el portal de soporte del fabricante bajo la cuenta de Gobierno del Estado de Nuevo León, la cual será proporcionada al LICITANTE ADJUDICADO posterior al fallo. Las especificaciones técnicas mínimas de virtual son las siguientes: ● Factor de Forma: Máquina Virtual ● Máximo de vCPU: 16 ● NICs Virtuales (Mínimo/Máximo): 1/6 ● Almacenamiento Virtual (Mínimo/Máximo): 250GB/12TB ● Memoria Virtual (Mínimo/Máximo): 4GB/128GB ● NICs (Mínimo/Máximo): 1/6 ● Max Configured Domains: 1500 ● Recipient-based Policies per domain: 1500 ● Recipient-based Policies per system: 7500 ● Server Mode Mailboxes: 3000 ● Email Routing Msg/s: 875000 ● Antispam throughput Msg/s: 817000 ● AV/AS throughput Msg/s: 758000 A continuación, se describen características específicas que se deberán proporcionar por parte del licitante: ● La solución deberá basarse en "appliance" de propósito específico (virtual o físico) No se tendrán en cuenta los equipos de uso general (PCs o servidores) en los que se puede instalar y /o ejecutar un sistema operativo regular, como Microsoft Windows, FreeBSD, Solaris de Sun o GNU / Linux ● Deberá poderse instalar en rack estándar en caso de un appliance físico, y en caso de ser una solución de licenciamiento se permitirá su instalación en nubes privadas tales como VMware ESXi, Microsoft Hyper-V, KVM, Citrix XenServer y FortiHypervisor, así como en nubes públicas como Microsoft Azure y Amazon Web Services ● Deberá ser capaz de funcionar como un gateway SMTP para los servidores de correo existentes. ● Deberá ser capaz de actuar como gateway, en calidad de MTA (Mail Transfer Agent). ● Deberá ser capaz de funcionar de una manera transparente, actuando como un proxy transparente para el envío de mensajes a los servidores de correo protegidos. ● Deberá poder ser instalado en forma de proxy SMTP transparente, para el análisis de correo saliente, buscando evitar el reporte en Blacklist ● Puede ser implementada como un cliente WCCP y recibir correo y analizar mediante este protocolo. ● Deberá soportar su implementación en modo de servidor, operando como un servidor de correo MTA independiente con buzones para los usuarios. ● Deberá ser capaz de almacenar localmente mensajes de correo electrónico para su entrega a los usuarios a través de correo Web, POP3 y / o IMAP. ● Deberá tener disponible un API basado en REST para fines de monitoreo,

	automatización y orquestación ● Deberá ser licenciada sin importar el número de buzones que proteja. El licenciamiento es basado en el performance del hardware suministrado (correo por hora) ● Deberá soportar listas blancas y negras (White/Black List) por usuario, por dominio y globalmente para todo el sistema. ● Deberá permitir la sobre escritura, la edición y personalización de los mensajes de notificación de antivirus y anti-spyware. ● Deberá poder retrasar el envío de correo sobredimensionado a horarios que sean de menos carga. ● Deberá poder definir el reenvío de correo (relay) a una IP específica con base a la IP origen del mensaje. ● Deberá proporcionar soporte para múltiples dominios de correo electrónico. ● Deberá ser compatible con la implementación de políticas por destinatario, de dominio, del tráfico entrante o saliente. ● Deberá ser capaz de entregar el correo en función de los usuarios existentes en una base de LDAP ● Deberá soportar cuarentena por usuario, permitiendo que cada usuario pueda gestionar sus propios mensajes en cuarentena la eliminación o la liberación de los que no son spam, lo que reduce la responsabilidad del administrador y la posibilidad de bloquear el correo electrónico legítimo. La cuarentena se debe acceder a través de la página web y POP3. ● Deberá ser capaz de programar el envío de informes de cuarentena. ● Deberá ser capaz de realizar el almacenamiento de correo electrónico (Archivado/archiving), basado en el envío y recepción de políticas, con el apoyo también de almacenamiento remoto. ● Deberá ser capaz de mantener la cola de correo (Queue) en caso de fallo en la conexión de salida, retrasos o errores de entrega. ● Deberá ser capaz de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP. ● Deberá ser capaz de mantener listas de reputación del remitente sobre la base de: número de virus enviados, la cantidad de correos electrónicos considerados correo no deseado, la cantidad de destinatarios equivocados. ● Deberá ser compatible con el enrutamiento en IPv4 y IPv6. ● Deberá permitir el almacenamiento de correo electrónico y de cuarentena a nivel local o servidor remoto. ● Deberá tener características antispam, antivirus, anti-spyware y anti-phishing. ● Deberá ser capaz de realizar la inspección del correo de Internet entrante y saliente. ● Deberá contar con un Wizard para el fácil y rápido aprovisionamiento de las configuraciones básicas del equipo y de los dominios a proteger ● Deberá proporcionar protección contra ataques de denegación de servicio, tales como Mail Bomb. ● Deberá proporcionar un control DNS reverso para la protección contra los ataques spoofing. ● Deberá conectar con la base de datos del fabricante para descargar

	actualizaciones de Anti-Spam en cuanto esté disponible. ● Detección si el origen de una conexión es lícito basado en una base de datos de reputación de IPs suministrada por el fabricante. ● Detección si un correo es spam revisando las URLs que esta contenga, comparándolas con la base de datos de reputación suministrada por el fabricante. ● La revisión de URLs deberá permitir seleccionar las categorías URL que serán permitidas o no en los correos analizados. Esta base de datos de categorías será actualizada por el fabricante. ● Deberá contar con mecanismos de detección de SPAM nuevo, mediante el análisis continuo de los correos recibidos y su posterior correlación con eventos ocurridos a nivel mundial, permitiendo así definir y detectar nuevas reglas de SPAM. ● Deberá ser capaz de realizar análisis Heurístico y definir umbrales máximos de acuerdo con el comportamiento del correo y así determinar si un correo es spam. ● Deberá ser capaz de realizar análisis Bayesiano para determinar si un correo es spam. ● Deberá ser capaz de detectar si el correo electrónico es un boletín de noticias (Newsletter) ● Deberá contar con técnica que detecten SPAM mediante el uso de Greylist, las cuales clasifican el correo con base en su comportamiento en el inicio de sesión, como bloquear todos los correos y permitir solo los reenvíos. ● Deberá ser capaz de filtrar mensajes de correo electrónico basados en los URI (Uniform Resource Identifier) contenidas en el cuerpo del mensaje. ● Deberá ser capaz de realizar análisis sobre la base de palabras prohibidas (Banned Words). ● Deberá contar con Diccionarios predefinidos de palabras que pueden ser escaneados en el correo electrónico, además definir pesos a cada diccionario o palabra creada para definir si un correo es SPAM. ● Creacion de listas blancas o negras de palabras. ● Deberá permitir la gestión del spam con la capacidad de aceptar, encaminar (Relay), rechazar (Reject), descartar (Discard), poner en cuarentena personal, sobreescribir el destinatario, Archivar, enviar copia oculta BCC, reenviar a otro Host, Insertar un TAG o un nuevo encabezado. ● Deberá ser capaz de realizar documentos de análisis de imagen y PDF identificando con base en esto si el correo es SPAM. ● Deberá ser capaz de soportar las listas negras de terceros tales como DNSBL y SURBL. ● Deberá ser compatible con la lista gris para las cuentas de correo electrónico en IPv4 e IPv6. ● Deberá ser capaz de detectar las direcciones IP falsificadas (Forged IP). ● Permite identificar imágenes que hagan alusión a contenido SPAM. Deberá soportar el análisis de las siguientes extensiones GIF, JPG, PNG ● Deberá poder validar si el destinatario del correo entrante es un buzón válido ● Deberá ser compatible con Sender Policy Framework (SPF). ● Deberá ser compatible con Domain Keys Identified Mail (DKIM). ● Deberá ser compatible con Domain BasedMessage Authentication

	(DMARC). ● Deberá identificar altos volúmenes de conexiones y aplicar límites basados en senders e Ips. ● Deberá ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico. ● Deberá permitir su configuración a través del acceso web (HTTP, HTTPS). ● Deberá ser capaz de permitir la creación de administradores únicos para la administración y configuración de por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen. ● Deberá ser capaz de proporcionar al menos dos niveles de gestión de acceso: lectura / escritura (Read/Write) o de sólo lectura (Read Only) ● Deberá permitir la creación de perfiles de configuración granular, donde cada perfil puede agregar características de configuración específicas, tales como anti-spam, anti-virus, autenticación, entre otros ● Deberá soportar doble factor de autenticación para el login de usuarios administradores. ● En modo server, deberá poder Sincronizar contactos y calendarios con clientes de correo (MUA) ● En modo server, deberá soportar los protocolos WebDAV y CalDAV para la publicación y sincronización de calendarios ● Deberá contar con algún mecanismo para la fácil migración de buzones y cuentas desde un servidor a la nueva solución estando en server mode. ● Deberá ser capaz de almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog). ● Deberá permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica. ● Deberá generar informes por demanda o programados a intervalos de tiempo específicos. ● Deberá generar y enviar informes en formato PDF o HTML.
Concentrador de VPN Site to Site	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. La matriz podrá ser entregada conforme a lo que está disponible en la instalación del Gobierno de Nuevo León. Las especificaciones de hardware mínimas para los 3 equipos son las siguientes por cada equipo: Servicio de VPN • Soporte grupal para conexiones VPN IPsec, que ahora permite importaciones grupales desde AD / LDAP / etc. para una fácil configuración de la política de acceso grupal • ofrece conexiones ilimitadas de acceso remoto ilimitado VPN SSL o IPsec sin cargo adicional. • Site-to-Site VPN SSL: • IPsec, 256- bit AES/3DES, PFS, RSA, X.509 certificados, pre-shared key. • L2TP y PPTP. • Acceso remoto:

	• SSL, IPsec, soporte de clientes VPN iPhone/iPad/Cisco/Android VPN. • Cliente SSL para Windows y descarga de configuración vía portal de usuario. • Portal de autoservicio con cifrado único con soporte para RDP, HTTP, HTTPS, SSH,Telnet y VNC • Procesadores de flujo dedicados para mejorar el rendimiento para respaldar la visibilidad y la protección que necesita. • Inspección TLS 1.3 • Motor de inspeccion TLS de alto rendimiento admite TLS 1.3 sin efecto en el rendimiento, los ultimos paquetes de cifrado para una compatibilidad maxima y una visibilidad mejorada de los flujos de trafico cifrado directamente desde el panel de control. • Motor DPI: • Motor DPI de transmisión con escaneo sin proxy de todo el tráfico para AV, IPS, amenazas web, control de aplicaciones, inspección SSL, así como aprendizaje profundo y sandboxing. • Procesador de flujo: • Descarga y aceleración inteligente de SaaS, SD-WAN y tráfico en la nube como VoIP, video y otras aplicaciones de confianza • SD_WAN • Selección de enlaces y enrutamiento basados en el rendimiento, equilibrio de carga, transiciones de cero impactos entre enlaces en caso de interrupción, centralizada administrada en la nube y aceleración en FastPath de del tráfico de túnel VPN. Firewall, Redes y Ruteo Deberá incluir funciones de red, enrutamiento y SD-WAN, como firewall con estado basado en zonas, NAT, VLAN, perfiles SD-WAN, selección de enlaces WAN y monitorización basados en el rendimiento, equilibrio de carga, transiciones de enlaces WAN con cero impacto y aceleración en FastPath del tráfico de aplicaciones de confianza, tráfico VPN IPsec y flujos de tráfico cifrado por TLS. • Inspección profunda de paquetes • Default Zonas LAN, WAN, DMZ, LOCAL, VPN • Modificación de políticas NAT con mascara IP. • Protección inundación: DoS, DDoS y bloqueo de escaneo de puertos. • Bloqueo de Países • Ruteo: estático, multicast (PIM-SM) y dinámico (RIB, BGP, OSPF) • Soporte de VLAN DHCP y tag • Soporte Multiple bridge • WAN link balancing: Múltiples conexiones de internet, estado del enlace, tolerancia a fallos, asignación de peso y balanceo automático. • Configuración completa de DNS, DHCP y NTP. • DNS dinámico. • Soporte IPv6 Administración de Ancho de Banda

	• Flexible compartir QoS a redes o usuarios (tráfico de Web y App). • Asignación a usuario de cuota carga/descarga o total cíclica o no cíclica. • Optimización de VoIP en tiempo real Autenticación • Transparente, autenticación proxy (NTLM/Kerberos) o clientes autenticados. • Autenticación vía: Active Directory, eDirectory, RADIUS, LDAP and TACACS+. • Servicio de autenticación de agente para Active Directory SSO, STAS, SATC. • Certificados de autenticación para iOS y Android. • Single sign-on: Active directory, eDirectory • Servicio de autenticación para IPsec, L2TP, PPTP, SSL. • Portal cautivo. Portal de Autoservicio de Usuario • Descarga del cliente de Autenticación • Descarga de cliente de acceso remoto de SSL (Windows), y archivos de configuración (otros OS). • Cambio de usuario y contraseña. • Revisión uso de internet personal. • Acceso a mensajes de cuarentena (requiere Email Protección). Despliegue Zero Touch • Deberá soportar la opción de despliegue Zero Touch que permita realizar la configuración inicial desde la consola central y exportar después de su carga en el dispositivo desde una unidad flash durante el inicio, lo que vuelve a conectar automáticamente en el dispositivo con consola central. Sistema de Prevención contra Intrusos (IPS) • Alto-rendimiento, next-gen IPS inspección profunda de paquetes Motor con patrones IPS selectivos para un máximo rendimiento y protección. • Miles de firmas. • Soporta personalización de firmas IPS. • Implementación flexible de políticas IPS como parte de una red o usuario completamente personalizado. ATP • Protección contra amenazas avanzadas (Detecta y bloquea tráfico que intenta ponerse en contacto con servicios de comando y control usando múltiples-capas mediante DNS, AFC, Y firewall)

	Control y Protección en Sitios Web • Proxy completamente transparente para antimalware y filtrado web • Protección mejorada de amenazas avanzadas • Base de datos de filtros de URL con millones de sitios en 92 categorías, respaldados por • Políticas de tiempo de cuota de surf por usuario / grupo • Políticas de tiempo de acceso por usuario / grupo • Análisis de malware: bloquea todas las formas de virus, malware web, troyanos y spyware en HTTP / S, FTP y correo electrónico basado en la web • Protección avanzada contra malware web con emulación de JavaScript • Protección en tiempo real, búsqueda en la nube para la última amenaza de inteligencia • Exploración en tiempo real o por lotes • Análisis y ejecución de HTTP y HTTPS en cualquier red y política de usuario con reglas y excepciones • Completamente personalizables • Validación del certificado • Aplicación de YouTube para escuelas • Navegación Segura en navegadores Control de Ancho de Banda para aplicaciones y páginas web • Opciones mejoradas de configuración del tráfico (QoS) por categoría web o aplicación para limitar o garantizar la carga / descarga o la prioridad total de tráfico y la velocidad de bits individual o compartida Administración Centralizada • Administración Centralizada en la Nube • Gestión de grupos de firewalls: sincronización de políticas entre los grupos de firewalls.x • Copias de seguridad y actualizaciones de firmware: almacenamiento y programación • Despliegue Zero Touch: para nuevos firewalls desde la nube • Orquestación de SD-WAN: orquestación de VPN de sitio a sitio con un solo clic. • Generación de informes de firewall en la nube: informes multifirewall con opciones para guardar, programar y exportar informes (30 días de retención de datos) • XDR y MDR Connector: soporte para los servicios XDR y MDR Rendimiento • Rendimiento de Firewall hasta 80,000 Mbps. • IMIX del Firewall 37,000 Mbps. • Latencia del Firewall (UDP de 64 bytes) 4 US • Rendimiento del IPS 36,500 Mbps. • NGFW 30,000 Mbps.

	• Rendimiento de la Protección contra amenazas 8,650 Mbps.
	• Conexiones Concurrentes 17,200,000.
	• Conexiones Nuevas por Segundo 450,000.
	• Rendimiento de VPN IPsec 75,550 Mbps.
	• Túneles simultáneos VPN IPsec 8,500.
	• Túneles simultáneos VPN SSL 8,500
	• Inspección TLS/SSL de Xtream 10,600 Mbps.
	• Conexiones simultaneas de SSL/TLS de Xtream 276,480
	Almacenamiento (cuarentena local/registros)
	• 2 discos SSD tipo SATA-III Integrado de 240 GB (SW-RAID-1) como mínimo.
	Interfase y puertos:
	• 4 x GbE cobre
	• 4 x 2.5 GbE cobre
	• 4 x 2.5 GbE cobre
	• 8 x Transceptores SFP+ / SFP 10 Gbe en fibra
	• Deberá contar con los siguientes cables requeridos mínimos para aprovisionamiento:
	• 5 x fibra LC to LC 3 mts OM3/OM4 Multimodo en color celeste
	• Pares de puertos de omisión 2
	• Puertos de Administración
	  • 1 x RJ45 MGMT
	  • 1x COM RJ45
	  • 1 x Micro-USB (cable incl.)
	• No. de Ranuras para puertos Flexi 2
	• Puertos USB
	  • 2xUSB 3.0 (Frontal)
	Display de Visualización
	• Modulo LCD multifunción
	Fuentes de Alimentación y consumo eléctrico
	• 2 Fuentes de Poder internas en modo hot-swap
	• Alcance automático interno AC-DC 100-240 VCA
	• 3.7-7.4 A
	• 50-60 Hz
	• 151 W/515.74 BTU/h en modo inactivo
	• 268.35 W/916.56 BTU/h máx.
	Condiciones de Temperatura para funcionamiento

	• 0 a 40 °C (en funcionamiento) • -20 a +70 °C (almacenamiento Dimensiones y Peso • Ancho 438 x Profundidad 44 x Altura 510 mm. • Peso 9.7 Kg/21.38 Lbs. (fuera del embalaje) Montaje • 1 unidad de Rack (Kit de Rieles Incluidos) Certificaciones del Equipo • CB (Certification Body) • CE (Conformite Europene) • UKCA (UK Conformity Assessment) • UL (Underwriters Laboratories) • FCC (Federal Communications Commission) • ISED (Innovation Science and Economic Development) • VCCI (Voluntary Control Council for Interference) • KC (Korea Certification) • RCM (Regulatory Compliance Mark) • NOM (Norma Oficial Mexicana) • ANATEL (Agencia Nacional de Telecomunicaciones) • CCC (China Compulsory Certification) • BSMI (Bureau of Standards, Metrology and Inspection) • TEC • SDPPI • El Licitante será responsable de las garantías relacionadas con todos los componentes, tanto de hardware como de software, así como de las actualizaciones que con motivo de la mejora continua de funcionalidades por parte del fabricante Instalación y configuración • Instalación, configuración y puesta en marcha
Servicio de Evaluación de Controles, Riesgo Tecnológico de Ciberseguridad	El servicio de evaluación de controles y riesgo deberá obtener los siguientes beneficios: ● Mejorar la seguridad de la información ● Agilizar las pruebas de penetración ● Identificar el nivel de riesgo tecnológico existente en la plataforma tecnológica ● Desarrollar un plan de tratamiento de los riesgos identificados incluyendo priorización y tiempos estimados de las iniciativas ● Identificar vulnerabilidades de los equipos de cómputo ● Salvaguardar la Confidencialidad, Integridad y Disponibilidad de los datos personales de los funcionarios

	● Priorizar las inversiones en infraestructura tecnológica El licitante deberá realizar una auditoria mensual para evaluar la seguridad de la Información y vulnerabilidades y obtener un Dictamen de Resultados completo sobre todas las amenazas encontradas y respectivas clasificaciones de riesgo. Este dictamen será esencial para los procesos de corrección de las vulnerabilidades, que deben ejecutarse poco después de la finalización del proceso de auditoría. El Dictamen, resultado de la auditoria, deberá presentar información suficiente para que se identifique el nivel de exposición del Gobierno del Estado de Nuevo León hacia amenazas de ciberseguridad y deberá incluir las recomendaciones necesarias. Así mismo, como parte del servicio se requerirá, un Plan de Remediación con las actividades necesarias y recomendadas por el licitante para lograr reducir daños por incidentes de seguridad y aumentar la disponibilidad de nuestros servicios tecnológicos. El servicio deberá incluir las siguientes características: ● El licitante deberá considerar como parte de su propuesta técnica las revisiones y pruebas de seguridad en los componentes de la infraestructura del Gobierno del Estado de Nuevo León, para identificar y reportar las vulnerabilidades de seguridad, mediante su verificación y detección; así como descartar los falsos positivos, falsos negativos, documentando los hallazgos y recomendaciones de remediación correspondientes. ● Deberá presentarse como parte del Dictamen de Resultados en un "mapa de riesgo" donde quede documentado la severidad y la probabilidad de que la vulnerabilidad sea explotada, así como indicar recomendaciones para su atención y mitigación por parte del Gobierno del Estado de Nuevo León. Características de la Auditoría para las pruebas de Penetración Pentest y evaluación de controles de seguridad: ● El servicio se deberá realizar a aproximadamente 6000 activos informáticos del Gobierno del Estado de Nuevo León. ● Las pruebas de evaluación de controles y riesgos tecnológicos que se ejecuten deberán considerar al menos los siguientes rubros: o El licitante deberá realizar, por evento, actividades sobre activos tecnológicos que soporten la operación del Gobierno del Estado de Nuevo León divididos de la siguiente manera: **Pruebas de evaluación de riesgo tecnológico caja gris** ● El servicio deberá considerar al menos las siguientes fases: o Reconocimiento. o Identificación y priorización de Vulnerabilidades. o Preparación del ataque. o Explotación. o Post-Explotación. o Generación de resultados. ● Se deberá realizar una evaluación de los niveles de seguridad en la plataforma tecnológica localizada en el centro de datos y en el perímetro con la finalidad de obtener el nivel de riesgos al que se encuentra. ● Se deberán realizar pruebas de evaluación de riesgo tecnológico a la plataforma tecnológica del Gobierno del Estado de Nuevo León, bajo demanda, la cantidad de activos solicitados por evento será definido al momento de la solicitud (una vez al mes); se considerarán los siguientes servicios:

	● Diagnóstico de caja gris a la infraestructura tecnológica del Gobierno del Estado de Nuevo León desde el interior del Gobierno del Estado de Nuevo León, donde a través de un acceso de red y con cierta información de los dispositivos a evaluar se realizará el diagnóstico de manera enunciativa más no limitativa a: la infraestructura, los servidores, sistemas, bases de datos, usuarios internos, equipos de cómputo y servicios de directorio activo con las siguientes características: o El servicio no deberá impactar el rendimiento de los equipos que son evaluados por lo que se debe evitar la instalación de agentes. o Considerar que por la criticidad de la operación de la ENTIDAD las pruebas de penetración podrán ser suspendidas en forma inmediata por cualquier eventualidad operativa. o Dada la criticidad de los servicios de Directorio Activo en la institución, es preciso que de penetración ética exponga las vulnerabilidades en el momento donde se incluya la enumeración de Usuarios y Grupos del Directorio Activo y la posibilidad de creación de cuentas de Administrador del Dominio; así como la capacidad de descifrar "hashes" de contraseña. o Las pruebas de penetración éticas deberán ser aplicadas de acuerdo con la periodicidad e intensidad requerida de los procesos de la institución. o Pruebas con escenarios predefinidos para ejecutar evaluaciones de Directorio Activo y Ransomware. o Pruebas de caja Gris: Ejecutar pruebas de penetración granulares con puntos de partida específicos y definición de objetivos/resultados finales. o Evaluación de vulnerabilidades: Evaluar e identificar en el momento explotación de vulnerabilidades en la red basado en puntuación CVSS. o Proporcionar actualizaciones en el momento de como un ataque progresa a través de la organización, desde los usuarios, hacia los sistemas, indicando tácticas, técnicas y procedimientos del atacante. o Se deberá documentar cada TTP ejecutado en las pruebas según la descripción de la Matriz de MITRE ATTACK vigente. Deberá tener la capacidad de realizar pruebas concurrentes en diferentes redes y centros de datos con una visión unificada de los resultados ● La auditoría periódica para evaluar las vulnerabilidades y pruebas de penetración internas se realizarán desde las instalaciones del Gobierno del Estado de Nuevo León, mediante un análisis controlado. El Gobierno del Estado de Nuevo León definirá el sitio y gestionará accesos físicos y/o lógicos (accesos remotos seguros vía VPN) al mismo. ● En ninguna circunstancia se permitirá la instalación de código o agentes para la ejecución de las pruebas. Con el objeto de asegurar un oportuno control del proyecto y mitigar posibles riesgos que comprometan la disponibilidad del servicio, el licitante deberá elaborar un plan de trabajo donde se incluyan cada una de las fases en las que se ejecutara el proyecto, la metodología a emplear como parte de la entrega de servicio. Al respecto, se enlistan, de manera enunciativa más no limitativa, las fases que como mínimo deberá considerar el licitante dentro de su propuesta. El plan está abierto a que se agreguen las fases que el licitante considere, con la finalidad de que el Gobierno del Estado de Nuevo León reciba de manera oportuna los servicios, sin embargo, será indispensable cubrir, por lo menos, las siguientes fases: ● Fase de planificación. ● Fase de ejecución.

	● Fase de resultados. El licitante será el responsable de ejecutar las tareas técnicas y administrativas para el arranque del servicio El personal designado por parte del licitante asistirá a las Oficinas de la Dirección de Infraestructura Tecnológica de la Subsecretaría de Tecnologías a una reunión de trabajo para la definición general del proyecto y logística, la cual se llevará a cabo en una sesión inicial a los 5 (cinco) días hábiles antes del inicio de la prestación del servicio en donde, entre otros aspectos, se definirán: 1. De manera conjunta el licitante y el personal del Gobierno del Estado de Nuevo León definirán y elaborarán los formatos para la administración del proyecto, de conformidad con el "Calendario y Plan de Trabajo" propuesto por el licitante en su propuesta técnica. 2. El Gobierno del Estado de Nuevo León en común acuerdo con el licitante, podrá realizar modificaciones al calendario del plan de trabajo en cualquier momento si así se requiere, por las funciones propias de la institución, con el fin de no alterar la operación y atender las cargas de trabajo de las diversas áreas administrativas del Gobierno del Estado de Nuevo León, quien se reserva el derecho de realizar modificaciones en el transcurso de la auditoría, de tal forma que no afecte la fecha límite de entrega del Dictamen de Resultados periódicos. ● El Gobierno del Estado de Nuevo León designará al personal que coordinará el servicio con el licitante a más tardar cinco días hábiles posteriores a la firma del contrato. Dicha designación será notificada por escrito
Entregables para el Servicio de Evaluación de Controles, Riesgo Tecnológico de Ciberseguridad	● El licitante deberá entregar el Dictamen con los resultados de la auditoría al Gobierno del Estado de Nuevo León a la finalización de cada evento de revisión, en un lapso no mayor a 10 días hábiles por cada periodo mensual. ● Al término de cada revisión, el licitante en conjunto con el Gobierno del Estado de Nuevo León formalizará un acta de cierre de la ejecución del servicio en la cual se considerará la aceptación de los entregables de acuerdo con las especificaciones del contrato. El licitante deberá considerar entregar lo siguiente: ● Entregables como parte de la propuesta técnica. ○ Plan general de trabajo conforme a lo establecido en la descripción del servicio, el cual deberá estar firmado por el director del proyecto y por el representante legal quien firme la propuesta, con la finalidad de hacer más amplia la propuesta del licitante. ● Entregables mensuales a los 10 dias habiles como parte de la prestación del servicio. ○ El Dictamen periódico de Resultados deberá entregarse en papel membretado y firmado por cada uno de los involucrados, el cual deberá contener como mínimo los siguientes rubros: ● Dictamen de Resultados de la Auditoria preventiva: ● Prueba Penetración y Reportes del análisis ○ Prueba Penetración y Reportes del análisis ● Periodicidad del servicio ○ El servicio se ejecutará de forma mensual, considerando la entrega de 36 reportes a lo largo de la vigencia del contrato

	● Contenido ○ Vulnerabilidades identificadas durante la prueba, ordenadas por prioridad basadas en los resultados del análisis de penetración efectuado. ○ Objetivos de penetración exitosos (explotados) identificados durante la prueba, ordenados por criticidad. ○ Dispositivos descubiertos durante la prueba, incluyendo criticidad de cada dispositivo respecto a vulnerabilidades y objetivos de penetración, incluyendo servicios de "Discovery". ○ Credenciales comprometidas, obtenidas o descifradas. ○ Tendencia general de riesgos de pruebas anteriores. ● El licitante deberá entregar reporte con información del patrón de ataque y el conjunto de técnicas que un atacante pudiera emplear para explotar las vulnerabilidades que incluya la siguiente información: ○ Cuales técnicas fueron exitosas durante cada prueba específica. ○ Cuales técnicas y tácticas MITRE ATT&CK fueron utilizadas. ○ La secuencia en la cual todas esas técnicas fueron utilizadas para explotar vulnerabilidades. ○ Cómo y para qué los atacantes pudieran usar los ataques exitosos. ○ El número de sistemas impactados. El de resultados debe ser entregado en forma digital a la Dirección de Infraestructura Tecnológica ● De forma física deberá entregarse los siguientes documentos ● Al inicio del servicio NDA firmado de manera autógrafa por los siguientes actores: el representante legal de la empresa y responsable del servicio. ● Durante la ejecución de los servicios y la emisión mensual del reporte: NDA firmado de manera autógrafa por cada uno de los consultores que intervengan en la ejecución, emisión y documentación del dictamen mensual. ● Dictamen periódico en sobre cerrado y sellado con firma autógrafa por parte de los responsables de la ejecución, emisión y documentación de los informes ● En sobre cerrado, se entregará la contraseña de los archivos digitales que sean provistos como parte de la entrega del dictamen mensual.
Experiencia del Licitante para el Servicio de Evaluación de Controles, Riesgo Tecnológico de Ciberseguridad	El licitante deberá comprobar como parte de su propuesta ser una empresa cualificada y certificada en materia de tecnologías de centros de datos y seguridad de la información que preste el servicio con herramientas (software) que pudiera contar registro de propiedad intelectual, que se trate de un producto terminado en el mercado y NO deberá considerar para el servicio de evaluación de la Seguridad de la Información y Vulnerabilidades herramientas de uso libre para la ejecución del servicio Adicionalmente, el licitante deberá presentar como parte de su propuesta técnica, información relativa a los marcos metodológicos, buenas prácticas o marcos de trabajo a los que se alinea y servicio propuesto, para garantizar que se apega a

	prácticas internacionales orientadas al análisis de riesgos y vulnerabilidades digitales o al proceso de gestión de riesgos y/o vulnerabilidades según corresponda. Asimismo, debe incluir como parte de su propuesta técnica los siguientes perfiles para la provisión del servicio: “EL LICITANTE” Deberá comprobar que el personal está certificado para la instalación, configuración y operación de los servicios y acreditar la experiencia de al menos 36 meses de cada recurso. El licitante será responsable de todas las actividades realizadas por su personal durante la vigencia de la prestación de los servicios. Así mismo, el Gobierno del Estado de Nuevo León se reserva el derecho de solicitar por escrito el reemplazo del personal asignado por el licitante, en caso de que éste no acate los lineamientos institucionales de conducta o su desempeño no sea el esperado y como consecuencia pueda causar algún perjuicio. En este sentido, el Gobierno del Estado de Nuevo León notificará dicha situación al licitante a fin de que, en un plazo no mayor a 5 días hábiles posteriores, presente el reemplazo que cubra el o los perfiles en cuestión. El personal del licitante que tenga acceso a información que sea proporcionada por el Gobierno del Estado de Nuevo León, deberá considerar que dicha información tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos para tal efecto. Así mismo, el licitante no podrá difundir y divulgar por cualquier medio, la información que obtenga o a la que tenga acceso durante o con motivo de las actividades desarrolladas al amparo del contrato por virtud de la prestación del servicio a traves de un documento en el que se obliguen a guardar la debida reserva y confidencialidad durante la vigencia del servicio. El licitante se limitará a desarrollar solo las actividades descritas en el presente anexo técnico

Servicio de Pruebas Estáticas de Seguridad en las Aplicaciones (SAST)	El servicio de escaneo estático automatizado al código fuente de los aplicativos, para las pruebas de seguridad de aplicaciones estáticas (SAST) el cual deberá de analizar los archivos fuentes de la aplicación, además de identificar con precisión la causa del problema para corregir los defectos de seguridad subyacentes.
	
	• Evaluación con enfoque de caja blanca (white – box)
	• Análisis de código estático:
	  o Calidad del Software
	  o Complejidad de la Aplicación
	  o Deuda técnica (costo del desarrollo vs mitigación de riesgos)
	  o Riesgos de Seguridad del Software
	• Validación técnica de los mecanismos de control de los servicios web:
	  o Injection
	  o Broken Authentication and Session Management
	  o Cross-Site Scripting (XSS)
	  o Security Misconfiguration
	  o Sensitive Data Exposure

	○ Missing Function Level Access Control ○ Cross-Site Request Forgery (CSRF) ○ Using Components whit Know Vulnerabilities ○ Unvalidated Redirects and Forwards • Idenficación y eliminación de vulnerabilidades en el código fuente, binario o byte • Lenguajes soportados: PHP, Python, Java (incluido Android), Framework basados JavaScript, AJAX, JSP, ASP.NET, C# (.NET), RPG, ILE, PL/SQL, T-SQL, Angular, TypeScriptm, Vue.js,HTML. • Metodología a través de la revisión de seguridad del código fuente que deberá de consistir en un examen sistemático del código fuente de las aplicaciones, el cual deberá tener como finalidad descubrir los errores que puedan conducir a vulnerabilidades que debiliten la integridad del sistema. • Metodología de revisión de código fuente de la organización OWASP la cual deberá contar con diferentes fases desde el levantamiento de requerimientos hasta la elaboración del reporte técnico final. • Las fases de la prueba son: ○ Levantamiento de requerimientos y análisis funcional ○ Identificación de flujos datos ○ Análisis transaccional ○ Identificación de problemas y análisis de riesgo ○ Identificación de soluciones ○ Generación de reporte técnico de hallazgos y remediación
Entregables de Servicio de Pruebas Estáticas de Seguridad de las Aplicaciones (SAST)	● El proveedor adjudicado deberá entregar lo siguiente: ● Informe/Reporte Técnico personalizado ● Informe/Reporte Ejecutivo generado por herramienta a solicitud ● Informe/Reporte Basado en: ○ CWE Top 25 2019 ○ CWE/SANS Top 25 ○ DISA CCI 2 ○ DISA STIG ○ Develo per Workbook ● FISMA Compliance: ○ FIPS-200 ○ GDPR ○ MISRA ○ OWASP Mobile Top 10 ○ OWASP Top 10 ● PCI DSS Compliance: ○ Application Security Requirements

	● PCI SFF Compliance: ○ Secure Software Requirements ● Informes de remediación de vulnerabilidades Al término de cada revisión, el licitante formalizará un acta de cierre de la ejecución del servicio en la cual se considerará la aceptación de los entregables
Servicio de protección para Aplicaciones web especializados para protección de Ciberseguridad.	El servicio deberá contar con protección para aplicaciones incluyendo Políticas, Reglas, e Interfaces, así como elaborar una matriz de validación de servicios. Este servicio deberá cumplir con las siguientes características: Soportar por lo menos 80 aplicaciones y un ancho de banda de al menos 100 Mbps. 1. La implementación de 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. 2. Deberá soportar cualquier aplicación web, sin importar la plataforma, tamaño del sitio, lenguaje o escenario de implementación. 3. Deberá ofrecer los siguientes servicios en una única plataforma integrada 4. Web Application Firewall WAF 5. Servicio de Protección de APIs 6. Protección contra Bots 7. Detección de Backdoors en aplicativos Web 8. CDN 9. Servicio de Balanceo Aplicativo 10. Almacenamiento en Caché 11. Optimización de Contenido 12. Servicio de Mitigación de ataques DDoS L3/L4/L7 13. Servicio de Mitigación de ataques DDoS al servicio DNS 14. Herramientas de monitoreo de conexiones, ancho de banda y ataques. 15. Capacidad de exportar los eventos de seguridad a una herramienta tipo SIEM 16. Debe de soportar el modelo de seguridad positiva definido por OWASP y proteger contra el Top 10 de ataques a aplicaciones definido por OWASP 17. Deberá detectar y bloquear los intentos de instalar y/o operar backdoors en los Aplicativos Web. 18. Deberá hacer bloqueos a partir del País de Origen (GeoBlocking) Todas las soluciones de tipo software propuestas deberán ser registradas en el portal de soporte del fabricante bajo la cuenta de Gobierno del Estado de Nuevo León, la cual será proporcionada al LICITANTE ADJUDICADO posterior al fallo
Servicio de Mesa de Ayuda	El licitante deberá contar con una Mesa de Servicios, que sea la que utilice para la administración del servicio y la atención de reportes de falla, con las siguientes características: ● El servicio se deberá proporcionar mediante un Centro de Operaciones de Seguridad (SOC) propiedad del Licitante. Se deberán incluir la documentación que así lo demuestre.

	● Dicho SOC deberá ubicarse dentro del Estado de Nuevo León. ● El servicio debe considerar el soporte de 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 con el tipo de incidente. ● El licitante deberá proveer de un canal de comunicación telefónico 7x24 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 comprobar contar con un Sistema de Mesa de Servicios y acreditar al menos los siguientes especialistas, quienes operaran fuera de las instalaciones de la convocante, esta plantilla será la que se utilice para la administración del servicio y la atención de reportes de fallas. ● 5 especialistas Con copia de Cédula Profesional a nivel Licenciatura o Ingeniería en Electrónica y Comunicaciones, Telecomunicaciones, Informática, Tecnologías de la Información, Sistemas Computacionales o ramas afines a TIC. Presentar copia de certificación en ITIL en cualquier versión y al menos uno debe ser el coordinador con ITIL intermedio y cualquiera de los especialistas debe acreditar maestría en áreas a fines a TIC. ● Para garantizar los cumplimientos y niveles de servicios objeto de este proyecto, El Licitante deberá acreditar la experiencia de 36 meses de todos sus recursos humanos señalados mediante su currículum vítae debiendo contener, nombre completo, señalar años de experiencia en el perfil solicitado, teléfono, correo electrónico, descripción y vigencias de las certificaciones solicitadas de acuerdo con cada perfil. ● El licitante deberá contar con personal especializado en la administración, gestión y soporte en herramientas de gestión de incidentes. ● 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.
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 correspondiente. ● 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 implementada.
Entregables para todos los Servicios incluidos en la descripción de cada servicio o como parte integral de lo solicitado	● Informe documental de la situación, de las soluciones actualmente implementadas e integradas en Gobierno del Estado de Nuevo León. ● Informe documental de la situación, final posterior a la implementación, actualización de las soluciones. ● Documentación: de procesos internos para la atención de servicios, e interacciones con Gobierno del Estado, así como procesos relativos a la identificación y resolución de incidencias de seguridad ● Documentos de Planeación, Implementación, Verificación, validación y pruebas, Puesta en Marcha, para cada una de las soluciones propuestas. ● El licitante 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 NO interrupción del servicio. ● El licitante ganador deberá entregar la documentación, tanto en versión impresa como en electrónica, correspondiente a las memorias técnicas de todos y cada uno de los detalles de implementación, que sirva como referencia para posibles ajustes y/o actualizaciones. ● El licitante 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 ● Deberá comprobar al menos 3 ingenieros con certificados vigentes que demuestren conocimientos y habilidades avanzadas para diseñar, instalar, configurar, operar, gestionar y solucionar problemas en las diferentes implementaciones de la plataforma de seguridad perimetral operando con la unidad requirente. ● La Dirección de Infraestructura Tecnológica de la Subsecretaría de Tecnologías de la Secretaría de Administración se reserva el derecho de solicitar documentos, reportes o informes adicionales conforme sea requerido y conforme la evolución de los servicios se presente.
Forma de Pago:	36 pagos mensuales dentro de los 30 días hábiles, entrega de factura a mes vencido a entera satisfacción del usuario.
Lugar de entrega:	Torre Administrativa, Piso 18, Washington No. 2000, Col. Obrera, CP. 64010, Monterrey, Nuevo León
Tiempo de entrega:	15 hábiles después de la firma del contrato

Nombre y Firma de Representante Legal

ENTREGABLES DENTRO DEL SOBRE DE SU PROPUESTA TÉCNICA.

Entregables:
1.- Deberá comprobar experiencia de 36 meses en proyectos directamente relacionados con la propuesta, acreditándolo mediante copias simples de al menos 3 contratos debidamente firmador, ya sea con el sector público o iniciativa privada.
2.- Deberá comprobar como parte de su propuesta técnica la documentación que avale la experiencia debidamente firmada por el representante legal de ser una empresa cualificada y certificada en materia de tecnologías de centros de datos y seguridad de la información que preste el servicio con herramientas (software) que pudiera contar registro de propiedad intelectual, que se trate de un producto terminado en el mercado y NO deberá considerar para el servicio de evaluación de la Seguridad de la Información y Vulnerabilidades herramientas de uso libre para la ejecución del servicio.
3.- Deberá presentar como parte de su propuesta técnica, información relativa a los marcos metodológicos, buenas prácticas o marcos de trabajo a los que se alinea y servicio propuesto, para garantizar que se apega a prácticas internacionales orientadas al análisis de riesgos y vulnerabilidades digitales o al proceso de gestión de riesgos y/o vulnerabilidades según corresponda.
4.- Deberá comprobar que el personal está certificado, para la instalación, configuración y operación de los servicios requeridos y acreditar la experiencia de al menos 36 meses de cada recurso.
5.- Deberá acreditar que cuenta con una Mesa de Servicios 7x24 para recibir reportes de la Unidad Requirente. Conforme a lo especificado en la ficha técnica.
6.- Deberá comprobar contar con 5 especialistas, con copia de Cédula Profesional a nivel Licenciatura o Ingeniería en Electrónica y Comunicaciones, Telecomunicaciones, Informática, Tecnologías de la Información, Sistemas Computacionales o ramas afines a TIC. Presentar copia de certificación en ITIL en cualquier versión y al menos uno debe ser el coordinador con ITIL intermedio y cualquiera de los especialistas debe acreditar maestría en áreas a fines a TIC.
7.- Deberá acreditar la experiencia de 36 meses de todos sus recursos humanos señalados mediante su currículum vítae debiendo contener, nombre completo, señalar años de experiencia en el perfil solicitado, teléfono, correo electrónico, descripción y vigencias de las certificaciones solicitadas de acuerdo con cada perfil.
8.- Deberá contar con personal especializado en la administración, gestión y soporte en herramientas de gestión de incidentes
9.- Deberá comprobar al menos 3 ingenieros con certificados vigentes que demuestren conocimientos y habilidades avanzadas para diseñar, instalar, configurar, operar, gestionar y solucionar problemas en las diferentes implementaciones de la plataforma de seguridad perimetral operando con la unidad requirente.

_____

Nombre y Firma de Representante Legal