FICHA TÉCNICA

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

Equipo:	SERVICIOS ADMINISTRADOS SOLICITADOS	**Cantidad:**	01
Servicios Administrados solicitados	Los servicios administrados de seguridad perimetral de la red Informática del Gobierno del Estado de Nuevo León junto con otros servicios especializados, protegen los bienes, procesos y servicios basados en el uso de las tecnologías de información y comunicaciones, e información misma reside en medios electrónicos, a través de una solución integral de tecnología de alta especialidad y servicios de acuerdo a las siguientes características: ● La implementación contará con una actualización sobre la infraestructura de seguridad perimetral actual 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. ● 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 podría causar pérdida de información, robo de información, o suspensión de procesos de gobierno. ● El Servicio mensual contará de revisiones 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 ● El 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. ● El Servicio de protección para Aplicaciones y Portales web especializados la solución deberá soportar al menos 80 sitios sin importar la plataforma o tamaño del sitio, lenguaje o escenario de implementación. ● 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 la evaluación de controles y analizar de riesgo que permita mejorar la seguridad de la información, mediante la identificación del nivel de riesgo tecnológico existente en la plataforma tecnológica y el desarrollo de un plan de tratamiento de los riesgos identificados incluyendo priorización y tiempos estimados de las iniciativas. ● Servicio de capacitación continúa 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.		

Entregable Principal General como parte del servicio administrado global.	Informe mensual impreso y en versión electrónica acerca del servicio de solicitado y asistencia técnica proporcionado en forma mensual.
Servicio de renovación de licenciamiento para seguridad perimetral	El servicio de renovación de licenciamiento deberá tener Implementación y actualización de software para protección de amenazas para dar continuidad a la infraestructura existente de Seguridad Perimetral de firewalls. 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 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.) ● Deberá contar con actualización de firmas de ataques y poder programarse 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 posibles nuevos ataques. ● Deberá contar con la funcionalidad de DNS Sinkhole para la reescritura de resoluciones de nombres maliciosos. ● Deberá tener capacidad de identificar la aplicación sin importar el puerto o protocolo que ésta utilice. Permitiendo así conocer y permitir o denegar las dependencias de cada aplicación y limitar las aplicaciones a sus puertos estándar ● Deberá poder crear políticas basadas en el control por aplicación, por categoría (cuando menos 72 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 El servicio administrado deberá incluir las siguientes funcionalidades y características para el Filtrado de Contenido: ● Deberá ofrecer opciones de uso en 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. ● 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 descripción 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.
	● Validación en tiempo real del tráfico para evitar ataques evasivos Web
	
	El servicio deberá incluir las siguientes funcionalidades y características de VPN (Red Privada Virtual):
	
	● La solución 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, 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.
	● La solución 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.
	● La solución deberá contar al menos con 1,000 túneles simultáneos sitio a sitio 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.
	  ● Deberá proteger contra el Phishing y el robo de credenciales
	  ● Por medio del filtrado de contenido deberá poner en cuarentena todos los dispositivos comprometidos
	● Deberá prevenir el uso de herramientas de elusion y evasion
	● La solución deberá contar con acceso seguro a las aplicaciones SaaS y bloquear las aplicaciones no autorizadas en las políticas asignadas al dispositivo.
	● Permitirá el acceso seguro y sin clientes para funcionarios de diferente cargo.
	● Deberá ofrecer identificación de usuario confiable y brindar información inmediata y precisa al host para la visibilidad de aplicaciones y políticas
	
	El servicio deberá cumplir con las siguientes funcionalidades y características enfocado a dar continuidad a la administración de los equipos y reporteo:

	● Administración de políticas y objetos a través de la interfaz gráfica embebida en el equipo Firewall basada en Web y Administración del equipo a través de CLI (ssh y puerto consola) y adicionalmente 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. ● 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. El servicio deberá incluir las siguientes funcionalidades y características para análisis de archivos de forma aislada contra malware: ● Deberá identificar amenazas desconocidas con datos compartidos de la comunidad de análisis de malware empresarial más grande de la industria, incluidas las amenazas enviadas desde redes, puntos finales, la nube y socios externos. ● Capacidades de análisis de memoria en tiempo de ejecución inteligente, estática, dinámica y de aprendizaje automático para detectar y prevenir las amenazas evasivas.

	● Deberá proveer aprendizaje automático alimentado por modelos de amenazas alojados continuamente en la nube, entregados hacia firewalls de próxima generación físicos y virtuales. ● Genera automáticamente protecciones a lo largo del ciclo de vida del ataque cuando se descubre una nueva amenaza por primera vez, bloquea archivos maliciosos, accede a URL maliciosas y tráfico C2. ● Proveer análisis de comportamiento detallado para ayudar a comprender cómo funciona el malware recién descubierto. Proveer registros integrados que permiten identificar rápidamente a los usuarios infectados e investigar posibles infracciones con un análisis detallado y visibilidad de eventos de amenazas desconocidos. ● Ejecuta archivos desconocidos en varias versiones de sistemas operativos y aplicaciones simultáneamente para comprender completamente el alcance de una amenaza. ● Realiza un seguimiento eficiente de la actividad maliciosa durante el tiempo de ejecución y crea capturas de memoria cuando sucede algo interesante. Capacidad de detección de malware conocido y desconocido con actualizaciones en tiempo real y actualizado de manera automática con detecciones de todo el mundo. El tiempo de respuesta debe de ser de 5 minutos. Los archivos mínimos que se deben de escanear son: Ejecutables (EXE), DLL, Office (Word, Excel, PowerPoint), PDF, APK, JAR (Java), Archivos Linux ELF, archivos script (BAT, JS, VBS, PS1, Shell script, and HTA), archivos encriptados (TLS/SSL) MacOS X archivos y Adobe Flash 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 ● Deberá contar con detección del uso de algoritmos de generación de dominios para detener la comunicación a servidores C2 ● Deberá tener capacidad de análisis predictivos y detecciones impulsadas por aprendizaje automático, este servicio previene las últimas y más sofisticadas amenazas de la capa DNS en tiempo real. Los clientes se benefician de una visibilidad y cobertura completa de todos sus usuarios, dispositivos y ubicaciones dentro de su red ● Deberá contar con capacidades de Detecciones pioneras en la industria, utiliza detecciones pioneras en la industria para evitar C2, exfiltración de datos, phishing y entrega de malware ● Deberá contar con capacidad de creación de políticas específicas para los tipos de tráfico de DNS cotejando hacia una base de datos escalable y en la nube en tiempo real para determinar las acciones de aplicación apropiadas ● Deberá contar con uso de ML para detectar y categorizar de forma adecuada y rápida las amenazas a través de DNS Deberá tener capacidad de detección usando un servicio de elusión de proxy y anonimizadores.
Entregables para el Servicio de renovación de licenciamiento para seguridad perimetral	El Informe a entregar será en formato checklist con evidencia de la actualización y renovación del software indicado en el servicio a ejecutar. El departamento de Infraestructura realizará la validación del entregable y visto bueno del mismo para la aceptación del servicio entregado, lo cual será un requisito para proceder con el pago pactado, siempre y cuando se hayan cubierto los criterios de aceptación y aceptación del entregable.
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. ● Copias de los contratos arriba mencionados que avalen la experiencia indicada. ● 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 diseñar, instalar, configurar, operar, gestionar y solucionar problemas en las diferentes implementaciones de la plataforma de seguridad perimetral operando con la convocante. Comprobar con inscripción en el seguro social de dichos ingenieros y el curriculum vitae de los mismos. **Los documentos listados en esta sección, son documentos que deberán presentarse como parte de la propuesta de licitante.**
Documentos o Cartas para la solución propuesta que deberán presentarse como parte de la 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 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 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. **Los documentos listados en esta sección, son documentos que deberán presentarse como parte de la propuesta de licitante.**
Servicio de protección para Aplicaciones y Portales web especializados para protección de Ciberseguridad.	El servicio de renovación deberá contar con protección para aplicaciones y portales incluyendo Políticas, Reglas, e Interfaces, así como elaborar una matriz de validación de servicios. Este servicio deberá cumplir con las siguientes características: La solución requiere soportar por lo menos 80 aplicaciones y un ancho de banda de al menos 100 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 Protección 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 Caché 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 deshabilitar/habilitar 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 licitante PCI Nivel 1 ● La solución deberá contar con la certificación "SOC 2" tipo "I y II", con los cuales garantice que los sistemas utilizados, su diseño y su efectividad operacional, son adecuados para cumplir con los principios de confianza definidos por la AICPA ● El licitante deberá contar con una capacidad de red global de al menos 6 Tbps ● 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 desencadenan, 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 híbrido.

	● 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: 1) TCP SYN+ACK 2) TCP FIN a) TCP RESET b) TCP ACK c) TCP ACK+PSH d) TCP Fragment e) UDP f) ICMP g) IGMP h) HTTP Flood i) Brute Force j) Connection Flood k) Slowloris l) Spoofing m) DNS Flood n) Mixed SYN+UDP or ICMP+UDP Flood o) TCP SYN+ACK p) Ping Of Death q) Smurf r) Reflected ICMP and UDP s) Teardrop t) Zero-day DDoS attacks u) 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 global, 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 caché. ● La solución deberá soportar las siguientes capacidades para el almacenamiento en caché ● Contenido Estático ● Contenido Dinámico ● Servir Páginas desde Memoria ● Almacenamiento caché desde el lado del Usuario ● La solución deberá tener la opción de generar reglas personalizadas para el almacenamiento en caché ● El Servicio de DNS 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 que forman parte del Servicio de renovación de licenciamiento para seguridad perimetral	Informe mensual impreso y en versión electrónica acerca del servicio de solicitado y asistencia técnica proporcionado en forma mensual.
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 como parte del "Servicio de Evaluación de Controles, Riesgo Tecnológico de Ciberseguridad", deberá realizar una auditoria periódica automatizada 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 cibernéticas y deberá incluir las recomendaciones necesarias para que se tomen medidas para proteger el ambiente. Asimismo, como parte del servicio se requerirá anexo al Dictamen de resultados de la auditoría, un Plan de Remediación con las actividades necesarias y recomendadas por el personal experto del 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 y económica las revisiones y pruebas de seguridad en los componentes de la infraestructura de la 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. ● Los hallazgos deberán ser presentados 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.

	● En caso de que el licitante encuentre una vulnerabilidad con una criticidad alta, esta deberá estar claramente identificada en la entrega del Dictamen resultado de la auditoría de vulnerabilidades.
	
	Características de la Auditoría periódica 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, que se citan de manera enunciativa pero no limitativa:
	● La metodología para la ejecución de Pruebas de Penetración utilizada por el licitante deberá tener como objetivo establecer el proceso y la forma en la que el licitante ejecuta dichas pruebas, por medio de esta deberá ser posible estandarizar y homologar la operación en apego al marco de MITRE ATTACK
	● El licitante deberá realizar, por evento, un servicio de pruebas de penetración con actividades continuas sobre la totalidad de 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 negra, gris
	  ● Pruebas de preparación de Ransomware
	● El servicio deberá considerar de manera automatizada al menos las siguientes fases:
	  ● Reconocimiento.
	  ● Identificación y priorización de Vulnerabilidades.
	  ● Preparación del ataque.
	  ● Explotación.
	  ● Post-Explotación.
	  ● 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 (una vez al mes); se considerarán los siguientes servicios:
	  ○ Diagnóstico de caja negra/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:
	  ● La solución no deberá impactar el rendimiento de los equipos que son evaluados por lo que se debe evitar la instalación de agentes.
	  ● 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.
	  ● Dada la criticidad de los servicios de Directorio Activo en la institución, es preciso que la solución de penetración ética exponga las vulnerabilidades en tiempo real 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.
	  ● Las pruebas de penetración éticas deberán ser aplicadas de acuerdo con la periodicidad e intensidad requerida de los procesos de la institución.
	  ● Pruebas con escenarios predefinidos para ejecutar evaluaciones de Directorio Activo y Ransomware.

	● Pruebas de caja Gris: Ejecutar pruebas de penetración granulares con puntos de partida específicos y definición de objetivos/resultados finales. ● Evaluación de vulnerabilidades: Evaluar e identificar en tiempo real explotación de vulnerabilidades en la red basado en puntuación CVSS. ● Proporcionar actualizaciones en tiempo real de como un ataque progresa a través de la organización, desde los usuarios, hacia los sistemas, indicando tácticas, técnicas y procedimientos del atacante. ● Se deberá documentar cada TTP ejecutado en las pruebas según la descripción de la Matriz de MITRE ATTACK vigente. ● La solución 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 al mismo. ● Cabe señalar que, con base en las condiciones actuales de salud pública, el Gobierno del Estado de Nuevo León podrá permitir la ejecución de las pruebas mencionadas de manera remota, previo acuerdo con el licitante, siempre que se garantice un ambiente controlado y no afecten los resultados de éstas. ● Bajo 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, <u>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.</u> 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: 1. Fase de planificación. 2. Fase de ejecución. 3. Fase de resultados. El licitante será el responsable de ejecutar las tareas técnicas y administrativas para el arranque del servicio en coordinación con el Gobierno del Estado de Nuevo León. El personal designado por parte del licitante asistirá a las Oficinas de la Dirección de Infraestructura Tecnológica de la Secretaria de Administración del Gobierno del Estado de Nuevo León 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 3 (tres) días hábiles posteriores al 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. 3. El Gobierno del Estado de Nuevo León designará al personal que coordinará el servicio con el licitante a más tardar dos 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 8 días hábiles.
	● El Dictamen deberá incluir una guía de Remediación para fortalecer la plataforma tecnológica y minimizar las vulnerabilidades detectadas.
	● Al término de cada revisión periódica, 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 y económica.
	  ● Plan general de trabajo conforme a lo establecido en la descripción del servicio.
	
	● Entregables periódicos 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.

	● Planes de remediación:
	  ● Proporcionar pasos con detalles completos de como remediar cada vulnerabilidad identificada.
	  ● Definir prioridades de remediación enfocadas en vulnerabilidades de raíz, definiendo estrategias para enfocarse en los puntos donde los atacantes pudieran encontrar más éxito.
	
	● El Dictamen periódico de resultados debe ser entregado en forma digital, y protegido con contraseña únicamente 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 ser una empresa cualificada y certificada en materia de tecnologías de centros de datos y seguridad de la información que preste el servicio con una herramienta (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 herramientas de uso libre para la ejecución del servicio. Deberá presentar como parte de su propuesta técnica la documentación que avale lo señalado; como pudiera ser: carta de consultor autorizado, carta de distribuidor autorizado, cartas que avalen la experiencia, debidamente firmadas por el representante legal del licitante, así como carta de reconocimiento de relación comercial, firmada por el representante comercial de la marca en México de la solución propuesta. 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 la solución 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: Especialista en Seguridad: ● Cantidad: 1 Recurso ● Descripción: Personal que evaluará todos los conceptos de seguridad para dictaminar El personal designado por parte del licitante para la prestación del servicio será única y exclusiva responsabilidad de este último, por lo que el Gobierno del Estado de Nuevo León queda exento de cualquier responsabilidad de éste en cualquier situación legal, laboral o de cualquier otra índole. El licitante será responsable de todas las actividades que se realicen durante la prestación de los servicios. Asimismo, 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. Asimismo, 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. El licitante sólo podrá desarrollar las actividades descritas en el presente anexo técnico.
Servicio de Capacitación Continua especializada	Los servicios de capacitación deberán ser provistos por entidades certificadoras y autorizadas por el marco de referencia, el fabricante o el ente certificador correspondiente. ● Se deberá considerar al menos 2 personas a Introducción de framework de NIST de ICS2 ● Se deberá considerar al menos 1 personas para el Curso de CISM de ISACA ● Se deberá considerar al menos 1 personas para el Curso de CISSP de ISC2 ● Se deberá considerar al menos 3 personas para el Curso de CRISC de ISACA ● Se deberá considerar al menos 3 persona para el Curso de CSX-F de ISACA ● Se deberá considerar al menos 4 persona para el Curso de CompTIA Security+ ● Se deberá considerar al menos 4 personas para el Curso de Administrador de la plataforma de seguridad perimetral ● Se deberá considerar al menos 4 personas para el curso de administración de protección de aplicaciones ● Se deberá considerar al menos 4 personas para el curso de administración de protección de correo electrónico Estos cursos se deberán ofrecer en el Área Metropolitana del Estado de Nuevo León o de forma virtual en línea de acuerdo a disponibilidad, y deberán de agendarse durante la vigencia del servicio solicitado. De igual manera deberá incluirse los vouchers respectivos para realizar el examen de certificación correspondiente con al menos 2 oportunidades incluidas.
Entregables como parte del servicio de capacitación continua especializada	• Diplomas de participación a los cursos de entrenamiento y capacitación emitido por la organización, ente certificador o fabricante. • Voucher de entrenamiento y examen válido con fechas definidas previamente con el equipo a cargo en Gobierno del Estado, y conforme a la disponibilidad de las entidades certificadoras, el fabricante o las entidades autorizadas para la aplicación de los exámenes. • Apoyo en el trámite correspondiente a cada uno de los candidatos a examen, en el proceso de registro y toma del examen correspondiente conforme sea requerido.
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.

	● 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 comprobar contar con un Sistema de Mesa de Servicios de con al menos 10 especialistas fuera de las instalaciones de la convocante y que sea la que se utilice para la administración del servicio y la atención de reportes de fallas. Comprobar con inscripción en el seguro social. ● 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.
Entregables durante la vigencia del servicio de mesa de ayuda	Informe mensual impreso y en versión electrónica acerca del servicio de solicitado y asistencia técnica proporcionado en forma mensual, donde se especifique al menos número de incidente, cantidad de incidentes, descripción de incidentes, tiempos de solución y atención, ingeniero o áreas involucradas, entre otra información que pudiera ser requerida por parte del Gobierno del Estado de Nuevo León.
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. La solución podrá ser entregada conforme a la solución que se encuentre disponible en el mercado, pudiendo ser una solución en la nube, una solución virtual o bien un equipo appliance (equipo físico). En caso de considerar appliance o equipo físico, las especificaciones de hardware mínimas son las siguientes: ● Factor de Forma: Montaje en Rack 1U ● Almacenamiento: 2x 2 TB (2x 2 TB Opcional ● 4 Puertos Cobre 10/100/1000 ● 2 Puertos SFP Gigabit ● Gestión de Almacenamiento RAID: Hardware 0, 1, 5, 10, Hot Spare (Basado en el recuento de unidades) ● Número Máximo de Dominios: 800 ● Políticas máximas por Dominio: 600 ● Políticas Máximas por sistema: 2000 ● Buzones máximos en modo servidor: 1500 ● Ruteo de correo Msg/s: 800000 ● Rendimiento de AntiSPam Msg/s: 500000 ● Rendimiento AV/AS Msg/s: 400000 En caso de considerar licenciamiento para instalar en equipos virtuales, las especificaciones de mínimas 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 (Minimo/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 con la solución propuesta: ● Solución debe 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 ● La solución debe 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 ● La solución debe ser capaz de funcionar como un gateway SMTP para los servidores de correo existentes. ● La solución debe ser capaz de actuar como gateway, en calidad de MTA (Mail Transfer Agent). ● La solución debe ser capaz de funcionar de una manera transparente, actuando como un proxy transparente para el envío de mensajes a los servidores de correo protegidos. ● Debe poder ser instalado en forma de proxy SMTP transparente, para el análisis de correo saliente, buscando evitar el reporte en Blacklist ● La solución puede ser implementada como un cliente WCCP y recibir correo y analizar mediante este protocolo. ● La solución debe soportar su implementación en modo de servidor, operando como un servidor de correo MTA independiente con buzones para los usuarios. ● Debe ser capaz de almacenar localmente mensajes de correo electrónico para su entrega a los usuarios a través de correo Web, POP3 y / o IMAP. ● Debe tener disponible un API basado en REST para fines de monitoreo, automatización y orquestación ● La solución debe ser licenciada sin importar el número de buzones que proteja. El licenciamiento es basado en el performance del hardware suministrado (correo por hora) ● La solución debe soportar listas blancas y negras (White/Black List) por usuario, por dominio y globalmente para todo el sistema. ● La solución debe permitir la sobrescritura, la edición y personalización de los mensajes de notificación de antivirus y anti-spyware. ● La solución debe poder retrasar el envío de correo sobredimensionado a horarios que sean de menos carga. ● La solución debe poder definir el reenvío de correo (relay) a una IP específica con base a la IP origen del mensaje. ● La solución debe proporcionar soporte para múltiples dominios de correo electrónico. ● La solución debe ser compatible con la implementación de políticas por destinatario, de dominio, del tráfico entrante o saliente. ● La solución debe ser capaz de entregar el correo en función de los usuarios existentes en una base de LDAP ● La solución debe 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. ● La solución debe ser capaz de programar el envío de informes de cuarentena. ● La solución debe 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. ● La solución debe ser capaz de mantener la cola de correo (Queue) en caso de fallo en la conexión de salida, retrasos o errores de entrega. ● La solución debe ser capaz de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP. ● La solución debe 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. ● La solución debe ser compatible con el enrutamiento en IPv4 y IPv6. · ● La solución debe permitir el almacenamiento de correo electrónico y de cuarentena a nivel local o servidor remoto. ● La solución debe tener características antispam, antivirus, anti-spyware y anti-phishing. ● La solución debe ser capaz de realizar la inspección del correo de Internet entrante y saliente. ● La solución debe contar con un Wizard para el fácil y rápido aprovisionamiento de las configuraciones básicas del equipo y de los dominios a proteger ● La solución debe proporcionar protección contra ataques de denegación de servicio, tales como Mail Bomb. ● La solución debe proporcionar un control DNS reverso para la protección contra los ataques spoofing. ● La solución se debe conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones de Anti-Spam. ● La solución puede detectar si el origen de una conexión es lícito basado en una base de datos de reputación de IPs suministrada por el fabricante. ● La solución puede detectar 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 debe 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. ● La solución debe 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 asi definir y detectar nuevas reglas de SPAM. ● La solución debe ser capaz de realizar análisis Heurístico y definir umbrales máximos de acuerdo al comportamiento del correo y así determinar si un correo es spam. ● La solución debe ser capaz de realizar análisis Bayesiano para determinar si un correo es spam. ● La solución debe ser capaz de detectar si el correo electrónico es un boletín de noticias (Newsletter) ● La solución debe 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. ● La solución debe ser capaz de filtrar mensajes de correo electrónico basados en los URI (Uniform Resource Identifier) contenidas en el cuerpo del mensaje. ● La solución debe ser capaz de realizar análisis sobre la base de palabras prohibidas (Banned Words). ● La solución debe 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. ● La solución permite crear listas blancas o negras de palabras. ● La solución debe 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. ● La solución debe ser capaz de realizar documentos de análisis de imagen y PDF identificando con base en esto si el correo es SPAM. ● La solución debe ser capaz de soportar las listas negras de terceros tales como DNSBL y SURBL. ● La solución debe ser compatible con la lista gris para las cuentas de correo electrónico en IPv4 e IPv6. ● La solución debe ser capaz de detectar las direcciones IP falsificadas (Forged IP). ● La solución permite identificar imágenes que hagan alusión a contenido SPAM. Debe soportar el análisis de las siguientes extensiones GIF, JPG, PNG ● La solución debe poder validar si el destinatario del correo entrante es un buzón válido ● La solución debe ser compatible con Sender Policy Framework (SPF). ● La solución debe ser compatible con Domain Keys Identified Mail (DKIM). ● La solución debe ser compatible con Domain BasedMessage Authentication (DMARC). ● La solución debe identificar altos volúmenes de conexiones y aplicar límites basados en senders e Ips. ● La solución debe ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico. ● La solución debe permitir su configuración a través del acceso web (HTTP, HTTPS). ● La solución debe ser capaz de permitir la creación de administradores únicos para la administración y configuración de la solución por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen. ● La solución debe ser capaz de proporcionar al menos dos niveles de gestión de acceso: lectura / escritura (Read/Write) o de sólo lectura (Read Only) ● La solución debe 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. ● La solución debe soportar doble factor de autenticación para el login de usuarios administradores ● La solución, estando en server mode, debe poder Sincronizar contactos y calendarios con clientes de correo (MUA) ● En modo server, debe soportar los protocolos WebDAV y CalDAV para la publicación y sincronización de calendarios ● La solución debe contar con algún mecanismo para la fácil migración de buzones y cuentas desde un servidor a la nueva solución estando en server mode. ● La solución debe ser capaz de almacenar los registros y eventos a nivel local y también enviarlos a servidores ● remotos (Syslog). ● La solución debe permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica. ● La solución debe generar informes por demanda o programados a intervalos de tiempo específicos ● La solución debe generar y enviar informes en formato PDF o HTML.
Entregables durante la vigencia del servicio de Seguridad para protección del Correo institucional entrante y saliente.	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 que forman parte del servicio de Seguridad para protección del Correo institucional entrante y saliente.	• 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 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 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 la solución implementada.
Entregables para todos los Servicios incluidos en el servicio que pudieran encontrarse incluidos en la descripción de cada servicio o como parte integral del servicio solicitado	● Informe documental de la situación, diseño, arquitectura de las soluciones actualmente implementadas e integradas en Gobierno del Estado de Nuevo León. ● Informe documental de la situación, diseño, arquitectura de la solución final posterior a la implementación, actualización de las soluciones. ● Documentación relativa a: 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, Arquitectura, Diseño, 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 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 la solución implementada, 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 funcional del Gobierno del Estado de Nuevo León. ● El Gobierno del Estado de Nuevo León y sus representantes responsables de la recepción de servicio se reserva el derecho de solicitar documentos, reportes o informes adicionales conforme sea requerido y conforme la evolución de los servicios se presente.
Vigencia	12 (doce) meses de servicio.
Tiempo de entrega	Al día siguiente del fallo definitivo respectivo.
Forma de pago	30% de anticipo previa entrega de la garantía correspondiente y el 70% restante dividido en 12 pagos mensuales a entera satisfacción del solicitante.

_____

NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL

CHECK LIST REQUISITOS A PRESENTARSE DENTRO DEL SOBRE DE SU PROPUESTA TÉCNICA SERVICIOS ADMINISTRADOS DE SEGURIDAD PERIMETRAL Y SERVICIOS ESPECIALIZADOS DE SEGURIDAD INFORMATICA PARA LA RED INFORMÁTICA DEL GOBIERNO DEL ESTADO DE NUEVO LEÓN.

- 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.
    - Copias de los contratos arriba mencionados que avalen la experiencia indicada.
    - 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 diseñar, instalar, configurar, operar, gestionar y solucionar problemas en las diferentes implementaciones de la plataforma de seguridad perimetral operando con la convocante. Comprobar con inscripción en el seguro social de dichos ingenieros y el currículo vitae de los mismos.
- 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 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 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.
- Con el objeto de asegurar un oportuno control del proyecto y mitigar posibles riesgos que comprometan la disponibilidad del servicio, **el licitante deberá integrar a detalle como parte de su propuesta técnica un plan de trabajo con cada una de las fases en las que dividirá el proyecto, la metodología que empleará para la entrega del servicio, así como un cronograma del proyecto**.

  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 deberá ser una empresa cualificada y certificada en materia de tecnologías de centros de datos y seguridad de la información que preste el servicio con una herramienta (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 herramientas de uso libre para la ejecución del servicio. Deberá presentar como parte de su propuesta técnica la documentación que avale lo señalado; como pudiera ser: carta de consultor autorizado, carta de distribuidor autorizado, cartas que avalen la experiencia, debidamente firmadas por el representante legal del licitante, así como carta de reconocimiento de relación comercial, firmada por el representante comercial de la marca en México de la solución propuesta

- El licitante deberá presentar como parte de su propuesta técnica, al menos información relativa a los marcos metodológicos, buenas prácticas o marcos de trabajo a los que se alinea la solución 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.

- 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 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.