FICHA TÉCNICA

SERVICIOS ADMINISTRADOS DE SEGURIDAD PERIMETRAL DE LA RED INFORMÁTICA DEL GOBIERNO DEL ESTADO DE NUEVO LEÓN

Requisición No. 198663

Cantidad: 1 Servicio

COMPONENTE	DESCRIPCIÓN
Servicio solicitado	Servicios administrados de seguridad perimetral de la Red Informática del Gobierno del Estado de Nuevo León, que permita proteger los bienes, procesos y servicios basados en el uso de las tecnologías de información y comunicaciones, e información que obre en medios electrónicos, a través de una solución integral de tecnología de alta especialidad y servicios de acuerdo a las siguientes características: • Implementación de una solución integral de tecnología de alta especialidad para proveer servicios administrados de seguridad perimetral de la red informática del Gobierno del Estado de Nuevo León, diseñada especialmente para la protección de los activos tecnológicos que operan en la red y en los sitios principales. • Servicio de protección de seguridad de la red para los servicios de Internet, servicios inherentes a la zona desmilitarizada, correo electrónico, aplicativos, sistemas, servicios en línea, filtrado de correo electrónico, DNS y bases de datos, para así obtener el mejor rendimiento e incrementar la eficiencia de operación para los usuarios y mitigar los riesgos de afectación para estos servicios, de la actividad de software mal intencionado, que podría causar pérdida de información, robo de información, o suspensión de procesos de gobierno. • Servicio de detección de posibles amenazas potenciales de seguridad en la red relacionadas con la seguridad de la información, a nivel de la infraestructura tecnológica de los Nodos de Comunicaciones principales, que pudieran impactar en la confidencialidad, integridad y disponibilidad de la información de manera preventiva, a fin de tomar acciones correctivas y de mejora, y con apego a las mejores prácticas y a los procesos relacionados a la seguridad de la información. • Servicio de Mesa de Ayuda 7x24x365 para proporcionar asistencia y soporte técnico sobre cualquier funcionalidad de la solución propuesta, a través del esquema de servicios administrados en forma compartida.
Servicio basado en clusters de alta disponibilidad	Se requiere que el servicio de Seguridad Perimetral esté basado en una solución de al menos una infraestructura configurada en 2 (dos) Clusters físicos de alta disponibilidad en Modo Activo-Pasivo y una Consola de Administración. El licitante deberá entregar junto con su propuesta la referencia necesaria para acceder a los documentos públicos en el portal de internet del fabricante y que puedan ser descargados para su consulta.

COMPONENTE	DESCRIPCIÓN
	Se requiere que la sustitución de la infraestructura tecnológica actual hacia la nueva infraestructura, tomando de base que la infraestructura actual está basada en equipos Check Point Modelo 15400, 2 clusters, y 1 Smart-1 3050 de segunda generación. Se requiere la migración de la configuración de la infraestructura actual de la marca Check Point a la nueva infraestructura, que contemple todo lo necesario, incluyendo Objetos de red, NAT, Políticas, e Interfaces, así como elaborar una matriz de validación de servicios. La solución propuesta de deberá contar al menos con el siguiente Equipo Requerido: Considerar al menos 2 (dos) Clusters Físicos, cada cluster constituido por 2 (dos) Firewalls de siguiente generación Modo Alta Disponibilidad (HA) Activo-Pasivo o Activo-Activo, los cuales deberán cumplir con al menos las siguientes características: • El equipo deberá proveer los servicios de: Firewall, VPN y Prevención de Amenazas • Ser una solución en hardware (dispositivo o "*appliance*"). • Contar con la Consola de Administración Centralizada • Desempeño de firewall con control de aplicaciones: al menos 18 Gbps • Desempeño de Prevención de Amenazas (IPS , Antivirus, Antispyware, Protección de Malware día cero habilitados simultáneamente): al menos 8 Gbps • Desempeño de VPN: al menos 3 Gbps • Sesiones soportadas al menos : al menos 4,000,000 • Túneles IPSec VPN Soportados: al menos 1,000 • Ruteadores virtuales soportados: al menos 10 • Zonas de seguridad soportadas: al menos 500 • Puertos de Red: al menos 4 x 100/1000/10000, 4 x 1 GbE en Cobre y 1 x 10 GbE en SFP+ en SR. • Capacidad de VPN client to site para al menos 600 usuarios móviles con soporte de Windows 10, Windows 8, MacOS 10 en adelante, Android 5.0 en adelante y IOS 10.0 en adelante. • Capacidad de generar al menos 1,000 VPN Site to Site. • Interfaz de administración fuera de línea adicionales a las solicitadas a la inspección. • Al menos dos interfaces predefinidas para la funcionalidad de alta disponibilidad adicionales a las solicitadas a la inspección. • La solución deberá contar con certificación ICSA Labs y Nist USG v6 tipo NPD para modulo Firewall e IPS.

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

COMPONENTE	DESCRIPCIÓN
	• Deberá incluir, sin costo ni hardware adicional, tecnología que permita descifrar el tráfico SSL y SSH. Deberá permitir lo siguiente: Bloqueo de sesiones SSL con certificados expirados, Bloqueo de sesiones SSL con certificados no confiables, y Bloqueo de sesiones SSL y SSH para mecanismos de cifrado no soportados. • Deberá incluir la capacidad de limitar la transferencia de archivos no autorizados. • Deberá permitir el control de trasferencia de archivos por aplicación, identificando más de 30 tipos de archivos (DLL, ZIP, EXE, etc.) • Deberá incluir sin costo y en el mismo equipo tecnología de identificación de malware moderno contando con la detección de comportamientos maliciosos, detección de tácticas de evasión y aprendizaje de máquina (machine learning). • Deberá incluir la capacidad de análisis malware día cero de archivos ejecutando archivos desconocidos en un SandBox virtualizado. • Deberá incluir la inspección de malware en día cero para documentos del tipo: Ejecutables (EXE), DLL, Office (Word, Excel, Powerpoint) , VBS, Linux ELF, Powershell script, RAR, BAT, 7-zip, PDF, APK, JAR (Java), MacOS y Adobe Flash. • Deberá incluir mecanismos para establecer redes privadas virtuales (VPN) IPsec Site to Site con las siguientes características: Cifrado 3DES, AES 128, 192 y 256 bits, Autenticación MD5, SHA1, SHA256, SHA384, SHA512. • El firewall deberá tener la capacidad de operar en los siguientes modos de manera simultánea mediante el uso de sus interfaces físicas modo sniffer (monitoreo y análisis del tráfico de la red), capa 2 (L2) y Capa 3 (L3): Modo sniffer: Para inspección vía un puerto espejo del tráfico de datos de la red, Modo Capa-2 (L2): Para inspección de datos en línea y tener visibilidad y control del tráfico a nivel aplicación, Modo Capa-3 (L3): Para inspección de datos en línea y tener visibilidad y control del tráfico a nivel aplicación. • Con capacidad de generar ruteo virtual para al menos 10 ruteadores virtuales y manejo de tráfico entre diferentes zonas de seguridad y sub-redes, soportando al menos 500 zonas de seguridad. • Deberá contar con soporte para los siguientes servicios: Soporte de al menos 4,000 redes virtuales VLANs 802.1q, Traducción de direcciones de red (NAT) por fuente y destino, por direcciones IP dinámicas y pool de puertos, Traducción de direcciones IPv6 NAT64, Al menos 20,000 direcciones en tabla de ruteo en IPv4 • Al menos 20,000 direcciones en tabla de ruteo en IPv6, PPPoE, Enrutamiento BGP, OSPFv3 y RIP2, Soporte de enrutamiento con base en políticas, Soporte de enrutamiento multicast PIM-SM o PIM-SSM, IGMP v1, v2, v3, BFD (Bidirectional Forwarding Detection), DHCP server y DHCP Relay. • Deberá incluir fuentes de poder redundantes. • En caso de aplicaciones desconocidas, deberá contar con un editor de firmas. • Deberá incluir control de tráfico IPv4 e IPv6, este último también incluye visibilidad e inspección de amenazas en aplicaciones y control de contenido IPv6, debe ser soportado en interfaces trabajando en Capa 2 (L2) y Capa 3 (L3). • Deberá soportar SLAAC en interfaces de IPv6.

COMPONENTE	DESCRIPCIÓN
	• Deberá soportar alta disponibilidad en esquemas activo-activo y activo-pasivo. • Activar alta disponibilidad con base en el estado de interfaz o Monitoreo de conectividad para activar alta disponibilidad. • Deberá soportar geo localización para la creación de políticas con base en la región/país o zona geográfica. • Deberá incluir características para la definición de criterios y complejidad mínima para contraseña y soportar al menos los siguientes criterios: Longitud mínima de contraseña, Número mínimo de mayúsculas, Número mínimo de minúsculas, Número mínimo de caracteres numéricos, Número mínimo de caracteres no alfanuméricos, Prevenir el uso de contraseñas previas, Prevenir el uso de nombre de usuario como contraseña, Advertencia de expiración de contraseña, Forzar el cambio de contraseña en un periodo específico. • Capacidad para crear listas dinámicas a partir del registro de algún evento en el log de seguridad, obteniendo leer de forma dinámica el origen y/o destino IP para asociarlo a una etiqueta dinámica, por ejemplo, a partir del registro de un evento tipo malware asociará a la dirección IP víctima de forma automática a una etiqueta dinámica de direcciones IPs, donde se asociarán a una política restrictiva de seguridad para impedir conexiones subsecuentes a dicho evento. • Soporte a la creación de políticas de autenticación cuando el destino sea de altamente restringido sin la necesidad de instalar algún cliente en el endpoint, es decir de forma transparente, solicitará automáticamente al usuario final autenticación tipo Multifactor (MFA), evitando el acceso a servidores únicamente por usuario y contraseña. Este módulo deberá ser compatible al menos con PingID, Duo y Okta. Se requiere que cumpla con las siguientes funcionalidades y características para la administración del equipo y reporteo: • La administración de políticas y objetos deberá realizarse a través de interface gráfica embebida en el equipo Firewall basada en Web y Administración del equipo a través de CLI (ssh y puerto consola) y adicionalmente va una consola de administración centralizada basada en un appliance con capacidad de almacenamiento de al menos 6 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, y categoría y subcategoría de aplicaciones utilizadas. • Envío de reportes por correo de manera automática.

COMPONENTE	DESCRIPCIÓN
	• 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. Deberá incluir las siguientes funcionalidades y características para la Prevención de Amenazas: • El equipamiento deberá tener un rendimiento mínimo de 8 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.

COMPONENTE	DESCRIPCIÓN
	• 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.) • La actualización de firmas de ataques deberá poder realizarse de manera diaria y semanal. • Los dispositivos deberán tener los siguientes mecanismos y 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, re ensamble 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 soportar 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. • La solución deberá contar con un modulo de protección a ataques DNS del tipo DGA, DNS tunneling y machine learning, basado en nube consiguiendo tener predictibilidad de posible nuevos ataques. • Deberá contar con la funcionalidad de DNS Sinkhole para la re-escritura de resoluciones de nombres maliciosas. Se requiere que incluya las siguientes funcionalidades y características para el Filtrado de Contenido: • Deberá poder ofrecer la opción de usar ya sea una base de datos de URLs de terceros o la desarrollada por el fabricante.

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

COMPONENTE	DESCRIPCIÓN
	• 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 via IPSec en dado caso que no sea posible se auto-conectará vía SSL. • La solución deberá contar al menos con 1,000 túneles simultáneos sitio a sito y al menos 600 túneles cliente a sitio soportando Windows, MacOS, Google ChromeOS, Android y IOS. • La solución de VPNs cliente a sitio deberá contar 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.
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 contar con un Sistema de Mesa de Servicios fuera de las instalaciones de la convocante y que sea la que utilice para la administración del servicio y la atención de reportes de falla. • El licitante deberá contar con una herramienta de gestión de incidentes alineada a las mejores prácticas de ITIL V3. La herramienta deberá contemplar con al menos 5 procesos certificados a través de Pink Verify. Lo anterior deberá poder

COMPONENTE	DESCRIPCIÓN
	validarse a través del sitio: https://www.pinkelephant.com/en-US/PinkVERIFY/PinkVERIFYToolsets • El licitante deberá contar con personal especializado en la administración, gestión y soporte en herramientas de gestión de incidentes. • El licitante deberá contar con el conocimiento en mejores prácticas como ITIL.
Certificaciones	El licitante deberá contar con la certificación debidamente acreditada y vigente de la norma ISO 9001:2015 NMX-CC-9001-IMNC-2015 para Sistemas de Gestión de la Calidad con alcance de certificación aplicable a Servicios de Soporte y Atención a Clientes de Redes, Telecomunicaciones, Telefonía, Enlaces y Videoconferencia, Mesa de Ayuda, Ingeniería de Sistemas y de Operaciones de Seguridad (SOC), Centros de Datos y Continuidad de Negocio, avalada por organismos oficiales acreditados para ello. El licitante deberá contar con la certificación PINK Verify para la herramienta del Servicio de Mesa de Ayuda, que acredite mediante el certificado correspondiente. El licitante deberá contar con la certificación debidamente acreditada y vigente de la norma NMX-R-025-SCFI-2015 para cumplir con la Igualdad Laboral y No Discriminación, avalada por organismos oficiales acreditados para ello. Todos los certificados relacionados con el personal podrán ser presentados en copia simple y deberán señalar el mecanismo para su validación en línea. En caso de que el portal de validación requiera usuario y contraseña éstos deberán ser proporcionados como parte de su propuesta técnica. El licitante deberá acreditar mediante constancia de movimientos afiliatorios que cuenta con personal propio, con antigüedad de al menos 6 (seis) meses previos a la fecha de publicación de la licitación pública, y que tengan los siguientes perfiles y certificaciones: Al menos 8 ingenieros certificados por el fabricante de la solución de seguridad y la herramienta del Servicio de Mesa de Ayuda con su correspondiente acreditación que certifique que estan debidamente capacitados en dichas plataformas. Al menos 1 ingeniero con la certificación máxima que otorgue el fabricante de la solución, con su correspondiente acreditación. Líder de gestión de incidentes de seguridad y análisis forense digital quien será el encargado de la gestión situacional y del análisis de causa raíz de los incidentes mayores de seguridad. Deberá acreditar al menos 3 años de experiencia en posición similar, y deberá acreditar que cuenta con las siguientes certificaciones: GIAC Certified Forensic Examiner, CMO Ceftified Mobilize Operator, Certified Hacking Forensic Investigator. Líder de gestión de servicios de seguridad quien será el encargado de la gestión del servicio y el punto de contacto para escalaciones relacionadas con los servicios.

COMPONENTE	DESCRIPCIÓN
	Deberá acreditar al menos 5 años de experiencia en posición similar, y deberá acreditar que cuenta con las siguientes certificaciones: ISO 20000, ISO 27001, Al menos 4 niveles intermedios de ITIL. Líder de auditoría de seguridad quien será el encargado de implementar y supervisar controles de seguridad relacionados con la operación de los servicios. Deberá acreditar al menos 3 años de experiencia en posición similar, y deberá acreditar que cuenta con las siguientes certificaciones: ISO 20000, ISO 27001, SCRUM Master. Líder de operaciones de seguridad quien será el encargado de coordinar las actividades relacionadas con el servicio, incluyendo el sistema de gestión de seguridad de la información. Deberá acreditar al menos 5 años de experiencia en posición similar, y deberá acreditar que cuenta con las siguientes certificaciones: ISO 20000, ISO 27001, Certificaciones en al menos herramienta de seguridad DNS, ITIL Foundations. Líder de transición de servicio quien será el encargado de coordinar las actividades relacionadas con la implementación de los componentes del servicio, incluyendo su liberación a producción. Deberá acreditar mediante la fecha de expedición de su certificado al menos 3 años de experiencia como profesional de la administración de proyectos (PMP), y deberá acreditar que cuenta con las siguientes certificaciones: PMP (Emitido por el Project Management Institute - PMI), ITIL Foundations in IT Service Management, Certificación Nivel Experto emitida por el fabricante de la solución de gestión de la mesa de ayuda (ITSM).
Cartas	El licitante deberá presentar carta de Distribuidor Autorizado por el fabricante de la marca de la solución propuesta, la cual deberá ser en papelería membretada del fabricante, contener la firma autógrafa del representante legal del fabricante, hacer referencia al número de licitación pública, mencionar que el licitante es distribuidor autorizado de la marca, y contener los datos del emisor, tales como nombre, correo electrónico y teléfono, para validación de la emisión de la carta. El licitante deberá presentar carta de Personal Capacitado y Especializado por el fabricante de la marca de la solución propuesta, la cual deberá ser en papelería membretada del fabricante, contener la firma autógrafa del representante legal del fabricante, hacer referencia al número de licitación pública, mencionar en forma explícita que el licitante cuenta con personal capacitado y especializado para la instalación, configuración y operación de los bienes y las soluciones ofertadas, requeridas en el presente procedimiento, y contener los datos del emisor, tales como nombre, correo electrónico y teléfono, para validación de la emisión de la carta. El licitante deberá presentar carta de que el equipo ofertado para la solución, no se encuentra con anuncio de fin de venta, la cual deberá ser en papelería membretada del fabricante, contener la firma autógrafa del representante legal del fabricante, hacer referencia al número de licitación pública, mencionar en forma explícita que el fabricante manifiesta que el equipamiento ofertado para la solución, no se encuentra

COMPONENTE	DESCRIPCIÓN
	con anuncio de fin de venta, y contener los datos del emisor, tales como nombre, correo electrónico y teléfono, para validación de la emisión de la carta. El licitante deberá entregar una carta 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
Experiencia del licitante	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 5 contratos debidamente firmados, ya sea con el sector público o iniciativa privada. En caso de que los contratos sean con la iniciativa privada, éstos deberán contar con autorización expresa de divulgación por parte del cliente. Deberá presentarse por cada contrato, al menos un CFDI (Comprobante Fiscal Digital) de algún pago de los servicios.
Garantía de la solución	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	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 propuesta bajo el siguiente esquema: • La transferencia de conocimientos se impartirá después de que se hayan concluido las pruebas de verificación de funcionalidad. • La transferencia de conocimientos será impartida dentro de las instalaciones del usuario o bien, en el lugar que éste designe. • Se determinará de común acuerdo con el usuario el programa para la capacitación corresponiente. • Se elaborará un acta de cierre de la transferencia de conocimientos, la cual será validada y aceptada por el personal designado por el usuario. • Como parte de la transferencia de conocimientos, el licitante entregará a quien designe el usuario, la memoria técnica de la instalación, configuración y operación de la solución implementada.
Entregables	El proveedor ganador deberá entregar un documento, tanto en versión impresa como en electrónica, que contenga la descripción de cada una de las etapas del Plan de Trabajo rector del proceso de migración a la nueva plataforma de servicios administrados. Dicho documento deberá contener al menos los siguientes apartados: Planeación, Diseño, Implementación, Verificación, validación y pruebas, Puesta en Marcha.

COMPONENTE	DESCRIPCIÓN
	El proveedor ganador deberá entregar un documento, tanto en versión impresa como en electrónica, que contenga previo acuerdo con el usuario, en donde se detalle los procedimientos a seguir para establecer el programa de ventanas de mantenimiento, y procurando la interrupción del servicio. El proveedor ganador deberá entregar la documentación, tanto en versión impresa como en electrónica, correspondiente a las memorias técnicas de todos y cada uno de los detalles de la solución implementada, que sirva como referencia para posibles ajustes y/o actualizaciones. El proveedor ganador deberá entregar una carta en papelería membretada, en la que se especifique que todos los Entregables fueron entregados a entera satisfacción del Gobierno del Estado de Nuevo León, firmada de conformidad por el usuario funcional del Gobierno del Estado de Nuevo León. Informe mensual impreso y en versión electrónica acerca del servicio de seguridad perimetral y asistencia técnica proporcionado en forma mensual.
Tiempo de entrega	8 semanas, a partir de la fecha del contrato.
Forma de pago	40% de anticipo y resto en pagos mensuales contra entrega de la factura correspondiente, a entera satisfacción del Gobierno del Estado de Nuevo León.