Ficha Técnica

SERVICIOS ESPECIALIZADO PARA IMPLEMENTACIÓN END POINT PROTECTION CON EDR Y ATENCIÓN A INCIDENTES INCLUIDA PROVISTA POR EL FABRICANTE, PARA PROTECCIÓN DE USUARIOS FINALES

"Las características descritas en la presente ficha técnica son mínimas mas no limitativas"

Información General de la Contratación

Secretaría	SECRETARÍA DE ADMINISTRACIÓN
Unidad Administrativa / Dependencia solicitante:	DIRECCIÓN DE INFRAESTRUCTURA TECNOLÓGICA
Fecha de elaboración	2025-05-06
Justificación de la contratación	Servicio especializado de consultoría para implementación y administración de la solución de detección avanzada de malware, investigación proactiva y respuesta automatizada para 5,500 endpoint suministrado al Gobierno del Estado de Nuevo León, así como el soporte proporcionado en sus diferentes plataformas de inteligencia de seguridad y protección por el fabricante a traves de sus canales.
Descripción detallada de la contratación	Solución: Se deberá contar con las siguientes características: Servicio Especializado de Consultoría para la Plataforma integrada de protección administrada y automatizada para 5,500 End Point Protection hasta el 31 de Diciembre del 2027 • Capacidad de administración en una plataforma de detección y repuesta “on -premises” y/o en la nube. • Administración de agentes en equipos terminales (endpoints) a partir de una consola central para consolidar y sea fácil de administrar e implementar. • Capacidad de integrar instancias adicionales, de manera amigable y controlado, dejando evidencia de cada paso (Logs) exitoso y no exitoso. • Protección contra ataques y amenazas generalizadas, emergentes, ataques sin archivos, análisis de comportamiento basado en Machine Learning protección contra exploits, igualmente deberá tener protección contra ransomware y spyware avanzado, protección proactiva previo a la ejecución mediante “control adaptativo de anomalías” basado en análisis del comportamiento de los usuarios. • Que incluya prevención y responda a las amenazas utilizando Inteligencia Artificial. • Integración con sistemas de correlación de eventos SIEM, de cualquier tecnología • Administración de niveles de acceso a los sistemas de seguridad basado en roles y funciones RBAC. • Administración de cifrado en discos presente en dispositivos externos, en caso necesario borrado de datos, en caso de pérdida por robo o extravío de dispositivos protegidos con la solución. • Realizar automatización de tareas de rutina, tales como administración de vulnerabilidades, parches, sistema operativo e instalación de software de terceros a través de la plataforma. • Administración y supervisión de políticas de seguridad, así como de las configuraciones, generando alertas a los administradores de potenciales implicaciones a la protección del GENL. • Deberá incluir funciones de Detección y Respuesta para facilitar el análisis de causa-raíz de los hallazgos de seguridad o vulnerabilidad a nivel detección y respuesta (EDR), como resultado se deberá generar reportes informativos de los incidentes detallados, incluyendo mas no limitado a: archivos afectados, claves de registro, conexiones asociadas, inyecciones de vulnerabilidades, entre otros, igualmente deberá incluir forma de acceder a procesos de investigación y contención ante los incidentes detectados. • Administración y generación de indicadores de compromiso (IoCs) que indiquen los resultados de los escaneos a los dispositivos de la organización que cuenten con un agente instalado de la solución, como parte de la búsqueda proactiva de amenazas. Deberá contar con la capacidad de integrarse o de integrar con IoCs de terceros en formatos open IOC. • Capacidad de respuesta y aislamiento con un solo clic para prevenir la ejecución de archivos en dispositivos de usuario, aislar los dispositivos infectados y realizar borrado de archivos de riesgo o amenazas.

	• Facilidad de Consulta amigable / configurable de “Dashboard” para toma de decisiones, según corresponda • Herramienta para poder generar simulaciones de ataques vía mail “Gamefication” y poder en su caso ubicar las áreas de oportunidad de incrementar campañas de concientización a empleados detectados con riesgo de posibilidad de infecciones internas. Implementación: Instalación, configuración y puesta en marcha de la consola de administración, y un máximo de hasta 50 endpoint, la restante instalación de los endpoint será a cargo del personal de la Dirección de Infraestructura Tecnológica.

Entregables

Entregables dentro del sobre técnico

- Curriculum de la Empresa

- Documento que avale que el proveedor participante guarda relación directa con el fabricante.

- Propuesta Técnica-Comercial de la oferta, así como la documentación legal.

Entregables durante el desarrollo de la contratación

Facturas de las licencias relacionada con la adquisición materia de este requerimiento con los primeros 12 meses de Julio del 2025 a Julio del 2026 y los segundos 12 Meses de Julio del 2026 a Julio del 2027 y una tercer factura de julio del 2027 al 31 de diciembre del 2027.

Tiempos y lugares

Vigencia
Del 07 de julio de 2025 hasta el 31 de diciembre de 2027.

Tiempo de Entrega
A partir del fallo hasta el 07 de julio de 2025.

Lugar de entrega

Dirección de Infraestructura Tecnológica de la Subsecretaria de Tecnologías, Washington 2000, piso 18, Torre Administrativa, Col. Obrera, CP 64010 en Monterrey, Nuevo León.

Personal y garantías

Perfil del proveedor

Experiencia en la comercialización e implementación de soluciones End Point Protection para entidades gubernamentales o grandes organizaciones.

Capacidad técnica y operativa para brindar soporte y asistencia técnica especializada durante la implementación y post-venta.

Cumplimiento normativo con los requerimientos legales y administrativos aplicables a la contratación con el sector público.

Responsable de entrega-recepción

Victor Arturo Sevilla Garboza- Procesos y Proyectos

Garantías del producto o servicio

• Garantías del servicio hasta el 31 de diciembre del 2027

• Soporte técnico especializado 5x8NBD por parte del fabricante y/o proveedor, con tiempo de atención de máximo 3 horas.

Pagos y penalidades

Forma de pago

Dentro de los 30 días hábiles posteriores a la visualización total de las licencias, previa entrega de la factura correspondiente, a entera satisfacción del usuario.

Penalidades

Pena convencional al licitante ganador en caso de retraso en el cumplimiento de la entrega de los servicios objeto del contrato del 0.1% diario del valor de lo no entregado, por cada día de retraso a la fecha indicada como plazo máximo para llevar a cabo la entrega del bien o servicio.

Adicionales

Notas adicionales

Las características técnicas son las deseables y mínimas, más no limitativas

_____

Nombre y Firma del Representante Legal.