



ANEXO No. 1
FICHA TÉCNICA DE LOS BIENES Y SERVICIOS A ADQUIRIR

OBJETO: ADQUISICIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE PLATAFORMAS DE CIBERSEGURIDAD QUE PERMITAN CORRELACIONAR SOLUCIÓN PROTECCIÓN DE ENDPOINT Y SERVIDORES CON EDR Y XDR Y PROTECCIÓN DE CORREO PARA LA ALCALDÍA DE TOCANCIPÁ.

ÍTEM	BIEN	CODIGO UNSPSC	UNIDAD MEDIDA	DESCRIPCION DEL BIEN	CANT
1	Software de seguridad y protección	43233200	UNIDAD	Solución integral y unificada anti-malware de seguridad para endpoints, que combine múltiples capacidades de protección en un solo agente y consola de administración, la solución debe tener una consola para definir políticas de seguridad para la prevención de amenazas, control de acceso y cumplimiento, protección de datos, despliegue y actualizaciones de agentes del Endpoint. La solución debe incluir una Gestión Basada en nube en modalidad SaaS que permite gestionar equipos, con su debido licenciamiento, puesta en funcionamiento, soporte de fábrica y garantía. La solución requerida debe proveer como mínimo: • Gestión Basada en la Nube (SaaS) sin requerir infraestructura de gestión local. • Consola de Administración Única, para administrar todas las capacidades de protección (anti-malware, control de acceso, DLP, etc.), políticas, informes y despliegue de agentes. • Agente Único (Single Agent), ejecutarse en el endpoint mediante un único agente liviano que integre todas las funcionalidades de seguridad requeridas. • Soporte Multiplataforma, soportar como mínimo los siguientes sistemas operativos empresariales: Windows (Escritorio/Servidor), macOS y Linux • Despliegue y Actualizaciones Centralizadas • Alta Disponibilidad y Escalabilidad • Prevención de Ejecución de Malware, Capacidad de detección y bloqueo de amenazas conocidas • Detección sin Firma (Heurística/Comportamental), análisis heurístico, inteligencia artificial o machine learning para detectar y bloquear malware de día cero y amenazas polimórficas • Protección Específica contra Ransomware. • Análisis de Comportamiento del Sistema (Endpoint Detection and Response - EDR), recolección de telemetría de endpoints y la visibilidad de la cadena de eventos del ataque. • Análisis y Control de Aplicaciones, Capacidad para identificar y bloquear la ejecución de aplicaciones no autorizadas o potencialmente no deseadas • Control de Dispositivos Periféricos (USB/Removibles) • Firewall de Host Bidireccional, módulo de firewall capaz de definir políticas de tráfico entrante y saliente. • Control de Contenido Web y Filtrado de URL, aplicar políticas de filtrado de contenido por categorías para mejorar la productividad y seguridad. • Prevención de Pérdida de Datos (Data Loss Prevention - DLP) Básico, monitorear y bloquear la transferencia de datos sensibles. • Soporte Técnico de Fábrica 24/7	500
2	Software de seguridad y protección	43233200	UNIDAD	Solución integral y unificada anti-malware de seguridad para endpoints, que combine múltiples capacidades de protección en un solo agente y consola de administración, la solución debe tener una consola para definir políticas de seguridad para la prevención de amenazas, control de acceso y cumplimiento, protección de datos, despliegue y actualizaciones de agentes desde los servidores, La solución debe incluir una Gestión Basada en nube en	10



				modalidad SaaS que permite gestionar equipos, con su debido licenciamiento, puesta en funcionamiento, soporte de fábrica y garantía. La solución requerida debe proveer como mínimo: • Soporte Extendido para SO de Servidor, garantizar soporte total (funcionalidad completa de prevención, EDR y XDR) • Visibilidad EDR en Tiempo Real, donde el sistema debe recolectar telemetría crítica de bajo nivel: actividad de red saliente/entrante • Correlación XDR y Movimiento Lateral, correlacionar eventos de seguridad entre el servidor y otros endpoints • Capacidad de establecer políticas de Whitelisting (lista blanca) que permitan la ejecución solo de aplicaciones y servicios previamente aprobados. • Control de Acceso y Puertos de Red permitir la definición de políticas de red basadas en el rol del servidor • Firewall de Host Bidireccional, módulo de firewall capaz de definir políticas de tráfico entrante y saliente. • Control de Contenido Web y Filtrado de URL, aplicar políticas de filtrado de contenido por categorías para mejorar la productividad y seguridad. • Prevención de Pérdida de Datos (Data Loss Prevention - DLP) Básico, monitorear y bloquear la transferencia de datos sensibles. • Soporte Técnico de Fábrica 24/7	
3	Software de seguridad y protección	43233200	UNIDAD	Protección de correo electrónico que combine capacidades de filtrado multicapa con tecnologías de inteligencia artificial para detectar y bloquear amenazas avanzadas como phishing, ransomware y ataques BEC con sandboxing integrado para análisis dinámico de archivos adjuntos y URLs, junto con cifrado automático para emails sensibles y políticas de DLP . Debe ofrecer integración con plataformas de colaboración en la nube (Microsoft 365) sin requerir agentes adicionales, y contar con una consola de gestión centralizada y reporting detallado para cumplimiento normativo. La consola de administración debe ser Saas y contener las siguientes especificaciones: ●La solución debe tener Protección contra phishing por suplantación de identidad con procesamiento de lenguaje natural ●Manejo de protocolos SPF,DKIM y DMARC ●La solución debe realizar Análisis de reputación ●La solución brinda Protección de antispam, escaneo de malware y sandbox cloud ●Debe poder realizar Detección de URL maliciosas y Reescritura de URL en el momento del clic además de brindar Detección de anomalías del encabezado ●Debe permitir Filtrar por país de origen e idiomas ●Análisis de nombres para mostrar (VIP y marcas) ●Debe contar con Verificaciones de dominios similares ●Políticas DLP de múltiples reglas para grupos y usuarios individuales ●Debe contar con Listas de control de contenido (financieros, contenidos confidenciales, información de salud y PII) ●Cifrado TLS aplicado ●Estándar S/MIME ●Autenticación del remitente ●Cifrado de mensajes y archivos adjuntos basado en push ●La solución debe ofrecer un control integral sobre el flujo de correo electrónico, asegurando la seguridad en todas las direcciones. También escanear minuciosamente tanto los mensajes entrantes para detectar amenazas como los salientes para prevenir la fuga de datos y el spam. ●La solución debe permitir la implementación de políticas a nivel de dominio, grupo y usuario. ●Se debe ofrecer un control granular sobre el correo sospechoso a través de la cuarentena de administrador y usuario, permitiendo a los administradores revisar y liberar mensajes, mientras que los usuarios pueden gestionar sus propios correos en cuarentena.	400



				• Debe tener Banners de correo electrónico entrante (remite nte confiable, externo, no confiable) • Debe permitir Sincronización de AD o sincronización de Azure AD • Integración mediante API (sin interrupción de flujo de correo, Microsoft nube	
4	Software de seguridad y protección	43233200	UNIDAD	Protección de sistemas operativos desatendidos para equipos servidores con funcionalidades de EDR y XDR: • Soporte Extendido para SO Antiguos, para versiones de sistemas operativos de servidor que hayan alcanzado su Fin de Vida como Windows Server 2008/2012, o versiones específicas de RHEL/CentOS • Protección sin Conexión (Offline Protection) mantener una alta eficacia de detección y prevención incluso si el servidor desatendido pierde temporalmente la conexión con la consola SaaS • Correlación de Endpoints y Servidores capaz de diferenciar y correlacionar automáticamente los eventos de seguridad entre servidores y endpoints de usuario • Detección de Anomalías de Comportamiento (UEBA Ligero) incluyendo algoritmos para establecer una línea base del comportamiento normal de los servidores desatendidos y alertar sobre desviaciones anómalas • Prevención de Pérdida de Datos (Data Loss Prevention - DLP) Básico, monitorear y bloquear la transferencia de datos sensibles. • Soporte Técnico de Fábrica 24/7	1
5	Ingeniería de software o hardware	81111500	UNIDAD	Servicios profesionales de ingeniería para implementación y soporte de las soluciones de protección de endpoints, servidores, email, inventario de activos, gestión de vulnerabilidades y control remoto.	1

El presente Anexo Técnico establece las condiciones técnicas mínimas obligatorias que deberá cumplir el contratista seleccionado para la ejecución del objeto contractual. La verificación de cumplimiento de las especificaciones requeridas se adelantará durante la etapa de evaluación de ofertas y su seguimiento estará a cargo de la supervisión designada por el Municipio de Tocancipá.

Proyectó:
Ing. Waldo Gómez Manrique
Profesional Universitario / SA
Alcaldía Municipal de Tocancipá