FICHA TÉCNICA

OBJETO: RENOVACIÓN DE LICENCIAS DE ANTIVIRUS PARA PREVENIR MALWARE Y ATAQUES CIBERNÉTICOS EN LOS EQUIPOS DE CÓMPUTO LA ALCALDÍA DE MOSQUERA - CUNDINAMARCA

DESCRIPCIÓN GENERAL

ÍTEM	DESCRIPCIÓN DEL BIEN O PRODUCTO	NUMERO DE PARTE	UNIDAD DE MEDIDA	CANTIDAD
1	Central Intercept X Advanced with XDR - 200-499 users - 12 MOS - Renewal - GOV	CIXXDU12AGNCA A	Unidad	400
2	Horas de soporte	N/A	Horas	10

DETALLE	REQUERIMIENTO TÉCNICO MÍNIMO
ESPECIFICACIONES DEL SOFTWARE	● La renovación debe contemplar que la solución ofertada debe ser de categoría: Pro, teniendo en cuenta la estructura de la Alcaldía de Mosquera. ● Término de licenciamiento por un lapso de un (1) año contado a partir de la fecha de activación de cada una de las licencias adquiridas. ● Ante nuevos eventos de amenazas y vulnerabilidades por infección de virus tipo Ransomware que ofrezca una mayor protección, reversión de actividades maliciosas, Phishing, prevención de ataques BadUSB y otros, el fabricante debe ofrecer un mecanismo que permita implementar y tomar las acciones de seguridad, para prevenir una infección, eliminar el virus y eliminar los daños, por el término de vigencia del licenciamiento. ● El software debe generar reporte de los virus detectados y acciones realizadas por el término de vigencia del licenciamiento. ● Entregar durante el tiempo de licenciamiento todas las mejoras del producto de forma gratuita (cambios de versiones, parches, soporte directo de fábrica, etc.). ● Herramienta XDR (Extended Detection and Response) que permita hacer un monitoreo en tiempo real, tomando respuestas automatizadas contra amenazas evasivas y desconocidas. ● Control de aplicaciones, dispositivos y web.
ACTUALIZACIÓN CONSOLA DE ADMINISTRACIÓN	● Consola basada en la nube que no requiera un servidor dedicado y que pueda instalarse en una estación Windows (Todas las versiones vigentes) incluyendo máquinas con pocos recursos. ● Monitoreo de sistemas para protección de equipos contra nuevas amenazas. ● Administración de tareas: monitoreo de actividades de escaneo de malware en tiempo real. ● La generación de tareas automáticas como actualizaciones a horas programadas, instalaciones, escaneos bajo demanda, tareas de contingencia, etc. ● Verificar el estatus de cada nodo, recopilando información como: máquinas fuera de control, escáner de acceso no activo, máquinas desactualizadas, top de máquinas infectadas, consolidación de información y generación de estadísticos en formato HTML. ● Generar búsqueda de máquinas en el árbol administrativo por: definición de firmas, nombre de máquina, máquinas sin protección, dirección IP, grupo o dominio, sistema operativo, última vez que fue vista por la consola, etc. ● Capacidad para ofrecer información de seguridad en tiempo real con gráficos fáciles de leer. ● Búsqueda en tiempo real, clasificación y filtrado por nombre, sistema operativo, dirección IP, FQDN o etiqueta. ● Cada servicio de seguridad tiene su plantilla de política configurable con opciones específicas para activar / desactivar y configurar funcionalidades como el análisis antimalware, las capacidades de la zona de pruebas en la nube, las opciones de aprendizaje automático, la introspección del hipervisor, el cortafuego, el control de acceso a la red, la inclusión en la lista blanca de aplicaciones, la lista negra de aplicaciones y el acceso a la web. control, control de dispositivos, ubicación de dispositivos, aplicación de autenticación y acciones a tomar en caso de malware y dispositivos no compatibles detectados, como bloqueo remoto, desbloqueo, borrado, cifrado SD. ● La consola de administración debe implementar políticas de seguridad en forma centralizada, tales como: El bloqueo de puertos de las estaciones, el bloqueo de carpetas compartidas, la denegación de permisos de escritura, etc. ● La comunicación entre el agente y el servidor de la consola de administración debe ser bidireccional y por eventos; es decir, la comunicación se debe realizar sólo cuando la consola tenga una actualización para entregar, o cuando el equipo tenga una novedad que reportar. ● La consola de administración debe notificar al administrador cuando se implementa una nueva política de prevención de infecciones. ● La consola de administración debe realizar la instalación de los productos en forma remota y centralizada por el término de vigencia del licenciamiento. La consola de administración debe ser la única punta de actualización y se encarga de actualizar a los demás productos.

Acreditación como canal autorizado del fabricante: El proponente deberá acreditar que es un canal autorizado por el fabricante de la solución antivirus, como mínimo en la categoría GOLD PARTNER y/o PLATINUM PARTNER, mediante la presentación del correspondiente certificado de distribución o documento equivalente expedido por el fabricante.

El certificado deberá encontrarse vigente al momento de la presentación de la oferta y contar con una fecha de expedición no mayor a treinta (30) días calendario anteriores a la fecha de presentación de la oferta, es decir, la fecha en la que el proponente radique su propuesta dentro del proceso de contratación.

PERSONAL NECESARIO PARA LA EJECUCIÓN DEL CONTRATO

Ingeniero de Sistemas y/o afines:

El oferente deberá acreditar mediante certificación suscrita por el oferente o representante legal, de que cuenta con un (01) ingeniero de sistemas, telemática, telecomunicaciones, electrónico y/o afines con experiencia profesional relacionada de un (01) año en el cual se haya desempeñado realizando labores sobre la herramienta de la solución de antivirus. El cual responderá personalmente a dictar las capacitaciones y soporte en el manejo de la herramienta. Con el fin de no afectar el funcionamiento del software y realizar de la manera óptima la renovación según las indicaciones de fábrica.

El oferente adjuntará con la propuesta los siguientes documentos:

1. Carta de compromiso, suscrita conjuntamente por el oferente o representante legal y el ingeniero de sistemas y/o afines ofertado, en la cual se comprometen para el acompañamiento en las fechas establecidas por el supervisor del contrato.
2. Hoja de vida con sus respectivos soportes:
    a. Académicos: Diploma de bachiller y de pregrado, Acta de Grado, Tarjeta Profesional, Certificación actualizada de antecedentes profesionales expedida por el COPNIA o por quien haga sus veces.
    b. Certificación(es) de Experiencia profesional relacionada que sea verificable por la Entidad.
    c. **Carta de autorización para la presentación de documentos del personal técnico:** El proponente deberá aportar una carta de autorización suscrita por el personal técnico (Ingeniero) propuestos para la ejecución del contrato, mediante la cual autoricen expresamente al proponente a presentar, ante la Entidad, su hoja de vida, certificaciones académicas, certificaciones de experiencia y demás documentos de soporte requeridos, dentro del presente proceso de contratación. La autorización deberá identificar al profesional, al proponente y al proceso contractual al que se refiere.
3. Certificación de ingeniero en el manejo de la herramienta de antivirus, expedida por el fabricante.

Los anteriores, corresponden a los aspectos mínimos de calidad y cantidad requeridos por el Municipio, sin perjuicio de las normas técnicas y medidas aplicables a este tipo de bienes y servicios, motivo por el cual se entiende que además de los aspectos y características expresamente señaladas, se entiende también incluidas aquellas que hacen parte integral del servicio requerido.

_____

Firma
Nombre:
Representante Legal