FICHA TÉCNICA

Fecha: 27 de mayo de 2024

ÍTEM	1
DENOMINACIÓN DEL BIEN O SERVICIO	Software de Seguridad de Transacciones y de Protección contra virus.
CODIGO UNSPSC	43233205
DENOMINACIÓN TÉCNICA DEL BIEN	Renovación de 382 licencias Kaspersky Endpoint Security EDR Optimum, para estaciones de trabajo y servidores de archivos.
UNIDAD O MEDIDA	UNIDAD
IDENTIFICACIÓN ADICIONAL REQUERIDA	1. Software antivirus con protección proactiva de antivirus, antispyware y un firewall personal, para la detección y eliminación de virus, troyanos, gusanos, Ransomware, adware, spyware, phising, rootkits y otras amenazas informáticas. 2. Solución unificada que incluya antivirus, Anti-malware, Firewall, Protección con asistencia en la nube, Control de aplicaciones, Marcado de aplicaciones en lista blanca, Control web, Control de dispositivos, Protección de servidores de archivos, Mobile Device Management (MDM), Seguridad para terminales móvil, Cifrado, Configuración e implementación de sistemas, Análisis avanzado de vulnerabilidades, Gestión de revisiones, Integración con sistemas siem, reportes gráficos en formato XML, CSV, PDF, Consola de administración web y MMS, gestión de usuarios y asignación de roles predeterminados para cada usuario de Windows o interno de la aplicación, optimizando el uso de los recursos de los equipos informáticos y de la red de datos. 3. La solución debe incluir un componente de prevención de ataques a nivel de USB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo. 4. La solución propuesta debe incluir formación en ciberseguridad dentro de la aplicación. 5. Los módulos propuestos deben ser de entrenamientos en ciberseguridad agnósticos entre los que se encuentren Respuestas a Incidentes, Software Malicioso, Aseguramiento de Directorio Activo y Seguridad para servidores, entre otros. 6. La solución debe incluir un componente de protección frente a amenazas en la red que monitoree el tráfico de red entrante en busca de actividad característica de los ataques de red. 7. La solución debe bloquear el equipo que realiza el ataque y restringir el envío de paquetes de red durante un periodo determinado de al menos una hora. 8. La solución debe permitir activar y administrar la protección contra los siguientes tipos de ataques a la red, mínimamente: Inundación de red (flooding) ataques de tipo "Port scan", Ataques de spoofing de MAC 9. El canal que distribuya las licencias debe tener autorización otorgada por el fabricante en el nivel platino, superior o equivalente. 10. Actualización y Administración Centralizada mediante acceso remoto, permitiendo monitorear el estado de protección de los

	equipos y actualizarlos de forma centralizada y programada con actualizaciones incrementales. 11. Permitir Actualizaciones de software y de firmas y bases de datos de conocimiento diarios, semanales, mensuales, etc., de acuerdo con las políticas de seguridad de la Entidad y del fabricante del software adquirido. 12. El término de garantía de las licencias debe ser mínimo de un (1) año. 13. Soporte 5x8 (cinco (5) días con ocho (8) horas diarias) en sitio o remotamente, vía telefónica o por correo electrónico según sea el caso, durante el tiempo de licencia sin costos adicionales para el Municipio. 14. El proveedor debe contar con membresía platino o superior otorgada por el fabricante, sobre las licencias de antivirus requeridas. 15. Soportar protocolos 1Pv4 e 1Pv6. 16. La herramienta de software debe contar con los mecanismos de seguridad propios que eviten la desinstalación o inactivación por parte del usuario final. 17. El licenciamiento debe ser por un año contado a partir del 29/06/2024, 7:01 p. m. 18. La herramienta debe permitir más de una configuración de idioma para la aplicación, tanto en usuario final como en la consola de administración, como mínimo en idioma Español. 19. El Proveedor debe garantizar que todo el software que ponga a disposición de las Entidad para la prestación del servicio se encuentra debidamente licenciado o suscrito cumpliendo con las políticas de distribución y uso de software del fabricante. 20. El proveedor debe suministrar la última versión del software que se encuentre liberada en el mercado al momento de la entrega
PATRONES MINIMOS DE DESEMPEÑO	1. Compatibilidad Sistemas Operativos: Microsoft Windows Vista, 7, 8, 8.1, 10 o superior (32 y 64 bits), Windows Server (2008 o superior 32 y 64 bits) y fácil de utilizar tanto para los usuarios finales como para el administrador de la red. 2. Consola en arquitectura cliente - servidor. **SOPORTE TÉCNICO** El proveedor deberá estar en la capacidad de prestar soporte remoto para la herramienta por el tiempo de adquisición de la misma, este requisito no ocasionará costo adicional para la Entidad. El proveedor clasificará los incidentes, problemas y solicitudes y les dará resolución de acuerdo con: Prioridad alta: Incidentes - Emergencia - Fallas graves que generen una indisponibilidad critica del negocio de la Entidad Compradora.- Situación que afecta gravemente el uso de la herramienta en los equipos donde se encuentra instalada, como pérdida de datos, caída del sistema, restricciones de acceso a la plataforma, entre otros. Prioridad media: Problemas - Degradación en el servicio que afectan el desempeño o confiabilidad de los procesos de negocio de la Entidad Compradora. -

	Un problema que implica una pérdida parcial no fundamental de la capacidad de uso de la aplicación. - Un problema donde el software funciona, pero su uso en el entorno o funcionalidad se ve gravemente reducido. Prioridad baja: Solicitudes / Consultas - Solicitudes de Soporte menores o de información que no tienen impacto en los procesos de negocio de la Entidad Compradora. - Solicitud de información técnica de los servicios, solicitudes de documentación de servicios, solicitudes de información y aclaraciones acerca del uso y operación de las herramientas. - Solicitudes de asesoramiento para la configuración, implementación y administración de servicios. - Consultas relacionadas con la herramienta suministrada. Los tiempos de respuesta serán: Prioridad alta: 4 horas. Prioridad media: 8 horas. Prioridad baja: 24 horas. El Proveedor debe contar como mínimo con los siguientes canales de atención a requerimientos: Telefónico y Correo electrónico. El Proveedor pondrá a disposición remotamente el personal para prestar el servicio de soporte técnico remoto. El horario para la prestación del servicio requerido es de lunes a viernes de 7 a. m. a 5 p. m. **ENTREGA E INSTALACIÓN** El Proveedor debe realizar la entrega e instalación de la(s) renovaciones en modalidad Remota o en sitio

JOSE TOBÍAS DIAS ALARCON
Secretario TIC

Elaboró: Fredy Ignacio Mendoza Cely
Profesional Universitario