FICHA TÉCNICA

Objeto: RENOVACIÓN DE LICENCIA DE SOFTWARE VICARIUS VRX, PARA LA DETECCIÓN Y REMEDIACIÓN DE VULNERABILIDADES Y AMENAZAS DE CIBERSEGURIDAD DE LA ALCALDÍA DE MOSQUERA

El contratista deberá realizar la prestación de servicio de las actividades, de conformidad con el Ítem 1, al 4 además de cumplir con el perfil mínimo exigido y demás condiciones técnicas, de acuerdo a la descripción del bien o servicio:

Códigos UNSPSC

CLASIFICACIÓN UNSPSC	1 nivel	2 nivel	3 nivel	4 nivel
	SEGMENTO	**FAMILIA**	**CLASE**	**PRODUCTO**
Servicio de licencias del software del computador	81000000	81110000	81112500	81112501
Servicios de implementación de aplicaciones	81000000	81110000	81111500	81111508

Plazo estimado

El plazo de ejecución del presente contrato será de tres (03) meses, contados a partir de la suscripción acta de inicio.

ESPECIFICACIONES DEL BIEN O SERVICIO:

El municipio de Mosquera requiere contratar RENOVACIÓN DE LICENCIA DE SOFTWARE VICARIUS VRX, PARA LA DETECCIÓN Y REMEDIACIÓN DE VULNERABILIDADES Y AMENAZAS DE CIBERSEGURIDAD DE LA ALCALDÍA DE MOSQUERA, en los términos de la invitación a presentar propuesta de conformidad con el alcance del contrato, de la siguiente manera:

ÍTEM	DESCRIPCIÓN	CANTIDAD	UNIDAD
1	Licencia de software para la detección y remediación de vulnerabilidades y amenazas de ciberseguridad por 12 meses para 500 equipos o dispositivos, según especificaciones técnicas.	1	UNIDAD
2	Hora de soporte presencial o virtual	10	HORA
3	Hora de capacitación o transferencia de conocimiento	5	HORA

A través de las necesidades previamente descritas, el proponente deberá garantizar el cumplimiento de los siguientes requisitos:

ESPECIFICACIONES TÉCNICAS DEL SOFTWARE PARA DETECCIÓN Y REMEDIACIÓN DE AMENAZAS Y VULNERABILIDADES

El software requerido, deberá incluir como mínimo las siguientes características:

- Aprovisionado en la nube (cloud) en la modalidad SaaS (Software as a Service).
- Solución integrada para la gestión de vulnerabilidades.
- Visibilidad y cobertura en tiempo real de sistemas operativos, aplicaciones y cambios de configuración.
- Contar con al menos dos (2) métodos de autenticación.
- Soportar varios roles de usuarios.
- Segregar diferentes activos entre diferentes grupos de usuarios con diferentes niveles de permisos.
- Tener la posibilidad de instalar un proxy en la red para aplicar técnicas de patching caching, compatible con sistemas operativos Linux mediante paquetes de DEB o RPM, sin costos adicionales.

- Permitir la actualización de servidores sin interrupciones de servicio.
- Clasificación de los riesgos basada en activos y/o aplicaciones.
- Presentar la clasificación de riesgos y priorización de las vulnerabilidades desde CVE (Common Vulnerabilities and Exposures) y la situación del entorno.
- Análisis predictivo de amenazas de día cero (Zero-Day).
- Protección contra vulnerabilidades del día 0.
- Actualización constante de vulnerabilidades.
- Contar con un motor de acciones recomendadas.
- Permitir la ejecución de scripts de corrección en toda la plataforma.
- Contar con integración con herramientas de terceros para hacer Network Scanning (ejemplo Nmap)
- Contar con agentes instalables en sistemas operativos Windows, Linux y Mac OS.
- Permitir el despliegue de los agentes por línea de comandos.
- Permitir la implementación de los agentes a través de GPO
- Gestión y aplicación de parches en tiempo real, propios del sistema operativo y de terceros.
- Remediación de vulnerabilidades mediante tareas automatizadas
- Capacidad de aplicar configuraciones mediante Scripting y línea de comandos remota.
- Generar informes exportables a CSV y PDF de:
    - Vulnerabilidades encontradas
    - Resumen ejecutivo con información resumida sobre el escaneo.
    - Informe detallado con la información técnica necesaria para reproducir los problemas identificados.
- Permitir integraciones con sistemas de gestión de eventos e información de seguridad (SIEM).

ACUERDO DE NIVEL DE SERVICIO (ANS)

Proveer el soporte necesario que se requiera para las actividades relacionadas con la implementación y óptimo funcionamiento del software, de conformidad con objeto del contrato, según el siguiente acuerdo de nivel de servicio requerido por la entidad:

Descripción	Imputable a las horas de soporte	Tiempo máximo de apropiación	Tiempo máximo de solución
Fallas comunes: Asociadas al funcionamiento normal de la solución. No implican indisponibilidad de los servicios de la entidad	NO	5 HORAS	24 HORAS
Fallas graves: Asociadas al funcionamiento normal de la solución, implica indisponibilidad de los servicios de la entidad.	NO	1 HORA	12 HORAS
Solicitudes de asistencia técnica: Implica la gestión de configuraciones programadas, ventanas de mantenimiento, validaciones, ajustes, actualizaciones y optimizaciones de la solución.	SI	5 HORAS	48 HORAS

PERSONAL NECESARIO PARA LA EJECUCIÓN DEL CONTRATO

Ingeniero de sistemas, telemática, telecomunicaciones, electrónico y/o afines, con especialización en ciberseguridad y/o seguridad informática y/o ISO 27001: El oferente deberá acreditar 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 software para la detención y remediación de vulnerabilidades y amenazas de ciberseguridad. Los cuales responderán personalmente a dictar las capacitaciones y soporte en el manejo de la herramienta.

El oferente adjuntará con la propuesta los siguientes documentos:

1. Carta de compromiso, suscrita por el personal ofertado en la cual se compromete para el acompañamiento en las fechas establecidas por el supervisor del contrato.
2. Hojas de vida del personal necesario, la cual debe llevar los siguientes documentos anexos:
    a. Carta de autorización cada uno de los ingenieros, para la presentación de sus documentos en el actual proceso.
    b. Certificado de antecedentes disciplinarios expedido por el COPNIA o entidad que aplique, según la especialidad del profesional (si aplica).
    c. Certificado de experiencia profesional relacionada, de cada uno de los ingenieros, como mínimo de un (01) año en los cuales se hayan desempeñado como ingenieros realizando labores sobre la herramienta de la solución de seguridad perimetral.
3. Certificación en el uso del software, para cada uno de los ingenieros, expedida por el fabricante.

- **Nota 1:** El proponente debe garantizar que la cantidad de personal que corresponda a la demanda y calidad requerido por la Administración Municipal.

- **Nota 2:** El proponente deberá anexar de todo el equipo de trabajo solicitado, los respectivos soportes de formación académica, certificaciones de experiencia, hoja de vida, copia de la matricula profesional (cuando aplique), certificado de vigencia y antecedentes disciplinarios emitido por el consejo profesional que corresponda al cierre del presente proceso.