

ANEXO TÉCNICO

1. Objeto del Contrato

“RENOVACIÓN DE LA SUSCRIPCIÓN, ACTUALIZACIÓN DEL LICENCIAMIENTO, SOPORTE Y MANTENIMIENTO DEL SISTEMA ANTIVIRUS DE LA ALCALDIA DEL MUNICIPIO DE YUMBO”.

2. Antecedentes

La entidad ha consolidado su infraestructura tecnológica a través de la implementación de diversas soluciones que garantizan la operación segura, eficiente y continua de sus servicios. Entre estas, se encuentra una solución avanzada para la protección de endpoints que en la actualidad permite a la Entidad mitigar riesgos cibernéticos, garantizar la seguridad de los dispositivos terminales y responder a incidentes de manera efectiva. Dado que el licenciamiento actual está próximo a vencerse, es indispensable renovar este servicio para cubrir los 540 dispositivos de la entidad (520 estaciones de trabajo y 20 servidores) y mantener el cumplimiento con estándares internacionales como ISO/IEC 27001 y las guías de MITRE ATT&CK.

3. Justificación Técnica

La renovación del componente tecnológico descrito es fundamental para garantizar la continuidad operativa de la infraestructura tecnológica de la entidad, fortaleciendo la seguridad, eficiencia y confiabilidad de los servicios críticos que soportan sus actividades institucionales. Este proceso abarca la renovación de garantías para la solución de protección de endpoints.

La solución de protección de endpoints es indispensable para preservar la integridad de los datos y la seguridad de los dispositivos utilizados por la entidad. Esta solución proporciona capacidades avanzadas de detección, prevención y respuesta ante incidentes de seguridad, cumpliendo con estándares internacionales como ISO/IEC 27001 y alineándose con las guías de MITRE ATT&CK, lo que asegura un entorno seguro y confiable para los 540 dispositivos cubiertos por la suscripción.

Este proceso de renovación no solo responde a las necesidades operativas de la entidad, sino que también promueve el cumplimiento de las normativas nacionales en tecnología, seguridad y protección de datos, como la Ley 1581 de 2012 (Protección de Datos Personales) y el Decreto 2145 de 2021 (Política Nacional de Ciberseguridad). Al renovar estos componentes, la entidad asegura la continuidad y modernización de su infraestructura tecnológica, alineándose con sus objetivos estratégicos y cumpliendo con los estándares exigidos en el sector público.

4. Renovación de solución de protección de Endpoints

La renovación de la solución de Detección y Respuesta en Endpoints (EDR) es un componente clave para asegurar el cumplimiento de los lineamientos y regulaciones establecidos por la legislación colombiana en materia de protección de datos personales, ciberseguridad y gobierno digital. Su implementación permite a la entidad fortalecer la prevención, detección y respuesta ante incidentes de seguridad, mitigar riesgos cibernéticos y garantizar la protección de la información crítica y los activos digitales. En línea con estas premisas, la renovación del licenciamiento debe cumplir con los siguientes aspectos técnicos:

- **Cumplimiento normativo**

La solución EDR deberá apoyar el cumplimiento de la normativa colombiana vigente en materia de protección de datos personales, ciberseguridad y gobierno digital, incluyendo la Ley 1581 de 2012 y los lineamientos de la Estrategia de Ciberseguridad Nacional, así

como su alineación con buenas prácticas y estándares internacionales en seguridad de la información.

- **Monitoreo y detección avanzada**

La solución deberá contar con capacidades de monitoreo continuo y detección avanzada en tiempo real, que permitan identificar comportamientos anómalos, amenazas cibernéticas e indicadores de compromiso, garantizando una gestión proactiva de los incidentes de seguridad.

- **Prevención y protección proactiva**

La solución deberá integrar mecanismos automáticos de prevención y mitigación de amenazas, orientados a evitar la materialización de riesgos sobre los activos de información y a preservar la disponibilidad y seguridad de los sistemas de la entidad.

- **Respuesta a incidentes**

La solución deberá permitir la respuesta automática y manual ante incidentes de seguridad, facilitando la contención, análisis y remediación de amenazas, sin afectar la continuidad de los servicios institucionales.

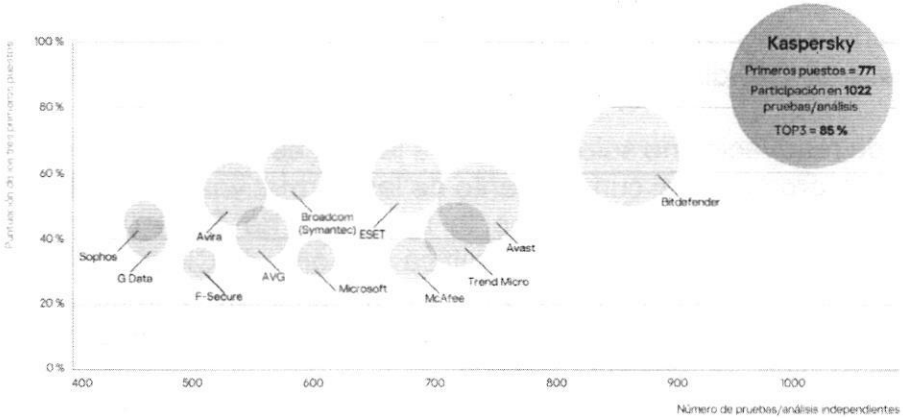
- **Visibilidad y trazabilidad**

La solución deberá proporcionar visibilidad integral de la actividad en los endpoints, así como registros e informes que soporten los procesos de auditoría, control y seguimiento en ciberseguridad.

- **Gestión centralizada**

La solución deberá permitir la administración centralizada de endpoints y servidores, garantizando compatibilidad con la infraestructura tecnológica existente y facilitando la aplicación y supervisión de políticas de seguridad.

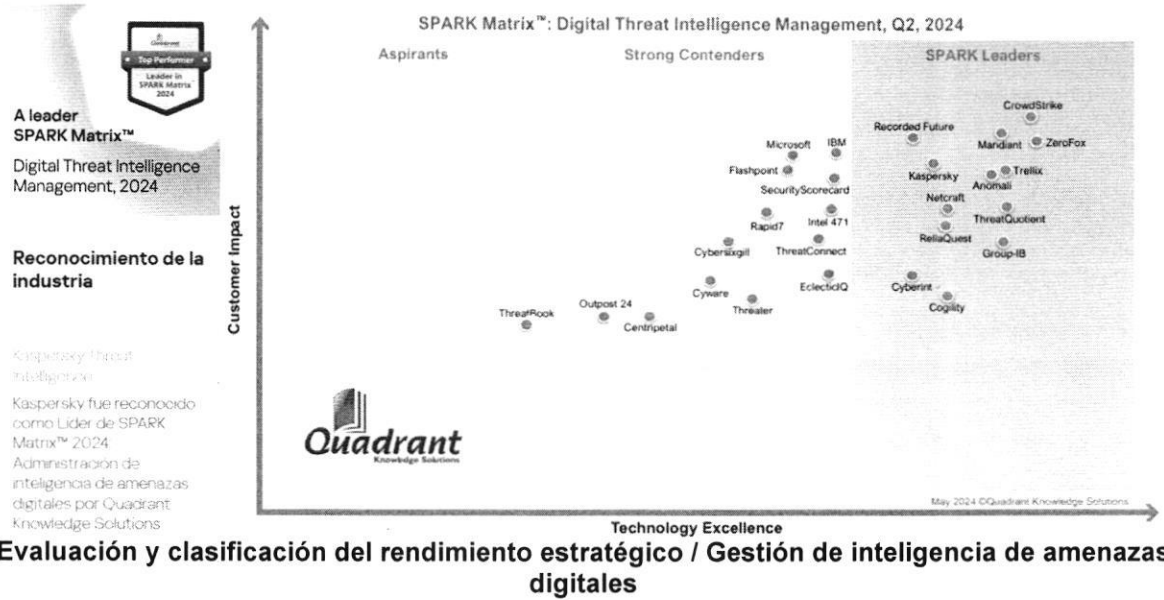
Actualmente la entidad cuenta con una solución del fabricante Karspersky Endpoint Detection And Response Optimum para 540 usuarios (520 Estaciones de trabajo y 20 servidores) sobre la cual vale la pena resaltar en términos de la idoneidad de esta solución de protección endpoint que durante el período de 2013 a 2024, los productos de Kaspersky participaron en 1022 pruebas y análisis independientes. Los productos lograron 771 primeros puestos y quedaron 871 veces entre los tres primeros.



TOP3 2013-2024¹

Adicionalmente, cuenta con reconocimientos como el que se menciona a continuación

¹<https://content.kaspersky-labs.com/fm/site-editor/9f/9f77eb7eda30fb94e680f07fa94833fd/source/top3-2013-2024-20250411es-es.pdf>
<https://content.kaspersky-labs.com/se/media/top3/TOP3-2024-en.pdf>



Los oferentes deberán garantizar que la solución ofertada cumpla con las siguientes especificaciones técnicas mínimas:

Ítem	Especificación Técnica Requerida
1. Licencia / Usuarios	Licenciamiento para un mínimo de 540 usuarios por un periodo de 6 meses. (520 Estaciones de trabajo y 20 servidores)
2. Consola de Gestión	La solución debe contar con una plataforma centralizada basada en la nube o en instalación local que permita la gestión unificada de todos los endpoints desde una sola consola.
3. Servicios profesionales	Actualización de la consola de gestión y agentes de las estaciones de trabajo a su última versión.
5. Soporte	Soporte gestionado 8x5 de la consola de gestión por término de la vigencia de la garantía (6 meses)