CONTRALORÍA
GENERAL DE SANTIAGO DE CALI

01110-

Santiago de Cali, 24 de septiembre de 2025

Doctor
LUKAS STEEVENT GONZÁLEZ PEÑALOZA
Secretario General
Presente

Luis Gonzalez P.
Aprobado

Asunto: Solicitud de renovación y actualización de 350 licencias de antivirus corporativo kaspersky Endpoint Security, soporte y mantenimiento para la Contraloría General de Santiago de Cali.

ANTECEDENTES:

En el año 2016 se realizaron nuevos estudios a fin de evaluar la oferta en el mercado de los antivirus para llevar a cabo una nueva contratación de última tecnología que respondiera a las necesidades de la entidad y se llevó a cabo el proceso de contratación de los servicios del antivirus de marca Kaspersky.

El año 2017 por medio de un proceso de mínima cuantía, se celebró contrato con una empresa con sede en Bogotá que ofrecía los servicios de soporte sobre la misma marca de antivirus, pero se presentaron muchos inconvenientes por temas de distancia de ubicación, demora en prestar el servicio de soporte y dificultades para hacer revisiones “in house” en momentos que no se disponía de internet para conexión remota.

En los años posteriores, los procesos de mínima cuantía realizado para tal fin, ha arrojado como ganadores a empresas caleñas quienes han presentado respuesta rápida y efectiva ante los servicios de soporte requeridos por la entidad.

El software antivirus requiere actualización constante tanto de las bases de datos de los virus como de las mejoras o nuevas versiones del software con el fin de estar protegidos día a día contra los virus y las distintas formas que ellos que surgen, razón por la cual se debía mantener un contrato de actualización y soporte por un año.

JUSTIFICACIÓN:

El objetivo del proceso informático es orientar y apoyar en la adquisición, actualización y uso de las tecnologías de información y comunicación (TIC) que soportan los procesos en la Contraloría General de Santiago de Cali, encaminados a lograr la continuidad de los servicios informáticos y de telecomunicaciones así como la disponibilidad y accesibilidad mediante su implementación, administración, mantenimiento y control, apuntando al cumplimiento del Eje Estratégico 4: fortalecimiento e innovación

institucional en su objetivo 4.17 Aplicar las mejores prácticas de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios en la entidad, y la política de gobierno digital como eje trasversal que permite mayor eficiencia a nivel interno y externo.

La Contraloría General de Santiago de Cali, en su mapa de riesgos, ha identificado los riesgos de Perder la integridad y disponibilidad en las Bases de datos de producción y Eliminar y/o Alterar la información registrada en la red corporativa y/o los sistemas de información por parte de un servidor público en beneficio propio o de un tercero, con posibilidad de afectación Económica y Reputacional por actos deliberados de forma intencional por parte de los usuarios debido a Instalación y Ejecución de Software Dañino, que de materializarse podría ocasionar interrupción o trauma en el ejercicio del control fiscal y sanciones, que tendrían un impacto catastrófico para la Entidad.

Con el fin de prevenir la materialización de riesgos de seguridad digital ya mencionados y mantener la operación y continuidad de los servicios informáticos y de telecomunicaciones, así como la disponibilidad y accesibilidad de la información, se hace necesario renovar y actualizar 350 licencias del software ANTIVIRUS KASPERSKY NEXT ENDPOINT DETECTION AND RESPONSE OPTIMUM a KASPERSKY NEXT XDR OPTIMUM 19092025 por un año y contratar el servicio de soporte y asistencia técnica con una empresa que cuente con oficinas en la ciudad de Cali.

A continuación, se presenta la ficha técnica mínima de los participantes:

DENOMINACIÓN DE BIEN O SERVICIO
Licencias de antivirus, antispyware, anti spam, firewall personal y autenticación de sitios de confianza con actualizaciones por un (1) año

DESCRIPCIÓN		
A	Software antivirus con protección proactiva de antivirus, antispyware, con robusta tecnología anti spam y un firewall personal, para la detección y eliminación de virus, troyanos, gusanos, malware, spyware, Ransomware, phising, rootkits y otras amenazas informáticas.	
B	Solución unificada que incluya antivirus, antispyware, anti spam y firewall, en una única aplicación, optimizando el uso de los recursos de los equipos informáticos y de la Contraloría General de Santiago de Cali	
C	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.	
D	Compatibilidad Sistemas Operativos: 10 o posterior, Windows Server (2008 o posterior) y fácil de utilizar tanto para los usuarios finales como para el administrador de la red.	

E	El término de garantía de las licencias debe ser mínimo de un (1) año, contado a partir de la fecha del acta de instalación y recibo a satisfacción de las licencias.	
F	Soporte 5x8 vía telefónica o e-mail durante el tiempo de licencia sin costos adicionales para la Contraloría General de Santiago de Cali.	
G	Asistencia en sitio 5 x 8 sin costo adicional, cuando el soporte telefónico o vía e-mail no resuelva los problemas presentados.	
H	Protección de sistema operativo, archivos disco duro o diskette, memorias USB, mensajes de alerta para virus, búsqueda automática o programada de virus en los PC. para sistemas operativos en clientes Windows 10 y posterior. Escaneo en acceso y en demanda Protección del sistema Las licencias deben incluir protección para macro virus de las herramientas Microsoft.	
I	Protección para servidores Windows Server programación de tareas por consola. Escaneo en acceso y en demanda.	
J	Protección para servidores ambiente Linux.	
K	Detecta amenazas complejas Aislamiento del host Iniciar un escaneo del host Eliminación de archivos (Eliminación de procesos Impedir que el proceso se ejecute)	
L	Evaluación y Gestión de Vulnerabilidades Inventario y Control de Licencias Distribución Software Implementación Sistema Operativo Integración con SEM Cifrado de Datos Seguridad Móvil Gestión de Dispositivos Móviles (MDM) Gestión de Aplicaciones Móviles (MAM) Seguridad para servidoras Control de aplicaciones Control de dispositivos Control WEB Anti-Malware + Firewall	
M	**Servicios de actualización:** Actualización del servidor de administración Kaspersky Security Center a la nueva versión. Instalación y configuración Servidor de Administración Kaspersky Security Center Cloud Instalación en las estaciones de trabajo físicas del módulo de protección XDR Optimum. Instalación componente de seguridad XDR Optimum en los servidores y estaciones virtuales. Creación en el servidor de administración Kaspersky Security Center de directivas de seguridad integradas con el módulo XDR Optimum.	

	Configuración de respuestas automáticas de amenazas detectadas. Creación de directivas de seguridad integradas con el módulo XDR Optimum en el servidor de administración Kaspersky Security Center. Configuración de respuestas automáticas ante amenazas detectadas. Configuración de tareas de Análisis de indicadores de compromiso (IoC). Con base en amenazas descubiertas Configuración de consola, herramienta de inventario, herramienta de cifrado, tareas de escaneo de acuerdo a lo solicitado y capacitación sobre estas herramientas al personal de soporte de la oficina de informática. Configuración de protección automática de exploits e inteligencia de seguridad en la nube mediante la activación y configuración del KSN. Creación de los paquetes de instalación para los servidores y estaciones virtuales. Instalación de las licencias de los servidores y estaciones de trabajo .Configuración Servidor de administración de servidores y estaciones Creación de directivas, tareas de actualización y análisis en los servidores y estaciones virtuales. Configurar sistema de prevención e intrusiones HIPS, junto con el system watcher y el firewall para asegurar y proteger las actividades de las aplicaciones en la red. Creación de plantilla de control de aplicaciones con listas blancas y dinámicas que permitan permitir y bloquear la ejecución de las aplicaciones en ambientes controlados. Configuración de reglas de control de acceso de dispositivos de forma granular de conexión de los dispositivos de almacenamiento extraíbles al igual que los periféricos, definiendo derechos de usuario para las operaciones de lectura y escritura. Configuración de aplicación de parches de seguridad y actualización de vulnerabilidades desde la consola de administración. Creación de paquetes de distribución y actualización del sistema operativo. Configuración de las plantillas personalizadas para la generación de informes de hardware, software y administración de licencias.	
N	Ingeniero certificado en soporte técnico kaspersky que apoyen en manejo ,capacitación y administración de consola y agentes de la plataforma KASPERSKY NEXT XDR OPTIMUM. el canal debe ser certificado gold Kaspersky next xdr optimum	
O	Licencias para proteger buzones de Correo electrónico Microsoft 365 mínimo 1.6 por cada licencia. Licencias para proteger dispositivos móviles (Celulares o Tabletas) mínimo 2.0 por cada licencia.	

P	Mínimo 100 solicitudes en el portal de inteligencia de amenazas de kaspersky	
Q	**Formación:** Capacitación al equipo de TI en administración. Formación al equipo a los usuarios par que participe en la cultura de seguridad. capacitación CITO (Cibersecurity for IT Online)	

Servicio de soporte técnico

DESCRIPCIÓN		
A	Soporte 7x24x365	
B	Soporte en sitio cuando se requiera	
C	Mínimo 4 visitas al año de soporte en sitio para revisión y diagnóstico de agentes en clientes y servidores y la consola.	
D	Configuración de consola, servidores, portátiles y PC´S.	
E	Instalación y configuración en consola y agentes de nuevas versiones y mejoras del producto.	
F	Instalación de nuevas versiones y mejoras del software liberadas por el fabricante.	
G	Apoyo técnico al personal de la Oficina de Informática.	
H	Tiempo del servicio 1 año	
I	soporte directo con el Fabricante durante el periodo que se encuentre activa la licencia	

Atentamente,

NELSON ACOSTA NUÑEZ
Jefe Oficina de Informática

LSG/NHR/T:\Informatica\PROYECTOS\2026\Antivirus2026\NecesidadAntivirus2026.docx

	Nombre	Cargo	Firma
Proyectó	Lorena Salgado Gutiérrez	Secretaria	
Revisó	Noralba Hoyos Ruíz	Profesional Universitario	
Aprobó	Nelson Acosta Núñez	Jefe Oficina de Informática	

Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.