|

BOGOTÁ D. C., 26

26/10/2026

ASUNTO: SOLICITUD COTIZACIÓN.

RESPETADOS SEÑORES, RECIBAN UN CORDIAL SALUDO.

La Federación Colombiana de Municipios, como administrador legal del Sistema Integrado de Información sobre Multas y Sanciones por Infracciones de Tránsito – Simit, se encuentra adelantando un estudio de mercado, cuyo objeto es el siguiente:

1. OBJETO.

"Adquirir los códigos de activación de la actualización y soporte antivirus Kaspersky, para la Federación Colombiana de Municipios en cumplimiento de la función pública asignada."

2. DESCRIPCIÓN Y JUSTIFICACIÓN DE LA NECESIDAD

La Federación Colombiana de Municipios, como administrador legal del Sistema Integrado de Información sobre Multas y Sanciones por Infracciones de Tránsito Simit, se encuentra adelantando un estudio de mercado para "Adquirir los códigos de activación de la actualización y soporte antivirus Kaspersky, para la Federación Colombiana de Municipios en cumplimiento de la función pública asignada".

Es necesario para la FEDERACIÓN COLOMBIANA DE MUNICIPIOS la adquisición, para la debida activación, renovación, mantenimiento y soporte de las doscientos cincuenta (250) licencias de KASPERSKY XDR OPTIMUM, incluyendo las actualizaciones de mejoras de la herramienta y mantenimientos correspondientes para brindar el servicio funcional y técnico requerido para la gestión de seguridad y el cumplimiento de la función pública asignada.

3. FORMA DE PAGO:

Un único pago correspondiente al 100%, dentro de los 30 días posteriores a la entrega del licenciamiento, radicación de la factura y aprobación por parte del supervisor.

4. CLASIFICADOR DE BIENES Y SERVICIOS – UNSPSC

El bien o servicio objeto del presente proceso de selección está codificado en el clasificador de Bienes y Servicios UNSPSC, como se indica a continuación:

COD. SEGMENTO	COD. FAMILIA	COD. CLASE	COD. PRODUCTO	DESCRIPCIÓN	OBJETO POR CONTRATAR
43000000	43230000	43233200	43233205	Software de seguridad de transacciones y de protección contra virus	"Adquirir los códigos de activación de la actualización y soporte antivirus Kaspersky, para la Federación Colombiana de Municipios en cumplimiento de la función pública asignada."

81000000	81110000	81111800	81111801	Seguridad de los computadores, redes o internet	"Adquirir los códigos de activación de la actualización y soporte antivirus Kaspersky, para la Federación Colombiana de Municipios en cumplimiento de la función pública asignada."

5. CONDICIONES TÉCNICAS MÍNIMAS

A continuación, se presenta los requerimientos técnicos:

DESCRIPCIÓN	CANTIDAD	PRODUCTO
"Adquirir los códigos de activación de la actualización y soporte antivirus Kaspersky, para la Federación Colombiana de Municipios en cumplimiento de la función pública asignada."	250	KASPERSKY XDR OPTIMUM

A. CONSOLA DE ADMINISTRACIÓN Y PLATAFORMA DE GESTIÓN CONDICIÓN TÉCNICA MÍNIMA

- La solución, el licenciamiento y todos sus componentes suministrados para servidores, estaciones de trabajo y dispositivos móviles deben ser del mismo fabricante. No se aceptarán soluciones compuestas de distintos fabricantes.
- El contratista deberá suministrar una **consola de administración centralizada**, ya sea en modalidad nube o local (on-premise), con todos los módulos que permitan gestión, monitoreo, configuración y respuesta completa de los agentes instalados en los endpoints.
- La consola debe contar con un **dashboard unificado** que muestre métricas, estadísticas, estado de protección de los endpoints, alertas activas clasificadas por criticidad (alta, media, informacional) y eventos de respuesta ante incidentes.
- Debe contar con mecanismo de comunicación vía **API REST** para integración con soluciones externas de seguridad como SIEM, SOAR y plataformas de ticketing.}
- La consola debe permitir la **correlación de alertas** provenientes de múltiples fuentes, consolidando señales débiles en un panorama amplio y significativo para reducir la carga cognitiva del equipo de seguridad y mejorar el Tiempo Medio de Detección (MTTD).
- Debe permitir la sincronización con el **Directorio Activo (Active Directory)** de la entidad, habilitando el bloqueo de usuarios y acciones de respuesta de terceros directamente desde la consola.
- La consola debe permitir la aplicación de políticas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y dispositivos individuales.
- La consola debe soportar el despliegue remoto de agentes y la distribución de actualizaciones de forma centralizada y programada.
- La consola debe gestionar actualizaciones automáticas de definiciones de amenazas, motores de detección y componentes de respuesta, desplegándolas a los agentes bajo tareas programadas.
- Debe permitir exclusiones de análisis por sitio web, archivo, carpeta, proceso o aplicación, tanto a nivel global como por política específica.
- La consola debe soportar la definición de roles administrativos con diferentes niveles de acceso a configuración, políticas y registros de auditoría.
- Debe permitir la programación de análisis y escaneos sobre máquinas individuales o grupos, con periodicidad definida por el administrador.
- La comunicación entre la consola y los agentes debe realizarse usando protocolos seguros y cifrados.

- Los mensajes, notificaciones y alertas generados por los agentes deben estar disponibles en idioma español o permitir su configuración.
- La consola debe permitir la generación y exportación de informes gerenciales en formatos CSV y PDF, con posibilidad de envío automático programado a correos electrónicos configurados.
- La consola debe mostrar información de inventario de endpoints: nombre del equipo, sistema operativo, dirección IP, versión del agente, fecha de última actualización, eventos recientes y estado de protección (activo, inactivo, desprotegido).
- Debe incluir un módulo de unificación de alertas que correlacione eventos dispersos en un único caso o incidente enriquecido, permitiendo trazabilidad completa de la amenaza.
- Desde la consola se deben poder ejecutar acciones de respuesta remota sobre los endpoints: iniciar análisis, forzar actualización, aislar equipo, ejecutar verificación completa, mover a grupo, aplicar política y eliminar archivos en cuarentena.
- La consola debe registrar un log de auditoría seguro de toda la actividad de administración para cumplimiento de regulaciones, auditorías de seguridad y análisis forense.
- La consola debe permitir la integración con un módulo de Cloud Sandbox, habilitando el envío manual de archivos sospechosos para detonación y análisis dinámico, con retorno de resultados como indicadores de compromiso (IOC) para análisis futuros.
- Debe contar con un módulo de control de dispositivos periféricos: USB, unidades de CD/DVD, dispositivos MTP/PTP, Bluetooth, infrarrojo, entre otros, con opciones de: Permitir, Bloquear, Solo Lectura; con excepciones configurables por Modelo o ID del dispositivo.
- La consola debe contar con funcionalidades de gestión de TI: administración centralizada de vulnerabilidades, parches de seguridad, actualizaciones de software de terceros y cifrado de discos.

B. FUNCIONALIDADES DE PROTECCIÓN EN ESTACIONES DE TRABAJO (ENDPOINTS) CONDICIÓN TÉCNICA MÍNIMA

- Los agentes deben actualizarse de forma frecuente y automática, garantizando la integridad de las definiciones de amenazas mediante cifrado y firmas digitales.
- La solución debe incluir protección en tiempo real sobre los protocolos HTTP, HTTPS, FTP y SMTP, con análisis de phishing, filtrado de contenido web y análisis de correo electrónico.
- Debe incluir protección contra ataques de día cero provenientes de Internet, correos electrónicos y páginas web maliciosas, con tecnología de detección basada en aprendizaje automático (ML).
- La solución debe incluir capacidades de antimalware multicapa con protección automatizada contra virus, troyanos, gusanos, keyloggers, spyware, adware, rootkits, bots y otras amenazas avanzadas.
- Debe incluir protección contra ransomware con capacidad de remediación activa de la acción de cifrado malicioso, sin depender exclusivamente de detección por firmas.

- El motor de detección debe utilizar múltiples tecnologías: análisis por firmas, heurística, análisis de comportamiento dinámico y modelos de inteligencia artificial para detectar amenazas conocidas y desconocidas.
- Debe incluir capacidades de XDR esencial: correlación de eventos multi-fuente, análisis de causa raíz, trazabilidad de la amenaza dentro y fuera del endpoint, respuesta guiada y automatizada ante incidentes.
- La solución debe permitir el análisis de todos los medios de almacenamiento externo: memorias USB, discos externos, unidades ópticas y otros dispositivos de entrada.
- Debe incluir supervisión continua de comportamiento en los endpoints con alertas automáticas ante anomalías o desviaciones de comportamiento normal del usuario o proceso.
- La instalación del agente debe poder realizarse mediante Active Directory, políticas de consola de administración o descarga directa del portal del fabricante.
- Los agentes deben generar reportes de amenazas detectadas y acciones ejecutadas, con notificaciones automáticas a correo electrónico preconfigurado.
- La solución debe incluir control adaptativo de anomalías para automatizar el refuerzo del sistema y la configuración de políticas de seguridad según el comportamiento real del usuario.
- Debe contar con un módulo de seguridad en la nube (Cloud Security) que detecte los servicios en la nube utilizados, bloquee accesos no autorizados (Shadow IT) e identifique datos sensibles almacenados en aplicaciones como Microsoft 365.
- La solución debe soportar despliegue híbrido: nube y/o local (on-premise), permitiendo reducir el costo total de propiedad según la infraestructura de la entidad.

C. FUNCIONALIDADES ESPECÍFICAS EN SERVIDORES

CONDICIÓN TÉCNICA MÍNIMA

- Todos los ítems anteriores aplicables a entornos de servidor deben cumplirse plenamente para servidores Windows Server y Linux.
- La remediación o creación de firmas para amenazas de día cero no deberá superar las 48 horas desde el reporte al fabricante.
- La solución debe incluir un sistema de detección y prevención de intrusos basado en host (HIPS) que proteja recursos del sistema y aplicaciones contra ataques internos y externos.
- Debe incluir capacidad de detección de tráfico malicioso de Comando y Control (C2/C&C) y bloqueo de actividad sospechosa en servidores de archivos, Exchange y bases de datos.
- La solución debe proporcionar una vista de inventario de aplicaciones instaladas en servidores, con capacidad de bloquear nuevas instalaciones no autorizadas.
- Debe incluir funcionalidades habilitadas de Antimalware + EDR/XDR para servidores, con análisis de comportamiento en tiempo de ejecución.
- La solución debe proveer validación de seguridad por niveles con seguimiento de posibles cadenas de ataque (kill chain) en entornos de servidor.

D. LICENCIAMIENTO Y COMPATIBILIDAD
CONDICIÓN TÉCNICA MÍNIMA

- Se deberán entregar 250 licencias entre estaciones de trabajo y servidores, de acuerdo con el volumen definido en la oferta económica.
- El licenciamiento deberá ser por un período de un (1) año, a nombre de la entidad contratante, contado a partir del recibo a satisfacción del supervisor del contrato.
- La solución debe ser compatible con los siguientes sistemas operativos: SP1, Windows 10 y superior, Windows Server 2008 R2 SP1, Windows Server 2016 o superior, macOS, Linux (distribuciones principales) y Oracle Linux.
- El licenciamiento debe incluir por cada licencia: protección de 1 dispositivo (escritorio o servidor), hasta 2 dispositivos móviles y acceso a capacitación para profesionales de TI.

E. INSTALACIÓN E IMPLEMENTACIÓN
CONDICIÓN TÉCNICA MÍNIMA

- El contratista deberá realizar la instalación, implementación, integración, configuración y puesta en marcha de la solución, siguiendo las mejores prácticas del fabricante, sin costo adicional para la entidad.
- El contratista deberá entregar un cronograma detallado de actividades con tiempos y responsables.
- Debe entregarse un manual de procedimientos de administración y operación de la solución.
- El contratista debe entregar reporte de instalación exitosa en el 100% de los equipos definidos en el alcance del contrato.
- Todos los procedimientos de instalación, configuración y transferencia de conocimiento se realizarán en sitio y/o remoto (instalaciones de la entidad contratante).

F. SOPORTE Y MANTENIMIENTO
CONDICIÓN TÉCNICA MÍNIMA

- El contratista deberá garantizar soporte en esquema 8x5x365 (5 días a la semana, horario laboral, durante la vigencia del contrato) con tiempo de respuesta máximo de 2 horas desde la solicitud, con asignación de número de caso.
- En caso de brotes de infección, ataques activos o incidentes críticos, el contratista apoyará con recurso humano y tecnológico hasta la restitución del servicio.
- La entidad podrá reportar hasta 185 solicitudes en el portal de inteligencia de amenazas del fabricante sin costo adicional durante la vigencia del contrato.
- Se deben obtener durante el periodo contratado todas las nuevas versiones del software, beneficios y actualizaciones del producto adquirido.
- Se deberá realizar una HealthCheck a los seis (6) meses de la implementación, revisiones de configuración y ajustes a la consola de administración.
- Realizar mensualmente un acompañamiento programado para realizar la verificación de la configuración, actualización y estado actual de la consola.

G. TRANSFERENCIA DE CONOCIMIENTO Y CAPACITACIÓN CONDICIÓN TÉCNICA MÍNIMA

- El contratista debe incluir una transferencia de conocimiento certificada por el fabricante, con una intensidad horaria de 8 horas, para al menos cuatro (4) funcionarios, cubriendo los siguientes temas: administración de la plataforma; funcionalidades XDR y de respuesta a incidentes; ejecución y elaboración de reportes; gestión de alertas, casos e investigaciones; y configuración de políticas de seguridad.
- El soporte técnico y la atención de incidentes, problemas e inquietudes deben ser proporcionados directamente por el proveedor para todos los niveles de prioridad, durante toda la vigencia del contrato.
-

H. PLATAFORMA DE CAPACITACIÓN AUTOMATIZADA EN CONCIENTIZACIÓN DE SEGURIDAD (ASAP)

- La solución debe incluir acceso a una plataforma en línea eficaz y fácil de usar que forme las habilidades de ciberseguridad de los empleados y los motive a comportarse de manera correcta, con administración automatizada dze la capacitación.
- La plataforma debe incluir un curso principal con formación integral sobre concientización dividida por nivel de complejidad, y un curso exprés con formación breve y atractiva en formato de audio y video para actualización periódica de conocimientos.
- Debe incluir un simulador de phishing integrado, con envío automático de ataques simulados a los empleados para seguimiento del progreso y evaluación permanente de habilidades de resistencia ante este tipo de ataques.
- La plataforma debe cubrir más de 500 habilidades clave de ciberseguridad, con contenido interactivo y variado que incluya lecciones, pruebas y ataques de phishing simulados, maximizando la retención mediante aprendizaje en intervalos incrementales.
- La administración de la capacitación debe ser completamente automatizada, con notificaciones, recordatorios y programación automática de todos los elementos de entrenamiento, accesibles desde un panel de control centralizado con informes detallados hasta el nivel individual.
- Debe permitir la sincronización con Active Directory para carga y organización automática de empleados en grupos de capacitación.

I. PLATAFORMA DE CAPACITACIÓN EN CIBERSEGURIDAD PARA PERSONAL DE TI (CITO — Cybersecurity for IT Online)

- La solución debe incluir acceso a una capacitación interactiva dirigida al personal involucrado en TI, que desarrolle sólidas habilidades de ciberseguridad y de respuesta ante incidentes de primer nivel, dotando a los profesionales informáticos de habilidades prácticas para reconocer posibles escenarios de ataque en incidentes aparentemente benignos.
- La capacitación debe realizarse completamente en línea, con acceso desde navegador, sin requerir instalación adicional. Cada módulo debe incluir una breve introducción teórica, consejos prácticos y entre 4 y 10 ejercicios prácticos sobre herramientas y software de seguridad.
- El programa debe cubrir mínimo los siguientes seis (6) módulos: Software malicioso;

Archivos y programas potencialmente no deseados (PuP); Conceptos básicos de investigación; Respuesta ante incidentes de phishing; Seguridad para servidores; y Seguridad de Active Directory.

- Esta capacitación está recomendada principalmente para servicios de asistencia técnica (help desk) y administradores de sistemas, así como para todos los miembros del equipo de TI que no son expertos en ciberseguridad.
- Debe estar disponible en formato SCORM para integración con plataformas LMS institucionales, o en modalidad en la nube.

6. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será contado a partir del cumplimiento de requisitos de perfeccionamiento y ejecución y sin sobrepasar el 29 de diciembre de 2026.

La vigencia del soporte y mantenimiento de KASPERSKY XDR OPTIMUM será de un (1) año a partir de la terminación de la licencia actual el cual finaliza el 29 de diciembre de 2026.

7. GARANTÍAS (PÓLIZA)

• Cumplimiento del contrato: Equivalente al diez por ciento (10%) del valor total del contrato, por un término igual al plazo del contrato y un (1) año más.

• Calidad y correcto funcionamiento de los bienes: Equivalente al diez por ciento (10%) del valor total del contrato, por un término igual al plazo del contrato y un (1) año más.

• Calidad del servicio: Equivalente al diez por ciento (10%) del valor total del contrato, por un término igual al plazo del contrato y un (1) año más.

8. DATOS MÍNIMOS EN LA COTIZACIÓN DEL PROPONENTE DEBEN TENER:

Oferta donde se cumpla las condiciones mínimas requeridas y describiendo los servicios ofertados.

Nota 1: Esta solicitud de cotización, no genera compromiso para la Federación Colombiana de Municipios, toda vez que su fin es el de soportar el análisis del mercado y estudios del sector.
Nota 2: Con la cotización de precios por favor informar a partir de cuándo y por cuanto tiempo es el soporte de las licencias a adquirir.
Nota 3: Favor enviar la cotización incluyendo el Registro Único Tributario – RUT y RUP actualizado.
Nota 4: Entrega de la certificación o documentación necesaria en un plazo no superior a 8 días donde se evidencia la renovación y soporte de doscientos cincuenta (250) licencias.

Nota 5: El plazo de ejecución del contrato será contado a partir del cumplimiento de requisitos de perfeccionamiento y ejecución y sin sobrepasar el 29 de diciembre de 2026.

Gracias por la atención prestada y esperamos poder contar con su participación.

Proyecto: Ing. Carlos Felipe Gómez Chacón – Profesional DTI