Bogotá, 13 de mayo de 2026.

Ref.: Solicitud de cotización

La Caja de Sueldos de Retiro de la Policía Nacional (CASUR) se complace en comunicar su interés en la contratación de la adquisición de licencias antivirus.

Por lo anterior, les extendemos una cordial invitación a presentar su cotización con plazo hasta el **día 19 de mayo de 2026**, siguiendo las especificaciones detalladas a continuación:

1. **OBJETO**: **ADQUISICION DE LICENCIAS ANTIVIRUS**

2. **CLASIFICADOR DE BIENES Y SERVICIOS DE LAS NACIONES UNIDAS:**

Según el decreto 1082 articulo 2.2.1.2.1.5.1. Numeral 2 del año 2015, se hace necesario clasificar los bienes de acuerdo con el clasificador de bienes y servicios de las naciones unidas para estandarizar productos y servicios, conocido por las siglas UNSPSC.

SEGMENTO	**FAMILIA**	**CLASE**	**PRODUCTO**
43000000	43230000	43231500	43231512
Difusión de Tecnologías de la información y telecomunicaciones.	Software	Software funcional especifico de la empresa	Software de manejo de licencias.

ANEXO No 2 – ESPECIFICACIONES TÉCNICAS

No.	CONDICIONES TÉCNICAS MÍNIMAS
1.	**CONSOLA DE ADMINISTRACIÓN**
1.1	La solución, el licenciamiento y todos sus componentes suministrados para servidores y estaciones de trabajo deben ser del mismo fabricante. No se aceptarán soluciones compuestas de distintos fabricantes.
1.2	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.
1.3	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.
1.4	Debe contar con mecanismo de comunicación vía **API REST** para integración con soluciones externas de seguridad como SIEM, SOAR y plataformas de ticketing.
1.5	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).
1.6	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.
1.7	La consola debe permitir la aplicación de **políticas diferenciadas** por grupos de usuarios, usuarios individuales, grupos de máquinas y dispositivos individuales.
1.8	La consola debe soportar el **despliegue remoto de agentes** y la distribución de actualizaciones de forma centralizada y programada.
1.9	La consola debe gestionar actualizaciones automáticas de definiciones de amenazas, motores de detección y componentes de respuesta, desplegándolas a los agentes bajo tareas programadas.
1.10	Debe permitir exclusiones de análisis por sitio web, archivo, carpeta, proceso o aplicación, tanto a nivel global como por política específica.
1.11	La consola debe soportar la definición de **roles administrativos con diferentes niveles de acceso** a configuración, políticas y registros de auditoría.
1.12	Debe permitir la **programación de análisis y escaneos** sobre máquinas individuales o grupos, con periodicidad definida por el administrador.
1.13	La comunicación entre la consola y los agentes debe realizarse usando **protocolos seguros y cifrados**.
1.14	Los mensajes, notificaciones y alertas generados por los agentes deben estar disponibles en **idioma español** o permitir su configuración.
1.15	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.
1.16	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).
1.17	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.

1.18	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.
1.19	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.
1.20	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.
1.21	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.
1.22	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.
2.	**FUNCIONALIDADES GENERALES DEL ANTIVIRUS EN ESTACIONES DE TRABAJO**
2.1	Los agentes deben actualizarse de forma frecuente y automática, garantizando la integridad de las definiciones de amenazas mediante **cifrado y firmas digitales**.
2.2	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.
2.3	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)**.
2.4	La solución debe incluir capacidades de **antimalware multicapa** con protección automatizada contra virus, troyanos, gusanos, keyloggers, spyware, adware, rootkits, bots y otras amenazas avanzadas.
2.5	Debe incluir protección contra **ransomware** con capacidad de remediación activa de la acción de cifrado malicioso, sin depender exclusivamente de detección por firmas.
2.6	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.
2.7	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.
2.8	La solución debe permitir el análisis de todos los medios de almacenamiento externo: **memorias USB, discos externos, unidades ópticas** y otros dispositivos de entrada.
2.9	Debe incluir **supervisión continua de comportamiento** en los endpoints con alertas automáticas ante anomalías o desviaciones de comportamiento normal del usuario o proceso.
2.10	La instalación del agente debe poder realizarse mediante **Active Directory, políticas de consola de administración** o descarga directa del portal del fabricante.
2.11	Los agentes deben generar reportes de amenazas detectadas y acciones ejecutadas, con notificaciones automáticas a correo electrónico preconfigurado.
2.12	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.
2.13	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.

2.14	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.
3	**FUNCIONALIDADES ESPECIFICAS DEL ANTIVIRUS EN SERVIDORES**
3.1	Todos los ítems anteriores aplicables a entornos de servidor deben cumplirse plenamente para servidores **Windows Server y Linux**..
3.2	La remediación o creación de firmas para amenazas de día cero no deberá superar las **48 horas** desde el reporte al fabricante.
3.3	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.
3.4	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.
3.5	La solución debe proporcionar una **vista de inventario de aplicaciones instaladas en servidores**, con capacidad de bloquear nuevas instalaciones no autorizadas.
3.6	Debe incluir funcionalidades habilitadas de **Antimalware + EDR/XDR** para servidores, con análisis de comportamiento en tiempo de ejecución.
3.7	La solución debe proveer **validación de seguridad por niveles** con seguimiento de posibles cadenas de ataque (kill chain) en entornos de servidor.
4.	**LICENCIAMIENTO Y COMPATIBILIDAD**
4.1	Se deberán entregar 370 **licencias entre estaciones de trabajo** y **servidores**, de acuerdo con el volumen definido en la oferta económica.
4.2	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.
4.3	La solución debe ser compatible con los siguientes sistemas operativos: **Windows 7 SP1, Windows 10 y superior, Windows Server 2008 R2 SP1, Windows Server 2016 o superior, macOS, Linux (distribuciones principales) y Oracle Linux**.
4.4	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.
5.	**INSTALACIÓN**
5.1	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.
5.2	El contratista deberá entregar un **cronograma detallado** de actividades con tiempos y responsables.
5.3	Debe entregarse un **manual de procedimientos** de administración y operación de la solución.
5.4	El contratista debe entregar reporte de instalación exitosa en el **100% de los equipos** definidos en el alcance del contrato.
5.5	Todos los procedimientos de instalación, configuración y transferencia de conocimiento se realizarán **en sitio** y/o remoto (instalaciones de la entidad contratante).
6.	**SOPORTE Y MANTENIMIENTO**
6.1	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.
6.2	En caso de brotes de infección, ataques activos o incidentes críticos, el contratista apoyará con recurso humano y tecnológico hasta la **restitución del servicio**.
6.3	La entidad podrá reportar hasta **185** solicitudes en el portal de inteligencia de amenazas del fabricante sin costo adicional durante la vigencia del contrato.

6.4	Se deben obtener durante el periodo contratado **todas las nuevas versiones del software**, beneficios y actualizaciones del producto adquirido.
6.5	Se deberá realizar una HealthCheck a los seis (6) meses de la implementación, revisiones de configuración y ajustes a la consola de administración.
7.	**CERTIFICACIONES DEL CONTRATISTA**
7.1	El personal que realizará la implementación debe acreditar título como **ingeniero, técnico o tecnólogo en sistemas** o carreras afines, más **certificaciones oficiales del fabricante.**
7.2	El contratista debe ser **Partner de Negocios silver o superior** del fabricante, acreditado mediante carta de certificación vigente expedida por este y dirigido al presente proceso La Caja de Sueldos de Retiro de la Policía Nacional - CASUR.
7.3	El contratista deberá presentar mínimo **(2) certificaciones de experiencia** en contratos de suministro y mantenimiento de soluciones de seguridad similares, con fecha de expedición no mayor a **2 años**.
7.4	El contratista deberá certificar que realizará todas las actividades de implementación dentro del valor contratado, **sin costos adicionales** para la entidad
7.5	El oferente dentro de su propuesta deberá adjuntar las hojas de vida del personal que realizará la implementación de la solución, donde se evidencie mediante certificación que este personal a participado en implementaciones iguales o similares a las del presente proceso, no inferiores al año 2023.
7.6	El software ofertado debe estar reconocido y evaluado positivamente en pruebas independientes de laboratorio como: **AV-Test, SE Labs y MITRE ATT&CK Evaluations**, en la categoría de soluciones de protección y detección avanzada de endpoints (EPP/EDR/XDR).
8.	**TRANSFERENCIA DE CONOCIMIENTOS**
8.1	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.
8.2	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.
9.	**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 de 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
10.	**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
	Debe emitir **certificados personales** al personal que complete cada módulo de la capacitación
	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

Por medio de la presente, certifico que cumplo con cada uno de los requisitos exigidos de carácter técnico, y doy por entendido con la firma del presente documento que los acepto y daré cumplimiento a los mismos.

Proponente_____
NIT O C.C No _____
Representante legal_____
C.C No _____

ANEXO No. 1
OFERTA ECONÓMICA

ITEM	PRESENTACIÓN	UNIDAD DE MEDIDA	CANTIDAD	VALOR UNITARIO	IVA	VALOR TOTAL
1	Adquisición de licencias XDR para estaciones de trabajo (Windows)	UND	350			
2	Adquisición de licencias antivirus para servidores (Windows Server, Linux, Oracle Linux)	UND	20			
3	Soporte esquema 8x5x365x2	UND	El solicitado en el ítem 6.1, 6.2, 6.3 y 6.4, del anexo técnico			

Los Oferentes deben verificar el precio de referencia incluido impuestos de cada ítem, pues este será el precio para el comité económico evaluador, quien rechazará la oferta del proponente cuyo precio sea superior al presupuesto asignado al presente proceso.

NOTA 1: La oferta económica más favorable será aquella que haya ofertado el menor valor por item.

NOTA 2: El IVA aplicado al bien o servicio es de _____%.

NOTA 3: La oferta económica debe indicar el valor del IVA (en caso de que el bien se halle gravado, y si está exento, tal situación se debe especificar).

Exento de IVA SI:_____ NO:_____

El oferente es responsable de IVA SI: _____ NO: _____

EL OFERENTE QUE NO DILIGENCIE EL PRESENTE FORMATO DE MANERA INTEGRAL SERÁ CAUSAL DE RECHAZO

Por medio de la presente, certifico que cumplo con cada uno de los requisitos exigidos y doy por entendido con la firma del presente documento que los acepto, daré cumplimiento a los mismos y mantendré los precios ofertados.

Atentamente,

_____

Firma representante legal del Oferente

Nombre: _____

Cargo: _____

Documento de Identidad: _____