



**AVISO DE CONVOCATORIA PÚBLICA
SELECCIÓN ABREVIADA POR SUBASTA INVERSA
No. MJD- SASI-007-2026**

El Ministerio de Justicia y del Derecho, en cumplimiento de lo exigido en el artículo 2.2.1.1.2.1.2 del Decreto 1082 de 2015 en concordancia con el artículo 2, numeral 2, literal a) de la Ley 1150 de 2007, informa a la comunidad en general que iniciará proceso de contratación, bajo la modalidad de Selección Abreviada por Subasta Inversa Electrónica.

1. El nombre y dirección de la Entidad Estatal.

MINISTERIO DE JUSTICIA Y DEL DERECHO, ubicado en la Calle 53 No. 13-27 de la ciudad de Bogotá D.C.

2. La dirección, el correo electrónico y el teléfono en donde la Entidad Estatal atenderá a los interesados en el Proceso de Contratación, y la dirección y el correo electrónico en donde los proponentes deben presentar los documentos en desarrollo del Proceso de Contratación.

Sistema Electrónico para la Contratación Pública SECOP II <https://www.colombiacompra.gov.co/secop/secop-ii>
Buzón electrónico: gestion.contractual@minjusticia.gov.co
Teléfono de contacto: +57 (601) 444 31 00

3. El objeto del contrato a celebrar, identificando las cantidades a adquirir.

Objeto: "Adquirir licenciamiento y servicios de ciberseguridad para fortalecer la prevención, protección, detección, investigación y respuesta ante amenazas e incidentes de seguridad en el Ministerio de Justicia y del Derecho".

El contrato a celebrar corresponde a un LICENCIAMIENTO DE SOFTWARE. Los bienes y servicios objeto del presente proceso se detallan a continuación:

5.1 ESPECIFICACIONES TÉCNICAS - ITEM 1	
SOFTWARE	Suscripcion Cisco Secure Endpoint premier EDR Premier - AMP4E-PRE-CL-LIC , Cisco Secure Endpoint premier Tier Suscription
Cantidad Licencias	1.020
Tipo Licencia	Licenciamiento por suscripción para un (1) año
PREVENCION	
Reputación de archivos:	La solución debe contar con capacidades de análisis de reputación de archivos, mediante la consulta de bases de datos locales y/o en la nube que permitan clasificar los archivos como confiables o maliciosos. Esta funcionalidad debe contribuir a la prevención y detección temprana de amenazas, que permita el bloqueo o puesta en cuarentena de archivos identificados como maliciosos desde el punto de entrada, sin requerir análisis intensivo del procesador.
Antivirus:	Incluye motores antivirus basados en definiciones y constantemente actualizados para terminales Windows, Mac o Linux. Soportar la detección personalizada basada en firmas, lo que permite a los administradores ofrecer capacidades de control sólidas y aplicar listas de bloqueo. La base de datos de firmas antivirus debe residir localmente en cada punto final, para no depender de la conectividad en la nube para funcionar.
Detección de	Soportar detección de variantes o malware polimórfico mediante huellas digitales

malware polimórfico:	sueeltas.
Machine learning analysis:	Debe permitir entrenamiento mediante algoritmos para "aprender" a identificar archivos y actividades maliciosas en función de los atributos del malware conocido.
Exploit prevention:	Soportar la función de prevención de exploits para defender los puntos finales de ataques de inyección de memoria basados en exploits
Script protection:	Soportar visibilidad mejorada de las secuencias de comandos que se ejecutan en sus puntos finales para proteger contra ataques basados en secuencias de comandos, comúnmente utilizados por el malware.
Behavioral protection:	Permitir el análisis de comportamiento para monitorear continuamente toda la actividad de los usuarios y terminales, de esta forma proteger contra comportamientos maliciosos en tiempo real, al comparar un flujo de registros de actividad con un conjunto de patrones de actividad de ataque que se actualizan dinámicamente a medida que evolucionan las amenazas.
Device Control:	Permite controlar el uso de dispositivos de almacenamiento masivo USB y evitar ataques desde estos dispositivos. Permitir los administradores de punto final revisar eventos de conexión/desconexión de dispositivos, acceder a eventos de infracción, usar la API para administrar configuraciones y reglas de control de dispositivos, entre otros. Permitir a los administradores definir el comportamiento predeterminado cuando los dispositivos están conectados y crean reglas granulares para respaldar aún más diversos enfoques para controlar estos dispositivos.
DETECCION	
Malicious activity protection:	Soportar Monitoreo continuo de toda la actividad del terminal y proporcionar detección en tiempo de ejecución y bloqueo del comportamiento anormal de un programa en ejecución en el terminal.
Cloud-based indicators of compromise:	Tener inteligencia de amenazas que analice constantemente el malware para descubrir nuevos tipos de amenazas y crear perfiles forenses y de comportamiento para amenazas emergentes, también conocidos como indicadores de compromiso (IoC). Los datos forenses, como ubicaciones de archivos o modificaciones de los valores de las claves de registro, son datos que usa la herramienta para ayudar a los administradores a identificar los sistemas que han sido vulnerados.
Host-based IoCs:	Permitir que los administradores pueden escribir sus propios IoC personalizados para usarlos en la respuesta a incidentes para buscar indicadores posteriores al compromiso en toda la implementación del endpoint.
Vulnerabilities:	Identificar vulnerabilidades del sistema operativo en su entorno para ayudar a reducir la superficie de ataque.
Baja prevalencia:	Debe Identificar automáticamente los archivos ejecutables que existan en cantidades bajas en sus puntos finales y analizar esas muestras en nuestro entorno de pruebas basado en la nube para descubrir nuevas amenazas.
Talos Threat Hunting (funcionalidad exclusiva de Licenciamiento Premier): Servicio proactivo de búsqueda.	Debe soportar la capacidad de Talos Threat Hunting, servicio proactivo de búsqueda de amenazas debe realizar analítica para detectar amenazas evasivas avanzadas, debe integrarse en Cisco Secure Endpoint. Nivel de licenciamiento Premier, esta herramienta bebe contar en su base de datos de consultas predefinidas que permita ejecutar búsquedas complejas en tiempo real sobre todos los endpoints, obteniendo una fotografía (snapshot) profunda lo cual debe ser sometido analítica profunda con el propósito de ejecutan cacerías altamente automatizadas y guiadas por playbooks, produciendo alertas de alta fidelidad lo anterior debe generar un informe donde se describa la cadena de ataque (cómo fue identificado, cómo evolucionó) y proveer recomendaciones sobre los siguientes pasos de respuesta
EDR completo e integración con Cisco XDR (funcionalidad exclusiva de Premier):	Debe soportar capacidades completas de Endpoint Detection and Response (EDR) con integración nativa a la plataforma Cisco XDR. Esta capacidad debe permitir simplificar las investigaciones de seguridad mediante un EDR avanzado y un contexto ampliado sobre datos de endpoint, web, correo y red a través de Cisco XDR.
Respuesta segura de punto final	
Dashboards and inbox:	Permitir informes con los eventos y puntos finales con clasificación por prioridad y se vinculación a flujos de trabajo para realizar un seguimiento del progreso durante la investigación.

Endpoint forensics:	Soportar herramientas como la trayectoria de archivos y la trayectoria de dispositivos que utilizan las capacidades de análisis continuo para mostrarle el alcance completo de una amenaza. Identifica todas las aplicaciones, procesos y sistemas afectados para identificar al paciente cero, así como el método y el punto de entrada.
Dynamic analysis:	Incluir un entorno de pruebas integrado y altamente seguro para analizar el comportamiento de los archivos sospechosos.
Retrospective security:	Soportar la correlación de la información de nuevas amenazas con su historial pasado y automáticamente pone en cuarentena los archivos en el momento en que comienzan a exhibir un comportamiento malicioso.
Command line visibility:	Soportar visibilidad de los argumentos de la línea de comandos. Debe poder descubrir comportamientos difíciles de detectar, como el uso de vssadmin para eliminar copias fantasma o desactivar safe boots, explotaciones basadas en PowerShell, escalada de privilegios, modificaciones de listas de control de acceso e intentos de enumerar sistemas.
Endpoint isolation:	Permitir aislar con un solo clic un punto final infectado junto con la capacidad de incluir en la lista blanca recursos de red confiables.
Advanced search:	Proporcionar consultas predefinidas, lo que le permite ejecutar rápidamente consultas complejas en cualquiera o en todos los puntos finales. Permite obtener una visibilidad más profunda de lo que sucedió con cualquier punto final en un momento dado al tomar un snapshot de su estado actual.
EDR para terminales	
	La solución deberá proporcionar capacidades de Endpoint Detection and Response (EDR) para la detección, investigación y respuesta ante eventos de seguridad en los endpoints.
Soporte y compatibilidad de plataforma	
Windows	- Windows 10, 11 - Windows Server 2016, 2019, 2022 o superior.
Linux	- Red Hat Enterprise Linux 7, 8 y superiores - CentOS 7, 8 y superiores. - Oracle Linux RHCK (Red Hat Compatible Kernel) 7, 8 y superiores. - Oracle UEK (Unbreakable Enterprise Kernels) 7, 8 y superiores. - Alma Linux 8 - Rocky Linux 8 - Ubuntu Linux 18.04, 24.04 - Amazon Linux 2 - Kernel 4.14 and above - SUSE Enterprise Linux 15 / openSUSE Leap 15 - Debian Linux 10, 11
MacOS	- macOS 10.14, 10.15, 11, 12 - iOS 14.4 o superior.
Integración con herramientas del Ministerio de Justicia	Se debe integrar de forma nativa con el agente de security internet gateway (CISCO) que tiene la entidad actualmente.

5.2 ESPECIFICACIONES TÉCNICAS - ITEM 2	
ESPECIFICACIONES TÉCNICAS – CISCO XDR	
SOFTWARE	Suscripción Cisco XDR-ADV Cisco XDR Advantage tier suscription.
Cantidad Licencias	200
Tipo Licencia	Calculo dado por el fabricante CISCO en conocimiento de las herramientas ya integradas en el ministerio: La solución Cisco XDR Advantage requerida para el Ministerio de Justicia

	y del Derecho corresponde a doscientas (200) licencias, dimensionadas para soportar una capacidad de ingesta de datos de eventos de seguridad de hasta cuatrocientos gigabytes (400 GB) mensuales, con una tasa de retención de noventa (90) días. Cada licencia de Cisco XDR permite una capacidad de ingesta mensual de 2 GB. En consecuencia, para el Ministerio, las doscientas (200) licencias requeridas permiten disponer de una capacidad de ingesta proyectada de 400 GB mensuales, de acuerdo con el dimensionamiento realizado por el fabricante Cisco. La capacidad de ingesta deberá permitir el procesamiento y análisis de los eventos de seguridad provenientes de las fuentes contempladas dentro del alcance de la solución, incluyendo Cisco Secure Endpoint, Cisco Umbrella, Cisco ISE, Cisco Duo, Microsoft Office y el firewall perimetral, de acuerdo con las capacidades de integración y configuración requeridas para la operación de la solución.
Capacidades clave de la plataforma	
Analítica de seguridad y correlación:	Debe contar con un motor nativo de analítica y correlación capaz de ingerir eventos EDR y XDR, logs de flujo de red y de nube pública, correlacionando eventos en el tiempo para revelar ataques multietapa. Debe visualizar los incidentes mediante un grafo de ataque (Attack Storyboard) con verificación instantánea del ataque y línea de tiempo del incidente.
Fuentes de telemetría nativas:	Debe analizar y correlacionar de forma nativa, como mínimo, las siguientes seis (6) fuentes de telemetría: endpoint, red, firewall, correo electrónico, identidad y DNS.
Priorización de incidentes:	Debe asignar a cada incidente un puntaje de prioridad en una escala de 1 a 1000, compuesto por el riesgo de la detección (basado en las tácticas, técnicas y procedimientos -TTP- del marco MITRE ATT&CK) y el valor del activo afectado, permitiendo a los analistas enfocarse primero en los incidentes de mayor impacto.
Automatización y flujos de trabajo (workflows):	Debe permitir la creación de flujos de trabajo de automatización y orquestación mediante un editor gráfico de bajo o nulo código (low-to-no-code), con disparadores por incidente, correo electrónico, webhook o programación (schedule), así como acceso a un catálogo (Automation Exchange) de flujos de trabajo preconfigurados de instalación en un clic.
Playbook de respuesta a incidentes:	Debe incluir un Playbook de respuesta guiada para incidentes basado en el modelo SANS PICERL (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned), con acciones automatizadas ejecutables directamente desde el incidente y capacidad de personalizar o crear playbooks propios.
Contexto de activos (Asset Insights):	Debe consolidar en un inventario unificado la información de dispositivos y usuarios proveniente de las distintas integraciones (Asset Insights), permitiendo asignar un valor a cada activo para su uso en la priorización de incidentes.
Investigación y caza de amenazas (Threat Hunting):	Debe proveer una funcionalidad de investigación que permita consultar de forma simultánea múltiples fuentes de inteligencia de amenazas (Cisco Talos y de terceros) y el histórico de la organización, con vista de grafo, línea de tiempo ajustable, y posibilidad de iniciar investigaciones a partir de un incidente, un observable o texto libre.
Forense digital (XDR Forensics):	Debe incluir capacidades de forense digital integradas al flujo de trabajo del incidente, con recolección de más de 350 artefactos por endpoint (incluyendo equipos comprometidos o parcialmente cifrados), preservación de la cadena de custodia y shell remoto interactivo para acciones de contención, erradicación y recuperación.
Inteligencia de amenazas:	Debe incluir de forma nativa y sin costo adicional el acceso a la inteligencia de amenazas de Cisco Talos, así como a repositorios propios de inteligencia cargados por el cliente, para enriquecer la investigación y la caza de amenazas.

Licenciamiento e integración nativa	
Licenciamiento Cisco XDR:	Debe incluir licenciamiento de la plataforma Cisco XDR nivel Advantage, el cual incluye integración con herramientas Cisco y herramientas de terceros, con una capacidad de almacenamiento equivalente a las licencias solicitadas por mes y una tasa de retención de 90 días para la telemetría ingerida.
Telemetría e integraciones con terceros:	Al ser de nivel Advantage, debe incluir integraciones con soporte comercial de Cisco, seleccionadas por el fabricante, con herramientas de terceros documentadas en la documentación oficial del fabricante y según la arquitectura actual de la entidad.
Cisco Secure Cloud Analytics:	solución SaaS que proporciona análisis de comportamiento en redes para mejorar la detección de amenazas y fortalecer la postura de seguridad en entornos de nube híbrida. Su integración con Cisco XDR permite consolidar, correlacionar y analizar eventos de seguridad en tiempo real, facilitando la detección y respuesta rápida a amenazas. Entre sus capacidades destacan la priorización de incidentes basada en el impacto empresarial y el valor de los activos, el acceso a un análisis extenso de telemetría para investigaciones más efectivas, y la combinación de datos de inventario con información de seguridad para un contexto integral de los activos. Además, ofrece recomendaciones automatizadas para respuestas rápidas y precisas, mejorando la eficiencia de los analistas de seguridad y reduciendo el tiempo de respuesta ante incidentes. Cisco Secure Cloud Analytics es una plataforma integral de análisis y detección de amenazas que, al integrarse con Cisco XDR, potencia la visibilidad, correlación y respuesta automatizada en entornos de red y nube, ayudando a la Entidad a identificar y mitigar amenazas de manera más rápida y eficiente
integración con plataformas no nativas	Integración de Cisco XDR con las plataformas de seguridad de terceros compatibles que integre el ministerio de justicia y no contempladas dentro de las integraciones nativas de Cisco, incluyendo, según corresponda, la configuración de conectores, el mapeo de fuentes de telemetría, la normalización de eventos y la validación de la información y correlación resultante en la consola de Cisco XDR..
Integración nativa con Umbrella, Cisco Duo, Cisco ISE y Secure Endpoint:	La plataforma Cisco XDR debe integrarse de forma nativa con Cisco Umbrella, Cisco Duo, Cisco ISE y Cisco Secure Endpoint, consumiendo automáticamente la telemetría de cada una de estas soluciones (eventos, indicadores de compromiso, autenticaciones, contexto de identidad y postura de red, aislamiento de endpoints) sin requerir desarrollos o configuraciones manuales adicionales, permitiendo la correlación unificada de eventos entre estas fuentes y la ejecución de acciones de respuesta (como el aislamiento de un endpoint o el bloqueo de un usuario/dispositivo) directamente desde la consola de Cisco XDR.
Correlación y de priorización incidentes:	Debe proporcionar un tablero unificado que correlacione automáticamente los eventos e indicadores de compromiso provenientes de Secure Endpoint con los de otras fuentes integradas, priorizando los incidentes según su severidad e impacto para agilizar la investigación y respuesta por parte del equipo de seguridad del Ministerio.
Seguridad del acceso administrativo:	La consola deberá permitir autenticación multifactor, federación con el proveedor de identidad institucional cuando esté soportada, control de acceso basado en roles y mínimo privilegio, separación de funciones y registro auditable de inicios de sesión, cambios de configuración, acciones de respuesta y administración de integraciones.
Protección y tratamiento de datos:	El contratista deberá acreditar cifrado de la información en tránsito y en reposo, informar ubicación o regiones de tratamiento y subencargados aplicables, aplicar controles de acceso y confidencialidad, notificar incidentes que afecten datos o el servicio del Ministerio y garantizar la exportación y eliminación segura de la información al finalizar el contrato, de acuerdo con la normativa colombiana y las condiciones del fabricante.
Criterios de aceptación técnica:	La puesta en producción se aceptará cuando se evidencien: suscripciones activas y asignadas al Ministerio; cobertura y salud de los conectores; capacidad y retención contratadas; integraciones acordadas operativas; generación y correlación de eventos de

	prueba; acciones de respuesta autorizadas; roles y MFA configurados; tableros, alertas y reportes; documentación de arquitectura, configuración, integraciones, operación y escalamiento; y acta de pruebas aprobada por el supervisor.
--	---

5.3 ESPECIFICACIONES TÉCNICAS - ITEM 3	
SOPORTE TÉCNICO - SVS-XDR-SUP-P Cisco support signature for XDR	
Tiempo	Para los servicios descritos, la asistencia tendrá una vigencia de un (1) año, asociada a la vigencia de la suscripción Cisco XDR Advantage.
Certificado Suscripcion	El contratista deberá entregar el certificado o documento expedido por el fabricante que acredite la activación y vigencia del servicio de soporte contratado.
Soporte Técnico	Soporte tecnico durante la vigencia de renovacion del licenciamiento. El servicio deberá incluir el soporte técnico asociado a la suscripción Cisco XDR Advantage, de conformidad con las condiciones y alcance establecidos por el fabricante. El contratista deberá gestionar y escalar ante Cisco los casos que requieran intervención del fabricante, efectuar el seguimiento correspondiente y mantener informada a la Entidad sobre el estado y evolución de los casos reportados. El soporte comprenderá la atención de incidentes, errores, fallas o comportamientos inesperados asociados al funcionamiento de la plataforma Cisco XDR Advantage, así como la orientación técnica relacionada con el producto y sus funcionalidades, dentro del alcance definido por el fabricante. Soporte en sitio en los casos que se requiera, lunes a viernes : 8:00 AM a 12:30 PM y de 1:30 PM a 5.30 PM. Soporte Remoto 24/7 - Soporte del fabricante Para la asistencia remota se requiere de disponibilidad 24/7 . Suministrar un número de PBX y/o Línea Nacional. Soporte por Correo Electrónico, 8:00 AM a 5.30 PM, suministrar un correo electrónico para efecto de formular peticiones de soporte. Para los tiempos de respuesta remitirse al numeral 5.3 tiempos de respuesta y solución, según criticidad. Los servicios asociados a la solución se prestarán principalmente de manera remota, en atención a la naturaleza de la solución EDR basada en la nube. No obstante, cuando se requiera, el contratista deberá brindar soporte en sitio en las sedes del Ministerio de Justicia y del Derecho ubicadas en la ciudad de Bogotá D.C., o donde se encuentren durante la ejecución del contrato, con el fin de atender actividades de soporte técnico, configuración, afinamiento o acompañamiento. Soporte a través de Página Web, radicación de problemas e Inquietudes por medio del mecanismo de correos o celular o “Envío de Tickets”.
Configuracion y Parametrizacion de acuerdo con los lineamientos del Ministerio de Justicia.	Realizar la afinacion de la configuración, parametrización y afinamiento de los componentes de la solución de seguridad con total compatibilidad y completo funcionamiento conforme a los lineamientos del Ministerio de Justicia, y de acuerdo al cronograma de actividades acordado entre el supervisor del contrato y el oferente. En los casos de nuevas versiones o funcionalidades adicionales del licenciamiento, realizar la implementación que sea necesaria. Brindar asesoria y acompañamiento para la administración de la solución de seguridad por el año del licenciamiento.
Mesas de trabajo	Mesas de trabajo

	Realizar una mesa de trabajo mensual, preferiblemente de manera virtual, para analizar el funcionamiento de la plataforma EDR, incluyendo el reporte de estado, análisis de alertas, niveles de riesgo y su impacto, así como la definición de acciones preventivas y de remediación, de acuerdo con los parámetros establecidos en el numeral 5 ESPECIFICACIONES TÉCNICAS. La programación, convocatoria y modalidad de las mesas de trabajo serán coordinadas por el supervisor del contrato, en conjunto con el contratista, y se definirán en el acta de inicio del contrato. En caso de requerirse, estas podrán realizarse de manera presencial en las sedes del Ministerio. En el marco de estas sesiones, el contratista deberá implementar y afinar las políticas que sean requeridas por el equipo de infraestructura del Ministerio de Justicia y del Derecho.
Transferencia de conocimiento	Transferencia de conocimiento técnico: Para mínimo dos (2) funcionarios de la Subdirección de Tecnologías del Ministerio en la sede principal ubicada en la Calle 53 No 13 – 27 de la ciudad de Bogotá, de lunes a viernes 8:00 AM a 12:30 PM o de 1:30 PM a 5.30 PM, una transferencia de conocimiento, con una duración mínima de ocho (8) horas. El plazo de ejecución de esta actividad se coordinará una vez suscrita el acta de inicio. La capacitación se debe desarrollar sobre las siguientes temáticas: • Administración de la consola • Configuración, parametrización y afinamineto de políticas • Generación de informes de la plataforma (Detalle de cantidad, análisis, contención, aislamiento, etc.) • Tratamiento y gestión de amenazas

5.4 ESPECIFICACIONES TÉCNICAS - Ítem 4	
Horas de especialista para integración, configuración y puesta en operación de Cisco EDR Secure Endpoint Premier y Cisco XDR Advantage	
Característica	Descripción
Nombre del servicio	Horas de especialista para integración, configuración y puesta en operación de Cisco Secure Endpoint Premier y Cisco XDR Advantage
Unidad de medida	Hora de especialista.
Cantidad	30
Alcance del servicio	Servicio especializado prestado por recurso humano con formación, experiencia y conocimientos técnicos en ciberseguridad, soluciones EDR/XDR y plataformas de seguridad informática, destinado a realizar las actividades de integración, configuración, parametrización, validación y puesta en operación de Cisco Secure Endpoint Premier y Cisco XDR Advantage, incluyendo la integración nativa entre ambas plataformas y la configuración de las fuentes de telemetría requeridas dentro del alcance definido por la Entidad. El servicio comprenderá la revisión de la configuración existente, identificación de los requerimientos de integración, configuración y parametrización de las plataformas, habilitación y validación de conectores, verificación del flujo de eventos y telemetría, ejecución de pruebas funcionales, validación de la correlación de eventos, realización de ajustes requeridos para su correcto funcionamiento, documentación de la configuración y transferencia de conocimiento al personal técnico designado por el Ministerio.

Nivel de educación	Profesional en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Telemática, Ciberseguridad o áreas afines.
Experiencia	Mínimo dos (2) años de experiencia en implementación, configuración, administración o integración de soluciones EDR, XDR, protección de endpoints o plataformas de seguridad informática.
Habilidades y destrezas	EDR, XDR; seguridad de endpoints; análisis de eventos; gestión de alertas; políticas de seguridad; integración de plataformas y gestión de incidentes de seguridad.
Certificación Cisco	Certificación vigente del fabricante Cisco relacionada con tecnologías de seguridad, ciberseguridad, Secure Endpoint, XDR o equivalente, de acuerdo con el alcance del servicio.
Actividades	Realizar el levantamiento y revisión de la configuración existente; configurar y parametrizar Cisco Secure Endpoint Premier; configurar y parametrizar Cisco XDR Advantage; realizar la integración nativa entre ambas plataformas; configurar configurar las fuentes de telemetría definidas por la Entidad dentro del alcance del servicio; validar el flujo de información y eventos; realizar pruebas funcionales; ajustar configuraciones, políticas y parámetros de seguridad; validar la generación, recepción y correlación de eventos y alertas; documentar las configuraciones e integraciones; elaborar informes técnicos; entregar recomendaciones técnicas y realizar transferencia de conocimiento al personal técnico designado por la Entidad.
Criterios de aceptación	Se deberá evidenciar la integración operativa entre Cisco Secure Endpoint Premier y Cisco XDR Advantage, así como la configuración y puesta en funcionamiento de las fuentes de telemetría e integraciones definidas por la Entidad dentro del alcance del servicio, incluyendo, cuando corresponda, las integraciones nativas y las integraciones con plataformas de terceros compatibles contempladas para la solución. Para las integraciones implementadas se deberá evidenciar el flujo, recepción, visualización y correlación de la información y eventos, así como la ejecución de las pruebas funcionales, los ajustes realizados, la documentación de las configuraciones e integraciones, el informe técnico y la transferencia de conocimiento al personal técnico designado por la Entidad.

4. La modalidad de selección del contratista.

Selección Abreviada por Subasta Inversa Electrónica, de conformidad con el artículo 2, numeral 2, literal a) de la Ley 1150 de 2007 y los artículos 2.2.1.2.1.2.1 y siguientes del Decreto 1082 de 2015. Los bienes y servicios objeto de la presente contratación corresponden a bienes y servicios de características técnicas uniformes y de común utilización.

5. El plazo estimado del contrato.

El plazo de ejecución del contrato se extenderá hasta el 31 de diciembre de 2026, previo cumplimiento de los requisitos de perfeccionamiento y ejecución, con el fin de garantizar el cierre administrativo y financiero del contrato dentro de la respectiva vigencia.

Los servicios y elementos objeto de la contratación tendrán una vigencia de un (1)

año, de acuerdo con la naturaleza y condiciones de cada uno de los ítems contratados, contada a partir de la fecha que corresponda para cada prestación.

- Para el caso del licenciamiento mediante suscripción y el soporte técnico asociado, la vigencia será de un (1) año contado a partir de la activación de la renovación, la cual deberá constar en el documento de licenciamiento entregado por el fabricante.
- Para las treinta (30) horas de servicios profesionales especializados para la integración, tendrán una vigencia de un (1) año contado a partir del inicio de ejecución del contrato y podrán ser utilizadas durante dicho período de acuerdo con las necesidades de la Entidad.

6. La fecha límite en la cual los interesados deben presentar su oferta y el lugar y forma de presentación de la misma.

La fecha de presentación de la oferta es la que consta en el cronograma del proceso consignado en la plataforma SECOPII, a través del Sistema Electrónico para la Contratación Pública SECOP II <https://www.colombiacompra.gov.co/secop/secop-ii>

7. El valor estimado del contrato y la manifestación expresa de que la Entidad Estatal cuenta con la disponibilidad presupuestal.

El presupuesto oficial: para la presente contratación **TRESCIENTOS CINCUENTA Y SEIS MILLONES NOVECIENTOS NOVENTA Y CINCO MIL OCHENTA PESOS M/CTE. (\$356.995.080,00) incluido IVA** y demás impuestos a que haya lugar, sin embargo, el valor del contrato será el valor de la oferta de quien resulte adjudicatario. Dicho valor fue determinado mediante estudio de sector y de mercado realizado por la Subdirección de Tecnologías y Sistemas de Información, utilizando la medida de tendencia central de media geométrica sobre las cotizaciones recibidas en el evento MJD-SI-033-2026.

La Entidad manifiesta que cuenta con la disponibilidad presupuestal que respalda el presente proceso, conforme se acredita con el Certificado de Disponibilidad Presupuestal que se relaciona a continuación:

Vigencia	No. CDP	Fecha CDP	Unidad Ejecutora	Rubro Presupuestal	Valor CDP
2026	21426	2026-09-30	12-01-01-000 MJD - GESTION GENERAL	C-1299-0800-8-20110C2-1299065-02 ADQUIS. DE BYS - SERVICIOS TECNOLÓGICOS - FORTALECIMIENTO DE LA GESTION TECNOLOGICA CON ENFOQUE DE INVESTIGACION, DESARROLLO E INNOVACION PARA EL MEJORAMIENTO DEL ACCESO A LA JUSTICIA A NIVEL NACIONAL	\$ 371.142.000

Vigencias Futuras: No aplica

8. Mención de si la contratación está cobijada por un Acuerdo Comercial.

De conformidad con la normatividad vigente, se procedió a verificar si el servicio que se pretende contratar, se encuentra o no cobijado por un acuerdo internacional de libre comercio, que permita tener un referente para el análisis del mercado requerido.

Acuerdo Comercial		Entidad Estatal incluida	Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción aplicable	Proceso de Contratación cubierto
		Si/No	Si/No	Si/No	Si/No
Alianza Pacífico	Chile	Si	No	No	No
	Perú	Si	No	No	No
	México	Si	No	No	No
Canadá		Si	No	No	No
Chile		Si	Si	No	Si
Corea		Si	No	No	No
Costa Rica		Si	No	No	No
Estados Unidos		Si	No	No	No
Estados AELC		Si	No	No	No
México		Si	No	No	No
Triángulo Norte	El Salvador	Si	No	No	No
	Guatemala	Si		No	No
	Honduras	No	N/A	No	No
Unión Europea		Si	No	No	No
Israel		Si	No	No	No
Reino Unido e Irlanda del Norte		Si	No	No	No
Comunidad Andina de Naciones – CAN		Si	Si	No	Si

Nota: La decisión de la Comunidad Andina de Naciones CAN aplica a todos los procesos contractuales independientemente del valor de los mismos.

9. Mención de si la convocatoria es susceptible de ser limitada a Mipyme.

De conformidad con lo señalado en el artículo 2.2.1.2.4.2.2 del Decreto 1082 de 2015, modificado por el artículo 5 del Decreto 1860 de 2021, la presente convocatoria **ES SUSCEPTIBLE DE LIMITARSE A MIPYMES** con mínimo un (1) año de existencia, toda vez que el presupuesto oficial del proceso, **TRESCIENTOS CINCUENTA Y SEIS MILLONES NOVECIENTOS NOVENTA Y CINCO MIL OCHENTA PESOS M/CTE. (\$356.995.080,00) incluido IVA es inferior al umbral establecido por el Ministerio de Comercio, Industria y Turismo (Umbral MiPymes: \$511.708.497,00).** Los interesados en solicitar la limitación a MiPymes deberán manifestarlo dentro del plazo definido en el cronograma, aportando los documentos que acrediten su calidad.

10. Enumeración y breve descripción de las condiciones para participar en el Proceso de Contratación.

Se dará aplicación al procedimiento de selección abreviada por Subasta Inversa, a través de la plataforma transaccional de SECOP II, de conformidad con lo dispuesto en el artículo 2.2.1.2.1.2.1 del Decreto 1082 de 2015.

En tal sentido, el contrato será adjudicado al proponente que haya sido habilitado jurídica, financiera y técnicamente y cuya oferta económica cumpla con las condiciones establecidas por la Entidad.

El proponente deberá observar las condiciones establecidas en el documento de



estudio previo y pliego de condiciones.

11. Indicar si en el Proceso de Contratación hay lugar a precalificación.

No aplica

12. El Cronograma.

El cronograma del proceso será el establecido en el Sistema Electrónico para la Contratación Pública SECOP II <https://www.colombiacompra.gov.co/secop/secop-ii>, y en el pliego de condiciones.

13. La forma como los interesados pueden consultar los Documentos del Proceso.

El proyecto de Pliego de Condiciones con sus respectivos anexos podrá ser consultados en el Sistema Electrónico para la Contratación Pública SECOP II <https://www.colombiacompra.gov.co/secop/secop-ii> a partir de su publicación.

El proyecto de pliego de condiciones estará publicado por el término de cinco (5) días hábiles

Las observaciones a los mismos podrán ser presentadas por los posibles oferentes durante el término antes señalado, a través del Sistema Electrónico para la Contratación Pública SECOP II <https://www.colombiacompra.gov.co/secop/secop-ii>

Dado en Bogotá D.C., a los _02_ días del mes de octubre de 2026.

Proyectó: Jhon Yamid Angulo Herrán- Contratista Grupo de Gestión Contractual
Revisó: Sandra Patricia Cardozo – Coordinadora E. Grupo de Gestión Contractual