

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

FECHA: 21 de octubre de 2026

AREA SOLICITANTE: Subdirección de Tecnologías y Sistemas de Información

1. 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.

2. CÓDIGO ESTÁNDAR DE PRODUCTOS Y SERVICIOS DE NACIONES UNIDAS (UNSPSC)

Teniendo como base la Guía para la Codificación de Bienes y Servicios de acuerdo con el código estándar de productos y servicios de Naciones Unidas, se logra identificar los productos a adquirir y su correspondiente código como se muestra a continuación:

Clasificación UNSPSC	Segmento	Familia	Clase	Producto
(E) Productos de Uso Final	43 difusión de Tecnologías de Información y Telecomunicaciones	43230000 Software	43233200 Software de seguridad y protección	43233205 Software de seguridad de transacciones y de protección contra virus
(F) Servicios	81 Servicios basados en Ingeniería, Investigación y Tecnología	81110000 Servicios Informáticos	81111800 Servicios de sistemas y administración de componentes de sistemas	81111801 Seguridad de los computadores, redes o internet

3. UNIDAD DE MEDIDA

Se Tiene en cuenta la siguiente unidad de medida para el presente proceso:

Ítem	Descripción	Unidad de Medida	Cantidad
Suscripcion Cisco Secure Endpoint premier EDR Premier			
1	AMP4E-PRE-CL-LIC , Cisco Secure Endpoint premier Tier Subscription	Unidad	1.020

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

Suscripción Cisco XDR Advantage Tier (análisis de datos de endpoint, web, correo y red)			
2	XDR-ADV Cisco XDR Advantage tier suscription	Unidad	200
3	SVS-XDR-SUP-P Cisco support signature for XDR	AÑO	1
4	Horas de especialista para integración, configuración y puesta en operación de Cisco Secure Endpoint Premier y Cisco XDR Advantage	Hora	30

4. NORMATIVIDAD APLICABLE

- Ley 1273 de 2009, Por medio de la cual se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales y las disposiciones que la reglamentan.
- Decreto 1360 de 1989 por el cual se reglamenta la inscripción de soporte lógico (software) en el registro nacional del derecho de autor
- CONPES 3995 de Julio 1 de 2020. Política Nacional de Confianza y Seguridad Digital.
- MANUAL DE COMPUTACIÓN EN LA NUBE. Febrero 2021. Consejería Presidencial para asuntos económicos y transformación digital.
- MINTIC. Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad de la información – MSPI, como habilitador de la Política de Gobierno Digital, cuyo Anexo 1 fue actualizado mediante la Resolución MinTIC 02277 del 3 de junio de 2025
- Decreto 767 de 2022. “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Directiva Presidencial 2 de 2022. Reiteración de la política pública en materia de seguridad digital.
- Decreto 1078 de 2015. “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- Decreto 338 de 2022, por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto 1078 de 2015 y se establecen lineamientos generales para fortalecer la gobernanza de la seguridad digital.
- Como referentes técnicos se aplicarán ISO/IEC 27001:2022, ISO/IEC 27002:2022 y las guías vigentes del Modelo de Seguridad y Privacidad de la Información (MSPI), en lo pertinente al alcance contractual.
-

5. ESPECIFICACIONES TÉCNICAS DEL BIEN O SERVICIO.

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

En la actualidad, con la evolución de la tecnología, los ciberdelincuentes han incrementado la cantidad y sofisticación de los ataques, generando amenazas cada vez más complejas y difíciles de detectar mediante herramientas de seguridad que operan de manera aislada. En este contexto, la solución de seguridad EDR opera bajo un esquema de servicio basado en la nube (SaaS), permitiendo el monitoreo centralizado de la actividad de los *endpoints* mediante el análisis y clasificación de datos, con el fin de ejecutar acciones de prevención, detección, contención y respuesta, prevenir infracciones, bloquear *malware* desde el punto de entrada y analizar continuamente la actividad de archivos que puedan representar amenazas.

Así mismo, se requiere escalar el licenciamiento de EDR a Cisco Secure Endpoint Premier, con el fin de robustecer la protección del Ministerio frente a ataques modernos y persistentes mediante funcionalidades propias de este nivel, tales como Talos Threat Hunting, que permite la búsqueda proactiva de amenazas sobre la telemetría de los *endpoints*, así como las capacidades avanzadas de EDR y su integración nativa con la plataforma Cisco XDR.

De igual forma, se requiere la incorporación de la plataforma Cisco XDR Advantage, con integración nativa a las suscripciones de Cisco Umbrella, Cisco Duo, Cisco ISE y Cisco Secure Endpoint actualmente implementadas en producción en el Ministerio, con el propósito de consolidar y correlacionar la telemetría proveniente de diferentes vectores de seguridad, facilitando una visión integral de los eventos, amenazas e incidentes y contribuyendo a reducir los tiempos de detección, análisis y respuesta frente a amenazas complejas y multivectoriales.

En atención a la incorporación de la plataforma Cisco XDR y a la necesidad de garantizar su adecuada integración y operación, se requiere contar con servicios especializados que permitan realizar las actividades técnicas necesarias para su puesta en funcionamiento y posterior administración. En este sentido, se contempla la contratación de horas de especialista para realizar la configuración, parametrización, integración nativa entre Cisco Secure Endpoint Premier y Cisco XDR Advantage, validación de los flujos de información, ejecución de pruebas funcionales, ajustes técnicos, documentación y transferencia de conocimiento al personal técnico designado por la Entidad.

Por lo anterior, el Ministerio requiere adquirir la renovación del licenciamiento de la plataforma de seguridad EDR (Endpoint Detection and Response), con actualización del licenciamiento de Cisco Secure Endpoint a nivel Premier; adquirir el licenciamiento de la plataforma Cisco XDR Advantage y el servicio de soporte asociado; y contratar las horas de especialista requeridas para la integración de Cisco XDR con la plataforma nativa EDR Cisco Secure Endpoint Premier, de acuerdo con las especificaciones técnicas establecidas en la presente Ficha.

A continuación, se detallan las cantidades estimadas de los bienes y servicios requeridos por el Ministerio:

Ítem	Descripción	Unidad de Medida	Cantidad
Suscripcion Cisco Secure Endpoint premier EDR Premier			
1	AMP4E-PRE-CL-LIC , Cisco Secure Endpoint premier Tier Suscription	Unidad	1.020

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

Suscripción Cisco XDR Advantage Tier (análisis de datos de endpoint, web, correo y red)			
2	XDR-ADV Cisco XDR Advantage tier suscripción	Unidad	200
3	SVS-XDR-SUP-P Cisco support signature for XDR	AÑO	1
4	Horas de especialista para integración, configuración y puesta en operación de Cisco Secure Endpoint Premier y Cisco XDR Advantage	Hora	30

El contratista entregará la documentación propia de la renovación de la suscripción (documento de licenciamiento) tal como la suministre el fabricante del software CISCO-EDR (ENDPOINT DETECTION AND RESPONSE) con actualización a licenciamiento Secure Endpoint Premier y adquisición del licenciamiento de la plataforma Cisco XDR con integración nativa a la solución Cisco Secure Endpoint, dentro de los primeros diez (10) días de ejecución del contrato.

El Licenciamiento y los servicios especializados requeridos tendrán una vigencia de un (1) año a partir de la renovación y adquisición.

NOTA1 : En caso de que la renovación o actualización del licenciamiento incluya nuevas funcionalidades propias de las soluciones Cisco Secure Endpoint Premier o Cisco XDR Advantage, diferentes de las descritas en el numeral 5 de la presente Ficha de Especificaciones y Condiciones Técnicas, y se requiera su implementación, configuración o parametrización para su puesta en funcionamiento, estas actividades deberán ser realizadas por el contratista sin generar costos adicionales para el Ministerio, siempre que correspondan a funcionalidades incluidas dentro de las suscripciones adquiridas y se encuentren dentro del alcance técnico contratado.

NOTA2: El oferente deberá presentar, junto con su oferta, carta suscrita por el representante legal en la cual manifieste que cuenta con el recurso humano requerido para la prestación de los servicios especializados objeto del presente proceso, de conformidad con los perfiles, requisitos de formación académica, experiencia, conocimientos y certificaciones establecidos en la presente Ficha de Especificaciones y Condiciones Técnicas.

Las hojas de vida y los documentos que acrediten la formación académica, experiencia, conocimientos técnicos y certificaciones vigentes expedidas por el fabricante, cuando estas sean requeridas para el rol correspondiente, serán verificados por el supervisor del contrato al inicio de la ejecución contractual.

En caso de requerirse durante la ejecución del contrato el cambio de alguno de los profesionales asignados a la prestación de los servicios, el contratista deberá informar previamente al supervisor del contrato y presentar para su aprobación la hoja de vida y los documentos que acrediten el cumplimiento de los requisitos exigidos para el profesional que realizará el reemplazo. El profesional propuesto deberá acreditar condiciones de formación académica,

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

experiencia, conocimientos y certificaciones iguales o superiores a las exigidas para el profesional inicialmente presentado.

La documentación correspondiente deberá ser remitida al supervisor del contrato con una antelación no inferior a cinco (5) días hábiles a la fecha prevista para el reemplazo, salvo situaciones excepcionales debidamente justificadas.

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 malware polimórfico:	Soportar detección de variantes o malware polimórfico mediante huellas digitales sueltas.
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

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

	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 debe 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 ejecutar 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

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

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.

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

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.

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

	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	
Análítica 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

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

		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

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

integración con plataformas no nativas	El contratista dispondrá de treinta (30) horas de servicios especializados para realizar integraciones no nativas de Cisco XDR con plataformas de terceros compatibles. Estas horas se destinarán prioritariamente a la integración con Microsoft Office 365 , y el firewall perimetral del Ministerio, firewall fortinet, de acuerdo con las capacidades técnicas y las restricciones del fabricante. Las integraciones nativas de Cisco XDR que resulten aplicables al entorno tecnológico del Ministerio deberán implementarse como parte de la solución contratada, de acuerdo con las capacidades del fabricante.
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 priorización de 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

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

	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.

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

	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”.
Configuración y Parametrización de acuerdo con los lineamientos del Ministerio de Justicia.	Realizar la afinación 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 asesoría 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

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

	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 afinamiento 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

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

	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

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

	la transferencia de conocimiento al personal técnico designado por la Entidad.
--	--

El contratista debe ser distribuidor autorizado en Colombia y estar facultado por el fabricante para vender, renovar, instalar y brindar soporte técnico, así como cumplir con las garantías del licenciamiento del software EDR y XDR. Dicha certificación deberá encontrarse vigente a la fecha de cierre del proceso de selección y el contratista deberá garantizar el mantenimiento de esta condición durante la ejecución y hasta la liquidación del contrato, cuando a ello haya lugar.

El proponente deberá presentar una certificación expedida por el fabricante Cisco, o por su representante autorizado en Colombia, que lo acredite como **Partner del portafolio de Cisco en la designación específica: Security Partner** y como **Partner Preferido de Cisco en la designación: Partner Preferido de Cisco Services**, que están dentro del marco del Programa Cisco 360 Partner.

La anterior información fue consultada en el sitio web del fabricante en el siguiente URL :*consultada el 10/09/2026* : <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m10/cisco-unveils-new-cisco-360-partner-program-to-accelerate-value-and-innovation-launching-in-2026.html>

La certificación debe ser expedida en una fecha no superior a treinta (30) días calendario anterior a la fecha de cierre del proceso.

5.6. PERFILES PROFESIONALES REQUERIDOS

Perfil	Formación académica	Experiencia solicitada	Disponibilidad requerida
Especialista en integración de soluciones EDR/XDR	Profesional en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ciberseguridad o áreas afines. Deberá acreditar certificación vigente del fabricante Cisco relacionada con tecnologías de seguridad, EDR, XDR, Cisco Secure Endpoint, Cisco XDR o	Mínimo dos (2) años de experiencia en implementación, configuración, administración y/o integración de soluciones EDR/XDR. Deberá acreditar experiencia específica en actividades de integración de plataformas de	Disponibilidad para ejecutar las treinta (30) horas de especialista contratadas para el Ítem 4 , de acuerdo con el cronograma de actividades concertado con el supervisor del contrato.

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

	equivalente, de acuerdo con el alcance del servicio.	seguridad , en soluciones Cisco Security.	
--	--	---	--

Los perfiles profesionales establecidos corresponden a las capacidades mínimas que deberá disponer el contratista para la ejecución de los servicios especializados objeto de la contratación. La cantidad de profesionales que el contratista destine para la prestación de los servicios será determinada por este de acuerdo con su modelo operativo y las necesidades de ejecución, siempre que garantice el cumplimiento integral de las obligaciones, actividades y Acuerdos de Nivel de Servicio (ANS) establecidos en la presente ficha.

El contratista deberá disponer del especialista que cumpla con el perfil requerido para la ejecución de las treinta (30) horas contratadas, destinadas a las actividades de integración, configuración, parametrización, validación, pruebas, documentación y transferencia de conocimiento.

5.7. TIEMPOS DE RESPUESTA, ATENCIÓN Y SOLUCIÓN

5.7.1. ANS para el soporte técnico asociado al licenciamiento – Ítem 3

Prioridad	Detalle	Tiempo de Respuesta	Tiempo de Solución
Crítico	Falla de la plataforma que hace imposible administrar la plataforma EDR y XDR Requiere atención virtual o visita en sitio.	1 hora	3 horas
Alto	Problema de amenazas de gran impacto donde continúa operando la plataforma EDR y XDR, pero de una manera imperfecta; impacto significativo para el MINISTERIO DE JUSTICIA Y DEL DERECHO, amenaza aspectos de Seguridad futura. Requiere atención virtual o visita en sitio	2 horas	4 horas
Medio	La plataforma EDR y XDR continúa funcionando con impedimentos menores. Las tareas pueden continuar con una mínima disminución de performance. Requiere atención virtual o visita en sitio	4 horas	8 horas
Bajo	Consulta técnica y/o de uso. Las tareas se desarrollan normalmente.	8 horas	16 horas
Planificado	Implementación de una solicitud de cambios que no es requerida de manera urgente. Las tareas se desarrollan normalmente.	Planificado	Planificado

El contratista será responsable del cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos contractualmente y deberá gestionar el acompañamiento y respaldo del fabricante cuando resulte necesario para la atención y solución de los incidentes. La intervención del fabricante no exime al contratista de su responsabilidad contractual frente al Ministerio de Justicia y del Derecho

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

En caso de que el contratista incumpla los tiempos de respuesta, atención, escalamiento, solución, continuidad o disponibilidad establecidos en los Acuerdos de Nivel de Servicio (ANS) definidos en el presente numeral, el Ministerio de Justicia y del Derecho evaluará, de acuerdo con las condiciones contractuales y la normatividad aplicable, la procedencia de las actuaciones administrativas y/o medidas a que haya lugar.

6. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA.

1. Tramitar y entregar a nombre del Ministerio de Justicia y del Derecho, dentro de un término no mayor a cinco (5) días hábiles contados a partir del inicio de la ejecución del contrato, los documentos que acrediten la renovación y activación del licenciamiento de Cisco Secure Endpoint Premier, la adquisición y activación del licenciamiento de Cisco XDR Advantage, así como los documentos correspondientes al soporte asociado al licenciamiento y demás elementos contratados, de conformidad con las especificaciones técnicas establecidas en el formato F-GC-04-38 Ficha de Especificaciones y Condiciones Técnicas (FECT).
2. Realizar un cronograma que incluya las actividades y tiempo de ejecución de la renovación y puesta en marcha/entrega de los diferentes elementos del contrato y fechas de transferencia de conocimiento, el cual deberá ser entregado al supervisor del contrato dentro de los cinco (5) días hábiles siguientes al perfeccionamiento del contrato.
3. Cumplir con las condiciones técnicas, actividades, lineamientos y estándares definidos en el formato F-GC-04-38 Ficha de especificaciones y condiciones técnicas (FECT).
4. Garantizar la disponibilidad de los recursos humanos necesarios para la correcta ejecución de las actividades contratadas, de acuerdo con los perfiles profesionales, formación académica, experiencia, certificaciones y demás requisitos establecidos en el formato F-GC-04-38 Ficha de especificaciones y condiciones técnicas (FECT).
5. Realizar las actividades de integración, configuración, administración, parametrización y afinamiento necesarias para la adecuada interoperabilidad y operación conjunta de las plataformas Cisco Secure Endpoint Premier (EDR) y Cisco XDR Advantage, de acuerdo con las especificaciones técnicas establecidas en la Ficha Técnica. El servicio deberá incluir la integración con las herramientas de seguridad y fuentes de telemetría de la Entidad y las especificaciones técnicas requeridas; bajo la aprobación del supervisor del contrato.
6. Gestionar, implementar y verificar las integraciones y fuentes de telemetría requeridas para el adecuado funcionamiento de las capacidades de monitoreo, análisis, correlación y respuesta de Cisco XDR Advantage, incluyendo las integraciones nativas con las soluciones de seguridad Cisco disponibles en la infraestructura institucional que resulten aplicables al Ministerio, así como las integraciones no nativas con plataformas de terceros técnicamente compatibles con Cisco XDR Advantage. Para estas últimas, se dispondrá de treinta (30) horas de servicios especializados. Lo anterior se realizará de acuerdo con las capacidades técnicas de la solución y las restricciones del fabricante
7. En caso de presentarse un cambio de infraestructura tecnológica, arquitectura o condiciones técnicas que afecten la operación de las soluciones EDR/XDR, realizar las actividades necesarias para su adecuación y

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

continuidad operativa, incluyendo la configuración, soporte y afinamiento de las políticas de la consola de administración, así como la reinstalación, configuración y puesta en funcionamiento de la consola de administración y/o de los agentes en todos los equipos (estaciones de trabajo y servidores) de las diferentes sedes del Ministerio de Justicia y del Derecho, ubicadas en Calle 53 # 13 – 27 Chapinero, Carrera 9 # 12 C – 10 Centro y Carrera 27 # 15 – 85 Paloquemao, o en aquellas donde se encuentren ubicadas o sean trasladadas las sedes del Ministerio en la ciudad de Bogotá D.C., durante la vigencia contractual

8. Realizar la transferencia de conocimiento técnico en las condiciones establecidas en la presente Ficha Técnica, dirigida al personal que sea designado por el Ministerio de Justicia y del Derecho, sobre la administración de las consolas, configuración, parametrización y afinamiento de políticas, generación de informes, gestión de alertas y tratamiento de amenazas, así como sobre las integraciones realizadas en desarrollo del contrato.
9. Prestar soporte técnico y asistir al personal de soporte técnico del Ministerio de Justicia y del Derecho sobre consultas de implementación, administración, configuración, afinamiento operación y uso de las plataformas Cisco EDR Secure Endpoint Premier y Cisco XDR Advantage.
10. Cumplir los Acuerdos de Nivel de Servicio (ANS) establecidos en el formato F-GC-04-38 Ficha de especificaciones y condiciones técnicas (FECT) que resulten aplicables a cada uno de los servicios contratados.
11. Brindar acompañamiento técnico, gestionar el escalamiento de los casos ante el fabricante Cisco cuando se requiera y efectuar el seguimiento correspondiente hasta la atención y/o solución del caso, de acuerdo con las condiciones del soporte y licenciamiento contratado, sin que la intervención del fabricante exima al contratista de su responsabilidad contractual frente al Ministerio de Justicia y del Derecho.
12. Realizar mantenimiento preventivo y correctivo, dentro del alcance de los servicios contratados, sobre las configuraciones y componentes administrables de las plataformas EDR/XDR, así como efectuar los ajustes necesarios para mantener su adecuada operación, disponibilidad y desempeño durante la vigencia contractual.
13. Garantizar que el personal del contratista que deba realizar actividades de manera presencial en las instalaciones del Ministerio se encuentre debidamente identificado (carnetizado) y cumpla con las normas y procedimientos de bioseguridad, ingreso y permanencia establecidos por la Entidad, así como con las obligaciones legales aplicables en materia de seguridad social y demás disposiciones correspondientes, conforme a la normatividad vigente en los casos de soporte en sitio.
14. Responder por las intervenciones, configuraciones, parametrizaciones o ajustes realizados de manera incorrecta que afecten el funcionamiento de las plataformas objeto del contrato y, en consecuencia, realizar oportunamente los ajustes y acciones correctivas a que haya lugar, sin generar costos adicionales para el Ministerio cuando la situación sea imputable al contratista.
15. Cumplir las instrucciones impartidas por el funcionario encargado del control y vigilancia del contrato y las demás que sean inherentes al objeto de la contratación.
16. Todas las demás inherentes o necesarias para la correcta ejecución del objeto contractual.

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

7. CONDICIONES GENERALES

A continuación, se detallan las condiciones del servicio en caso de que el Ministerio decida adelantar el proceso de contratación de la presente necesidad. Este desglose tiene como objetivo proporcionar información integral que le permita considerar todas las variables que podrían influir al estructurar y enviar la cotización.

7.1. LUGAR DE EJECUCIÓN:

Las actividades contractuales se ejecutarán principalmente de manera remota, teniendo en cuenta que el objeto del contrato comprende la renovación del licenciamiento de la plataforma de seguridad EDR (**Endpoint Detection and Response**), con actualización a **Cisco Secure Endpoint Premier**, la adquisición del licenciamiento de **Cisco XDR Advantage**, y la integración de dichas plataformas con las soluciones y fuentes de información definidas por la Entidad, . La operación de las plataformas se realiza principalmente bajo un esquema remoto/virtual

No obstante, cuando se requiera, el contratista deberá prestar 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, para atender actividades de soporte técnico, configuración, afinamiento o acompañamiento.

7.2. PLAZO DE EJECUCIÓN:

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.

7.3. FORMA DE PAGO:

El Ministerio pagará al Contratista seleccionado el valor del contrato así:

Un unico pago correspondiente al valor de la renovación de la suscripción, soporte y servicios de personal especializados (Ítems 1,2,3 y 4), una vez cumpla a satisfacción con la entrega de la documentación y activación que certifica la renovación del licenciamiento de la solución ofertada mediante suscripción y su integración con las herramientas existentes en el ministerio.

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

Para proceder al pago, deberá aportarse la siguiente documentación:

- Factura de cobro.
- Documentos que avalen el licenciamiento mediante suscripción por un (1) año de acuerdo con las Especificaciones Técnicas establecidas en el formato F-GC-04-38 Ficha de especificaciones y condiciones técnicas (FECT).
- Certificación del revisor fiscal o representante legal según corresponda, sobre el cumplimiento en el pago de los aportes parafiscales y de seguridad social de sus empleados de acuerdo con lo establecido en el artículo 50 de la Ley 789 de 2002 y artículo 23 de la Ley 1150 de 2007.

Los impuestos, tasas, contribuciones y retenciones que surjan del presente contrato serán cubiertos por el contratista, para cuyos efectos se harán las retenciones del caso y se cumplirán las obligaciones fiscales que ordene la normatividad vigente

PARÁGRAFO: La Entidad solamente reconocerá y pagará al contratista, los valores que resulten de los productos efectivamente recibidos a satisfacción por la Entidad. Si las cuentas de cobro o facturas, según sea el caso, no han sido bien elaboradas o no se acompañan de los documentos que las respalden, los términos solo empezarán a contarse desde la fecha en que quede corregida, o desde aquella en que se haya aportado el último de los documentos. Las demoras que se presenten por estos conceptos serán de responsabilidad exclusiva del CONTRATISTA, quien no tendrá por ello derecho al pago de intereses o compensación de ninguna naturaleza.

El pago antes señalado se realizará dentro de los cuarenta y cinco (45) días hábiles siguientes a la presentación de la factura y con sujeción al PAC y a la ubicación de fondos en la Tesorería del MINISTERIO de tal manera que la entidad no asume responsabilidad alguna por la demora que pueda presentarse en dichos pagos y, por lo tanto, el contratista cumplirá con sus obligaciones y no podrá aducir como justificación alguna para su no realización, demora en el pago.

El MINISTERIO efectuará las retenciones que en materia tributaria tenga establecida la Ley y respecto de las cuales sea su obligación efectuar la retención. En los demás casos, el contratista deberá cumplir con el pago de los impuestos, tasas o contribuciones que se deriven de la presente contratación.

Asimismo, deberán ser tramitadas por el contratista, las devoluciones o exenciones a que crea tener derecho ante la respectiva Administración de Impuestos, sin responsabilidad alguna por parte del MINISTERIO o costo para ella.

Nota 7: En caso de que el proveedor se encuentre obligado a facturar electrónicamente deberá aportar factura electrónica de acuerdo con lo establecido por la DIAN, este será requisito para el pago del respectivo contrato. Todas las facturas electrónicas para su reconocimiento tributario deberán ser validadas previo a su expedición, por la Dirección de Impuestos y Aduanas Nacionales (DIAN) o por un proveedor autorizado por esta. La factura electrónica solo se entenderá expedida cuando sea validada por el proveedor autorizado.

	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

Nota 8: FACTURA ELECTRÓNICA SIN VALIDACIÓN PREVIA: en estos casos, la factura se entenderá expedida con la entrega al adquirente y deberá ser enviada a la Dirección de Impuestos y Aduanas Nacionales (DIAN) o proveedor autorizado para su validación dentro de las 48 horas siguientes contadas a partir del momento en que se solucionen los problemas tecnológicos.

Los pagos antes señalados se realizarán con sujeción al PAC y a la ubicación de fondos en la Tesorería del Ministerio de Justicia y del Derecho de tal manera que el Ministerio no asume responsabilidad alguna por la demora que pueda presentarse en dichos pagos y, por lo tanto, el Contratista cumplirá con sus obligaciones y no podrá aducir como justificación alguna para su no realización, demora en el pago.

7.4. POSIBLES GARANTÍAS QUE SERÁN REQUERIDAS:

A continuación, se mencionan las garantías que deberá adquirir, solo en caso de llegar a ser el contratista, igualmente pueden variar o sufrir cambios en el proceso de contratación, luego de la verificación legal.

AMPARO	%	VIGENCIA
<i>Cumplimiento del Contrato</i>	<i>20 % del valor total del contrato</i>	Plazo del contrato y doce (12) meses más, contados a partir de la fecha de suscripción del contrato.
<i>Calidad del servicio</i>	<i>20 % del valor total del contrato</i>	<i>Plazo del contrato y doce (12) meses más, contados a partir de la fecha de suscripción del contrato.</i>
<i>Pago de salarios, prestaciones sociales legales e indemnizaciones laborales</i>	<i>5 % del valor total del contrato</i>	<i>Plazo del contrato y treinta y seis (36) meses más, contados a partir de la fecha de suscripción del contrato.</i>

7.5. MATRIZ DE RIESGOS

El Ministerio de Justicia y del Derecho elaboró el formato F-GC-04-37, que corresponde a la Matriz para la Identificación y Cobertura del Riesgo en los Procesos de Contratación. El propósito de este formato es comunicar de manera detallada los riesgos previsibles que podrían afectar el desarrollo normal de las actividades establecidas en esta Ficha de Especificaciones y Condiciones Técnicas.

Es necesario indicarles a las empresas interesadas que es obligatorio revisar este formato para una adecuada estructuración de su oferta o cotización. Además, facilita la elaboración de planes de contingencia y acciones que debe implementar para administrar los riesgos que le son asignados al contratista de tal forma que se garantice el cumplimiento efectivo del objeto contractual.

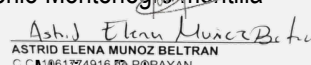
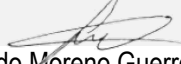
	FICHA DE ESPECIFICACIONES Y CONDICIONES TÉCNICAS (FECT)	Código: F-GC-04-38
		Versión: 02
		Fecha: 23/02/2024

El formato F-GC-04-37, que corresponde a la Matriz para la Identificación y Cobertura del Riesgo en los Procesos de Contratación se elaboró de acuerdo con la metodología propuesta por Colombia Compra Eficiente (CCE) detallada en el "Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación".

8. ANEXOS

Anexo 1. Formato F-GC-04-37 matriz para la identificación y cobertura del riesgo en los procesos de contratación.

9. APROBACIONES

PARTICIPACIÓN	NOMBRE	DEPENDENCIA
ELABORÓ	Jose Eliberto Fonseca Ruiz 	Subdirección de Tecnologías y Sistemas de Información
	John Antonio Montenegro Montilla 	
	 ASTRID ELENA MUÑOZ BELTRÁN C.C. 196174056 DE BOGOTÁ Astrid Elena Muñoz Beltrán	
REVISÓ	Jairo Armando Moreno Guerrero 	Subdirección de Tecnología y Sistemas de Información
APROBÓ	 Enrique farfan ruiz	Subdirección de Tecnología y Sistemas de Información