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

FECHA: 06/03/2026
AREA SOLICITANTE: Subdirección de Tecnología y Sistemas de Información

1. OBJETO

Adquirir la renovación de los servicios por suscripción de las plataformas Umbrella, DUO y Proxy, con el fin de asegurar la continuidad del servicio de **seguridad** en la navegación web, seguridad de identidad y protección frente a amenazas en la nube, fortaleciendo la ciberseguridad institucional.

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

Clasificación UNSPSC	Segmento	Familia	Clase	Producto
43233200	43 – Difusión de Tecnologías de Información y Telecomunicaciones	4323 - Software	432332 – Software de seguridad y protección	43233200 – Software de seguridad y protección
81111800	81 - Servicios basados en ingeniería, investigación y tecnología	8111 - Servicios Informáticos	811118 - Servicios de sistemas y administración de componentes de sistemas	81111800 – Servicios de sistemas y administración de componentes de sistemas

3. UNIDAD DE MEDIDA

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

ítem	Descripción	cantidad	Tiempo
1	Cisco Duo Advantage edition (formerly Access)	650	1 año
2	Cisco Umbrella Secure Internet Gateway Advantage + Enhanced Support for Umbrella.	650	1 año
3	Configuración y parametrización de los productos	50 Horas	1 año
4	Soporte técnico reactivo	100 Horas	1 año

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 1581de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales y las disposiciones que la reglamentan.
- 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 como habilitador de la Política de Gobierno Digital.
- 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".

5. ESPECIFICACIONES TÉCNICAS DEL BIEN O SERVICIO.

Según lo indicado en el boletín de COLCERT con fecha del 16 de enero de 2026[1] , se evidencia que: "Durante la semana analizada, el panorama de ciberseguridad en Colombia evidencia una intensificación relevante de los vectores de ataque dirigidos a la identidad digital y al acceso remoto. Amenazas como Tycoon 2FA, EvilProxy y Sneaky 2FA se consolidan como los principales riesgos, registrando incrementos significativos en su actividad frente al periodo anterior. Este comportamiento refleja campañas agresivas y sostenidas orientadas a la evasión de mecanismos de autenticación (MFA), orientadas al compromiso de credenciales corporativas. A este escenario se suma la aparición abrupta de XWorm lo que sugiere un entorno de amenazas altamente dinámico, con actores enfocados tanto en el acceso inicial como en el establecimiento de persistencia dentro de redes organizacionales."

NOTA: Tycoon 2FA, modalidad *phishing as a service*, que emplea páginas falsas para suplantar portales legítimos y capturar credenciales y códigos de autenticación; EvilProxy, herramienta que opera mediante un proxy inverso entre la víctima y el servicio real para interceptar información de acceso; Sneaky 2FA, kit que automatiza campañas orientadas a evadir la autenticación de doble factor (2FA), y XWorm es un troyano de acceso remoto (RAT)

Ante la evolución de los ataques cibernéticos que a diario se generan desde Internet, desde la plataforma tecnológica se cuenta con diversos recursos para la protección de la información, la cual es uno de los activos más valiosos con el que cuenta el Ministerio para su operación y gestión. Desde esta óptica y de acuerdo con las premisas de Seguridad de la Información, es necesario mantener el acceso seguro, la confidencialidad, integridad y disponibilidad de los servicios de información del MJD.

Por lo anterior, en atención a los requerimientos de seguridad digital establecidos por la Entidad, y conforme a las especificaciones técnicas descritas en la presente ficha, se requiere la implementación de herramientas que fortalezcan los mecanismos de protección institucional.

[1] Tomado de: https://www.colcert.gov.co/800/articles-425947_COLCERT_RS_20260116_021_Reporte_semanal_Inteligencia_de_Amenazas_Ciberneticas.pdf

Cisco Umbrella es una solución de seguridad flexible en la nube, la cual combina múltiples funciones de seguridad en una sola solución, por lo que puede extender la protección a dispositivos, usuarios remotos y ubicaciones distribuidas en cualquier lugar.

En primer lugar, se contempla la solución de autenticación multifactor basada en tecnología ZTNA (Zero Trust Network Access), la cual permite establecer políticas precisas de acceso, verificar de forma continua la identidad de usuarios y dispositivos, y mitigar riesgos asociados a accesos no autorizados, conforme a los lineamientos de seguridad y privacidad definidos por el Ministerio. Adicionalmente, se incluye el componente de Control de Navegación y Acceso Seguro a la Nube (CASB), que proporciona visibilidad, gestión y aplicación de políticas sobre el uso de aplicaciones y servicios en la nube, permitiendo detectar y bloquear actividades riesgosas, independientemente del lugar desde donde se acceda, en concordancia con la estrategia de seguridad digital y la normativa vigente. además de la seguridad de la capa DNS y la inteligencia de amenazas interactivas (Cisco Talos Group), Cisco Umbrella también incluye una puerta de secure web gateway, un firewall y una funcionalidad de agente de seguridad de acceso a la nube (CASB), además de la integración con Cisco SD-WAN, entregada desde un único servicio de seguridad en la nube. Con esto se protege las computadoras, tabletas y smartphones desde la capa DNS (Domain Name System) bloqueando las solicitudes a dominios maliciosos incluso antes de que se establezca una conexión, deteniendo las amenazas a través de cualquier puerto o protocolo antes de que lleguen la red[2].

En este contexto, se hace necesaria la renovación de las suscripciones a las plataformas Cisco Umbrella y Cisco Duo, soluciones que han sido previamente implementadas en la Entidad

En el marco de la estrategia de seguridad digital de la Entidad, es pertinente precisar que las soluciones Cisco Umbrella y Cisco Duo cumplen funciones complementarias .

Por una parte, **Cisco Duo** está orientado a la protección de la **identidad digital**, mediante la verificación robusta de usuarios y dispositivos antes de conceder el acceso a aplicaciones y recursos institucionales. Su enfoque se basa en

2

el principio de confianza cero (Zero Trust), incorporando autenticación multifactor (MFA), validación de postura de seguridad del dispositivo y controles de acceso adaptativos que reducen significativamente el riesgo de compromiso de credenciales.

Por otra parte, **Cisco Umbrella** proporciona protección frente a amenazas provenientes de Internet, actuando principalmente en las capas de DNS, web y aplicaciones en la nube. Esta solución permite bloquear conexiones hacia dominios maliciosos, prevenir descargas de contenido peligroso, aplicar políticas de navegación, habilitar funciones de firewall en la nube y ofrecer visibilidad sobre el uso de servicios SaaS.

En consecuencia, mientras Duo protege quién y desde dónde se accede, Umbrella protege a dónde se conectan los usuarios y qué contenido consumen, constituyéndose en controles complementarios y necesarios para la reducción integral de la superficie de ataque.

La Entidad requiere específicamente la suscripción **Cisco Umbrella Secure Internet Gateway (SIG) Advantage** junto con el esquema de soporte del fabricante, debido a que este nivel de licenciamiento integra en un único servicio capacidades avanzadas de:

- Seguridad DNS.
- Secure Web Gateway (SWG).
- Firewall como servicio (FWaaS).
- Funcionalidades CASB.
- Inteligencia de amenazas provista por Cisco Talos.

La adquisición de estos componentes de manera unificada garantiza interoperabilidad nativa, administración centralizada, correlación de eventos de seguridad y una postura de protección consistente para todos los usuarios, tanto en red interna como en trabajo remoto.

La contratación individual de funcionalidades generaría fragmentación operativa, mayores esfuerzos de integración, incremento en tiempos de respuesta ante incidentes y posibles brechas en la cobertura de seguridad, situación que contraviene los principios de eficiencia, integralidad y gestión del riesgo que rigen la arquitectura tecnológica del Ministerio.

Adicionalmente, el soporte directo asociado al licenciamiento asegura acceso a actualizaciones, acompañamiento especializado del fabricante, escalamiento oportuno de incidentes y mantenimiento de la vigencia tecnológica de la plataforma.

5.1 Especificaciones Técnicas

ESPECIFICACIONES TÉCNICAS DE LA HERRAMIENTA

DATOS DE FABRICACIÓN	**CONDICIONES**
Cantidad Licencias	650
Herramienta	Cisco Umbrella
Marca	CISCO
Tipo Licencia	Cisco Umbrella Secure Internet Gateway Advantage
Condiciones generales de las licencias	
Capa de Seguridad DNS	• La suscripción debe poder intervenir en las solicitudes de DNS para evitar que se hagan solicitudes a sitios peligrosos o con potenciales amenazas, así como también: • Permitir la visibilidad necesaria para proteger el acceso a Internet en todos los dispositivos de red, ubicaciones de oficina y usuarios de trabajo fuera de la red. • Generar informes detallados de la actividad DNS por tipo de amenaza a la seguridad o contenido web y la acción realizada • Dar la posibilidad de conservar registros de toda la actividad tanto tiempo como sea necesario • Permitir una rápida implantación en miles de ubicaciones y usuarios para proporcionar un retorno inmediato de la inversión.
Secure Web Gateway	• Incluir un proxy completo basado en la nube que pueda registrar e inspeccionar todo el tráfico web para una mayor transparencia, control y protección. Utilizando túneles IPSec, archivos PAC y proxy para reenviar el tráfico y obtener una visibilidad total, controles a nivel de URL y aplicación, y protección y protección avanzada frente a amenazas. Además: • Filtrar contenidos por categoría o URL específicas para bloquear destinos que infrinjan las políticas o las normativas de cumplimiento • Tener la capacidad de escanear de manera eficiente todos los archivos cargados y descargados de malware y otras amenazas mediante un motor de búsqueda de amenazas seguro y confiable. • Poder bloquear tipos de archivos (por ejemplo, bloquea la descarga de archivos .exe) • Estar en capacidad de hacer descifrado SSL completo o selectivo para proteger aún más su organización de ataques ocultos e infecciones que consumen mucho tiempo • Poder generar informes detallados con direcciones URL completas, identidad de red, acciones permitidas o acciones permitidas o bloqueadas, además de la dirección IP externa
Prevención de Pérdida de Información	• Analizar los datos sensibles en línea para proporcionar visibilidad y control sobre los datos confidenciales que salen de la organización. Incluir: • Incluir más de 80 clasificadores de contenido integrados, incluidos PII, PCI y PHI • Incluir clasificadores de contenido integrados personalizables con umbral y proximidad para ajustar y reducir los falsos positivos

	• Poder generar diccionarios definidos por el usuario con frases personalizadas (como nombres de códigos de proyectos) • Detectar y generar informes sobre el uso de datos confidenciales e informes detallados para ayudar a identificar el uso indebido • Poder inspeccionar el contenido de las aplicaciones en la nube y del tráfico web y aplicación de políticas de datos
Cloud Access Security Broker (CASB)	• Detectar, informar y crear alertas sobre las aplicaciones en la nube en uso. Permitir que esta información ayude a gestionar la adopción de la nube, reduzca el riesgo y bloquee el uso de aplicaciones en la nube ofensivas, inapropiadas o riesgosas y, permita bloquear el uso de aplicaciones, También debe: • Generar informes sobre la categoría del proveedor, el nombre de la aplicación y el volumen de actividad de cada aplicación descubierta • Dar detalles de la aplicación e información sobre riesgos, como la puntuación de reputación web, viabilidad financiera y certificaciones de cumplimiento pertinentes • Detectar malware en la nube para detectar y eliminar malware de aplicaciones de almacenamiento de archivos en la nube y garantizar que las aplicaciones permanezcan libres de malware. • Tener la capacidad para bloquear/permitir aplicaciones específicas en la nube • Restringir Tenants para controlar la(s) instancia(s) de aplicaciones SaaS a las que pueden acceder todos los usuarios o grupos/individuos específicos
Firewall en la Nube	• Proporcionar un Firewall en nube que proporcione visibilidad y control para el tráfico no web que se origina a partir de solicitudes dirigidas a Internet, en todos los puertos y protocolos. Además: • Permitir el despliegue, gestión y generación de informes a través de un panel de control único y unificado • Generar políticas personalizables (IP, puerto, protocolo, aplicación y políticas IPS) • Poder ser un Firewall de capa 3 / 4 para registrar toda la actividad y bloquear el tráfico no deseado mediante reglas de IP, puerto y protocolo • Generar visibilidad y control de aplicaciones de Capa 7 para identificar miles de aplicaciones y bloquearlas/permitirlas. • Tener la capacidad de detectar y bloquear la explotación de vulnerabilidades
Información correlacionada sobre amenazas para mejorar la respuesta a incidentes	• Tener inteligencia de amenazas, también tener la capacidad para responder a incidentes. para responder a incidentes. Pueda aprovechar herramientas de inteligencias de amenazas para obtener inteligencia sobre dominios, IPs y malware a través de Internet, permitiendo: • Obtener una visibilidad más profunda de las amenazas con la visión más completa de Internet • Priorizar las investigaciones de incidentes

	• Acelerar la investigación y respuesta a incidentes • Predecir el origen de futuros ataques localizando y mapeando las infraestructuras de los atacantes • Exponer infraestructuras de los agresores
Administración	
Panel de Control	• Permita administrar la implementación desde un único panel de administración. Esto incluye configurar políticas DNS, revisar identidades de dispositivos, usuarios o grupos, generar informes y poder realizar un troubleshooting del paso a paso, que realiza la herramienta de seguridad. Generar informes y dar toda la visibilidad al administrador.

ESPECIFICACIONES TÉCNICAS HERRAMIENTA ZERO TRUST Y MULTIPLE FACTOR DE AUTENTICACIÓN	
DATOS DE FABRICACIÓN	**CONDICIONES**
Cantidad Licencias	650
Herramienta	Cisco Duo
Marca	CISCO
Tipo Licencia	Cisco Duo Advantage edition (formerly Access)
GENERALES	
Descripción	• Solución de zero trust network access (ZTNA) y de múltiple factor de autenticación multifactor (MFA). Agrega políticas y control sobre qué usuarios, dispositivos y redes pueden acceder a las aplicaciones de la entidad. Analiza el comportamiento del usuario, la ubicación y los parámetros del dispositivo y le brinda el poder de establecer políticas de autenticación más precisas. Esto le permite proteger mejor a sus usuarios sin molestarlos.
Características Técnicas de la licencia	
Política y control	• Reduce el riesgo aplicando políticas y controles precisos. Permita que su equipo defina y aplique reglas sobre quién puede acceder a qué aplicaciones y en qué condiciones. Defina políticas de acceso por grupo de usuarios y por aplicación para aumentar la seguridad sin comprometer la experiencia del usuario final.
Información del dispositivo	• Rastrea las versiones de sistemas operativos, navegadores y complementos como Flash y Java en los dispositivos que acceden a sus recursos protegidos y proporciona una vista resumida en la página de descripción general de Device Insight. Puede ver fácilmente cuántos dispositivos de acceso están desactualizados en toda la entidad.
Escritorio	• Amplia el control sobre qué dispositivos Windows y macOS pueden acceder a los recursos de la organización según la postura de seguridad del dispositivo. • Verifica el cumplimiento de un dispositivo con su política de confianza configurable durante el inicio de sesión y bloquea el acceso desde sistemas en mal estado, también mejora la

	información de los terminales disponible para los administradores con detalles adicionales sobre el dispositivo.
Monitor de confianza	• Descubre y supervisa el comportamiento de autenticación anómalo. Permite crear un perfil de riesgo personalizado para centrarse en las aplicaciones, los usuarios o las ubicaciones más importantes. Permite examinar los factores de riesgo detallados de los eventos para determinar cuáles son procesables para la entidad.
Autenticación basada en riesgos	• Permite Detectar y mitigar automáticamente patrones de ataque comúnmente conocidos y anomalías de alto riesgo para proporcionar un mayor nivel de seguridad.
Protección contra phishing push	• Evita que los atacantes eludan MFA utilizando autenticadores FIDO2 resistentes al phishing.
Single Sign-On (SSO)	• Permitir el inicio de sesión solo una vez para acceder a múltiples aplicaciones con Duo SSO
Administración	
Panel de Control	• Permita administrar la implementación desde un único panel de administración. Esto incluye configurar el inicio de sesión único, crear y administrar aplicaciones, inscribir y activar usuarios, emitir y administrar contraseñas de SMS y códigos de omisión, administrar dispositivos móviles y ajustar la experiencia del usuario.

GARANTÍA Y SOPORTE TÉCNICO	
Tipo de asistencia y tiempos de respuesta	Para los servicios descritos la Asistencia será en Modalidad 8x5xNBD por un (1) año
Certificado Suscripción	El proveedor debe realizar acompañamiento técnico y tener la capacidad de escalar los casos directamente al fabricante de la solución durante la vigencia del licenciamiento Incluir certificado de la suscripción con la vigencia requerida.
Soporte Técnico	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, asistencia técnica 8:00 AM a 12:30 PM y de 1:30 PM a 5.30 PM. 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 5.2 tiempos de respuesta y solución, según criticidad. Los servicios deben ser prestados en las sedes del Ministerio de Justicia y del Derecho ubicadas en, Calle 53 número 13 - 27 Chapinero, Carrera 9 número 12 C – 10 Centro, y la Carrera 27 número 15 – 85, sector Paloquemao, todas las sedes ubicadas en la ciudad de Bogotá, D.C., o donde sea

	la sede del Ministerio en la ciudad de Bogotá D.C., con personal local para atender los requerimientos en los tiempos requeridos. Soporte a través de Página Web, radicación de problemas e Inquietudes por medio del mecanismo de correos o celular o "Envío de Tickets". Enhanced Support for Umbrella: Es un nivel de servicio de soporte técnico ofrecido por Cisco Systems para el producto Umbrella; En la oferta de "Offer Description" para Umbrella aparece una tabla donde el nivel "Enhanced" (anteriormente llamado "Gold") aparece con cobertura de soporte 24×7 por teléfono y web, con objetivo de respuesta de 30 minutos para llamados por teléfono en caso de gravedad alta. En consecuencia, se debe tener en cuenta lo especificado por CISCO en su documento: *Service Description - Software Support Service* numeral 2.3 Enhanced que se encuentra disponible en el siguiente enlace: Sopo https://www.cisco.com/c/dam/en_us/about/doing_business/docs/cisco-software-support-service.pdf?_gl=1*16it27x*_gcl_au*MTA1MDE3ODcxOS4xNzYwOTcyMzk2&_ga=2.97779487.1039227579.1762442999-72206852.1697559746.
Configuración y Parametrización de acuerdo con los lineamientos del Ministerio de Justicia.	Realizar la configuración y parametrización de los componentes y software con total compatibilidad y completo funcionamiento conforme a los lineamientos del Ministerio de Justicia, y de acuerdo con el cronograma de actividades acordado entre el supervisor del contrato y el oferente, en los casos de nuevas funcionalidades del licenciamiento.
Transferencia de Conocimiento	Transferencia de conocimiento técnico(Presencial o virtual): 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, sin costo adicional para la Entidad.

5.1.1 **Tiempo de Respuesta y Solución**

Prioridad	Detalle	Tiempo de Respuesta	Tiempo de Solución
Crítico	Falla que hace imposible administrar la plataforma de Umbrella o DUO. Requiere atención virtual o visita en sitio.	1 hora	3 horas
Alto	Problema de amenazas de gran impacto donde continúan operando las plataformas Umbrella y DUO, 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	Las plataformas Umbrella o DUO continúan 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

NOTA: Sin perjuicio de la aplicación de la consecuencia establecida en el ANS, en caso de que la empresa contratista incumpla con los tiempos de respuesta para los ANS estipulados en el numeral 5.2, el Ministerio evaluara la necesidad de realizar las gestiones tendientes a iniciar el proceso administrativo sancionatorio con el fin de imponer las sanciones pertinentes y de ser el caso hacer efectiva la póliza de cumplimiento.

5.2 Certificación de distribuidor autorizado

El proponente deberá presentar una certificación expedida por el fabricante Cisco, o por su representante autorizado en Colombia, que lo acredite como Cisco Partner de portafolio en Security y Networking , que estan dentro del marco del Programa Cisco 360 Partner, el Partner actualmente deberá estar autorizado para revender ofertas y servicios de Cisco, así como para utilizar ofertas y servicios de Cisco con el fin de proporcionar una oferta de servicios gestionados o en la nube a los usuarios finales del Partner en el territorio de Colombia.
La anterior información fue consultada en el sitio web del fabricante en el siguiente URL :*consultada el 27/02/2026 : 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 deberá tener una fecha de expedición no mayor a tres (3) meses con relación a la fecha de presentación de la propuesta

5.2.1 Soporte

El soporte para toda la plataforma de Cisco Umbrella, Cisco Duo, debe incluir los siguientes alcances:

- Asistencia inmediata disponible las veinticuatro (24) horas del día, los siete (7) días a la semana, todo el año.
- Asistencia en sitio en 4 horas, luego de notificar el incidente por parte del Ministerio para incidentes críticos (Prioridad).
- Respaldo directo del fabricante de la infraestructura de la Solución.
- Tiempo de respuesta telefónico a solicitudes de 1 hora luego de confirmado el registro del incidente.
- Suministro de versiones y releases de software de mantenimiento y versiones menores para los equipos cubiertos que incluya acompañamiento para realizar las actualizaciones en los casos que las mismas sean recomendadas por el fabricante para resolver un incidente.
- Soporte a las consultas sobre la operación o mantenimiento de la plataforma DUO y UMBRELLA.

NOTA 1: El personal técnico asignado a los servicios de soporte correctivo y soporte técnico deben ser certificados directamente por el fabricante en Cisco Umbrella Secure Internet Gateway Advantage, deben certificar la experiencia sobre esta labor y sobre los sistemas de equipos descritos en la ficha técnica en el numeral 5(Especificaciones Tecnicas). y esta experiencia debe ser mínimo de dos (2) años. Este requerimiento será verificado por el Supervisor del contrato en el momento de la ejecución de este.

5.2.2 SOPORTE REACTIVO (Mantenimiento)

El mantenimiento correctivo debe incluir lo siguiente:

- Diagnóstico y reparación Software.
- Identificación de riesgos y vulnerabilidades en las políticas, procesos y procedimientos existentes.
- Actualización del software operativo y actualización de parches de seguridad en los casos que sea requerido.
- Las ventanas de soporte (Mantenimiento) se establecerán de acuerdo con lo que determine el Supervisor del Contrato funcionario designado de la Subdirección de Sistemas del Ministerio de Justicia y del Derecho de manera que el impacto de la operación sea el mínimo posible.

5.3 Documentación y transferencia de conocimiento (Configuración y parametrización de los productos**)**

El contratista entregará la documentación propia de la suscripción del servicio tal como sea suministrado por el fabricante del software propuesto al supervisor del contrato, antes de la entrega en producción del software al Ministerio.

Una vez se entregue el servicio debidamente configurado, en producción y cuente con el aprobado del supervisor del contrato, el contratista realizará una transferencia de conocimiento (En modalidad presencial o virtual) de mínimo ocho (8) horas a los funcionarios que el ministerio designe para el manejo de la consola de administración y control del servicio propuesto, estas se otorgarán como valor agregado y no harán parte del consumo de **las** cincuenta (50) horas contratadas para las actividades de parametrización y configuración de los productos.

5.4 Recurso Humano Requerido

ÍTEM	PERSONAL	CANT	FORMACIÓN ACADÉMICA	EXPERIENCIA	DISPONIBILIDAD
1	Líder de Proyecto	1	• Ingeniero de Sistemas, electrónico o Telecomunicaciones o afines, con tarje profesional. • Especialización en Telemática y/o Redes de Telecomunicaciones y/o Gerencia de Tecnología o áreas afines. • Certificado vigente por el fabricante como Cisco CCIE Enterprise. • Certificación Lacnic Ipv6 Avanzado • Certificación Cisco Success Manager	Mínimo 4 años de experiencia profesional relacionada con el objeto contractual del proceso	Dedicación durante la vigencia del contrato de un (1) año.
2	Ingeniero de Soporte CCNP	1	• Ingeniero de Sistemas, electrónico o Telecomunicaciones o afines, con tarjeta profesional. • Certificado vigente por el fabricante como cisco CCNP • Certificación Lacnic Ipv6 Avanzado. • Certificación ITIL V4	Mínimo 4 años de experiencia profesional relacionada con el objeto contractual del proceso	Dedicación durante la vigencia del contrato de un (1) año.
3	Ingeniero Seguridad	1	• Ingeniero de Sistemas, electrónico o Telecomunicaciones o afines, con tarjeta profesional • Certificación Cisco CCNP Security • Certificación Lacnic Ipv6 Avanzado	Mínimo 3 años de experiencia profesional y experiencia en actividades de implementación de Soluciones de seguridad.	Dedicación durante la vigencia del contrato de un (1) año.
4	Ingeniero de soporte Junior	1	• Ingeniero de Sistemas, electrónico o Telecomunicaciones o afines, con tarjeta profesional • Certificado vigente por el fabricante como cisco CCNA.	Mínimo 2 años de experiencia profesional relacionada con	Dedicación durante la vigencia del

				el objeto del proceso	contrato de un (1) año.

El profesional mencionado en el ítem 3 del numeral 5.4Recurso Humano Requerido, durante la ejecución del contrato debe contar con certificación vigente expedida por el fabricante la cual corresponde a la certificación CCNP Security del ítem 5.4 recurso humano requerido, la cual cubre la instalación, configuración, puesta en producción y soporte del servicio de seguridad en la nube Cisco Umbrella

En un término no superior a tres (3) días a partir de la suscripción del contrato, el contratista deberá presentar los documentos correspondientes que acrediten las calidades de profesional graduado en ingeniería con su tarjeta profesional vigente.(Hoja de vida con certificaciones y diplomas de graduación)

El tiempo establecido para el uso del recurso humano requerido se encuentra establecido así:

ítem	Descripción	tipo	Unidad	Cantidad
1	Configuración y parametrización de los productos	Servicio	Hora	50
2	Soporte técnico reactivo	Servicio	Hora	100

6. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA.

1. Tramitar y entregar a nombre del Ministerio de Justicia y del Derecho en un término no mayor a cinco (5) días hábiles, los documentos que avalen la renovación de licenciamiento por suscripción de los productos Cisco Umbrella y DUO 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).
2. Realizar un cronograma que incluya las actividades de transferencia de conocimiento de las nuevas funcionalidades que traiga la actualización.
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. Realizar la configuración con las herramientas e insumos adecuados técnicamente para este tipo de labores. El costo de estas herramientas y/o insumos serán a cargo del contratista; así como el personal y la mano de obra.
5. Realizar un informe mensual del funcionamiento de la plataforma Cisco Umbrella y DUO, así como realizar una mesa de trabajo durante los primeros cinco (5) días de cada mes durante la vigencia del servicio
6. Coordinar y diseñar con el ingeniero designado de la Subdirección de Tecnologías y Sistemas de Información del Ministerio el plan de trabajo para la renovación, configuración y puesta en producción del licenciamiento mediante suscripción de las plataformas Cisco Umbrella y DUO, dentro de los cinco (5) días hábiles siguientes al inicio de ejecución del contrato.
7. Prestar todo el soporte técnico y asistir al personal de soporte técnico del Ministerio de Justicia y del Derecho sobre consultas relacionadas con las plataformas Cisco Umbrella y DUO durante la vigencia de la suscripción.

8. Configurar y soportar las plataformas Cisco Umbrella y DUO de administración en el caso de requerir la instalación de un nuevo agente en todos los equipos (estaciones de trabajo y servidores) de las diferentes sedes del Ministerio, ubicadas en, Calle 53 # 13 – 27 Chapinero, Carrera 9 # 12 C – 10 Centro y la Carrera 27 # 15 – 85 Paloquemao, todas las sedes ubicadas en la ciudad de Bogotá D.C, o donde sea la sede del Ministerio en la ciudad de Bogotá D.C. (En la eventualidad que se generen nuevos agentes durante la duración de la suscripcion)
9. Garantizar que el personal del Contratista que se encuentre en la entidad deberá estar debidamente carnetizado y cumplir con las normas de protección y bioseguridad, así como encontrarse afiliado al Sistema General de Seguridad Social Integral, conforme a la normatividad vigente en los casos de soporte en sitio.
10. 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.
11. Responder por cualquier intervención mal realizada y/o que esté en contra de las normas de funcionamiento y calidad y, en consecuencia, realizar los ajustes a que haya lugar.
12. Realizar la transferencia de conocimiento en las condiciones aprobadas por el supervisor del contrato, según lo establecido en el numeral 5.3 del documento Ficha Técnica que hace parte integral del proceso.
13. Entregar un informe detallado de las actividades realizadas en la plataforma, dos (2) días hábiles después de realizada la actividad, ya sea una actualización de software requerida o la solución a un incidente presentado en la plataforma.
14. Asignar personal profesional con los conocimientos y experiencia necesarios para realizar las labores indicadas de acuerdo con lo indicado en el numeral 5.4 del documento Ficha Técnica que hace parte integral del proceso.
15. Garantizar que el soporte técnico (Remoto), sea coordinado con el Administrador de la herramienta en el Ministerio de Justicia y del Derecho, e informado al supervisor del Área de soporte técnico en la entidad.
16. Responder por la integridad, autenticidad, veracidad y fidelidad de la información a su cargo, y por la organización, conservación y custodia de los documentos, teniendo en cuenta los principios de procedencia y orden original, el ciclo vital de los documentos y la normatividad archivística, sin perjuicio de las responsabilidades señaladas en la Ley 1952 de 2019.
17. Informar oportunamente de cualquier petición, o amenaza de quien, actuando por fuera de la ley, pretenda obligarlo a hacer u omitir algún acto u ocultar hechos que afecten los intereses de EL MINISTERIO.
18. Todas las demás inherentes o necesarias para la correcta ejecución del objeto contractual.

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:

La prestación del servicio se realizará en la sede del Ministerio de Justicia y del Derecho - Calle 53 número 13 - 27 de la ciudad de Bogotá, D.C, en la Carrera 9 # 12 C-10 (Sede Centro) de la ciudad de Bogotá D.C. y en la Carrera 27 número 15 - 85 (sector Paloquemao) en Bogotá o donde sea la sede del Ministerio en la ciudad de Bogotá.

PARAGRAFO: Para todos los efectos contractuales se tendrá como domicilio la ciudad de Bogotá D.C.

7.2. PLAZO DE EJECUCIÓN:
El plazo de ejecución del contrato será hasta el 31 de diciembre de 2026, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato.

El licenciamiento mediante suscripción y el soporte técnico tendrán un plazo de duración de un (1) año contado a partir del 21 de mayo de 2026, fecha de terminación de la vigencia del soporte actual de las plataformas.

7.3. FORMA DE PAGO:
El Ministerio pagará al Contratista seleccionado el valor del contrato así:

En un solo pago correspondiente al 100% del valor del mismo, una vez cumpla a satisfacción con la entrega de la documentación que certifica la renovación del licenciamiento y entrega de los servicios por suscripción de los productos Cisco Umbrella y Cisco DUO.

Para proceder al pago, deberá aportarse la siguiente documentación:

- Factura de cobro.
- Certificación de cumplimiento o recibo a satisfacción por parte del supervisor.
- 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.
- Informes mensuales de actividades de la ejecución del contrato, así como el informe final, presentado por el contratista y avalado por la supervisión del contrato por parte del MINISTERIO.

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 PRIMERO: 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.
PARÁGRAFO SEGUNDO: 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 TERCERO: 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 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.

PARÁGRAFO CUARTO: Los pagos antes señalados se realizarán dentro de los treinta (30) 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.

PARÁGRAFO QUINTO: 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.

PARAGRAFO SEXTO: 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.

PARAGRAFO SÉPTIMO: FACTURA ELECTRÓNICA SIN VALIDACIÓN PREVIA: en estos casos, la factura se entenderá expedida con la entrega al adquiriente 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.

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.

El contratista deberá constituir a favor del Ministerio Garantía de que tratan la Ley 80 de 1993, Ley 1150 de 2007, y el Decreto 1082 de 2015, considerando el objeto a contratar, las obligaciones contractuales y el valor del contrato, dicha garantía deberá constituirse con los siguientes amparos[3]:

AMPARO	*%*	*VIGENCIA*
Cumplimiento del Contrato	20% del valor total del contrato	Desde la suscripción del contrato y doce (12) meses más, contados a partir de la fecha de suscripción del contrato.
Calidad del servicio	20 % del valor total del contrato	Desde la suscripción del contrato y seis (12) meses más, contados a partir de la fecha de suscripción del contrato.
Pago de salarios, prestaciones sociales	5 % del valor total del contrato	Desde la suscripción del contrato y tres (3) años más, contados a partir de la fecha de suscripción del contrato.

[3] www.colombiacompra.gov.co – Guía para el manejo de garantías en procesos de contratación.

legales e indemnizaciones laborales		

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 interesada 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.

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".

Ver anexo Matriz de Riesgos

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	**JOSÉ ELIBERTO FONSECA RUÍZ** **ASTRID ELENA MUÑOZ BELTRAN** ASTRID ELENA MUNOZ BELTRAN C.C. 1061774916 de POPAYAN	Subdirección de Tecnologías y Sistemas de Información
REVISÓ	**JAIRO ARMANDO MORENO GUERRERO**	Revisión jurídica
APROBÓ	**JAIRO ERNESTO MEDINA MERCHAN** MEDINA MERCHAN JAIRO ERNESTO Firmado digitalmente por MEDINA MERCHAN JAIRO ERNESTO Fecha: 2026.06.18 16:56:23 -05'00'	Subdirección de Tecnologías y Sistemas de Información