TIPO DE CONTRATO A CELEBRAR
COMPRAVENTA

1. DEPENDENCIA o GERENCIA DEL PROYECTO QUE REQUIERE LA CONTRATACIÓN
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI

2. INFORMACIÓN BÁSICA DE INVERSIÓN QUE RESPALDA LA CONTRATACIÓN SOLICITADA	
Plan de Desarrollo- Distrital	*17 Bogotá Camina Segura*
2.1. Propósito	5-Bogotá confía en su gobierno
2.2. Logro	
2.3. Programa	33 fortalecimiento institucional para un gobierno confiable.
2.4. Proyecto	8089 fortalecimiento de los Componentes tecnológicos para garantizar la demanda en la operación de la UAERMV de Bogotá D.C.
2.5. Registro BPID No. y Fecha	INSCRITO el 17 de junio de 2024, registrado el 17- junio-2024-, Versión 6 del 25 de noviembre de 2025.
2.6. Código	2024110010161

3. DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial -UAERMV- está organizada como una Unidad Administrativa Especial del orden distrital del Sector Descentralizado, de carácter técnico, con personería jurídica, autonomía administrativa y presupuestal y con patrimonio propio, adscrita a la Secretaría Distrital de Movilidad, y tiene por objeto "programar y ejecutar las obras necesarias para garantizar la rehabilitación y el mantenimiento periódico de la malla vial local, intermedia y rural; así como la atención inmediata de todo el subsistema de la malla vial cuando se presenten situaciones que dificulten la movilidad en el Distrito Capital."

En concordancia con lo anterior y al tenor del artículo 109 del Acuerdo Distrital 257 de 2006, modificado por el Art. 95 del Acuerdo Distrital 761 de 2020, la UAERMV tiene las siguientes funciones:

- *Programar, ejecutar y realizar el seguimiento a la programación e información de los planes y proyectos de rehabilitación y mantenimiento de la malla vial intermedia, local y rural construidas y ejecutar las acciones de mantenimiento que se requieran para atender situaciones que dificulten la movilidad en la red vial de la ciudad.*
- *Suministrar la información para mantener actualizado el Sistema de Gestión de la Malla Vial del Distrito Capital, con toda la información de las acciones que se ejecuten.*
- *Atender la construcción y desarrollo de obras específicas que se requieran para complementar la acción de otros organismos y entidades del Distrito.*
- *Ejecutar las obras necesarias para el manejo del tráfico, el control de la velocidad, señalización horizontal y la seguridad vial, para obras de mantenimiento vial, cuando se le requiera.*
- *Ejecutar las acciones de adecuación y desarrollo de las obras necesarias para la circulación peatonal, rampas y andenes, alamedas, separadores viales, zonas peatonales, pasos peatonales seguros y tramos de ciclo rutas cuando se le requiera.*
- *Ejecutar las actividades de conservación del ciclo infraestructura de acuerdo con las especificaciones técnicas y metodologías vigentes y su clasificación de acuerdo con el tipo de*

intervención y tratamiento requerido (intervenciones superficiales o profundas).

Parágrafo 1. *En el caso de las intervenciones para mejoramiento de la movilidad de la red vial arterial, éstas deberán ser planeadas y priorizadas de manera conjunta con el Instituto de Desarrollo Urbano.*

Parágrafo 2. *Las obras a las que hacen mención los literales c, d y e responderán a la priorización que haga la Secretaría Distrital de Movilidad y deberán cumplir con las especificaciones técnicas establecidas por esta y/o por el Instituto de Desarrollo Urbano cuando no existan las especificaciones técnicas requeridas. Así mismo la Secretaría Distrital de Movilidad regulará lo pertinente frente a las características de los proyectos de acuerdo con la escala de intervención.*

Parágrafo 3. *La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial podrá suscribir convenios y contratos con otras entidades públicas y empresas privadas para prestar las funciones contenidas en el presente artículo."*

En cumplimiento de dichos lineamientos, la Oficina de Tecnologías de la Información de la UMV adelanta acciones de fortalecimiento de la infraestructura de ciberseguridad institucional, dentro de las cuales se encuentra la suscripción y modernización integral del soporte y servicios asociados a la plataforma de seguridad de endpoint y proteger la información confidencial de la UAERMV detectando, monitoreando y bloqueando el uso o transferencia no autorizada de información sensible.

Esta actuación garantiza la continuidad del servicio, la protección de la información institucional y el cumplimiento de los objetivos estratégicos de la UAERMV.

En conclusión, la presente actuación contractual se enmarca en los principios de la función administrativa previstos en el artículo 209 de la Constitución Política, y en los principios de planeación, economía, transparencia, responsabilidad y selección objetiva consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007, asegurando la eficiencia en el uso de los recursos públicos y la continuidad de los servicios tecnológicos que soportan la operación misional de la UAERMV.

De conformidad con lo establecido en el Acuerdo 2 de 2023 "Por el cual se establece la estructura organizacional de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial y las funciones de sus dependencias", la Oficina de Tecnologías de la Información tendrá las siguientes funciones:

- Proponer a la Dirección General la formulación de las políticas, planes, programas y proyectos en materia de tecnologías de la información, conforme a los lineamientos del Ministerio de las Tecnologías de la Información y las Comunicaciones, la Alta Consejería Distrital y en cumplimiento de los requisitos normativos vigentes.
- Formular y ejecutar acciones para el diseño, transición, provisión y mejora de los servicios que son soportados por las Tecnologías de la Información, de conformidad con los requisitos y acuerdos de nivel de servicio trazados por la Entidad y entidades competentes.
- Dirigir e implementar y hacer seguimiento a las políticas de seguridad de la información, de acuerdo con los lineamientos de las entidades distritales y nacionales competentes.
- Formular, ejecutar y actualizar el Plan Estratégico de Tecnologías de la Información, de acuerdo con las necesidades identificadas.
- Administrar el proceso de operación, mantenimiento y actualización del hardware, software y sistemas de información, de conformidad con la evaluación e identificación de necesidades.
- Prestar el soporte técnico requerido en la Entidad, de conformidad con los requisitos y acuerdos de nivel de servicio trazados.
- Desarrollar e implementar soluciones y servicios de tecnologías de la información, basados en estándares y buenas prácticas.
- Fortalecer la arquitectura empresarial, conforme a las directrices de orden nacional y distrital sobre

la materia.

- Gestionar la conectividad, el mantenimiento y actualización de las redes internas y externas, las comunicaciones fijas y móviles de la entidad, conforme a las necesidades identificadas.
- Administrar las aplicaciones institucionales de uso en la entidad y el desarrollo de nuevos aplicativos, basados en estándares y buenas prácticas.
- Gestionar alianzas estratégicas con otras entidades públicas o privadas para el desarrollo de las Tecnologías de la Información de la Entidad.
- Las demás que le sean asignadas y que correspondan a la naturaleza de la dependencia.

Para el actual gobierno Distrital se presenta El Plan de Desarrollo Distrital 2024-2027, “Bogotá Camina Segura”, fue aprobado en junio de 2024, en este se estableció el objetivo estratégico, “05 Bogotá confía en su gobierno", con el programa 33 Fortalecimiento institucional para un gobierno confiable y donde la entidad aporta al cumplimiento de la meta Plan de Desarrollo: Desarrollar el 100% de la estrategia de mejora y sostenibilidad del Modelo Integrado De Planeación y Gestión - MIPG en las entidades del Sector Movilidad.

Como parte de ejecución del plan de desarrollo, la UAERMV en el marco de sus funciones y misión institucional, formuló el Proyecto de inversión “8089 “Fortalecimiento de los Componentes tecnológicos para garantizar la demanda en la operación de la UAERMV de Bogotá D.C.”, y su cumplimiento se adelanta a través de las metas de inversión 1. Mantener, optimizar y modernizar un (1) Modelo Integrado de Planeación y Gestión - MIPG en la Entidad y 2. Adecuación y mantenimiento de 2 Sedes de la UAERMV. Su cumplimiento se adelanta a través de las metas de inversión: 1. Ejecutar 12 Proyectos encaminados a actualizar los módulos de los sistemas de información SIGMA, Calíope y Orfeo e Implementar el plan de mantenimiento de sistemas de información. 2. Actualizar (4) documentos que enmarquen la estrategia de TI en el Plan Estratégico de Tecnologías de la Información de la UAERMV para la vigencia 2025-2027 y 3. Garantizar la disponibilidad del 94% de los servicios tecnológicos que intervienen en los sistemas SIGMA, Calíope, Orfeo y Portales Web.

En el desarrollo de sus funciones, la UAERMV genera y procesa información sensible que reside y circula en los equipos de cómputo de la entidad, tanto propios como rentados (estaciones de trabajo, portátiles y servidores), así como en las aplicaciones misionales y administrativas soportadas en la arquitectura Cloud. Para salvaguardar esta información se cuenta con herramientas de seguridad perimetral, monitoreo, correlacionador de eventos, entre otros, sin embargo, estos controles no cubren la totalidad de amenazas ciberseguridad actuales. Por un lado, el antivirus tradicional nativo de los equipos de cómputo no detecta ni responde ante amenazas avanzadas que operan directamente sobre los equipos, por lo que se requiere una solución de **detección y respuesta en el endpoint (EDR)** que brinde visibilidad y protección continua sobre la totalidad de los equipos propios y rentados de la Unidad. Por otro lado, la entidad **no dispone actualmente de una herramienta de prevención de fuga de información (DLP)**, lo que la expone a la pérdida, extracción o divulgación no autorizada de datos sensibles. En consecuencia, es necesario incorporar capas adicionales de seguridad informática y ciberseguridad que fortalezcan la gestión de la confidencialidad, integridad y disponibilidad de los activos de información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

Bajo los lineamientos enunciados por el Ministerio de las Tecnologías de la Información y las Comunicaciones - MINTIC, definen las necesidades para que las entidades usen herramientas que velen por la seguridad de la información; estos dispositivos deben contar con sistemas operativos actualizados y con la capacidad de soportar los protocolos de red IPv6, tal y como se establece en la **Resolución 2710 de 2017 del MINTIC**.

Adicionalmente, las soluciones adquiridas deben integrarse con las herramientas de administración de la Unidad y ser totalmente compatibles e interoperables con los ecosistemas de seguridad perimetral ya implementados, de manera que aporten a la operación conjunta de los controles de seguridad. Todo ello en cumplimiento de las políticas de seguridad EGTI-DI-001 V4 – Políticas generales de tecnología y seguridad de la información.

Estas herramientas están orientadas al análisis constante y a la ejecución proactiva de acciones de detección, identificando de forma temprana las falencias o vulnerabilidades que puedan derivar en un evento o incidente de seguridad de la información. La materialización de estos riesgos puede comprometer los activos de información de la entidad y ocasionar afectaciones a la imagen corporativa, así como repercusiones legales y económicas, entre otras. En este sentido, el uso de soluciones como el EDR y el DLP permite implementar ambientes controlados de monitoreo continuo, detectar oportunamente posibles amenazas —incluida la fuga de información— y establecer mecanismos de defensa adecuados al interior de la entidad. Asimismo, facilitan la identificación de patrones de comportamiento de las amenazas, de manera que la UAERMV pueda responder de forma proactiva y evitar la materialización de riesgos de seguridad de la información.

En conclusión, mediante estas adquisiciones la entidad implementará medidas técnicas que fortalecerán la protección de sus equipos, datos e infraestructura tecnológica, la cual soporta la operación misional de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

La Oficina de Tecnologías de la Información de la UAERMV, en cumplimiento de la normativa vigente en materia de seguridad digital y gestión de riesgos tecnológicos, adelanta iniciativas de fortalecimiento de su arquitectura de ciberseguridad, que incluyen la actualización de políticas, procedimientos y controles, así como la renovación de componentes críticos de su infraestructura tecnológica.

La Entidad cuenta en la actualidad con una plataforma de seguridad integral compuesta por firewalls de nueva generación desplegados tanto en instalaciones físicas como en su infraestructura de nube pública (Oracle Cloud), una solución de control de acceso a la red con capacidad para gestionar más de setecientos (700) dispositivos concurrentes, un motor de análisis dinámico de amenazas mediante sandboxing, una plataforma centralizada de correlación de eventos e inteligencia de seguridad, un analizador de registros con capacidad analítica sostenida de dos mil (2.000) logs por segundo, una solución de protección avanzada del correo institucional con integración nativa a Microsoft 365, y una consola de gestión centralizada de políticas incorporada recientemente como parte de la modernización tecnológica en curso. Esta arquitectura, construida sobre un ecosistema de fabricante único y consolidada a lo largo de varios ciclos de inversión institucional, genera condiciones estructurales que hacen que la adquisición de capacidades de detección, respuesta y prevención en los endpoints, así como de prevención avanzada de fuga de información, deban articularse de forma nativa con la infraestructura existente, y no como capas tecnológicas aisladas. La incorporación de soluciones del mismo ecosistema sobre esta base instalada produce economías de escala concretas y verificables: elimina la necesidad de desarrollar conectores de integración a medida, descarta costos de middleware y evita licenciamientos adicionales de plataformas de orquestación para hacer interoperar tecnologías de distintos fabricantes. A ello se suma que el personal técnico de la Entidad ha acumulado conocimiento operativo, certificaciones de fabricante y experiencia de configuración sobre esta plataforma, lo cual reduce de forma significativa la curva de adopción, el riesgo de configuración incorrecta y los tiempos de respuesta ante incidentes, factores que en entornos de seguridad representan variables críticas y no meramente administrativas. En términos de protección efectiva, la integración nativa de la capa de endpoint con el firewall perimetral, el control de acceso a la red, el sandbox de análisis dinámico y el correlacionador de eventos permite construir flujos de respuesta automatizada y coordinada: una alerta generada en el endpoint puede derivar en una cuarentena de red ejecutada automáticamente por el control de acceso, un bloqueo de tráfico aplicado por el firewall, una detonación de muestra sospechosa en el sandbox y un evento correlacionado en tiempo real en el SIEM, todo ello dentro del mismo ecosistema tecnológico y sin dependencia de integraciones de terceros que introduzcan latencia, brechas de visibilidad o puntos de falla adicionales. Esta capacidad de respuesta orquestada no es replicable con el mismo nivel de eficacia y confiabilidad cuando se combinan soluciones de fabricantes distintos, dado que las integraciones entre ecosistemas heterogéneos dependen de APIs públicas con cobertura funcional limitada, acuerdos de interoperabilidad sujetos a cambios de versión y tiempos de sincronización que deterioran la efectividad de la respuesta en los primeros minutos críticos de un incidente. En consecuencia, la adquisición de las capacidades de protección de endpoint y prevención de fuga de información bajo los parámetros técnicos definidos en los presentes estudios no constituye una restricción a la pluralidad de oferentes sino la expresión técnicamente fundamentada del principio de planeación eficiente: preservar y

potenciar una inversión institucional acumulada, reducir el riesgo operativo y maximizar la cobertura de protección sobre la infraestructura tecnológica de la Entidad con el menor costo total de integración

Evaluación de soluciones existentes en la arquitectura actual

La entidad realizó un análisis técnico de las capacidades de las soluciones actualmente implementadas en su arquitectura de seguridad, particularmente aquellas orientadas a la protección perimetral y control del tráfico de red. Si bien dichas soluciones cumplen un papel fundamental dentro del esquema de defensa perimetral y segmentación de la red, su alcance funcional está orientado principalmente a:

- Inspección y control del tráfico de red,
- Prevención de intrusiones,
- Segmentación y control de acceso a nivel de red,
- Monitoreo del tráfico perimetral.

No obstante, las amenazas modernas han evolucionado significativamente y actualmente se caracterizan por técnicas como:

- uso indebido de credenciales legítimas,
- movimiento lateral dentro de la red,
- ataques sin archivos (fileless),
- abuso de herramientas del sistema operativo,
- compromisos de identidades y privilegios.

En este contexto, las buenas prácticas internacionales de arquitectura de ciberseguridad, tales como ISO/IEC 27001:2022, NIST Cybersecurity Framework y el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC, recomiendan complementar los controles perimetrales con capacidades especializadas de protección en endpoints y datos, dado que estos constituyen actualmente uno de los principales vectores de ataque en las organizaciones.

Durante el análisis de mercado se identificó que algunos fabricantes que cuentan con soluciones perimetrales también ofrecen módulos adicionales orientados a protección de endpoints y datos. En consecuencia, la entidad concluyó que la adopción de plataformas especializadas para la protección de endpoint y datos resulta más adecuada para fortalecer la postura de ciberseguridad institucional, complementando los controles perimetrales existentes y alineándose con las mejores prácticas internacionales de arquitectura de seguridad.

Madurez operativa de la entidad

La arquitectura tecnológica propuesta busca mantener un equilibrio entre:

- Fortalecimiento de seguridad,
- Sostenibilidad operativa,
- Capacidad de gestión interna.

En este sentido, los requerimientos técnicos definidos se orientan a seleccionar soluciones que sean proporcionales al nivel de riesgo institucional, pero que al mismo tiempo puedan ser administradas eficientemente con los recursos humanos disponibles. Este enfoque permite evitar tanto el subdimensionamiento de los controles de seguridad como la adopción de arquitecturas excesivamente complejas que puedan generar dificultades operativas.

Justificación de la solución propuesta

Con base en el análisis técnico, el estudio de mercado y la evaluación de la arquitectura actual, la entidad concluye que la implementación de plataformas modernas de protección de endpoint y protección de fuga de datos es necesaria para:

- Fortalecer la postura de ciberseguridad institucional,
- Reducir el riesgo de incidentes de seguridad,
- Mejorar la capacidad de detección y respuesta ante amenazas,
- Proteger la información institucional y los servicios misionales.

Las soluciones propuestas permitirán evolucionar desde un modelo de protección basado en antivirus tradicional hacia una arquitectura de seguridad moderna basada en telemetría, análisis de comportamiento y respuesta automatizada, alineada con las mejores prácticas internacionales.

Análisis de riesgo institucional asociado a la protección de endpoint y datos

El análisis de riesgos tecnológicos realizado por la entidad evidencia que los endpoints y los datos digitales representan actualmente uno de los principales vectores de ataque en los entornos tecnológicos modernos. De acuerdo con estudios internacionales de ciberseguridad y marcos de referencia como el NIST Cybersecurity Framework, una proporción significativa de los incidentes de seguridad actuales se origina a partir de:

- Robo o abuso de credenciales legítimas,
- Ejecución de código malicioso en estaciones de trabajo,
- Explotación de vulnerabilidades en equipos finales,
- Movimiento lateral dentro de la red institucional,
- Uso indebido de cuentas privilegiadas.

En este contexto, los controles tradicionales basados únicamente en antivirus y protección perimetral resultan insuficientes para detectar amenazas avanzadas que operan mediante técnicas como:

- Ataques sin archivos (fileless),
- Uso de herramientas administrativas del sistema,
- Ejecución de scripts maliciosos,
- Ataques dirigidos a servicios de identidad.

Estas amenazas pueden permanecer durante largos periodos dentro de la infraestructura tecnológica sin ser detectadas, comprometiendo progresivamente la confidencialidad, integridad y disponibilidad de la información institucional.

Riesgos identificados: En ausencia de mecanismos avanzados de detección y respuesta en endpoint y datos, la entidad se expone a riesgos relevantes tales como:

Compromiso de estaciones de trabajo y servidores: Los equipos de usuario y servidores constituyen el punto de entrada más frecuente para ataques de ransomware, malware avanzado y explotación de vulnerabilidades. Un compromiso exitoso de estos dispositivos puede permitir a un atacante:

- Ejecutar código malicioso,
- Acceder a información sensible,
- Instalar herramientas de persistencia,
- Expandir el ataque hacia otros sistemas.

Movimiento lateral dentro de la red: Una vez que un atacante compromete un equipo o una identidad,

puede desplazarse lateralmente dentro de la infraestructura tecnológica con el objetivo de:

- Comprometer servidores críticos,
- Acceder a bases de datos,
- Obtener información sensible,
- Interrumpir servicios institucionales.

La ausencia de visibilidad sobre el comportamiento de los endpoint dificulta la detección temprana de estas actividades.

Interrupción de servicios institucionales: La materialización de un incidente de seguridad puede generar impactos operativos significativos, tales como:

- Indisponibilidad de sistemas de información institucionales,
- Afectación de servicios misionales,
- Pérdida o alteración de información,
- Impacto reputacional para la entidad.

Dado que la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial es responsable de procesos asociados a la gestión y mantenimiento de la infraestructura vial de la ciudad, la continuidad de sus sistemas de información resulta fundamental para el cumplimiento de sus funciones institucionales.

Marco normativo y buenas prácticas

La necesidad de implementar capacidades avanzadas de protección en endpoint y datos se encuentra alineada con diversos marcos de referencia y lineamientos institucionales, entre los cuales se destacan:

1. ISO/IEC 27001:2022

La norma establece controles relacionados con:
- Protección contra malware,
- Monitoreo de actividades,
- Control de acceso,
- Detección de eventos de seguridad.

Estos controles requieren que las organizaciones cuenten con mecanismos que permitan detectar comportamientos anómalos y responder oportunamente ante incidentes de seguridad.

2. Modelo de Seguridad y Privacidad de la Información – MSPI

El MSPI del Ministerio TIC establece que las entidades públicas deben implementar controles que permitan:

- Monitorear permanentemente los activos tecnológicos,
- Detectar eventos de seguridad,
- Gestionar incidentes de manera oportuna.

La adopción de soluciones avanzadas de protección de endpoints y datos contribuye directamente al cumplimiento de estos lineamientos.

3. NIST Cybersecurity Framework

Este marco establece que las organizaciones deben desarrollar capacidades en las funciones de:

- Detect (Detectar)
- Respond (Responder)
- Recover (Recuperar)

Las plataformas modernas de protección de endpoints permiten fortalecer estas capacidades mediante:

- Telemetría avanzada,
- Análisis de comportamiento,
- Correlación de eventos,
- Respuesta automatizada.

Basados en lo anterior, con el fin de contar con plataformas con el mejor posicionamiento en el mercado para la protección de endpoints y datos, la entidad requiere cubrir la necesidad a través de un proceso de selección que le permita contratar soluciones que aporten e integren capacidades operativas a las plataformas ya existentes en el ecosistema de ciberseguridad de la Entidad, para generar valor por medio de la interoperabilidad, detección, protección y respuesta automatizadas ante amenazas cibernéticas de la siguiente manera:

1. **SOLUCIÓN DE ENDPOINT DETECTION AND RESPONSE O DETECCIÓN Y RESPUESTA DE ENDPOINTS AVANZADA (EDR).**

Generalidades: las cantidades de 450 endpoints se aplica para computadores de usuarios finales.

- La Entidad requiere del licenciamiento de la solución EDR Avanzado para 450 Endpoints.
- La solución de EDR debe proporcionar a la Entidad un conjunto de protecciones, tanto en pre-ejecución (esto es, antes de que la amenaza tenga capacidad para comprometer sus sistemas) como post-ejecución (cuando la amenaza interactúa con el servidor o equipo de trabajo), 100% basado en comportamiento (sin firmas estáticas) y cuya velocidad de respuesta proporciona una protección en tiempo real a los sistemas.
- La solución debe ser desplegada en la Nube del Fabricante (SaaS).
- La solución debe ser ofertada con un soporte de 24x7x365 por un periodo de doce (12) meses.

A continuación, se detallan y describen cada uno de estos mecanismos de protección requeridos:

Funcionalidades de Prevención.

- El EDR debe utilizar un motor antivirus de aprendizaje automático para detener la ejecución previa de malware. Esta capacidad Antivirus de Nueva Generación (Next-Generation Anti-Virus - NGAV) viene integrada en un agente único y ligero, lo que permite a los usuarios asignar protección antimalware a cualquier grupo de terminales sin necesidad de ninguna solución adicional.
- Disponer de aprendizaje automático, NGAV basado en kernel y Machine learning (ML).
- Enriquecer los eventos de seguridad con información sobre amenazas en tiempo real desde una base de datos en la nube que se actualiza continuamente.
- Proteger los endpoints desconectados de la red con una protección fuera de línea; este modo de operación se denomina modo autónomo.
- Proporcionar un control de dispositivos USB basado en múltiples parámetros.
- Debe estar en capacidad de eliminar tiempos de permanencia y Fatigas por exceso de alarmas (falsos positivos).

- Gestión de parches para sistemas operativos Windows, OS, Linux.

Funcionalidades de Descubrimiento.

- El EDR debe contar con un sistema automatizado de control de políticas de superficie de ataques, con evaluaciones y descubrimiento de vulnerabilidades que permiten al personal encargado de la seguridad.
- Descubrir y controlar dispositivos no autorizados (por ejemplo, dispositivos no protegidos o no administrados) y detectar dispositivos IoT.
- Realizar un seguimiento de aplicaciones ejecutadas, y su clasificación de seguridad.
- Descubrir y mitigar las vulnerabilidades del sistema y las aplicaciones con parches virtuales, mediante el análisis de sus comunicaciones e inhabilitando el acceso a su comunicación con el exterior.
- Al descubrir las vulnerabilidades debe mostrar la clasificación de reputación y el detalle de los códigos CVE aplicables.
- Reducir la superficie de ataque con políticas proactivas basadas en niveles de riesgo.

Funcionalidades de Detección y Protección.

El EDR debe detectar y desactivar el malware así sean amenazas del tipo sin archivos o file-less y otros ataques avanzados en tiempo real para proteger los datos y evitar brechas en la seguridad en la entidad. Tan pronto como el EDR detecte flujos y comportamientos sospechosos, inmediatamente debe desactivar las amenazas potenciales, bloquear las comunicaciones salientes y el acceso al sistema de archivos desde esos procesos sospechosos, por otro lado, debe evitar la exfiltración de datos, las comunicaciones de comando y control (C&C), la manipulación de archivos y el cifrado de ransomware. Al mismo tiempo, el backend del EDR debe continuar recopilando evidencias adicionales, enriqueciendo los datos de eventos y clasificando los incidentes para aplicar de forma automatizada una estrategia de respuesta a incidentes, permitiendo así automáticamente la continuidad del negocio incluso en dispositivos ya comprometidos cumpliendo como mínimo con los siguientes items:

- Se debe basar en la detección integrada de forma profunda en el sistema operativo, permitiendo la detección de ataques de infiltración sigilosa, los ataques basados en la memoria y los ataques “living off the land”.
- Debe proporcionar protección en los procesos en ejecución, el inicio y parada de procesos, y en las interacciones entre procesos, así como frente a actividades sospechosas asociadas a librerías (archivos DLL en el caso de sistemas operativos Windows).
- Debe poder detener las amenazas en tiempo real y eliminar el tiempo de permanencia de dichas amenazas en la organización, incluso en los endpoint desconectados de la red corporativa.
- Debe bloquear las comunicaciones de forma granular a nivel de proceso, evitando exfiltraciones de datos, movimientos laterales y conexión con redes de comando y control.
- Debe impedir a los procesos maliciosos el acceso a los sistemas de ficheros, protegiendo frente a cifrados de ransomware, y la creación/modificación/eliminación maliciosa de archivos y/o registros.
- Debe permitir definir listas blancas y negras para personalizar mediante exclusiones estas protecciones (por hash, nombre y/o ruta de archivo, o por aplicación, incluyendo datos de versión y fabricante).
- Debe proporcionar la capacidad para marcar, tanto manual como automáticamente, determinada actividad como falso positivo, evitando además que ocurran detecciones similares.
- Debe Proporcionar un análisis de todo el historial de eventos.
- Debe realizar la validación continua de la clasificación de amenazas.

Funcionalidades de Protección contra Ransomware.

La solución de EDR debe contar con políticas predefinidas y exclusivas para la prevención de secuestro de información por ataques de ransomware, por lo cual debe incluir más de 30 estrategias de protección diferentes.

Dichas estrategias deben incluir como mínimo:

1. Debug de Procesos.
2. Código dinámico.
3. Formato de archivo ejecutable incorrecto.
4. Una pila con código ejecutable.
5. El programa ejecutado no tiene instalador.
6. Programa crítico falso.
7. Empaquetador falso.
8. File Encryptor.
9. Proceso oculto.
10. Ejecutable inyectado.
11. Proceso inyectado.
12. Hilo inyectado.
13. Suma de comprobación no válida.
14. Ejecución no válida.
17. Empaquetador conocido.
18. Archivo malicioso detectado.
19. Proceso malicioso.
20. Ejecutable modificado.
21. Stack Parcialmente asignado.
22. Exploit de escalamiento de privilegios.
23. Proceso vacío.
24. Manipulación de pilas.
25. Aplicación sospechosa.
26. Empaquetador sospechoso.
27. Ejecutable manipulado.
28. Ejecutable no confirmado.
29. Ejecutable sin asignar.
30. Código grabable.

Funcionalidades de Remediación.

La Solución de EDR propuesta debe orquestar operaciones de respuesta a incidentes utilizando playbooks predefinidos en la solución, optimizando así la respuesta a incidentes y los procesos de remediación, revirtiendo de modo automático los cambios maliciosos realizados por amenazas ya contenidas, en un único dispositivo o en dispositivos distribuidos a lo largo del entorno de la entidad, las características de remediación deben cumplir como mínimo con los siguientes requerimientos:

- Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta.
- Debe estandarizar los procedimientos de respuesta a incidentes con la automatización de playbooks.
- Debe optimizar los recursos de seguridad, automatizando las acciones de respuesta a incidentes, como la eliminación de archivos, la finalización de procesos maliciosos, la reversión de cambios persistentes, la notificación a los usuarios, el aislamiento de aplicaciones y dispositivos, y la apertura de tickets.
- Debe permitir la respuesta a incidentes basada en el contexto utilizando la clasificación de incidentes y los sujetos de los ataques (como, por ejemplo, grupos de estaciones de trabajo).
- Debe proporcionar visibilidad completa de la cadena de ataque y los cambios maliciosos, mediante el seguimiento de código.
- Debe permitir automatizar la limpieza y reversión de los cambios maliciosos preservando así la integridad del sistema.
- La solución de EDR Se debe contar con un servicio de respuesta y detección gestionada (MDR) ante incidentes, proporcionado por técnicos del propio fabricante.
- Debe realizar la contención y respuesta de forma automática.

Funcionalidades de Investigación.

La solución de EDR debe enriquecer automáticamente los registros de los eventos con información detallada sobre el malware antes y después de la infección, para realizar análisis forenses en los endpoint infiltrados. Su interfaz guiada debe proporcionar una guía útil, mejores prácticas y sugerir los próximos pasos lógicos a los analistas de seguridad, estas características de investigación deben cumplir como mínimo con los siguientes requerimientos:

- Debe desactivar y bloquear automáticamente las amenazas, lo que permite a los analistas de seguridad cazar marcando sus propios tiempos.
- Debe contar con una tecnología propietaria de rastreo de código, permitiendo así visualizar la cadena de ataque completa y el "paciente cero", incluso si el dispositivo está fuera de línea.
- Debe conservar instantáneas de memoria, de los ataques sin archivo o file-less para la búsqueda de amenazas basada en memoria.
- La interfaz gráfica debe mostrar explicaciones claras por qué el evento está marcado como sospechoso o malicioso, enumera el marco de ataque MITRE correspondiente, así como el siguiente paso lógico para la investigación forense.

Funcionalidades de EDR.

La solución de EDR debe tener la capacidad de poder integrarse con diferentes plataformas de seguridad, creando así un marco robusto que pueda identificar y responder eficiente y eficazmente frente a los ataques como es recomendado por Gartner. La solución de EDR deberá integrarse al menos con las siguientes plataformas con las que cuenta la Entidad:

1. Next Generation Firewall (FortiGate).
2. Control de Acceso a la Red (FortiNAC).
3. SandBox (Fortisandbox).
4. Correlacionador de Eventos (FortiSIEM).
5. Debe contar con una Gestión Unificada.
6. Debe contar con la funcionalidad de identificación de incidentes entre productos.
7. Debe contar con la funcionalidad de investigación impulsada por inteligencia artificial.
8. Debe contar con la funcionalidad de respuesta automatizada.

Componentes de la Solución EDR.

La plataforma de seguridad del endpoint EDR debe ser una arquitectura distribuida, la cual debe constar de un agente en software, el cual debe ser compatible con los siguientes sistemas operativos y entornos con los que cuenta la Entidad, en versiones de 32 y 64 bits:

- Windows: 11.
- MacOS: Ventura 13 y superior.
- Windows Server: 2019, 2022 y superior.
- Linux: Oracle Linux 8, 9 y superior, Ubuntu server LTS 24.04 y superior, CentOS 8, 9 y superior.

En cuanto al hardware, debe ser un agente muy ligero; el cual no debe requerir más de 100MB de memoria RAM, y 20MB de espacio en disco.

2. SOLUCIÓN DE DATA LOSS PREVENTION O PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)

Generalidades: las cantidades de 450 endpoints que se aplica para protección de usuarios finales.

- Se requiere una solución DLP que permita a la Entidad anticipar y prevenir la fuga y/o perdida de datos.
- La solución debe contar con licenciamiento avanzado para 450 Endpoints, incluido conector para Microsoft Office 365.

- La solución debe ser desplegada en la Nube del Fabricante (SaaS).
- La solución debe ser ofertada con un soporte de 24x7x365 por un periodo de doce (12) meses.

Requerimientos técnicos.

- La solución debe prevenir la exfiltración y pérdida accidental de datos.
- La solución debe ser SaaS, en cloud, sin instalación de equipos ni colectores en tierra.
- La solución debe ser una sola licencia, que incluya todo lo solicitado sin módulos adicionales de componentes de seguridad no solicitados que puedan generar administraciones o coexistencia con diferentes configuraciones que no permitan centrarse en la función de DLP. No se permiten soluciones que deban incluir infraestructura en sitio como servidores o bases de datos.
- La solución debe inspeccionar y clasificar comportamientos aun sin crear reglas mediante el uso de Machine Learning.
- La solución debe tener la posibilidad de incluir analistas dedicados a detectar fugas de información en caso de requerirse directamente de fábrica.
- La solución debe proporcionar visibilidad inmediata sobre el movimiento y la actividad de los datos.
- La solución debe proporcionar visibilidad inmediata sin políticas sobre el movimiento de datos y los procesos empresariales.
- La solución debe proporcionar un agente unificado que consolide todas las funcionalidades de monitoreo y bloqueo.
- La solución debe tener capacidades de inteligencia artificial y aprendizaje automático.
- La solución debe integrar aprendizaje automático desde el primer día para establecer una línea base de la actividad individual del usuario y utilizar algoritmos de análisis de comportamiento para detectar comportamientos típicos frente a comportamientos novedosos o anómalos.
- La solución debe proporcionar capacidades adicionales de análisis y analítica para ofrecer insights a nivel organizacional.
- La solución debe permitir a las organizaciones activar servicios y obtener visibilidad de riesgos de datos en minutos para proteger datos sensibles desde el primer día.
- La solución debe detectar y responder a la manipulación de datos y actividades anómalas utilizando IA y ML.
- La solución debe ser capaz de monitorear amenazas internas y empleados de alto riesgo.
- La solución debe aplicar políticas de riesgo interno con acciones de seguridad proactivas en tiempo real.
- La solución debe mapear las actividades en un formato de MITRE.
- La solución debe identificar y mitigar amenazas internas a través de análisis avanzados de comportamiento de usuarios.
- La solución debe asegurar los datos en uso por aplicaciones SaaS y otras aplicaciones.
- La solución debe permitir políticas de protección de privacidad de datos como almacenamiento de datos y logs forenses en datacenters de la compañía, colocar seudónimos a los nombres de las cuentas que se están investigando para que el analista no sepa a quien se hace la revisión e incluir la autorización de investigaciones fuera de la caja (out-of-the-box) por parte de analistas.
- La solución debe proporcionar visibilidad integral de las interacciones de los usuarios con los datos en la nube y mantener la protección a medida que los datos se mueven fuera de la nube, asegurando la protección continua de la información sensible, independientemente de su ubicación o método de acceso.
- La solución debe monitorear y bloquear datos sensibles transferidos a través de navegadores web a dominios públicos externos (por ejemplo, Gmail, Hotmail, Yahoo, entre otros).
- La solución debe fortalecer las defensas contra posibles brechas de datos derivadas de la exposición de datos empresariales a través del uso no autorizado de aplicaciones, incentivando a los empleados a usar herramientas autorizadas.
- La solución debe diferenciar entre datos sensibles transferidos a soluciones en la nube empresariales y soluciones en la nube personales (por ejemplo, Microsoft oneDrive para Empresas vs. Microsoft

oneDrive Personal).

- La solución debe identificar el uso de Shadow AI y detener la carga de datos sensibles.
- La solución debe monitorear el uso de aplicaciones SaaS, incluyendo herramientas de Shadow AI como Gen-AI, e incorporar educación de usuarios basada en riesgos en el punto de acceso a datos sensibles.
- La solución debe cumplir con los requisitos de residencia de datos.
- La solución debe construir un inventario completo con puntuación de riesgo de las aplicaciones SaaS y herramientas GenAI utilizadas en toda la organización, con información sobre el ingreso, egreso y credenciales de datos.
- La plataforma debe monitorear la actividad en aplicaciones de inteligencia artificial (Por ejemplo, ChatGPT, Gemini, entre otros).
- La solución debe aplicar análisis de comportamiento de usuarios y entidades a gran escala.
- La solución debe incluir un asistente de IA que resuma y contextualice los datos asociados con actividades de alto riesgo para acelerar el análisis de incidentes.
- La solución debe analizar qué datos se están utilizando y cómo, permitiendo determinar la mejor respuesta.
- La solución debe clasificar y rastrear datos en tiempo real para proporcionar visibilidad y protección de datos inmediata, sin necesidad de políticas predefinidas.
- La solución debe estar disponible en la nube para facilitar su implementación y escalabilidad, como un servicio SaaS.
- La solución debe funcionar independientemente de la conexión de red y la ubicación.
- La solución debe utilizar tecnología de agente ligero compatible con sistemas operativos Windows, macOS y Linux para una implementación sin problemas y actualizaciones automáticas a escala empresarial. Las funciones deben ser similares en los tres sistemas operativos.
- La solución debe utilizar un agente escalable y ligero para recopilar y registrar datos.
- La solución debe permitir reducir los costos de ancho de banda, al no depender de un motor de escaneo de archivos basado en la nube.
- La solución debe utilizar agentes, extensiones de navegador y conectores en la nube para recopilar, enriquecer e indexar automáticamente la actividad a través de diferentes tipos de eventos (autenticación, web, email, aplicaciones, USB, creación de archivos, compartición y descarga de archivos).
- La solución debe proporcionar visibilidad profunda en las actividades de los usuarios, el acceso a datos y los sistemas para prevenir la salida de datos sensibles.
- La solución debe incorporar funcionalidades que permitan educar a los usuarios sobre el manejo adecuado de datos.
- La solución debe proporcionar capacitación basada en riesgos para entrenar a los empleados a tomar las decisiones correctas basadas en la detección de comportamientos inaceptables, reforzar las políticas de seguridad corporativa y promover una buena higiene cibernética.
- La solución debe proporcionar notificaciones personalizadas y recordatorios para reforzar la conciencia sobre las políticas de seguridad y dirigir a los usuarios a alternativas aceptables cuando se detecten aplicaciones no autorizadas. Las notificaciones deben poder enviarse a través de diálogos en el Endpoint, correo electrónico, y mensajería (por ejemplo: Microsoft Teams, Slack, etc).
- La solución debe aplicar políticas adaptativas basadas en riesgos que consideren factores de riesgo y permitan decidir qué acciones tomar, como notificar a los usuarios a través de mensajería (por ejemplo: Microsoft Teams, Slack, etc), capturar forenses de archivos y pantallas, aislar o bloquear un endpoint, terminar un proceso o bloquear actividades de alto riesgo.
- La solución debe integrarse fácilmente con los sistemas y plataformas existentes en la organización.
- La solución debe ser compatible con dispositivos y plataformas de colaboración.
- La solución debe proporcionar perfiles MDM, transmisión de eventos, webhooks y una API abierta para la integración con herramientas MDM, SIEM, SOAR, de automatización y de mesa de servicio existentes.
- La solución debe identificar y rastrear datos automáticamente según su origen, como sistemas de

recursos humanos o repositorios de código fuente, sin necesidad de incluir reglas iniciales para la detección.

- La solución debe aplicar políticas de DLP y de riesgo interno basadas en el origen de los datos y si se utilizó una cuenta corporativa o no corporativa para la salida de datos.
- La solución debe incorporar conectores de Microsoft Office 365.
- La solución debe mapear las actividades a una base de conocimientos de tácticas, técnicas y procedimientos de amenazas internas.
- La solución debe proporcionar visibilidad de datos, evaluación de riesgos y políticas de protección de datos listas para usar para proteger los activos de información críticos dentro y fuera de la red.
- La solución debe ayudar a cumplir con requisitos clave de cumplimiento, incluyendo PCI DSS, HIPAA, ISO 27001, NIST, PII, PHI, entre otros.
- La solución debe abordar los controles de cumplimiento normativo relacionados con la prevención de pérdida de datos con un esfuerzo mínimo utilizando políticas predefinidas de PII/PHI/PCI.
- La solución debe priorizar la privacidad bajo regulaciones como GDPR y CCPA.
- La solución debe utilizar técnicas de minimización de datos integradas, como la seudonimización y el almacenamiento forense localizado, para ayudar a los equipos de seguridad a detectar y mitigar amenazas mientras se protege la confidencialidad de los empleados.
- La solución debe minimizar los conjuntos de datos de investigación seudonimizados.
- La solución debe mapear las detecciones de actividades de alto riesgo a una base de conocimientos de tácticas, técnicas y procedimientos de amenazas internas y secuenciarlas automáticamente en incidentes con puntuación de riesgo para priorizar las investigaciones.
- La solución debe almacenar los registros forenses en centros de datos controlados por el cliente en la región.
- La solución debe incluir flujos de trabajo de autorización de investigación listos para usar para los analistas.
- La solución debe proporcionar un feed de actividad detallado y secuenciado en el tiempo que permita a los analistas ver la actividad de usuarios, datos y dispositivos antes, durante y después de un incidente.
- La solución debe permitir a los analistas de seguridad tomar acciones según la gravedad del riesgo, como mostrar un mensaje en pantalla al empleado, tomar una captura de pantalla, terminar un proceso, bloquear conexiones a un dispositivo o bloquear el teclado y el ratón de un dispositivo.
- La solución debe incluir gestión de casos integrada y reportes de riesgos que destaquen comportamientos descuidados, maliciosos y accidentales a lo largo del tiempo, permitiendo evaluar la efectividad de los controles de seguridad e identificar áreas de mejora.
- Los reportes deben poder exportarse fácilmente para compartir con la alta dirección.
- La solución debe proporcionar un dashboard para cumplimiento y auditoría.
- La solución debe soportar la generación de reportes personalizados basados en usuarios específicos.
- La solución debe soportar la generación de reportes personalizados basados en tipos específicos de datos.
- La solución debe soportar la generación de reportes personalizados basados en períodos específicos.
- Los reportes deben poder exportarse fácilmente para compartir con otras áreas de la entidad.
- La solución debe incluir reglas predefinidas para detectar prácticas de higiene cibernética deficientes, como la carga de archivos confidenciales a ubicaciones inesperadas, la conexión a redes Wi-Fi no seguras, la inserción de dispositivos de hardware maliciosos o el uso de aplicaciones no autorizadas para almacenamiento en la nube o dispositivos USB.
- La solución debe monitorear y bloquear datos sensibles transferidos a dispositivos USB.
- La solución debe monitorear datos sensibles transferidos a través de aplicaciones de terceros (por ejemplo, Putty).
- La solución debe monitorear datos sensibles copiados mediante capturas de pantalla.
- La solución debe monitorear datos sensibles copiados a través de pulsaciones de teclas (por ejemplo, imprimir pantalla).
- La solución debe monitorear datos sensibles copiados a nivel de archivo/carpeta.

- La solución debe monitorear datos sensibles copiados a nivel de comando (por ejemplo, símbolo del sistema, terminal).
- La solución debe monitorear datos sensibles copiados/descargados a una máquina virtual sin agente de punto final.
- La solución debe soportar el rastreo de múltiples archivos compartidos por un usuario.
- La solución debe soportar el monitoreo del movimiento de datos sensibles fuera de un conjunto definido de usuarios.
- La solución debe exportar un historial de todo el movimiento de datos dentro de la empresa, incluyendo datos provenientes de fuentes externas.
- La solución debe monitorear la descarga de datos sensibles por un usuario directamente desde una aplicación/servidor de aplicaciones.
- La solución debe proporcionar detalles de los datos sensibles descargados por un usuario durante un período especificado, incluyendo el número total de archivos, volumen de descarga, nombres de archivos y origen.
- La solución debe monitorear servicios y plataformas de correo electrónico (por ejemplo, MS Exchange, Office 365, Outlook, entre otros).
- La solución debe bloquear el montaje de unidades de almacenamiento removibles (por ejemplo, USB, HDD externo).
- La solución debe monitorear y bloquear datos sensibles impresos en impresoras físicas y/o PDF.
- La solución debe integrarse con otras herramientas de ciberseguridad (por ejemplo, SIEM).
- La solución debe integrarse con Active Directory, Azure AD y soluciones LDAP de terceros.
- La solución debe soportar MFA (Autenticación Multifactor).
- La solución debe soportar SSO (Inicio de Sesión Único) con Active Directory, Entra ID, GCP, Amazon, AWS.

La solución de DLP deberá integrarse al menos con las siguientes plataformas con las que cuenta la Entidad:

- Correlacionador de Eventos (FortiSIEM).
- Analizador (Fortianalyzer)
- Microsoft Office 365.

Componentes de la Solución DLP.

La plataforma de seguridad de DLP debe ser una arquitectura distribuida, la cual debe constar de un agente en software el cual debe ser compatible con los siguientes sistemas operativos y entornos con los que cuenta la Entidad, en versiones de 32 y 64 bits:

- Windows: 11.
- MacOS: Ventura 13 y superior.
- Windows Server: 2019, 2022 y superior.
- Linux: Oracle Linux 8, 9 y superior, Ubuntu server LTS 24.04 y superior, CentOS 8, 9 y superior.

Servicios y soporte.

- La solución debe incluir soporte directo con el fabricante en modalidad 7x24.
- La solución debe incluir acceso a un equipo especializado directo de fábrica que brinde orientación remota sobre implementación, actualizaciones y operaciones de la solución DLP.
- La solución debe incluir un servicio de buenas prácticas llevado a cabo por el fabricante que incluya el análisis inicial, revisión de políticas a implementar, ajuste de la solución, recomendaciones y seguimiento durante el primer mes de implementación y seguimiento mensual y final de la solución implementada. Debe realizarse directamente por el fabricante de la solución, no puede ser realizado por el oferente.

- La solución requerida debe incluir la licencia para Control de dispositivos integrada, DLP en línea para web, correo, Cloud Drive y conectores de medio, Clasificación de datos en tiempo real, análisis de riesgo de aplicaciones SaaS y de Inteligencia Artificial generativa, Entrenamiento de riesgos a usuarios finales, Soporte de librerías de cumplimiento regulatorio, etiquetas de Microsoft MIP/AIP, archivos forenses, gestión de incidentes y secuencia de tiempo de actividad. El entrenamiento debe incluir permitir hacer una evaluación de la justificación de incumplimiento.
- La solución requerida debe incluir las licencias necesarias para monitoreo de actividades de usuario y equipo final, analítica de comportamiento con Machine learning, detección de manipulación de datos, aislamiento de usuarios finales y bloqueo en tiempo real, detección de incidentes con puntuación de riesgo, captura de pantalla para análisis forense, gestión de caso, librería de detección de riesgo asociado a mapas de Mitre ATT&ck, conectores de integración con Google workspace, Microsoft office 365 y controles de compartir archivos.
- La solución debe ser ofertada con un soporte de 24x7x365 por un periodo de doce (12) meses.

La suscripción de las plataformas de protección de nueva generación basadas en la nube del fabricante incluye la implementación y el soporte por doce (12) meses, a partir de la firma del acta de inicio, con esquema de soporte 7x24 con fabricante y soporte local por parte del Contratista. El oferente debe incluir todo el software requerido para el cumplimiento de lo solicitado por la entidad.

El desarrollo del futuro contrato tiene como fin realizar el cumplimiento de la meta 3 “Garantizar la disponibilidad del 94% de los servicios tecnológicos que intervienen en los sistemas SIGMA, Calíope, Orfeo y Portales Web”.
En conclusión, la presente actuación contractual se enmarca en los principios de la función administrativa previstos en el artículo 209 de la Constitución Política, y en los principios de planeación, economía, transparencia, responsabilidad y selección objetiva consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007, asegurando la eficiencia en el uso de los recursos públicos y la continuidad de los servicios tecnológicos que soportan la operación misional de la UAERMV.

Cabe resaltar que esta adquisición se encuentra contemplada en la línea 8089-053 dentro del plan adquisiciones anual de la UAERMV del 2026.

2. ASPECTOS GENERALES DEL SECTOR

a) Aspectos de Tipo Económico (Macroeconómico y Microeconómico)

Contexto mundial

Según el FONDO MONETARIO INTERNACIONAL, FMI, en su último informe de julio de 2026, expone que, se proyecta que el crecimiento mundial sea del 3,0% en 2026 y del 3,4% en 2027, cifras que suponen una rebaja de la media del 3,5% observada en 2024–25 y que en términos acumulados prácticamente no varían con respecto a lo pronosticado en la edición de abril de 2026 de Perspectivas de la economía mundial (informe WEO). Esta leve desaceleración se debe a que los efectos de la guerra en Oriente Medio se ven contrarrestados en parte por el mayor ímpetu que la demanda imprime al ciclo tecnológico mundial gracias a los avances en inteligencia artificial (IA) y su adopción. El impacto varía considerablemente en función del grado en que cada país está expuesto a la guerra y su posición en la cadena de valor tecnológica. Los exportadores de energía situados fuera de la zona de conflicto se benefician de unos términos de intercambio favorables, mientras que las economías que han logrado aprovechar el auge impulsado por la tecnología registran una mayor actividad, aun si son importadoras de energía. En cambio, se observa un debilitamiento de la actividad entre los importadores de energía con una participación limitada en la cadena de valor tecnológica, grupo al que pertenecen muchos países de ingreso bajo. Se prevé que la inflación general a escala mundial aumente de un 4,1% en 2025 hasta un 4,7% en 2026, para después descender hasta el 3,9% en 2027. Estas proyecciones, ligeramente revisadas al alza con respecto a abril, indican que la tendencia de desinflación observada desde

principios de 2024 se ha estancado.

Los riesgos para las perspectivas están más equilibrados que en abril, pero no dejan de estar sesgados hacia un deterioro de la situación. La posibilidad de un recrudecimiento del conflicto en Oriente Medio se cierne sobre la región y podría prolongar la volatilidad de los precios de las materias primas, agravar los factores que amenazan las cadenas de suministro, elevar los precios e incidir negativamente en las condiciones financieras. La fragmentación del comercio podría acelerarse, y eso podría hacer mella en el producto y elevar los precios. La posible corrección de las expectativas generadas por la tecnología se suma a los riesgos desfavorables, que pueden verse amplificados por el desgaste de los márgenes para la aplicación de políticas. Los factores favorables para las perspectivas provienen de una normalización de los mercados energéticos más rápida de lo previsto, una inversión en tecnología superior a la esperada, la revitalización de una cooperación duradera que reduzca las barreras comerciales y reformas estructurales que fomenten el crecimiento a mediano plazo. Las prioridades para la política económica consisten en restablecer la estabilidad de precios, apoyándose en una comunicación clara, la independencia de los bancos centrales y una supervisión financiera sólida, al tiempo que se reconstituyen los márgenes fiscales y se recurre con prudencia a herramientas fiscales basadas en ayudas temporales y focalizadas que preserven las señales de precios. Se necesitan reformas estructurales que promuevan la seguridad energética, la preparación frente a la IA, el reequilibrio interno, y, además, debe reforzarse la cooperación internacional para aliviar las tensiones actuales.



La actividad y las perspectivas económicas mundiales están a merced de dos importantes fuerzas que tiran en sentidos opuestos y tienen efectos asimétricos en los distintos países. La primera es el shock de oferta negativo inducido por la guerra en Oriente Medio. La segunda es el actual shock tecnológico positivo, que se manifiesta en una aceleración del ciclo tecnológico mundial debida en gran medida a los avances y el uso de herramientas de IA.

La economía mundial en su conjunto hasta ahora ha soportado el shock de la guerra mejor de lo que se había temido. Las fluctuaciones y las repercusiones de los principales canales de transmisión —precios de las materias primas, expectativas de inflación y condiciones financieras— han sido relativamente limitadas. No obstante, el proceso de transmisión aún está en sus primeras fases: el uso comercial y estratégico de las existencias ha aliviado temporalmente la merma de los flujos de energía, mientras que los indicadores anticipados, como la presión sobre las cadenas de suministro y los índices de gerentes de compras, apuntan a

un menor dinamismo en el futuro. Además, en algunos países las tensiones son más pronunciadas que en otros.

Contexto nacional.

Para DELOITTE Colombia, en 2025 la economía colombiana creció 2.6%, impulsada principalmente por la recuperación del consumo y el dinamismo de algunos sectores de servicios. Sin embargo, el crecimiento continúa mostrando una composición heterogénea, con debilidad persistente en sectores intensivos en inversión como construcción y minería.

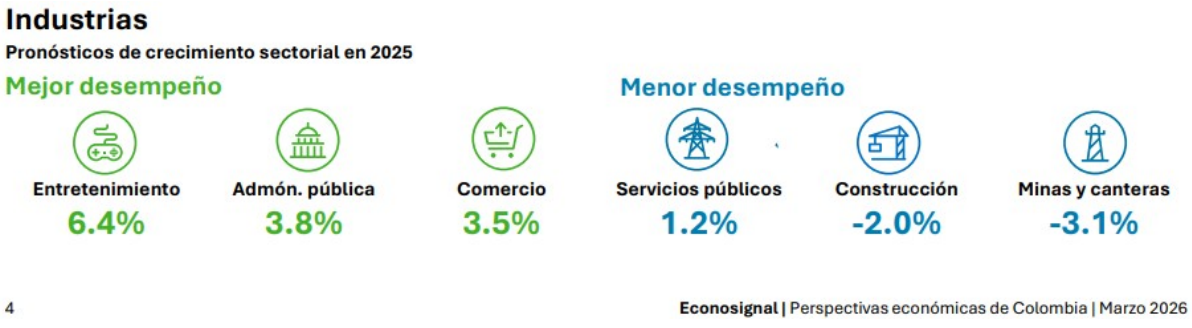
La inversión apenas creció 1.3% en 2025, reflejando una recuperación moderada, mientras que la baja ejecución del gasto público en capital continúa limitando una expansión más sólida de la formación bruta de capital fijo.

En materia de inflación, el proceso de desinflación observado durante 2024 se agotó esperando ahora un cambio de tendencia. En enero de 2026 la inflación fue 5,4% en un contexto de persistencia en servicios y efectos de indexación asociados, entre otros factores, al incremento del salario mínimo.

El mercado laboral ha mostrado resiliencia en términos de ocupación, aunque persisten desafíos en la calidad del empleo. La proporción de trabajadores que reciben menos de un salario mínimo continúa aumentando, lo que sugiere ajustes en la estructura del empleo en un contexto de costos laborales crecientes.

En este entorno, el Banco de la República mantiene una postura monetaria restrictiva, priorizando la convergencia de la inflación hacia la meta.

En conjunto, la economía colombiana continúa creciendo, pero sobre una base aún frágil, dependiente del consumo y con rezagos en inversión, lo que mantiene a la actividad vulnerable frente a choques externos y a restricciones internas de política económica.





Pronósticos macroeconómicos

Las proyecciones para 2026 y 2027 incorporan un escenario deterioro leve del crecimiento, con el PIB expandiéndose 2.5% en 2026 y 2.8% en 2027, acorde a condiciones financieras más restrictivas. Entre los riesgos a la baja se encuentra la corrección de las cuentas fiscales que podrían reducir el ritmo de crecimiento. La convergencia inflacionaria sería más lenta de lo previsto meses atrás, con una inflación de cierre de 6.5% en 2026 y 5.5% en 2027, reflejando persistencia en servicios y efectos de indexación.

	2026	2027
PIB (var. % real anual)	2.5%	2.8%
Inflación (var. % anual, cierre de año)	6.5%	5.5%
Tasa de cambio (USD/COP, cierre de año)	$3,830	$4,000
Tasa de interés (%, cierre de año)	11.25%	11.00%

En este contexto, la tasa de política monetaria se mantendría en terreno contractivo durante buena parte del horizonte de proyección, cerrando 2026 en 11.25% y 2027 en 11.00%, mientras que la tasa de cambio se ubicaría en torno a 3,830 en 2026 y 4,000 en 2027, en un entorno de dólar globalmente fuerte y fundamentos fiscales que aún limitan una apreciación sostenida del peso

Las proyecciones del equipo de Econosignal de Deloitte anticipan una recuperación moderada del consumo y una mejora en el crecimiento de la inversión. Aunque las tasas de interés altas seguirán presionando la inflación a la baja, el efecto será menor. El Banco de la República adoptará una postura cautelosa en sus próximas juntas debido a la coyuntura global.

Aunque no muy alejado, el análisis del Grupo CIBEST, conglomerado que cobija a Bancolombia, expone que la economía colombiana transita por una fase de recuperación paulatina, con señales alentadoras en el consumo, el mercado laboral y algunos sectores productivos. El crecimiento proyectado del PIB —2,6 % en 2025 y 3,0 % en 2026— refleja una reactivación impulsada por la demanda interna, especialmente por el consumo de los hogares, que ha ganado tracción gracias al proceso de desinflación y al ingreso récord por remesas. Sectores como entretenimiento, agro y comercio minorista lideran la recuperación, mientras se espera una mejora en la construcción para el próximo año. Sin embargo, esta reactivación no es lineal ni homogénea:

enfrenta tensiones estructurales, presiones fiscales y una inversión aún débil.

A nivel interno, el país se prepara para una transición transformadora en 2026. La inflación, aunque en descenso, se mantendrá fuera del rango meta por sexto año consecutivo, afectada por la persistencia en servicios, alimentos y el efecto de la indexación salarial. La política monetaria seguirá siendo cauta: se proyecta una tasa de interés de 8,25 % al cierre de 2026, aún en terreno contractivo. En paralelo, el gasto público, que ha sido motor de crecimiento y empleo, enfrenta límites estructurales. Los déficits fiscales —entre 6,5 % y 7,1 % del PIB— reflejan una presión creciente sobre la sostenibilidad macroeconómica. La activación de la cláusula de escape de la regla fiscal permitirá mantener este ritmo de gasto, pero también exigirá reformas profundas para evitar un mayor deterioro.

Tema	Indicador	Dato 2025	Proyección 2026
Mercado laboral	Desempleo nacional	9,2 %	9,4 %
Finanzas públicas	Déficit fiscal (% del PIB)	-7,1 %	-6,5 %
Balanza comercial	Exportaciones	+0,4 % (1S25)	-
Balanza comercial	Importaciones	+14,5 % (1S25)	↑
Balanza de pagos	Déficit cuenta corriente (% del PIB)	-2,4 %	-3,1 %
Inflación	IPC total	5,1 %	4,1 %
Inflación	Inflación alimentos	6,9 % (1S25)	6,2 %
Inflación	Inflación regulados	5,2 %	2,5 %
Inflación	Inflación servicios	5,4 %	4,3 %
Política monetaria	Tasa de interés (BanRep)	9,25 %	8,25 %

La economía colombiana muestra una dualidad estructural: el consumo representa el 77 % del PIB, mientras la inversión se mantiene rezagada en torno al 17 %. Esta composición limita el crecimiento potencial y evidencia un desplazamiento de recursos que compromete la capacidad de expansión futura. En este escenario, la transición hacia un modelo más equilibrado será clave. Como en un triatlón, el éxito no depende solo del rendimiento en cada disciplina, sino de la calidad de las transiciones. Colombia deberá desacelerar el gasto, fortalecer la inversión y planificar con precisión sus próximos pasos. La reactivación es una carrera de largo aliento, y 2026 será el año en que se definan las condiciones para sostenerla o perder el ritmo.

Banco de la Republica – Informe sobre política Monetaria, julio 2026 [1],

Durante el segundo trimestre de 2026 la inflación continuó aumentando y se alejó de la meta del 3%, impulsada por mayores costos laborales, un alto nivel de gasto de los hogares y del sector público, y aumentos en los precios de los alimentos. Al mismo tiempo, la economía colombiana registró un mayor crecimiento, explicado principalmente por el consumo y la inversión en maquinaria y equipo. Las expectativas de inflación permanecen elevadas y los niveles de gasto continúan siendo superiores a los que la economía puede sostener sin generar mayores presiones inflacionarias. En lo que resta de 2026 los precios seguirían aumentando su ritmo de crecimiento para moderarse gradualmente en 2027. En este entorno, el Banco de la República mantiene su compromiso de adoptar las medidas necesarias para el retorno gradual de la inflación a la meta del 3%.

La inflación continuó aumentando durante el segundo trimestre del año y se alejó de la meta del 3%, impulsada por mayores costos laborales, un consumo dinámico y algunas dificultades en la oferta que afectaron, principalmente, a los precios de los alimentos. Hacia adelante, se espera estos factores continúen presionando los precios en lo que resta de 2026 y que se moderen gradualmente durante 2027.

[1]https://www.banrep.gov.co/es/publicaciones-investigaciones/informe-politica-monetaria/julio-2026

- En junio los precios crecieron a un ritmo anual (6,1 %) superior al observado en marzo (5,6 %). Este comportamiento también se registró para los componentes menos volátiles de la canasta del consumidor (sin alimentos ni regulados). Con esto, la inflación continuó alejándose de la meta del 3 %.



- El mayor ritmo de aumento de los precios estuvo asociado a incrementos significativos en salarios y otros costos laborales, un gasto en la economía que continúa fuerte, y factores que afectaron la oferta agrícola, debido a efectos rezagados de las lluvias sobre las cosechas, paros y mayores costos de producción.

- Algunos factores ayudaron a moderar estas presiones, entre ellos el fortalecimiento reciente del peso frente al dólar y menores aumentos en los precios de las comidas fuera del hogar.

- Las proyecciones del equipo técnico indican que la inflación continuaría aumentando en lo que resta de 2026. Esto se explica por el efecto de los mayores costos laborales, incrementos esperados en los precios de los alimentos, los posibles efectos del fenómeno de El Niño, los aumentos en algunos servicios públicos y el continuo dinamismo del gasto de los hogares. A partir de 2027 los aumentos de precios comenzarían a moderarse y se irían acercando al 3 % en los próximos dos años, en parte como resultado de las acciones de política del Banco de la República.

- Las anteriores proyecciones están sujetas a una alta incertidumbre. Entre los principales factores que podrían afectar la evolución de los precios se encuentran las condiciones climáticas, los conflictos internacionales, la evolución y perspectivas de la política fiscal, y los cambios en algunos precios regulados como la gasolina y la energía.



La economía colombiana aumentó su crecimiento en el primer trimestre de 2026, impulsada, principalmente, por el mayor gasto de los hogares y del sector público, y la inversión en maquinaria y equipo. Aunque la economía seguiría creciendo durante los próximos trimestres, se espera que ese crecimiento sea más moderado que el observado recientemente. Esto se debe, en parte, a un menor dinamismo de los factores que habrían dado empuje a la actividad económica en los últimos meses, en un contexto donde persisten distintos elementos de incertidumbre tanto en el país como en el exterior.

- Durante el primer trimestre de 2026 la economía colombiana creció un 2,2 % anual, reflejo del buen desempeño del consumo, tanto privado como público, y de algunos componentes de la inversión (maquinaria y equipo).
- El gasto de los hogares siguió mostrando un comportamiento favorable, especialmente en la compra de bienes durables como vehículos, motocicletas, computadores y electrodomésticos.

- La inversión aumentó gracias a una mayor compra de maquinaria y equipo, aunque la actividad de construcción continuó mostrando debilidad.

- El mercado laboral mantuvo un comportamiento positivo, con más personas ocupadas y una tasa de desocupación que se situó en niveles históricamente bajos.

- La actividad económica continuaría creciendo en 2026 y 2027, pero a un ritmo más moderado, impulsada por unas condiciones de precios externos favorables, la recuperación gradual de la inversión, especialmente en infraestructura, y el aporte del turismo extranjero.

- La economía colombiana continúa enfrentando mucha incertidumbre relacionada con la situación internacional, las condiciones fiscales del país y posibles eventos climáticos que afecten la producción.

La Junta Directiva del Banco de la República mantiene su compromiso de lograr que la inflación vuelva gradualmente a la meta del 3 %. Este objetivo es especialmente importante en un momento en el que los precios crecen un ritmo elevado y el gasto de hogares y Gobierno sigue aumentando por encima de lo que sería sostenible.



La inflación subió y permanece muy por encima de la meta.

La economía y el mercado laboral continúan mostrando un comportamiento dinámico. Esto favorece el crecimiento del gasto y puede contribuir a que los precios continúen aumentando a un ritmo elevado.

La incertidumbre sobre los factores que afectarán los precios y la actividad económica en el futuro es muy grande. En particular, se destacan los factores de riesgo relacionados con los eventos climáticos (la fortaleza y duración de los efectos de un fenómeno de El Niño), la situación internacional y la política fiscal interna.

Tomando en cuenta las anteriores consideraciones, la Junta Directiva decidió en su reunión de junio incrementar en 75 puntos básicos la tasa de interés de política monetaria y en julio mantuvo una postura contractiva, dejando la tasa en 12,0%.

Futuras acciones de política dependerán de la nueva información sobre los precios, la actividad económica y de la evolución de los factores de riesgo señalados.

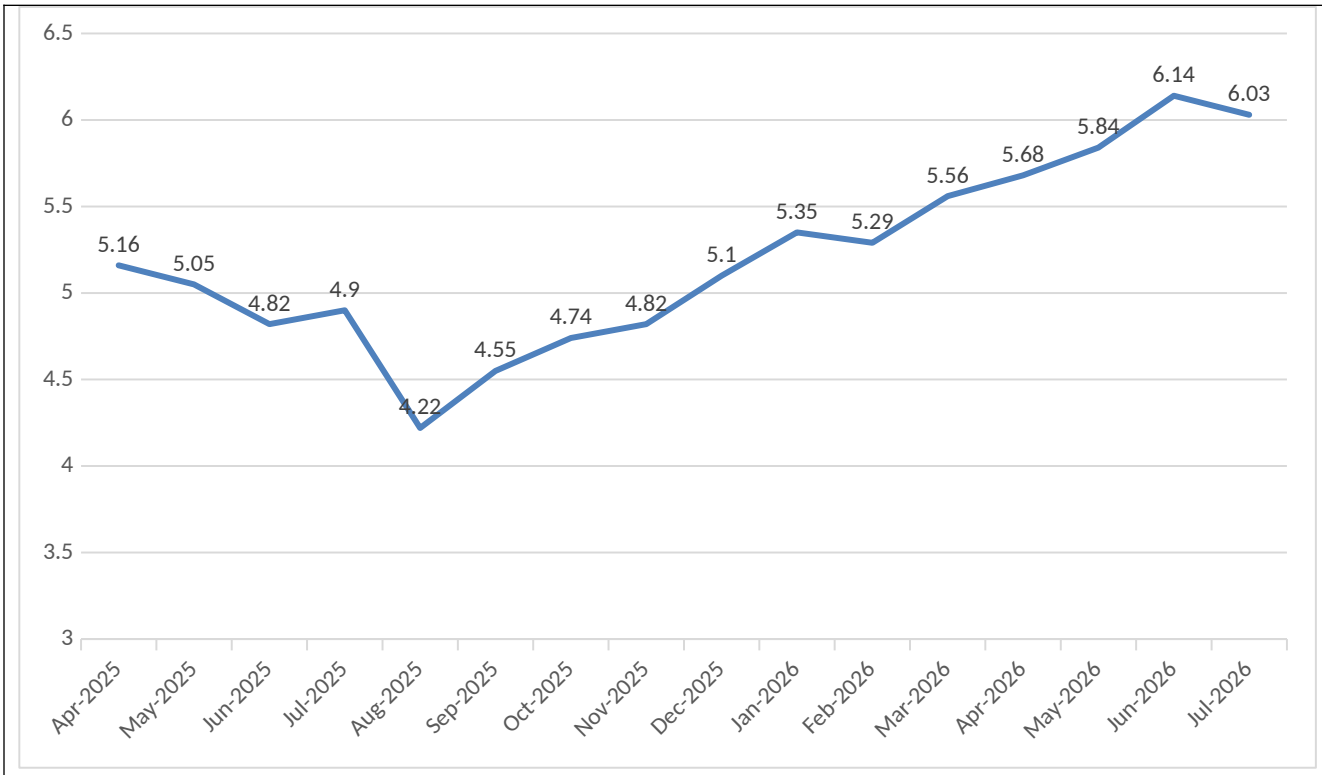
Con esta decisión, el Banco busca contribuir a que la inflación disminuya gradualmente hacia la meta del 3% en un tiempo razonable.

Indicadores Macroeconómicos: IPC[2]

En julio de 2026 la variación mensual del IPC fue 0,17%, la variación año corrido fue 4,94% y la anual 6,03%. En julio de 2026 la variación anual del IPC fue 6,03%, es decir, 1,13 puntos porcentuales mayor que la reportada en el mismo periodo del año anterior, cuando fue de 4,90%.

El comportamiento mensual del IPC total en julio de 2026 (0,17%) se explicó principalmente por la variación mensual de las divisiones Alojamiento, agua, electricidad, gas y otros combustibles y Restaurantes y hoteles. Las mayores variaciones se presentaron en las divisiones Alojamiento, agua, electricidad, gas y otros combustibles (0,55%) y Salud (0,38%).

[2] Tomado de https://www.dane.gov.co/index.php/estadisticas-por-tema/precios-y-costos/indice-de-precios-al-consumidor-ipc/ipc-informacion-tecnica



Fuente: DANE (2026), realización propia.

Indicadores Macroeconómicos: PIB[3]

En el segundo trimestre de 2026pr, el Producto Interno Bruto en su serie original, crece 3,5% respecto al mismo periodo de 2025pr. Las actividades económicas que más contribuyen a la dinámica del valor agregado son:

- Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales crece 10,0% (contribuye 1,7 puntos porcentuales a la variación anual).

- Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida crece 2,2% (contribuye 0,5 puntos porcentuales a la variación anual).

- Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios; Actividades de los hogares individuales en calidad de empleadores; actividades no diferenciadas de los hogares individuales como productores de bienes y servicios para uso propio crece 9,5% (contribuye 0,4 puntos porcentuales a la variación anual).

Durante el primer semestre de 2026pr, respecto al mismo periodo del año anterior, el Producto Interno Bruto presenta un crecimiento de 2,9%. Las actividades económicas que más contribuyen a la dinámica del valor

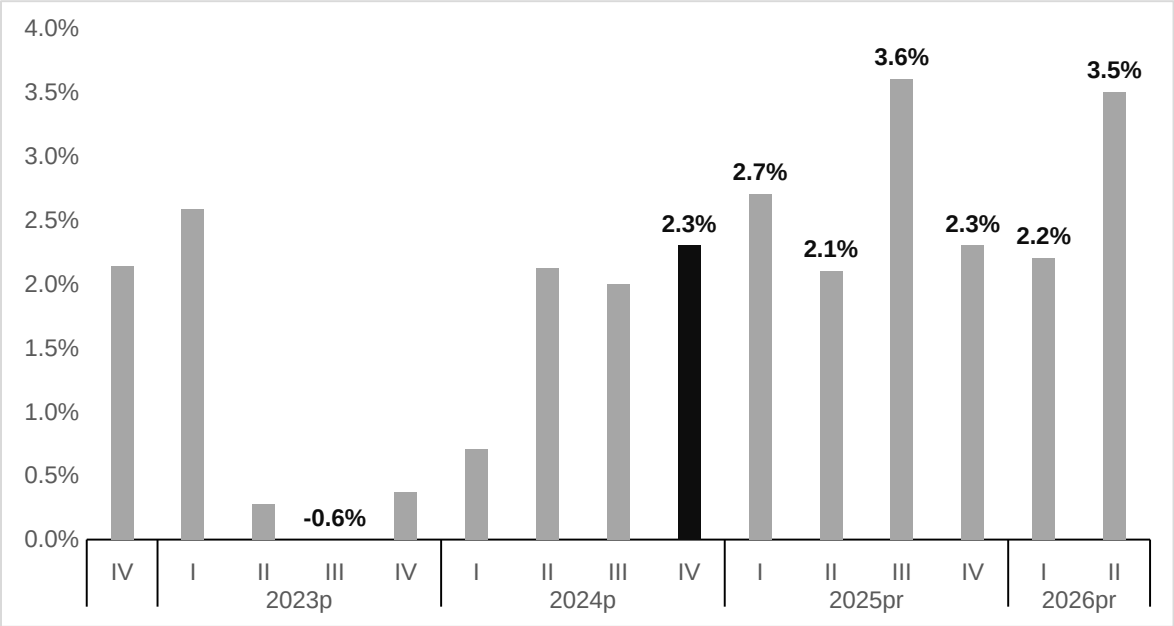
[3] Tomado de https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-nacionales-trimestrales/pib-informacion-tecnica

agregado son:

- Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales crece 7,9% (contribuye 1,3 puntos porcentuales a la variación anual).

- Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida crece 2,6% (contribuye 0,5 puntos porcentuales a la variación anual).

- Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios; Actividades de los hogares individuales en calidad de empleadores; actividades no diferenciadas de los hogares individuales como productores de bienes y servicios para uso propio crece 6,3% (contribuye 0,3 puntos porcentuales a la variación anual).

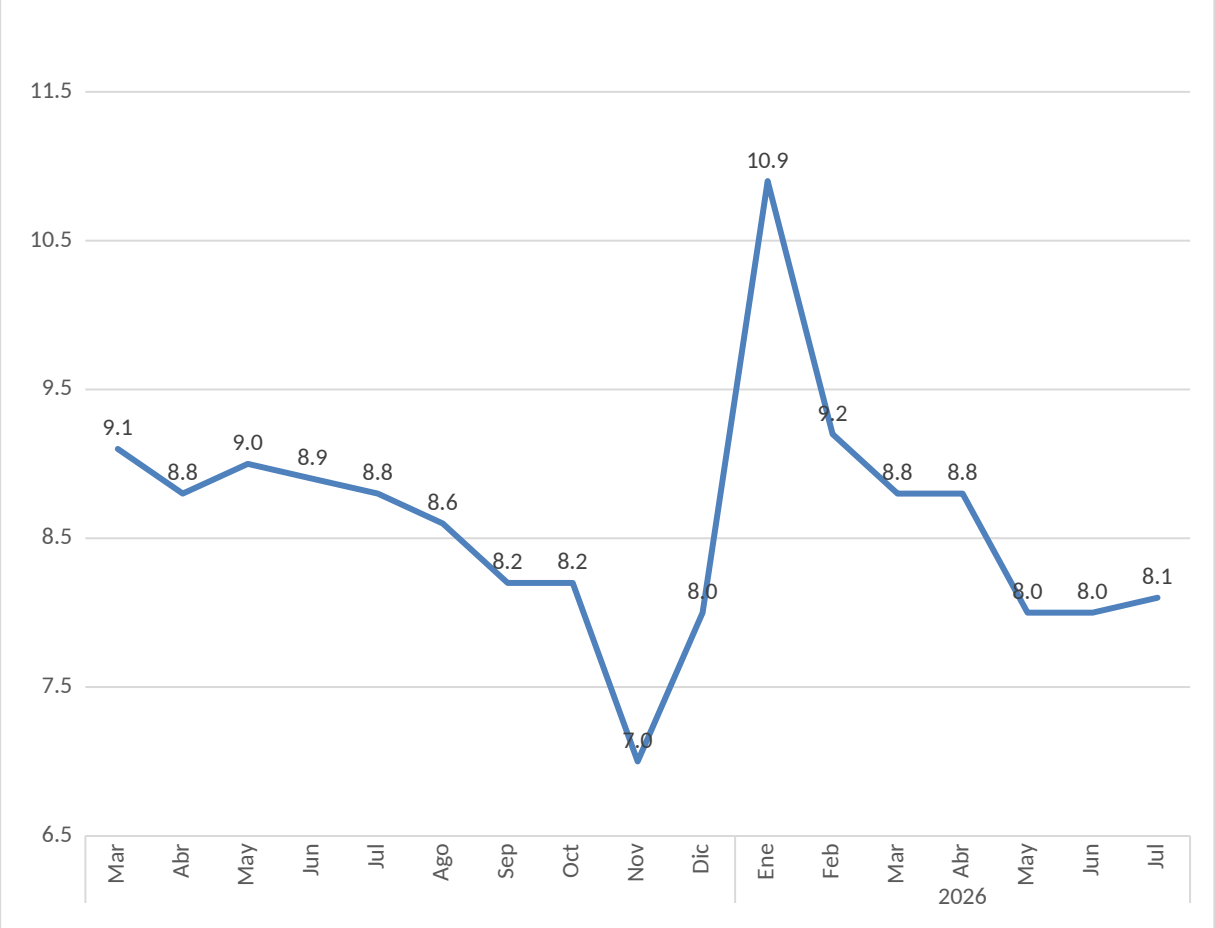


Fuente: DANE (2026).

Indicadores Macroeconómicos: EMPLEO[4]

Para el mes de julio de 2026, la tasa de desocupación del total nacional fue 8,1%, lo que representó una disminución de 0,7 puntos porcentuales respecto al mismo mes de 2025 (8,8%). La tasa global de participación se ubicó en 64,8% y la tasa de ocupación en 59,5%, en julio de 2025 estas tasas fueron 64,6% y 58,9%, respectivamente.

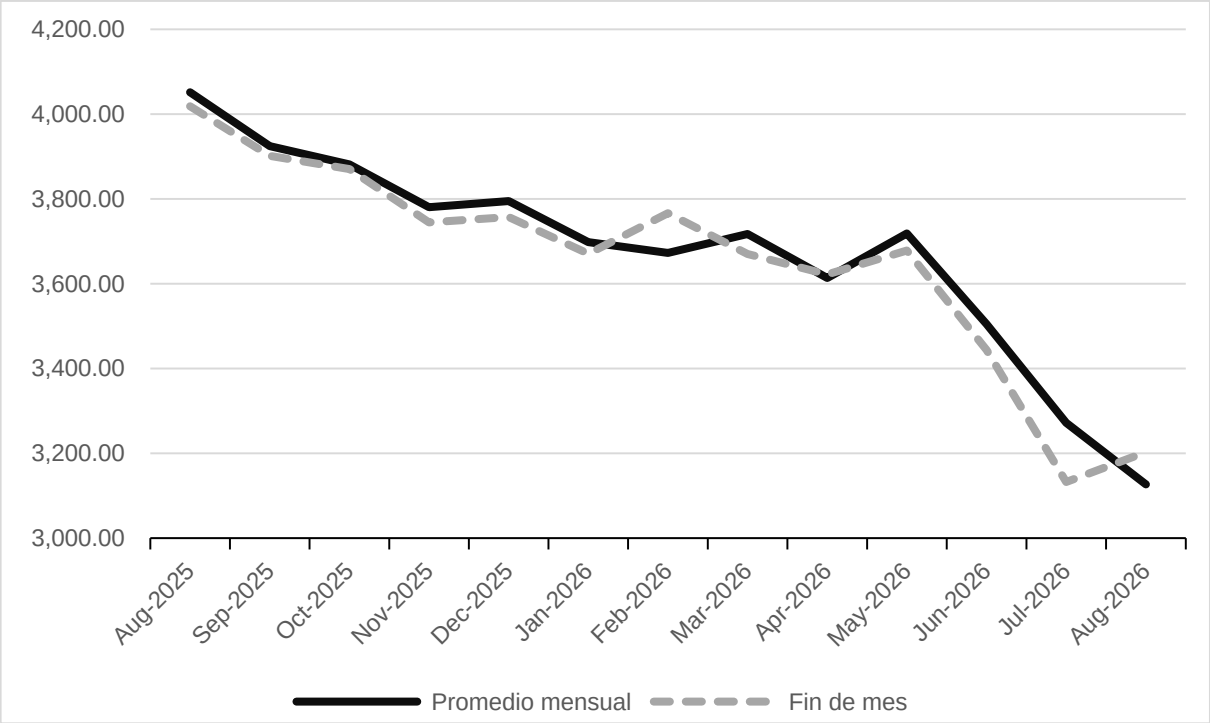
[4] Tomado de: https://www.dane.gov.co/index.php/estadisticas-por-tema/mercado-laboral/empleo-y-desempleo



Fuente: DANE (2026), realización propia.

Indicadores Macroeconómicos: TRM

Desde 1991 no existe en Colombia una tasa de cambio oficial; ninguna autoridad estatal fija el precio al cual se deban comprar o vender de manera obligatoria las monedas extranjeras. Por el contrario, en el país opera un esquema de flexibilidad cambiaria en el que el precio se encuentra determinado por la oferta y la demanda en el mercado de divisas y es acordado con libertad por cada una de las partes de la transacción (Resolución externa núm. 1 de 2018 de la Junta Directiva del Banco de la República). Como referencia, la Superintendencia Financiera de Colombia calcula y certifica la tasa representativa del mercado (TRM), que corresponde a una tasa de referencia del mercado de divisas. El cálculo y la certificación diaria de la TRM se efectúa con base en las operaciones registradas el día hábil anterior por los intermediarios del mercado cambiario (IMC).



Comportamiento histórico mensual de la TRM.

Fuente: Banco de la República (2026), realización propia.

En el gráfico anterior se observa que, entre agosto de 2025 y agosto de 2026, la Tasa Representativa del Mercado (TRM) en Colombia muestra una tendencia sostenida a la baja, la cual se mantiene solo se ve alterada en mayo de 2026, la mayor volatilidad, puede que sea asumido por la continuidad de la guerra en Medio Oriente y la política expansiva de la Fed en los Estados Unidos. Este comportamiento a la baja se da por un entorno político y económico exterior más incierto en Estados Unidos, así como bajas tasa de interés en ese mercado, pero altas en mercados de economías emergentes como Colombia.

Análisis de riesgos macroeconómicos

En conclusión, el análisis del PIB, el IPC, el empleo y la tasa de cambio refleja un panorama macroeconómico más inestable, de comportamientos mixtos, difíciles de predecir. Respecto de algunos riesgos previsibles, tenemos que:

1. Riesgo de Tasa de Cambio (TRM) y "Cloud-Inflation". Este es el riesgo más alto, ya que las plataformas de ciberseguridad de nueva generación (como CrowdStrike, SentinelOne o Microsoft) se facturan globalmente en dólares.

- Riesgo: Aunque el peso ha mostrado estabilidad relativa, existe un sesgo al alza por el alto déficit fiscal (cercano al 7% del PIB) y la caída en los precios del petróleo Brent (proyectado a $60 USD para finales

de año)[5].

- Impacto en el contrato: Un salto en el dólar encarece automáticamente las suscripciones mensuales de nube. Si el contrato es a largo plazo, una devaluación del 10% borraría el margen operativo del proveedor o forzaría ajustes en el canon.

2. Inflación de Servicios Técnicos y Soporte (IPC). La inflación anual en Colombia se situó en 6,01%[6]. Sin embargo, algunos analistas proyectan que podría repuntar hacia el 6,7% debido a la indexación de salarios y costos de energía. El componente de "Implementación y Soporte" depende de ingenieros especializados. La escasez de talento en ciberseguridad en Colombia ha inflado los salarios del sector por encima del IPC general.

El costo de mantener un SOC (Centro de Operaciones de Seguridad) operativo 24/7 ha subido significativamente este año[7].

3. Riesgo de Tasas de Interés y Capacidad Financiera.

- Situación de Tasas: El Banco de la República mantiene la tasa de intervención en niveles altos (12%) para contener la inflación.

- Impacto: Los contratos de implementación suelen requerir que el contratista invierta en infraestructura inicial o pago de licencias anuales por adelantado. Con tasas altas, el costo del capital es elevado.

- Riesgo: Si el proveedor no tiene solidez financiera, el alto costo del crédito podría retrasar la implementación o afectar la calidad del soporte técnico ante la falta de liquidez.

4. Riesgo de "Carrera Armamentista" de IA y Costos de Suscripción. El 94% de los líderes de ciberseguridad considera que la IA es el principal motor de cambio este año[8].

- Riesgo Macroeconómico-Tecnológico: Los fabricantes de software están aplicando incrementos de precios en sus suscripciones bajo el concepto de "Add-ons de IA" para detección predictiva.

- Impacto: Lo que hoy se contrata como "Suscripción Integral" podría quedar obsoleto o requerir pagos adicionales si las nuevas amenazas (como deepfakes de voz y video en tiempo real) exigen módulos que no estaban en el alcance inicial.

b) Aspectos de Tipo Técnico

Condiciones técnicas del servicio

Los requisitos técnicos y características se describen detalladamente en el Anexo 1. GCON FM 022 Formulación Estudio del Sector y Condiciones Técnicas de la Necesidad.

4. INFORMACIÓN GENERAL DEL CONTRATO SOLICITADO	
4.1. Objeto del contrato	8089-053 SUSCRIPCIÓN, IMPLEMENTACIÓN Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACIÓN PARA LA

[5] https://usbcali.edu.co/perspectivas-usd-cop-2026/
[6] https://www.dane.gov.co/index.php/estadisticas-por-tema/precios-y-costos/indice-de-precios-al-consumidor-ipc/ipc-informacion-tecnica
[7] https://blog.grupomicronet.com/es/principales-riesgos-de-ciberseguridad-en-colombia-y-c%C3%B3mo-afectan-a-las-empresas
[8] https://es.weforum.org/stories/2026/01/ciberriesgos-en-2026-lo-que-los-ejecutivos-deben-saber-sobre-ia-fraude-y-geopolitica/

<table>
<tr><td></td><td>PROTECCIÓN INTEGRAL DE LOS ACTIVOS DIGITALES DE LA UAERMV, ORIENTADA A LA PREVENCIÓN, DETECCIÓN Y RESPUESTA AVANZADA ANTE AMENAZAS EN ENDPOINTS Y PREVENCIÓN DE PÉRDIDAS DE DATOS</td></tr>
<tr><td>4.2. Código clasificador de bienes y servicios UNSPSC</td><td>El objeto de este contrato está codificado en la clasificación que se describe a continuación:
<table>
<tr><th>Clasificación UNSPSC</th><th>Segmento</th><th>Familia</th><th>Clase</th><th>Productos</th></tr>
<tr><td>43222501</td><td>(43000000) Difusión de tecnologías de información y telecomunicaciones.</td><td>(43220000) Equipos o plataformas y accesorios de redes multimedia o de voz y datos.</td><td>[43222500] Equipo de seguridad de red</td><td>[43222501] Equipo de seguridad de red cortafuegos (firewall)</td></tr>
<tr><td>43222502</td><td>(43000000) Difusión de tecnologías de información y telecomunicaciones.</td><td>(43220000) Equipos o plataformas y accesorios de redes multimedia o de voz y datos.</td><td>[43222500] Equipo de seguridad de red</td><td>[43222502] Equipo de seguridad de redes vpn</td></tr>
<tr><td>43233200</td><td>(43000000) Difusión de tecnologías de información y telecomunicaciones</td><td>[43230000] Software</td><td>[43233200] Software de seguridad y protección</td><td>[43233200] Software de seguridad informática</td></tr>
<tr><td>43233205</td><td>(43000000) Difusión de tecnologías de información y telecomunicaciones</td><td>[43230000] Software</td><td>[43233200] Software de seguridad y protección</td><td>[43233205] Software de seguridad de transacciones y de protección contra virus</td></tr>
</table></td></tr>
<tr><td>4.3. Plazo</td><td>El plazo de ejecución del contrato es de DOS (2) MESES, contados a partir de la suscripción de acta de inicio previo el cumplimiento de los requisitos de perfeccionamiento y ejecución (Registro presupuestal y aprobación de la garantía única), establecidos en el artículo 41 de la Ley 80 de 1993.

Nota Aclaratoria: El termino de cobertura de las suscripciones y soporte de la misma debe ser por DOCE (12) MESES, a partir de la firma del acta de inicio, con esquema de soporte 7x24 con fabricante y soporte local por parte del Contratista.</td></tr>
<tr><td>4.4. Normativa aplicable, Autorizaciones, permisos y/o licencias requeridas para su ejecución</td><td>• Ley 80 de 1993 “Por la cual se expide el Estatuto General de Contratación de la Administración Pública”.
• Ley 1150 de 2007 “Por medio de la cual se introducen medidas para la</td></tr>
</table>

	eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos." • Ley 1266 de 2008 "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones". • Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública". • Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales". • Ley 2069 de 2020 "Por medio del cual se impulsa el emprendimiento en Colombia" • Ley 1882 de 2018 "Por la cual se adicionan, modifican y dictan disposiciones orientadas a fortalecer la contratación pública en Colombia, la Ley de Infraestructura y se dictan otras disposiciones". • Ley 2195 de 2022 "Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones". • Decreto Ley 019 de 2012 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública". • Decreto 1078 de 2015 "Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones en Colombia". • Decreto 1082 de 2015 "Por medio del cual se expide el decreto único reglamentario del sector administrativo de planeación nacional". o Artículo 2.2.1.2.4.2.2 del Decreto 1082 de 2015 modificado por el artículo 5 del Decreto 1860 de 2021 – No Aplica (Ver estudio del sector). o Decreto 1082 de 2015, Art 2.2.1.2.4.2.16 y Decreto 380 de 2015 -No Aplica (Ver estudio del sector). o Aplicación Artículo 2.2.1.2.4.2.19. del Decreto 1082 de 2015 - No Aplica (Ver estudio del sector). • Política de Gobierno Digital. • Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) • Manual de Contratación de la UAERMV que se encuentre vigente. • Decreto 189 de 2020, "Por el cual se expiden lineamientos generales sobre transparencia, integridad y medidas anticorrupción en las entidades y organismos del orden distrital y se dictan otras disposiciones". • Directiva 03 de 2021 de la Presidencia de la República. • Decreto 1860 de 2021, "Por el cual se modifica y adiciona el Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional, con el fin reglamentar los artículos 30, 31, 32, 34 y 35 de la Ley 2069 de 2020, en lo relativo al sistema de compras públicas y se dictan otras disposiciones". o Aplicación Artículo 2.2.1.2.4.2.15 y 2.2.1.2.4.2.18 del Decreto 1860 de 2021 - Si Aplica (Ver estudio del sector). • CONPES de Seguridad Digital vigente. • Circular 013 de 2021 expedida por la Secretaría Distrital de la Mujer. • Decreto 310 de 2021 "Sobre Aplicación de los Acuerdos Marco de Precios"., No es posible aplicar teniendo en cuenta que el 24 de julio, Colombia

	Compra Eficiente suspendió durante 30 días el proceso de contratación. Según la resolución y el comunicado publicados por la entidad, la decisión buscaba dar claridad y tranquilidad a los interesados, a los organismos de control y a la ciudadanía, teniendo en cuenta las solicitudes de información de la Procuraduría y las 5.652 observaciones que habían presentado los interesados. (https://www.procuraduria.gov.co/Pages/procuraduria-advierte-posibles-irregularidades-proceso-cibers…) • Decreto 957 de 2019.
4.5. Decreto 643 de 2025, *artículo 29 (Si aplica). -En caso de que no aplique indicarlo así*	En cumplimiento de lo establecido en el inciso segundo del artículo 29 del Decreto 643 de 2025, que indica: "Se encuentran exceptuados de la aplicación de las medidas afirmativas previstas en este decreto, los procesos adelantados por acuerdo marco de precios, bolsa de productos, tienda virtual del Estado y las tipologías contractuales para la adquisición de bienes y servicios que por su naturaleza no requieran de personal para la ejecución del contrato y/o convenio, entre ellos arrendamiento de bienes inmuebles, compraventa, adquisición de bienes a través de la bolsa de productos, subastas a través de martillo, suministros, enajenación de bienes, comodatos, prestación de servicios profesionales y de apoyo a la gestión." • Se determina que, en virtud de la tipología contractual, esta normativa no es aplicable para la presente contratación, por tratarse de una compraventa.
4.6. Decreto 287 de 2026, artículo 2.2.1.2.4.2.7.1. Compras públicas accesibles y artículo 2.2.1.2.4.2.7.3. *Incorporación de criterios habilitantes diferenciales en favor de los emprendimientos y empresas de personas con discapacidad. (Si aplica). -En caso de que no aplique indicarlo así*	De conformidad con lo dispuesto en el Decreto 287 de marzo de 2026, en favor de lo previsto en las numerales 1, 7 y 8 del artículo 13 de la Ley 1618 de 2013 para los Procesos de Contratación en favor de personas con discapacidad, los emprendimientos y empresas de personas con discapacidad y las empresas empleadoras de personas con discapacidad, la entidad en cumplimiento del ARTÍCULO 2.2.1.2.4.2.7. DEFINICIÓN Y ALCANCE DEL SISTEMA DE PREFERENCIAS EN FAVOR DE LAS PERSONAS CON DISCAPACIDAD, ha decidido optar por la opción No. 2 y No. 3, numeral b), así: "2) En cumplimiento de lo previsto en el numeral 7 del artículo 13 de la Ley 1618 de 2013, relativo a la preferencia en la adjudicación y celebración del contrato para empleadores de personas con discapacidad, las Entidades Estatales deberán aplicar los criterios de desempate establecidos en este Decreto, cuando se configuren los supuestos correspondientes. 3) En desarrollo del numeral 8 del artículo 13 de la Ley 1618 de 2013, y para la implementación del Sistema de Preferencias como conjunto de medidas afirmativas, las entidades deberán planear, estructurar y ejecutar sus procesos de contratación considerando las herramientas previstas en los artículos 2.2.1.2.4.2.7.1. y siguientes del presente Decreto, medidas que componen el Sistema de Preferencias, a saber: [..] b) Incorporación de criterios habilitantes diferenciales en favor de los emprendimientos y empresas de personas con discapacidad [..]" Para dar aplicabilidad en el presente proceso, por lo tanto, en el estudio previo y los pliegos definitivos, se deberá reglar que, en caso de empate entre los proponentes, la oferta que incluya la contratación de personas en alguna condición de discapacidad deberá ser uno de los criterios para seleccionarla. Adicional, para las empresas catalogadas como emprendimientos y empresas de

<table>
<tr><td></td><td>personas con discapacidad, podrán acreditar experiencia con máximo cinco (5) contratos ejecutados y registrados en el RUP, mientras que los demás tipos de empresas, se deberá acreditar experiencia con máximo tres (3) contratos ejecutados y registrados en el RUP, cuyo objeto o alcance se encuentre relacionado con la suscripción, implementación y soporte de soluciones o plataformas de ciberseguridad, así:

<table>
<tr><th colspan="2">Número de contratos con los cuales el proponente cumple la experiencia</th><th rowspan="2">Valor mínimo a certificar (como % del Presupuesto Oficial expresado en SMMLV)</th></tr>
<tr><th>MiPymes, emprendimiento de mujeres y emprendimiento de empresas de personas con discapacidad</th><th>No MiPymes</th></tr>
<tr><td>Máximo 5</td><td>Máximo 3</td><td>100%</td></tr>
</table></td></tr>
<tr><td>4.7. Requerimientos y especificaciones mínimas*</td><td>La UAERMV requiere la suscripción, implementación, configuración, soporte y actualización de una plataforma de ciberseguridad de nueva generación para la protección integral de los activos digitales de la entidad, compuesta por una solución de Endpoint Detection and Response (EDR) y una solución de Data Loss Prevention (DLP), bajo esquema de servicio en la nube (SaaS).</td></tr>
<tr><td>4.8. Lugar de Ejecución y/o entrega</td><td>El lugar de entrega de los productos será en las instalaciones de la sede Administrativa de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, Ubicada en la Calle 26 # 69-76, Piso 3, Edificio Elemento, Torre Aire, sujeta a previa coordinación del almacén y de la Supervisión o quien hace sus veces.</td></tr>
<tr><td>4.9. Presupuesto Oficial de la Contratación, Valor Estimado del Contrato y su Justificación.</td><td>El valor para adelantar el proceso de contratación PRESUPUESTO OFICIAL ESTIMADO – POE, es de QUINIENTOS VEINTITRÉS MILLONES SEISCIENTOS CINCUENTA Y DOS MIL CUATROCIENTOS CUARENTA Y OCHO PESOS M/CTE ($523.652.448,00), este valor incluye IVA para el servicio “Servicios de instalación, configuración, pruebas, puesta en marcha, estabilización y soporte”, para los servicios “Solución EDR Avanzada” y “solución DLP Avanzada”, las soluciones de computación en la nube no pagan IVA porque están consideradas como un servicio excluido según el numeral 21 del artículo 476 del Estatuto Tributario; también incluye todos los gastos directos e indirectos, tasas e impuestos, contribuciones, pólizas, retenciones y demás descuentos de ley a que haya lugar, en los cuales incurra el contratista para cumplir cabalmente con el objeto contractual como lo son las estampillas del 3.6% aplicables el Distrito de Bogotá (Universidad Distrital 1.1 %, Proadulto Mayor 2% y Procultura 0.5%).</td></tr>
<tr><td>4.10. Forma y Requisitos de pago</td><td>La adquisición de las licencias EDR (Endpoint Detection and Response) y DLP (Data Loss Prevention) requeridas por la UAERMV, junto con su respectivo servicio de implementación e instalación, se realizará mediante un único pago, previa verificación del recibo a satisfacción de las licencias activas, la instalación y configuración completa de la solución, y la entrega del acta de puesta en marcha o documento equivalente suscrito por el supervisor del contrato.

Previa programación del PAC se cancelará con la presentación de la factura; la UAERMV requerirá para el pago de la factura, Certificación de cumplimiento de las obligaciones laborales y de pago de aportes a la seguridad social y parafiscales, de conformidad con lo señalado por el artículo 50 de la Ley 789 de 2002, la Ley 828 de 2003. Previa suscripción de pre acta y acta por parte del contratista y el supervisor</td></tr>
</table>

del contrato en los formatos establecidos por la entidad, la cual exige, además, el cumplimiento de las especificaciones técnicas, así como lo estipulado en el Manual de Supervisión e Interventoría de la UAERMV.

Con la presentación de la factura, se requerirá presentar al Supervisor la siguiente documentación mínima:

1. Pre acta y acta de solicitud de servicio suscrita por parte del contratista y el supervisor del contrato en los formatos establecidos por la entidad
2. Certificación por medio de la cual acredite que se encuentra al día en el pago de aportes parafiscales relativos al Sistema de Seguridad Social Integral, así como los propios del SENA, ICBF y cajas de compensación familiar, cuando corresponda, de conformidad con lo dispuesto en el artículo 23 de la Ley 1150 de 2007, concordante con lo señalado por el artículo 50 de la Ley 789 de 2002, la Ley 828 de 2003, el Decreto 1703 de 2002 y la Ley 100 de 1993.
3. Factura o documento equivalente
4. Registro Único Tributario (RUT) y Registro de Identificación Tributaria (RIT).
5. Formato de control financiero GEFI-FM-014
6. Los documentos relacionados en las obligaciones del contratista.
7. Informe de supervisión que evidencie el cumplimiento del objeto del contrato.

El original de los anteriores documentos debe ser radicado en la oficina de Radicación de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial - UMV o por correo electrónico habilitado por la UAERMV con todos sus anexos, según lo indique el supervisor.

La UAERMV solo adquiere obligaciones con el Contratista y bajo ningún motivo o circunstancia aceptará pagos a terceros. Si las facturas no han sido correctamente elaboradas o no se acompañan con los documentos requeridos para el pago, el término para el mismo empezará a contarse desde la fecha en que se presenten debidamente corregidas, o desde que se haya aportado el último de los documentos solicitados.

Las demoras que se presenten por estos conceptos serán responsabilidad del Contratista y no tendrán por ello derecho al reconocimiento de intereses o compensación de ninguna naturaleza. Adicionalmente, se deberá tener en cuenta lo estipulado en el Manual de Contratación de la UAERMV, adoptado mediante Resolución N° 571 del 6 de diciembre de 2021 o la que se encuentre vigente

Al momento de tramitarse el pago correspondiente, la Entidad liquidará y descontará los impuestos y tasas, tales como rete ICA, estampilla Universidad Distrital, estampilla ProAdulto Mayor, estampilla ProCultura, y todos aquellos a los que haya lugar. El valor de las estampillas corresponde a:

RUBRO	PORCENTAJE
UNIVERSIDAD DISTRITAL	1.1%
PROADULTO MAYOR	2%

	<table><tr><td>PROCULTURA</td><td>0.5%</td></tr><tr><td>**TOTAL**</td><td>3.6%</td></tr></table> **Nota**: El valor del contrato incluye IVA para el servicio “Servicios de instalación, configuración, pruebas, puesta en marcha, estabilización y soporte”, para los servicios “Solución EDR Avanzada” y “solución DLP Avanzada”, las soluciones de computación en la nube no pagan IVA porque están consideradas como un servicio excluido según el numeral 21 del artículo 476 del Estatuto Tributario; también incluye todos los gastos directos e indirectos, tasas e impuestos, contribuciones, pólizas, retenciones y demás descuentos de ley a que haya lugar, en los cuales incurra el contratista para cumplir cabalmente con el objeto contractual. Adicional a lo aquí señalado se deberá tener en cuenta lo estipulado en el Manual de Contratación de la UAERMV que se encuentre vigente. Justificación de la forma de pago: En atención a la naturaleza propia de este tipo de contratación. Las licencias se activan y transfieren en su totalidad al momento de la suscripción, habilitando de manera inmediata el derecho de uso pleno de las herramientas durante el periodo contratado; y el servicio de implementación e instalación, por su parte, corresponde a una actividad puntual y de corta duración —despliegue de agentes, configuración de políticas y puesta en marcha de las consolas de administración— que se agota con la entrega funcional de la solución, sin que existan hitos intermedios de ejecución susceptibles de pagos parciales independientes. Esta es además la modalidad de comercialización estándar del mercado para este tipo de soluciones, en la que el proveedor y/o fabricante condiciona la activación de las licencias y la prestación del servicio asociado al pago íntegro del contrato. Fraccionar el pago no solo carecería de respaldo en la forma real de ejecución del objeto contractual, sino que generaría cargas administrativas y financieras innecesarias tanto para la Entidad como para el contratista, en desmedro de los principios de economía y eficiencia que rigen la contratación pública. En consecuencia, se considera técnica y económicamente justificado que el pago se efectúe en un único desembolso.
4.11. Anticipo	No Aplica
4.12. Vigilancia y Supervisión y/o interventoría	La supervisión del contrato estará a cargo de JUAN CARLOS ALBA ALBARRACÍN – Profesional Especializado de la UAERMV, quien deberá cumplir con las obligaciones descritas en la Ley y en el Manual de Interventoría y Supervisión vigente de la UAERMV.
4.13. Persona Gerente del Proyecto	Se designa como responsable del proceso de contratación, al (la) Jefe de la Oficina de Tecnologías de la Información, quien será el encargado del seguimiento hasta la designación de supervisor del contrato que se genere a partir del presente estudio previo.

4.14. OBLIGACIONES DE LAS PARTES

4.14.1. OBLIGACIONES DEL CONTRATISTA

A. OBLIGACIONES Generales:

1. Desarrollar el objeto del contrato, conforme a las condiciones de calidad, oportunidad, y obligaciones

definidas en el contrato su ficha técnica, estudios previos, pliegos de condiciones y demás documentos constitutivos del mismo.
2. Cumplir durante la ejecución del contrato con los compromisos asumidos en especial en los factores técnicos de calidad establecidos durante el proceso de selección.
3. Cumplir con lo dispuesto en el Plan Institucional de Gestión Ambiental- PIGA-de la UAERMV, observando las normas sobre protección y conservación del medio ambiente, el uso eficiente de los recursos, la adecuada segregación de residuos, la participación en actividades de sensibilización ambiental y demás disposiciones aplicables.
4. Informar oportunamente a la UAERMV cualquier reclamación, ya sea directa o indirecta que pueda afectar el objeto del Contrato o las obligaciones. derivadas del mismo
5. Informar a la UAERMV cualquier circunstancia política, jurídica, social, económica, técnica, ambiental o de cualquier otra índole, que pueda influir en la ejecución del Contrato.
6. Custodiar y, al finalizar el contrato, devolver los insumos, suministros, herramientas, dotación, , inventarios y materiales proporcionados para la ejecución del objeto del contrato (si aplica).
7. Estar al día en el pago de sus obligaciones laborales frente al sistema de seguridad social integral y demás aportes relacionados con las obligaciones laborales.
8. En caso de que exista información sujeta a reserva legal, las partes deberán mantener la confidencialidad de dicha información y se debe comunicar a la otra parte sobre su carácter de confidencial.
9. Presentar informe al Supervisor(a) o Interventor del contrato, sobre el cumplimiento de las obligaciones, para efectos de pago (si aplica).
10. Cumplir con el objeto del contrato con total autonomía y bajo su propia responsabilidad, sin que exista vinculo de subordinación ni laboral entre el CONTRATISTA y la UAERMV.
11. Responder por sus acciones u omisiones derivadas de la celebración y ejecución del contrato, conforme a lo establecido en la Ley 80 de 1993, Ley 1150 de 2007 y sus Decretos Reglamentarios.
12. Acatar las instrucciones impartidas por la UAERMV durante la ejecución del contrato l para garantizar su correcta realización.
13. Presentar oportunamente los documentos exigidos por el Supervisor.
14. No ceder a peticiones o amenazas de personas que actúan fuera de la ley, que intenten obligarlo a realizar u omitir actos ilegales. Ante tales situaciones el contratista deberá informar a la UAERMV y a las autoridades competentes para que tomen las medidas necesarias.
15. Vincular y mantener durante la ejecución del contrato, el porcentaje mínimo de mujeres establecido para la rama de actividad.
16. Presentar ante el interventor o supervisor del contrato el certificado de Autoevaluación de estándares mínimos de Seguridad y Salud en el Trabajo (SG – SST) del año inmediatamente anterior según normatividad legal vigente
17. [16.] Cumplir con todas las demás obligaciones necesarias para el cumplimiento del objeto del contrato derivadas de su naturaleza y de los estudios previos.

B. OBLIGACIONES ESPECÍFICAS:

1. Cumplir a entera satisfacción con el objeto del contrato en los términos pactados, de conformidad con las condiciones jurídicas, técnicas, económicas y comerciales presentadas en la propuesta.
2. Cumplir con las características técnicas mínimas definidas en el documento anexo GCON-FM-022.
3. Suministrar todos los elementos necesarios para la instalación y puesta en funcionamiento de la solución de ciberseguridad, así como los gastos de transporte y desplazamiento de los equipos, sin generar costos adicionales para la UAERMV.
4. Garantizar la continuidad del licenciamiento sin interrupciones. Proveer licencias válidas, originales y actualizadas del software de seguridad y antivirus EDR.
5. Atender y responder a las solicitudes de concepto, observaciones y/o inquietudes que realice la UAERMV a través de la supervisión designada.
6. Garantizar que los elementos a entregar deben ser nuevos no remanufacturados con la calidad óptima

de fabricación que garantice la máxima durabilidad de los mismos.

7. Entregar junto con la solución de seguridad ofertada, una certificación emitida por el fabricante, por un 1 año; esta deberá incluir un esquema de soporte 7x24, acceso al portal de soporte, recursos técnicos y solicitud de soporte por incidentes vía web, chat y teléfono.
8. Entregar los productos y servicios en los plazos establecidos y realizar la instalación, configuración y puesta en marcha de la plataforma de seguridad *endpoint* de nueva generación.
9. Capacitar al personal técnico de la UAERMV en el uso, administración y monitoreo de las soluciones adquiridas. Entregar manuales, guías y documentación correspondiente.
10. Asegurar que las soluciones cumplan con las normas de seguridad y otras normativas aplicables en el país e las normas de confidencialidad y tratamiento de datos personales.
11. El contratista deberá responder en caso de que se presente algún tipo de falla, cuantas veces la Entidad lo requiera, para lo cual deberá garantizar la disponibilidad de personal para atender emergencias o imprevistos durante la ejecución del contrato y hasta la vigencia de la garantía requerida.
12. Reemplazar los elementos que por cualquier motivo sean catalogados como defectuosos para lo cual el supervisor del contrato comunicará por escrito al contratista la situación presentada y este (el contratista), de manera inmediata, dará respuesta suministrando plan de contingencia.
13. El contratista dentro de los cinco (05) días hábiles siguientes a la firma del acta de inicio del contrato deberá realizar de manera conjunta con la UAERMV el cronograma de trabajo (donde se programará la fecha de entrega, instalación y puesta en funcionamiento y todas las actividades que se deban llevar a cabo en la ejecución del contrato para su recibo a satisfacción), conforme a las necesidades de la entidad.

4.14.2. OBLIGACIONES DE UAERMV:

1. Exigir al CONTRATISTA la ejecución idónea y oportuna del objeto contratado a través del -Supervisor (Interventor)- que sea -designado (contratado)- para el efecto
2. Prestar su colaboración para el cumplimiento de las obligaciones del CONTRATISTA.
3. Realizar los pagos correspondientes, una vez se cumplan los requisitos establecidos para tal fin.

5. MODALIDAD DE SELECCIÓN DEL CONTRATISTA Y SU JUSTIFICACIÓN, INCLUYENDO SUS FUNDAMENTOS JURÍDICOS	
SELECCIÓN ABREVIADA POR SUBASTA INVERSA	Por tratarse de la contratación de bienes y servicios de tecnología de la información de características técnicas uniformes y de común utilización, con especificaciones técnicas y patrones de desempeño y calidad iguales o similares, tales como: soporte técnico especializado, componentes de monitoreo y gestión y garantía de la solución de ciberseguridad definida por el fabricante, la UAERMV hará uso de la modalidad de selección abreviada prevista en el literal a) del numeral 2° del artículo 2° de la Ley 1150 de 2007, bajo el procedimiento de subasta inversa establecido en el artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015, modificado por el artículo 6 del Decreto 1860 de 2021, el cual describe que dentro de las diferentes causales “La adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades, que corresponden a aquellos que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos”. Las soluciones tecnológicas objeto del contrato cuentan con condiciones objetivas de estandarización, expresadas en las fichas técnicas anexas, lo que permite establecer un precio máximo aceptable, fomentar la competencia entre proveedores que comercializan productos con prestaciones equivalentes, y asegurar la transparencia, eficiencia y economía del proceso.

6. REQUISITOS HABILITANTES Y CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE

La **UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACIÓN Y MANTENIMIENTO VIAL**, informa que dentro del proceso de estructuración se tuvieron en cuenta las guías y manuales definidos por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente, para la definición de criterios que permitan garantizar la pluralidad de oferentes, dando cumplimiento a lo ordenado en el Artículo 2.1.4.3.2.1. del decreto 1600 de 2024, por medio del cual "(…) se modifica el Capítulo 1 y 3 del Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, Decreto Reglamentario Único del Sector Presidencia de la República, en lo relacionado con las Subcomisiones Técnicas de la Comisión Nacional de Moralización y la Estrategia Nacional de Lucha Contra la Corrupción.

Así las cosas, se presentan a continuación los requisitos habilitantes y fator de selección de la propuesta:

-NOTA GENERAL SOBRE LOS REQUISITOS HABILITANTES: *El artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015 señaló que, para establecer los requisitos habilitantes del proceso de selección, se debe tener en cuenta lo siguiente:*

El Riesgo del Proceso de Contratación
El valor del contrato objeto del Proceso de Contratación
El análisis del sector económico respectivo
El conocimiento de fondo de los posibles oferentes desde la perspectiva comercial.

Es así como la Entidad Estatal no debe limitarse a la aplicación mecánica de fórmulas financieras para verificar los requisitos habilitantes.

Teniendo en cuenta lo anterior, es preciso que los requisitos habilitantes se establezcan de forma adecuada y proporcional a la naturaleza y valor del contrato, teniendo en cuenta los lineamientos dados por Colombia Compra Eficiente y las necesidades de la Entidad. La expresión adecuada y proporcional hace referencia a que haya una relación entre el contrato y la experiencia del proponente y su capacidad jurídica, técnica, financiera y organizacional, es decir, los requisitos habilitantes exigidos deben guardar proporción con el objeto del contrato, su naturaleza, valor, complejidad, plazo, forma de pago y el Riesgo asociado al Proceso de Contratación. -

6.1. HABILITANTES JURÍDICOS

Los interesados podrán participar como proponentes bajo alguna de las siguientes modalidades siempre y cuando cumplan los requisitos exigidos en el pliego de condiciones:

- Individualmente como: a) personas naturales nacionales o extranjeras, b) personas jurídicas nacionales o extranjeras.
- Conjuntamente, como proponentes plurales en cualquiera de las formas de asociación previstas en el artículo 7 de la Ley 80 de 1993.

Los proponentes deben:

- Tener capacidad jurídica para la presentación de la oferta.
- Tener capacidad jurídica para la celebración y ejecución del contrato.
- No estar incursos en ninguna de las circunstancias de inhabilidad, incompatibilidad, conflicto de interés o prohibición para contratar previstas en la Constitución y en la Ley.
- De No estar reportados en el último Boletín de Responsables Fiscales vigente publicado por la Contraloría General de la República. Esta disposición aplica para el proponente e integrantes de un proponente plural con domicilio en Colombia. Tratándose de proponentes extranjeros sin domicilio o sin sucursal en Colombia, deben declarar que no son responsables fiscales por actividades ejercidas en

Colombia en el pasado y que no tienen sanciones vigentes en Colombia que impliquen inhabilidad para contratar con el Estado

El proponente junto con la propuesta debe aportar las consultas de los sistemas de información de antecedentes, los cuales serán consultados por la entidad:

- Certificado de responsables Fiscales de la Contraloría General de la República.
- Certificado de Antecedentes Disciplinarios expedido por la Procuraduría General de la Nación.
- Certificado de Antecedentes Judiciales expedido por la Policía Nacional.
- Certificado de antecedentes registro nacional de medidas correctivas RNMC – Policía Nacional de Colombia.
- Certificado de Antecedentes disciplinarios Personería.
- El proponente debe acreditar no estar inhabilitado en los términos de la Ley 2097 de 2021 – REDAM. Para el caso de proponentes plurales este certificado deberá ser presentado por cada uno de los representantes legales de las personas jurídicas que lo conforman

Conforme con lo establecido en la Ley 2097 de 2021, articulo 6 que trata sobre las "Consecuencias de la inscripción en el registro de deudores alimentarios morosos", en el que se indica: "1. El deudor alimentario moroso solo podrá contratar con el Estado una vez se ponga a paz y salvo con sus obligaciones alimentarias. Esta inhabilidad también se predica del deudor alimentario moroso que actúe como representante legal de la persona jurídica que aspira a contratar con el Estado."

En consideración a norma en cita, reglamentada por el Ministerio de Tecnologías de la información y las Comunicaciones de Colombia por medio del Decreto 1310 de 2022, se deberá aportar el certificado que acredita la condición de deudor o no alimentario moroso del representante legal expedido por el Ministerio de las Tecnologías de la información y las comunicaciones -MINTIC, el cual puede ser descargado de forma gratuita desde la Carpeta Digital ciudadana https://carpetaciudadana.and.gov.co.

NOTA: Sobre la VERIFICACIÓN DE INEXISTENCIA DE ANTECEDENTES JUDICIALES Y VERIFICACIÓN EN EL REGISTRO NACIONAL DE MEDIDAS CORRECTIVAS DEL MINISTERIO DE DEFENSA NACIONAL – POLICÍA NACIONAL. La Entidad consultará y verificará en la página Web de Policía Nacional de Colombia los antecedentes penales de la persona natural y el representante legal de la persona jurídica o de los integrantes del consorcio, unión temporal. En virtud de la sugerencia realizada en la Directiva No. 016 del 5 de julio de 2018, expedida por la Secretaría Jurídica Distrital, la Entidad consultará y verificará en la página web del REGISTRO NACIONAL DE MEDIDAS CORRECTIVAS DEL MINISTERIO DE DEFENSA NACIONAL – POLICÍA NACIONAL que la persona que presenta la propuesta, a título de Persona Natural o Representante Legal, se encuentre al día en el pago de las multas que le hayan sido impuestas. En caso de que, verificado el anterior registro, se evidencie que quien presenta la propuesta no se encuentra al día en el pago de las multas impuestas, se le requerirá para que lo haga dentro del mismo término de subsanación y su cumplimiento se podrá verificar, tanto en el registro respectivo actualizado, o, también a partir del recibo de pago que el proponente aporte para tal efecto.

- Si el proponente es una entidad sin ánimo de lucro, su objeto social le debe permitir ejecutar el objeto del contrato que se pretende suscribir, y debe presentar el correspondiente certificado donde conste que se encuentra inscrita en el registro de entidades sin ánimo de lucro de la Cámara de Comercio o de la autoridad competente, con una vigencia máxima de 30 días anteriores al cierre del proceso de selección, y acreditar que su duración es igual al plazo para la ejecución del contrato y mínimo tres (3) años más.

  Igualmente deberán allegar el certificado de inspección, vigilancia y control expedido por la Subdirección Distrital de Inspección, Vigilancia y Control de Personas Jurídicas sin Ánimo de Lucro -Super- personas Jurídicas de la Alcaldía Mayor de Bogotá, o de la entidad competente, cuya fecha de

expedición no supere los noventa (90) días calendario anteriores al cierre del proceso.

6.1.1. CARTA DE PRESENTACIÓN DE LA PROPUESTA

Para acreditar el presente criterio habilitante el proponente deberá diligenciar el **ANEXO - CARTA DE PRESENTACIÓN DE LA PROPUESTA** adjunto al pliego de condiciones, en el cual se indica la información que cada proponente debe manifestar en la misma y cumplir en caso de ser favorecido.

NOTA 1: Se solicita aportar copia del documento de identificación de quien suscribe la Carta de Presentación de la propuesta.

NOTA 2: La carta de presentación de la propuesta debe estar debidamente firmada por el proponente cuando se trate de una persona natural o por el representante legal cuando se trate de una persona jurídica, consorcio o unión temporal.

NOTA 3: **ACTUACIÓN A TRAVÉS DE APODERADOS** Los proponentes podrán presentar propuestas directamente o por intermedio de apoderado, evento en el cual deberán anexar con la propuesta el acto de apoderamiento otorgado en legal forma, en el que se confiera al apoderado, de manera clara y expresa, facultades suficientes para actuar, obligar y responsabilizar a todos y cada uno de los integrantes en el trámite del presente proceso contractual y en la suscripción del contrato. El apoderado podrá ser una persona natural o jurídica, pero en todo caso deberá tener domicilio permanente, para efectos de este proceso, en la República de Colombia, y deberá estar facultado para representar conjuntamente al proponente y a todos los integrantes del proponente plural.

6.1.2. CAPACIDAD JURÍDICA – ACREDITACIÓN DE LA EXISTENCIA Y REPRESENTACIÓN LEGAL

El oferente debe adjuntar los documentos señalados, de acuerdo con la naturaleza si es persona natural o jurídica o proponente extranjero, (si es proponente plural cada integrante presentará su información individualmente).

Personas jurídicas

Las personas jurídicas acreditarán su capacidad jurídica mediante el certificado de existencia y representación legal expedido por la Cámara de Comercio de su domicilio, con fecha de expedición no mayor a treinta (30) días calendario anteriores a la presentación de la propuesta, o por la entidad competente para expedir dicho certificado.

La Entidad verificará la capacidad jurídica de la persona jurídica revisando los siguientes aspectos:

- Que el objeto social contemple las actividades necesarias para cumplir con el objeto del contrato.
- La calidad de representante legal de quien suscribe la oferta, verificada en el certificado de existencia y representación legal.
- Las facultades del representante legal para presentar la oferta y obligar a la persona jurídica al cumplimiento del contrato, conforme al certificado de existencia y representación legal.
- Que la vigencia de la persona jurídica no sea inferior al plazo del contrato, incluyendo, cuando corresponda, el término de su liquidación y el periodo adicional exigido para las garantías solicitadas.
- La inexistencia de inhabilidades, incompatibilidades o prohibiciones para contratar con el Estado, lo cual se declara en la Carta de Presentación de la Propuesta. La UAERMV verificará que los proponentes no se encuentren incursos en causales de inhabilidad o incompatibilidad, revisando, entre otros, el boletín de responsables fiscales, el certificado de antecedentes disciplinarios, el certificado de antecedentes judiciales y el RUP.

Notas:

1. Si la propuesta se presenta a nombre de una sucursal, deberán anexarse los certificados de la sucursal y de la casa principal que evidencien la actuación.
2. Cuando el representante legal tenga restricciones para contraer obligaciones en nombre de la persona jurídica, deberá presentar autorización expresa del órgano social competente (Asamblea, Junta Directiva, etc.), en la que conste que está facultado para presentar la propuesta y suscribir el contrato hasta por el valor de la oferta. En el caso de consorcios o uniones temporales, este documento será exigible a cada integrante que tenga restricciones.

Consultas adicionales de la Entidad:

- Certificado de responsables Fiscales – Contraloría General de la República.
- Certificado de Antecedentes Disciplinarios – Procuraduría General de la Nación.
- Certificado de Antecedentes Judiciales – Policía Nacional.
- Registro Nacional de Medidas Correctivas (RNMC) – Policía Nacional de Colombia.

Personas naturales

La Entidad verificará la capacidad jurídica de las personas naturales de la siguiente manera:

- La mayoría de edad, acreditada con cédula de ciudadanía para nacionales, y con cédula de extranjería o pasaporte para extranjeros.
- La inexistencia de inhabilidades, incompatibilidades o prohibiciones para contratar con el Estado, declarada en la Carta de Presentación de la Propuesta.
- Si el oferente es comerciante, deberá presentar el certificado de inscripción en el Registro Mercantil expedido por la Cámara de Comercio, con fecha de expedición no mayor a treinta (30) días anteriores al cierre de la recepción de ofertas.

Consultas adicionales de la Entidad:

- Certificado de responsables Fiscales – Contraloría General de la República.
- Certificado de Antecedentes Disciplinarios – Procuraduría General de la Nación.
- Certificado de Antecedentes Judiciales – Policía Nacional.
- Registro Nacional de Medidas Correctivas (RNMC) – Policía Nacional de Colombia.
- Certificado del Registro de Deudores Alimentarios Morosos (REDAM).

Nota sobre verificación de antecedentes y medidas correctivas:

La Entidad consultará en la página web de la Policía Nacional los antecedentes penales de la persona natural, del representante legal de la persona jurídica o de los integrantes del consorcio o unión temporal. En virtud de la Directiva 001 de 2021 de la Secretaría Jurídica Distrital, también verificará en el Registro Nacional de Medidas Correctivas del Ministerio de Defensa – Policía Nacional que el proponente se encuentre al día en el pago de las multas impuestas. En caso contrario, se le requerirá para subsanar dentro del término legal, pudiendo acreditarse el cumplimiento mediante el registro actualizado o el recibo de pago correspondiente.

Proponentes extranjeros:

Las personas jurídicas extranjeras deben acreditar su existencia y representación legal con el documento idóneo expedido por la autoridad competente en el país de su domicilio no anterior a tres (3) meses desde la fecha de presentación de la Oferta, en el cual conste que el representante legal no tiene limitaciones para contraer obligaciones en nombre de la persona jurídica, o aportando la autorización o documento correspondiente del órgano social directo que lo faculta.

Las sociedades extranjeras sin sucursal en Colombia deberán acreditar que cuentan con un apoderado debidamente constituido, con domicilio en Colombia y ampliamente facultado para representarlas extrajudicialmente hasta la constitución de la sucursal en Colombia, en caso de resultar aceptada su propuesta, de conformidad con lo señalado en el título VIII del Libro II del Código de Comercio Colombiano.

Si se trata de sociedades extranjeras sin sucursal en Colombia, de países que hagan parte de la *"Convención sobre la abolición del requisito de legalización para documentos públicos extranjeros"*, se tendrán en cuenta las siguientes reglas:

- El documento público relacionado con sociedades extranjeras en el cual se certifique la existencia de la sociedad y el ejercicio de su objeto social tendrá validez en Colombia con la sola Apostilla.
- Cuando el documento otorgado en el exterior deba ser autenticado, el interesado deberá velar porque la autoridad que autentica certifique sobre la existencia de la sociedad y sobre la extensión del objeto social, documento éste que se deberá apostillar.
- En el evento en el cual, en un Estado Parte de la Convención, la autoridad ante quien se autentican los documentos no tenga la facultad de certificar sobre la existencia de la sociedad y sobre el ejercicio del objeto social de la misma, el interesado podrá solicitar dichas certificaciones ante la autoridad competente del lugar. Para que surtan efectos en Colombia, estas certificaciones deberán a su vez ser apostilladas por la autoridad del Estado donde emana el documento. (Este requisito será exigible solo para el proponente que presente la oferta económica con el menor valor y para los efectos de la Aceptación de la Oferta).
- Si no existiera una autoridad local que pueda expedir las certificaciones de existencia de la sociedad y del ejercicio del objeto social de acuerdo con las leyes del respectivo país, el interesado podrá acudir ante el Cónsul Colombiano quien podrá certificar que tuvo a la vista las pruebas de la existencia de la sociedad y del ejercicio de su objeto conforme a las leyes del respectivo país. En este caso, como la Convención no se aplica a los documentos ejecutados directamente por agentes diplomáticos o consulares, deberá seguir el trámite ordinario de legalización, o sea que el Ministerio de Relaciones Exteriores de Colombia abonará la firma del Cónsul.

6.1.3. GARANTÍA DE SERIEDAD DE LA PROPUESTA.

El proponente, deberá otorgar a favor de la UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACIÓN Y MANTENIMIENTO VIAL – UAERMV - NIT. No. 900.127.032-7, y anexar con su propuesta, una garantía de seriedad de la oferta. Para el caso de las personas naturales o jurídicas extranjeras sin domicilio o sucursal en Colombia, podrán otorgar, como garantía, cartas de crédito Stand By, expedidas en el exterior.

En las propuestas presentadas por personas jurídicas la garantía debe ser tomada a nombre de la razón social que figura en el certificado de existencia y representación legal expedido por la Cámara de Comercio.

Cuando la oferta es presentada por un proponente plural, es decir, como Consorcio o Unión Temporal, la garantía deberá ser otorgada por todos sus integrantes, debidamente enunciado e identificado.

ETAPA	AMPAROS	%	VIGENCIA	JUSTIFICACIÓN
PRE CONTRACTUAL	**SERIEDAD DE LA OFERTA**	10 % del valor del presupuesto oficial.	TRES (3) MESES, contados a partir de la fecha de cierre de la presente Selección igualmente,	Cubre a la Entidad de los perjuicios derivados del incumplimiento de la oferta, en los siguientes eventos: No ampliación de la vigencia de la garantía cuando el plazo para la adjudicación o suscripción del contrato sea prorrogado, siempre que esa prórroga no exceda de tres (3) meses. Retiro de la oferta después de vencido el

			el proponente deberá mantenerla vigente hasta la aprobación de garantías del contrato	plazo para su presentación No suscripción del contrato sin justa causa por parte del adjudicatario La no constitución de la garantía de cumplimiento del contrato por parte del adjudicatario

NOTA: La no entrega de la garantía de seriedad junto con la oferta no será subsanable y en consecuencia será causal de rechazo de los ofrecimientos en consideración a lo indicado por el parágrafo 3º del artículo 5º de la Ley 1150 de 2007, incluido mediante el artículo 5º de la Ley 1882 del 15 de enero de 2018.

6.1.4. CERTIFICACIÓN DE PAGOS DE SEGURIDAD SOCIAL Y PARAFISCALES

PARA PERSONA JURÍDICA:

Las personas jurídicas deberán presentar con su propuesta una certificación expedida por el Revisor Fiscal, cuando así lo exijan los requerimientos legales, o por el representante legal, que acredite el pago de sus obligaciones respecto a los aportes a sus empleados a los sistemas de salud, riesgos profesionales, pensiones, y aportes a las Cajas de Compensación Familiar, el Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje. Esta certificación deberá corresponder a los últimos seis (6) meses del calendario en los que, legalmente, sean exigibles los pagos mencionados.

En el evento en que la sociedad tenga menos de seis (6) meses de constitución, deberá acreditar los pagos mencionados a partir de la fecha de su constitución.

PARA PERSONA NATURAL:

Cuando el proponente sea una persona natural, deberá certificar el pago de sus aportes y el de sus empleados (si los tuviere) a los sistemas de salud, riesgos profesionales, pensiones y aportes a las Cajas de Compensación Familiar, el Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje. Dicho documento debe certificar que, a la fecha de presentación de su oferta, ha realizado el pago de los aportes correspondientes de los últimos seis (6) meses del calendario que legalmente sean exigibles en la citada fecha, (o sea, en los cuales se haya causado la obligación de efectuar dichos pagos).

NOTA 1: En caso de que el proponente no tenga personal a cargo y por ende no esté obligado a efectuar al pago de aportes parafiscales y seguridad social por personal debe, también bajo la gravedad de juramento, indicar esta circunstancia.

NOTA 2: En caso de Consorcio, Unión Temporal o Promesa de Sociedad Futura, cada uno de sus integrantes debe cumplir con este requisito.

6.1.5. CERTIFICADO DE INSCRIPCIÓN EN EL REGISTRO ÚNICO DE PROPONENTES RUP.

El proponente deberá aportar el Registro Único de Proponentes de la Cámara de Comercio vigente y en firme a la fecha de cierre del proceso, expedido con fecha no mayor a treinta (30) días calendarios anteriores a la fecha de cierre del presente proceso de selección, de conformidad con el artículo 6 de la ley 1150 de 2007 y modificado por el artículo 221 del Decreto Ley 019 de 2012.

Cada integrante de unión temporal o consorcio, al momento de presentarse al proceso debe tener la inscripción en dicho registro igualmente, vigente y en firme.

Si el oferente no presenta con su propuesta el certificado de Registro Único de Proponentes (RUP) de la Cámara de Comercio, la Entidad requerirá al proponente a fin de que lo aporte dentro del plazo que la ley señale para el efecto.

La información contenida en el RUP debe encontrarse en firme al momento del cierre del proceso de contratación. En consecuencia, la Entidad Estatal evaluará las propuestas con base en el registro vigente y consolidado a esa fecha, sin que sea posible acreditar circunstancias ocurridas con posterioridad al cierre. Lo anterior se aplica incluso si, con posterioridad, se expide un nuevo RUP cuya información favorezca o perjudique al proponente, pues únicamente se tendrá en cuenta la información que estaba en firme antes del cierre del proceso, conforme a lo previsto en el artículo 5 de la Ley 1882 de 2018 y al Concepto C-353 de 2024.

NOTA: Aunque la Entidad puede consultar el documento del Registro Único de Proponentes del oferente a través de la plataforma SECOP II, es necesario que el proponente cargue este documento junto con la oferta, para que forme parte de los documentos generados directamente por él.

6.1.6. Documento de conformación del Consorcio o Unión Temporal:

Información de interés general: recuerde que este proceso de selección se lleva a cabo bajo las condiciones de la plataforma SECOP II. Por lo tanto, si presenta su propuesta como proponente plural (CONSORCIOS O UNIONES TEMPORALES), deberá realizar todos los trámites correspondientes a través de la plataforma mencionada. Para ello, puede consultar la guía de Colombia Compra Eficiente disponible en el siguiente enlace.

https://www.colombiacompra.gov.co/node/23695

https://www.colombiacompra.gov.co/sites/cce_public/files/cce_step/cce-sec-gi-06_guia_de_creacion_de_proponentes_plurales_en_el_secop_ii_29-05-2024.pdf

En todo caso, el proveedor debe verificar que la guía consultada corresponda a la última versión de los documentos guía publicados por Colombia Compra Eficiente.

Se entenderá por propuesta conjunta, una propuesta presentada en consorcio o unión temporal. En tal caso se tendrá como proponente, para todos los efectos, el grupo conformado por la pluralidad de personas y no las personas que lo conforman individualmente consideradas.

El Proponente deberá indicar en la carta de presentación y en el documento de conformación si su propuesta se formula a título de Consorcio o Unión Temporal, para lo cual deberá cumplir con los siguientes requisitos mínimos:

Indicar el tipo de asociación de que se trate: Consorcio o Unión Temporal.

Si se trata de Unión Temporal, sus miembros deberán señalar en la Propuesta la extensión (actividades y porcentaje) de su participación en la misma y en su ejecución, los cuales no podrán ser modificados sin el consentimiento previo y escrito de la Entidad.

Acreditar que la duración del consorcio o unión temporal debe extenderse por el plazo del contrato, su liquidación (si aplica) y un (1) año más, contados a partir de la fecha de cierre del presente proceso.

La designación de un representante que deberá estar facultado para actuar en nombre y representación del Consorcio o Unión Temporal. Igualmente deberá designar un suplente que lo reemplace en los casos de ausencia temporal o definitiva.

Los requisitos relacionados con la existencia, representación y capacidad jurídica de cada uno de los integrantes del consorcio o unión temporal, respecto de las personas que se asocien para la presentación de la propuesta, deberán acreditarse conforme se indica en los acápites respectivos de este documento.

6.1.7. COMPROMISO ANTICORRUPCIÓN:

Los Proponentes deben suscribir el compromiso anticorrupción, en el cual manifiestan su apoyo irrestricto a los esfuerzos del Estado Colombiano contra la corrupción.

6.2. HABILITANTES TÉCNICOS

6.2.1. CERTIFICACIÓN TÉCNICA DEL OFERENTE

El proponente deberá diligenciar el formato denominado CERTIFICACIÓN TÉCNICA DEL OFERENTE , mediante el cual acepta que conoce y se compromete a cumplir en su totalidad las especificaciones, características, requisitos técnicos y condiciones de entrega definidos en el formato GCON-FM-022, asumiendo las obligaciones que dicho compromiso acarrea.

6.2.2. CERTIFICACIONES DE PARTNER AUTORIZADO EMITIDA POR EL FABRICANTE

El proponente debe adjuntar junto con su propuesta carta emitida por el fabricante y dirigida a la entidad donde certifique que el proponente es Partner, canal o socio con el nivel más alto de membresía en la marca ofrecida en Colombia. La misma no debe ser con fecha superior a 30 días calendario anteriores a la fecha de cierre de este proceso (si se prorroga dicha fecha, esta certificación valdrá con la fecha inicial de cierre).

Nota 1: En caso de tratarse de un proponente plural (consorcio o unión temporal), el presente requisito podrá ser acreditado por cualquiera de sus integrantes, siempre que dicho integrante participe directamente en la ejecución del objeto contractual relacionado con la solución ofertada.

Nota 2: Para efectos de la evaluación se verificará que la certificación se encuentre vigente. Para la ejecución del contrato, el oferente adjudicatario deberá mantener vigente la certificación.

6.2.3 VERIFICACIÓN EXPERIENCIA

6.2.3.1 VERIFICACIÓN EXPERIENCIA PROPONENTE OBLIGADO A ESTAR INSCRITO EN EL REGISTRO ÚNICO DE PROPONENTES

El proponente persona natural o jurídica o plural deberá acreditar la experiencia con el certificado de inscripción, calificación y clasificación RUP de acuerdo con el clasificador de bienes y servicios en tercer nivel expresado en SMMLV, en alguno de los códigos indicados en la siguiente tabla:

Clasificación UNSPSC	Segmento	Familia	Clase	Productos
43222501	(43000000) Difusión de tecnologías de información y telecomunicaciones.	(43220000) Equipos o plataformas y accesorios de redes multimedia o de voz y datos.	[43222500] Equipo de seguridad de red	[43222501] Equipo de seguridad de red cortafuegos (firewall)
43222502	(43000000)	(43220000)	[43222500]	[43222502]

	Difusión de tecnologías de información y telecomunicaciones.	Equipos o plataformas y accesorios de redes multimedia o de voz y datos.	Equipo de seguridad de red	Equipo de seguridad de redes vpn
43233200	(43000000) Difusión de tecnologías de información y telecomunicaciones	[43230000] Software	[43233200] Software de seguridad y protección	[43233200] Software de seguridad informática
43233205	(43000000) 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

NOTA 1: Se podrá acreditar experiencia con contratos ejecutados en su totalidad.
NOTA 2: Los oferentes no podrán acreditar experiencia con contratos en ejecución
NOTA 3: De acuerdo con lo indicado en el Parágrafo 5° del Artículo 5º de la Ley 1150 de 2007 adicionado por el Artículo 5º de la Ley 1882 de 2018 *"(…) En los procesos de contratación, las entidades estatales deberán aceptar la experiencia adquirida por los proponentes a través de la ejecución de contratos con particulares. (…)".*
NOTA 4: Experiencia cuyo objeto o alcance se encuentre relacionado con la suscripción, implementación y soporte de soluciones o plataformas de ciberseguridad.

6.2.1.2 VERIFICACIÓN EXPERIENCIA PROPONENTE NO OBLIGADO A ESTAR INSCRITO EN EL REGISTRO ÚNICO DE PROPONENTES

Se exceptúa de la aplicación de las nomas del RUP a los proponentes extranjeros sin domicilio en Colombia, así como a aquellos que estén expresamente exceptuados por la ley. Los proponentes que no estén obligados a inscribirse en el RUP deberán acreditar su experiencia mediante la presentación de contratos ejecutados, terminados o liquidados, adjuntando los documentos soporte correspondientes.

Los documentos soporte con los que se pretende acreditar la experiencia de los proponentes no obligados a estar inscritos en el RUP deben contener como mínimo la siguiente información:

- Objeto o alcance se encuentre relacionado con la suscripción, implementación y soporte de soluciones o plataformas de ciberseguridad
- Número del Contrato (en caso de que exista).
- Contratante
- Nombre del contratista. (Si se ejecutó en Unión Temporal o Consorcio identificar los integrantes y su porcentaje de participación).
- Fecha de iniciación o suscripción (según aplique).
- Fecha de terminación.
- Valor final del contrato.

Los documentos con los cuales se puede complementar la información de experiencia son:

1.- Certificación de cada uno de los Contratos relacionados y ejecutados suscrito por el representante legal de la empresa compradora.

2.- Copia del Acta de Recibo Final, terminación o Acta de Liquidación del Contrato o del documento equivalente que haga sus veces y que se encuentre previsto en el contrato.

Si con los documentos anteriores el proponente no le es posible acreditar la información adicional o complementaria solicitada, podrá presentar la siguiente documentación o cualquier otra información proveniente de la actuación contractual:

- Si el contrato se suscribió en Consorcio o en Unión Temporal se podrá acreditar el porcentaje de participación, mediante copia del acuerdo de Consorcio o de Unión Temporal.

- La fecha de iniciación de la ejecución del contrato se podrá acreditar con la copia del acta de iniciación, de la orden de iniciación o con el documento previsto en el contrato.

- Las actividades desarrolladas, se podrán acreditar con la presentación de la copia del contrato correspondiente o copia del acta de actividades ejecutadas o el documento que haga sus veces.

Los documentos que sean allegados para acreditar la experiencia solicitada deberán estar suscritos por las personas competentes, así:

- Para contratos públicos, por el ordenador del gasto de la Entidad contratante o el funcionario competente.

- Para contratos privados suscritos con personas jurídicas, por el representante legal de la empresa contratante, o la persona delegada para suscribirlo.

- Para contratos privados suscritos con personas naturales, por la misma persona natural con quien se suscribió el contrato.

No se aceptarán certificaciones expedidas o suscritas por supervisores externos al contratante.

Las certificaciones o documentos emitidos en el exterior deberán presentarse sin necesidad de legalización. Sin embargo, para la firma del Contrato, el Proponente adjudicatario deberá presentar dichos documentos legalizados de acuerdo con la normatividad vigente en el momento de la firma del contrato.

En todo caso, aunque el proponente aporte una certificación para acreditar la experiencia, la UAERMV se reserva el derecho de solicitar otro documento adicional o hacer las verificaciones correspondientes directamente, sobre la información relacionada en el formato *GCON-FM-097*- Experiencia

NOTAS COMUNES APLICABLES A LA VERIFICACIÓN DE EXPERIENCIA:

A) ACREDITACIÓN DE LA EXPERIENCIA

Para verificar la experiencia acreditada en el Registro Único de Proponentes RUP o en los documentos soporte para aquellos proponentes no obligados a estar inscritos en el RUP, deberá diligenciar el formato *GCON-FM-097* – Experiencia.

Con base en la información suministrada en el formato GCON-FM-097 - Experiencia, la información contenida en el RUP (para los proponentes obligados a estar inscritos de acuerdo con la normatividad vigente), así como

aquella documentación aportada por los proponentes no obligados a estar inscritos en el RUP, Para no MiPymes, se verificarán hasta TRES (3) certificaciones de experiencia para el 100% del presupuesto oficial en SMMLV; para MiPymes, emprendimiento de mujeres y emprendimiento de empresas de personas con discapacidad y para empresas diferentes a las anteriores, hasta CINCO (5) certificaciones de experiencia para el 100% del presupuesto oficial en SMMLV. Un Consorcio o una Unión Temporal constituyen UN PROPONENTE.

NOTA 1: Experiencia cuyo objeto o alcance se encuentre relacionado con la suscripción, implementación y soporte de soluciones o plataformas de ciberseguridad.

La verificación se realizará de la siguiente manera:

Valor mínimo a certificar:

- 100% del Presupuesto Oficial expresado en SMMLV: $299,08

Se calificará a cada propuesta como HÁBIL, si la sumatoria de los valores totales ejecutados de los contratos presentados para acreditar la experiencia, expresada en SMMLV, es mayor o igual al valor mínimo a certificar establecido.

La verificación dará como resultado que la propuesta sea calificada como HÁBIL o NO HÁBIL por este requisito y se hará con base en la sumatoria de los Valores Totales ejecutados en SMML de los contratos relacionados en el formato *GCON-FM-097* – Experiencia, que cumplan con los requisitos establecidos.

En caso de que el número de contratos con los cuales el proponente acredita la experiencia no satisfaga el porcentaje mínimo a certificar se calificará la propuesta como NO HÁBIL.

B) CONDICIONES DE LA EXPERIENCIA ACREDITADA

a. Para relacionar la experiencia requerida, deberá diligenciarse el formato *GCON-FM-097* – Experiencia en el cual se consignará la información sobre experiencia del proponente, de acuerdo con la información reportada en el RUP o en los documentos soporte para aquellos proponentes no obligados a estar inscritos en el RUP, según aplique.

b. El proponente, deberá incluir en el formato mencionado, el valor ejecutado de cada contrato, expresado en SMML de acuerdo con la fecha de terminación, teniendo en cuenta la tabla publicada por el Banco de la Republica y cuyo archivo en formato Excel se puede descargar con el siguiente enlace https://www.banrep.gov.co/economia/pli/mercado_laboral.xls

Cuando se relacionen contratos en moneda extranjera, el proponente deberá realizar las conversiones respectivas a pesos colombianos e indicar en el mencionado formato el valor obtenido y su equivalente a SMMLV a la fecha de terminación del contrato, de acuerdo con los siguientes parámetros:

- Cuando el valor esté dado en dólares de los Estados Unidos de América (USD$) se convertirá a pesos colombianos utilizando para esta conversión la tabla Serie de datos promedio anual de la Serie empalmada de la tasa de cambio del peso colombiano frente al dólar (TRM y Certificado de cambio) correspondiente al año de terminación, para lo cual el proponente debe tomar la publicada por el Banco de la República para el año correspondiente en el siguiente enlace: http://www.banrep.gov.co/series-estadisticas/see_ts_trm.htm#cotizacion.

- Cuando el valor esté dado en moneda extranjera diferente al dólar de los Estados Unidos de América,

se realizará su conversión a dólares estadounidenses tomando como referencia el año de terminación contrato, de acuerdo con la tasa de cambio estadística publicada por el Banco de la República u organismo oficial del país de origen correspondiente al último día de ese año, luego se realizará su conversión a pesos colombianos, de conformidad con lo indicado en la viñeta anterior.

- Realizadas las conversiones correspondientes, se procederá a expresar los valores en SMML de acuerdo con el año de terminación, teniendo en cuenta la tabla publicada por el Banco de la Republica y cuyo archivo en formato Excel se puede descargar con el siguiente enlace https://www.banrep.gov.co/economia/pli/mercado_laboral.xls

- En todo caso, la Entidad revisará las conversiones realizadas por el proponente y en caso de encontrarse diferencias, errores aritméticos o inconsistencias con respecto a lo indicado en el CON-FM-097 - Experiencia, se realizarán las correcciones respectivas de acuerdo con el procedimiento indicado en este párrafo y el valor que se obtenga primará para todos los efectos.

c. En caso de existir diferencias entre la información registrada en el formato *GCON-FM-097* – Experiencia y la relacionada en el RUP, prevalecerá la información del RUP, la cual será utilizada para la evaluación.

En caso de existir diferencias entre la información registrada en el formato *GCON-FM-097* – Experiencia y la relacionada en los documentos soporte, para aquellos proponentes no obligados a estar inscritos en el RUP, prevalecerá la información contenida en la documentación soporte la cual será utilizada para la evaluación.

d. En caso de relacionarse más de TRES (3) para no MIPYMES o CINCO (5) para MIPYMES contratos, la UAERMV, para salvaguardar los principios de transparencia e igualdad, tendrán en cuenta sólo los TRES (3) para no MIPYMES o CINCO (5) para MIPYMES que cumplan con los requisitos establecidos en el pliego. Si la propuesta se presenta en Consorcio o Unión Temporal, todos sus miembros podrán diligenciar su experiencia conjuntamente en un mismo anexo.

e. En el caso de contratos ejecutados por el proponente como parte de un Consorcio o de una Unión Temporal, este deberá demostrar únicamente el valor correspondiente según su porcentaje de participación en la figura asociativa.

f. Para el caso de Consorcios o Uniones Temporales, se tendrá en cuenta la experiencia sumada de sus integrantes.

g. En caso de Unión Temporal éste integrante deberá estar incluido como ejecutor de las actividades para las cuales presentó la experiencia solicitada.

h. La experiencia de los proponentes personas jurídicas (sean individuales o miembros de un proponente plural), deberá, para ser aceptable, haberse obtenido con posterioridad a la fecha de constitución.

i. Cuando la persona jurídica que actúe como proponente tenga menos de tres (3) años de constitución al cierre del proceso, la experiencia de sus socios, accionistas o constituyentes podrá acumularse y ser contabilizada como experiencia de la persona jurídica proponente.
.
j. No podrá acumularse a la vez, la experiencia de los socios o Representante Legal y de la persona jurídica cuando estos se asocien entre sí para presentar propuesta bajo alguna de las modalidades previstas en el artículo 7 de la Ley 80 de 1993. Lo anterior para el caso de proponentes plurales.

k. Se considerará la experiencia aportada por el proponente que haya sido obtenida, a nivel nacional o en el extranjero con: Entidades del Estado y personas naturales o jurídicas de naturaleza privada

6.3. HABILITANTES DE CAPACIDAD FINANCIERA Y CAPACIDAD ORGANIZACIONAL

La entidad verificará la capacidad financiera y organizacional de los proponentes, excepto los extranjeros sin domicilio en Colombia, basándose en la información financiera contenida en el Registro Único de Proponentes.
Para tal efecto, el proponente o cada uno de los integrantes del proponente *(en caso de que éste sea un Consorcio o una Unión Temporal)* debe(n) presentar el registro único de proponentes RUP, expedido con una antelación no superior a treinta (30) días calendario a la fecha de cierre.

La información financiera deberá estar actualizada en el RUP mínimo al 31 de diciembre del año 2025.

Los proponentes extranjeros sin domicilio en el país, deberán diligenciar el ANEXO DE INFORMACIÓN FINANCIERA EXTRANJEROS, el cual debe estar soportado por el último balance de acuerdo con el cierre fiscal en el país de origen o en el balance de apertura si se trata de sociedades nuevas. En este caso, deberán aportar una certificación de un contador público con inscripción profesional vigente ante la Junta Central de Contadores de Colombia, en la que se certifique la fecha de cierre en el país de origen y se avale dicha información. Además, se deberá incluir una fotocopia de la tarjeta profesional, el certificado de vigencia de inscripción y el certificado de antecedentes disciplinarios expedido por la Junta Central de Contadores. Este certificado deberá estar vigente a la fecha de cierre del presente proceso y no deberá registrar sanciones durante el periodo certificado.
.
Para efectos de lo previsto en el párrafo anterior, el ANEXO DE INFORMACIÓN FINANCIERA EXTRANJEROS deberá ser presentado firmado tanto por el Representante Legal como por el contador público con inscripción profesional vigente ante la Junta Central de Contadores de Colombia. Este debe ir acompañado de una traducción simple al español y de los valores expresados en la moneda funcional colombiana, calculados a la tasa de cambio representativa del mercado correspondiente a la fecha de corte de la información financiera, de conformidad con el Código General del Proceso y el artículo 480 del Código de Comercio.

NOTA 1: En caso de que el proponente certifique que el monto por gasto de intereses o gastos financieros asciende a cero (0), se entenderá habilitado en lo referente al indicador de razón de cobertura de intereses (si aplica).

NOTA 2: En el caso de las Uniones Temporales y los Consorcios, los indicadores se calcularán con base en el porcentaje (%) de participación de cada integrante en el proponente plural, mediante la obtención del promedio ponderado (según estos porcentajes de participación), de cada uno de los componentes para los estados financieros que intervienen en los indicadores.

6.3.1. VERIFICACIÓN DE LA CAPACIDAD FINANCIERA:

Los indicadores de capacidad financiera buscan establecer unas mínimas condiciones que reflejan la salud financiera de los proponentes a través de su liquidez y endeudamiento. Estas condiciones muestran la aptitud del proponente para cumplir oportuna y cabalmente el objeto del contrato. La capacidad financiera requerida en un proceso de contratación debe ser adecuada y proporcional a la naturaleza y al valor del contrato. En consecuencia, la Entidad Estatal debe establecer los requisitos de capacidad financiera con base en su conocimiento relativo del sector a contratar y de los posibles oferentes. La capacidad financiera en el presente proceso se verificará con la medición de los siguientes indicadores:

ÍNDICE DE LIQUIDEZ: Este indicador determina la capacidad que tiene una empresa para enfrentar las obligaciones contraídas a corto plazo. Cuanto más elevado es el indicador de liquidez, mayor es la posibilidad de que la empresa consiga cancelar las deudas a corto plazo.

ÍNDICE DE ENDEUDAMIENTO: Este índice de Endeudamiento, establece la estrategia de financiamiento y la

vulnerabilidad de la empresa a esa estructura de financiamiento dada. Vale decir, que establece la proporción de los Activos Totales financiados con fondos ajenos (Pasivo Total).

RAZÓN DE COBERTURA DE INTERESES: Esta razón financiera nos da un resultado que significa que por cada peso de interés que la empresa debe pagar, se mide el grado hasta el cual las utilidades de la empresa pueden disminuir sin transformarse en pérdidas al cubrir los costos de interés.

INDICADORES PARA MIPYMES

INDICADORES DE CAPACIDAD FINANCIERA MÍNIMOS REQUERIDOS			
INDICADOR	**FORMULA**	**MARGEN SOLICITADO**	**CONSORCIO O UNIONES TEMPORALES**
LIQUIDEZ	Activo Corriente/ Pasivo Corriente	Mayor o igual 1,12	El proponente que presente propuesta debe cumplir por igual, con los indicadores mínimos. Los indicadores se calculan de acuerdo con la participación porcentual de cada uno de los integrantes de consorcio o unión temporal.
NIVEL DE ENDEUDAMIENTO	Pasivo Total/ Activo Total	Menor o igual a 0,72	
RAZON COBERTURA DE INTERES	Utilidad Operacional/ Gastos de intereses	Mayor o igual 1	

INDICADORES PARA NO MIPYMES

INDICADORES DE CAPACIDAD FINANCIERA MÍNIMOS REQUERIDOS			
INDICADOR	**FORMULA**	**MARGEN SOLICITADO**	**CONSORCIO O UNIONES TEMPORALES**
LIQUIDEZ	Activo Corriente/ Pasivo Corriente	Mayor o igual 1,13	El proponente que presente propuesta debe cumplir por igual, con los indicadores mínimos. Los indicadores se calculan de acuerdo con la participación porcentual de cada uno de los integrantes de consorcio o unión temporal.
NIVEL DE ENDEUDAMIENTO	Pasivo Total/ Activo Total	Menor o igual a 0,69	
RAZON COBERTURA DE INTERES	Utilidad Operacional/ Gastos de intereses	Mayor o igual 1	

6.3.2. VERIFICACIÓN DE LA CAPACIDAD ORGANIZACIONAL:

La capacidad organizacional es la aptitud de un proponente para cumplir oportuna y cabalmente el objeto del contrato en función de su organización interna. El Decreto 1082 de 2015 definió los indicadores de rentabilidad para medir la capacidad organizacional de un proponente teniendo en cuenta que está bien organizado cuando

es rentable. La capacidad organizacional en el presente proceso se verificará con la medición de los siguientes indicadores:

RENTABILIDAD DEL PATRIMONIO: Este indicador determina la rentabilidad del patrimonio del proponente, es decir, la capacidad de generación de utilidad operacional por cada peso invertido en el patrimonio. A mayor rentabilidad sobre el patrimonio, mayor es la rentabilidad de los accionistas y mejor la capacidad organizacional del proponente.

RENTABILIDAD DEL ACTIVO: Este indicador determina la rentabilidad de los activos del proponente, es decir, la capacidad de generación de utilidad operacional por cada peso invertido en el activo. A mayor rentabilidad sobre activos, mayor es la rentabilidad del negocio y mejor la capacidad organizacional del proponente. Este indicador debe ser siempre menor o igual que el de rentabilidad sobre patrimonio.

INDICADORES PARA MIPYMES

INDICADORES DE CAPACIDAD ORGANIZACIONAL MÍNIMOS REQUERIDOS			
INDICADOR	**FORMULA**	**MARGEN SOLICITADO**	**CONSORCIO O UNIONES TEMPORALES**
RENTABILIDAD DE PATRIMONIO - ROE	Utilidad Operacional/ Patrimonio	Mayor o igual a 0,14	El proponente que presente propuesta debe cumplir por igual, con los indicadores mínimos. Los indicadores se calculan de acuerdo con la participación porcentual de cada uno de los integrantes de consorcio o unión temporal.
RENTABILIDAD DE ACTIVO - ROA	Utilidad Operacional/ Activo Total	Mayor o igual a 0,06	

INDICADORES PARA NO MIPYMES

INDICADORES DE CAPACIDAD ORGANIZACIONAL MÍNIMOS REQUERIDOS			
INDICADOR	**FORMULA**	**MARGEN SOLICITADO**	**CONSORCIO O UNIONES TEMPORALES**
RENTABILIDAD DE PATRIMONIO - ROE	Utilidad Operacional/ Patrimonio	Mayor o igual a 0,18	El proponente que presente propuesta debe cumplir por igual, con los indicadores mínimos. Los indicadores se calculan de acuerdo con la participación porcentual de cada uno de los integrantes de consorcio o unión temporal.
RENTABILIDAD DE ACTIVO - ROA	Utilidad Operacional/ Activo Total	Mayor o igual a 0,1	

En caso de no cumplir con la Capacidad financiera y Capacidad organizacional aquí requerida, la propuesta se considerará **NO HÁBIL**.

6.4 FACTOR DE SELECCIÓN DE LA OFERTA.

EL PRECIO COMO ÚNICO FACTOR DE SELECCIÓN: Dado que la calidad de los bienes o servicios está

garantizada por condiciones estándar y por lo dispuesto expresamente en el numeral 3 del artículo 5 de la Ley 1150 de 2007, el precio será el único criterio de selección.

6.4.1. PRESENTACIÓN DE LA PROPUESTA ECONÓMICA INICIAL Y DURANTE EL DESARROLLO DE LA SUBASTA INVERSA

Para la presentación de la oferta económica, tanto la inicial como las posturas registradas durante la subasta inversa, el proponente deberá incluir los costos directos, indirectos, impuestos, tasas, contribuciones y cualquier otra erogación necesaria para la ejecución del contrato derivado de este proceso, considerando las especificaciones técnicas detalladas en los documentos del proceso de selección.

Cualquier error en el diligenciamiento de los valores relacionados en la oferta económica inicial como aquellas posturas que se registren en el desarrollo de la subasta inversa, no dará lugar a su modificación.

La relación ítems, precios y las correspondientes especificaciones técnicas, formará parte del contrato que se celebre con el proponente favorecido.

La presentación de la oferta económica se realizará a través del Sistema Electrónico para la Contratación Pública - SECOP II, en desarrollo del proceso de Subasta Inversa Electrónica, de conformidad con lo establecido en el artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015.

El evento de subasta inversa se llevará a cabo de forma electrónica, en la fecha y hora que se indique expresamente en el cronograma del proceso, y será precedido por la verificación del cumplimiento de requisitos habilitantes por parte de la UAERMV. Solo participarán en el evento de subasta aquellos proponentes que hayan sido calificados como HÁBILES.

Margen Mínimo de Mejora:

Durante la subasta, los proponentes podrán realizar ofertas sucesivas que mejoren el precio inicial presentado.

La Entidad establecerá como margen mínimo de mejora para los lances que se realicen durante el evento, un valor equivalente al uno por ciento (1%) del presupuesto oficial del contrato, expresado en pesos colombianos.

No se aceptarán lances que no cumplan con este margen mínimo de mejora, ni lances que se traduzcan en una oferta económica por fuera del rango de precios permitido, si este ha sido definido previamente en el estudio de mercado.

7. ANÁLISIS DE RIESGO Y LA FORMA DE MITIGARLO

De conformidad con el artículo 4° de la Ley 1150 de 2007 y en concordancia con el artículo 2.2.1.1.1.6.3 del Decreto 1082 de 2015, se consideran riesgos en la contratación aquellas circunstancias que, al presentarse durante el desarrollo y ejecución del contrato, pueden alterar su equilibrio económico. Sin embargo, debido a la previsibilidad, estos riesgos se regulan dentro de las condiciones inicialmente pactadas en el contrato, quedando excluidos del concepto de imprevisibilidad mencionado en el artículo 27 de la Ley 80 de 1993.

El principio básico de asignación de riesgos establece que estos deben ser asumidos por la parte que se encuentre en mejor posición para evaluarlos, controlarlos o gestionarlos. En consecuencia, se ha elaborado el análisis de riegos que se presenta en el anexo denominado “Matriz de Riesgos”, el cual hace parte integran del presente estudio previo.

En cumplimiento de lo dispuesto en el artículo 4° de la Ley 1150 de 2007 y el artículo 2.2.1.1.1.6.3 del Decreto 1082 de 2015, y atendiendo los lineamientos del Manual para la Identificación y Cobertura del Riesgo expedido por Colombia Compra Eficiente, se ha realizado la estimación, tipificación y asignación de los riesgos previsibles asociados a la presente contratación.

En este análisis se contemplaron riesgos técnicos, logísticos, financieros, jurídicos y operativos que podrían afectar el cumplimiento del objeto contractual, tales como: incumplimientos en tiempos de entrega, fallas en la interoperabilidad de la plataforma, riesgos asociados a cambios en los precios del mercado, o afectaciones derivadas de la obsolescencia tecnológica durante la vigencia del contrato.

Así mismo, se evaluó el riesgo que el proceso de contratación representa para el cumplimiento de los objetivos institucionales de la UAERMV, especialmente en materia de continuidad de los servicios de ciberseguridad, protección de activos tecnológicos e integridad de la infraestructura digital.

Como resultado de este ejercicio, se elaboró la Matriz de Riesgos de la Contratación, en la cual se identifican los riesgos, su probabilidad, impacto, medidas de mitigación y la parte responsable de su gestión.

8. ANÁLISIS QUE SUSTENTA LA EXIGENCIA DE GARANTÍAS DESTINADAS A AMPARAR LOS PERJUICIOS DE NATURALEZA CONTRACTUAL O EXTRACONTRACTUAL

El CONTRATISTA para garantizar el cumplimiento de sus obligaciones debe constituir una garantía a favor de la UAERMV, NIT (número de identificación), esta última debe figurar en el contrato de seguro en calidad de beneficiario y asegurado, la cual podrá consistir en una póliza de seguro expedida por una compañía de seguros legalmente establecida en Colombia —formato entidades estatales, en una garantía bancaria o en cualquier otro de los mecanismos de cobertura establecidos en el Decreto 1082 de 2015, siempre que cumpla con los términos y condiciones previstos en esa norma y/o en la legislación vigente aplicable y que incluya siguientes amparos así:

TIPO DE GARANTÍA	AMPAROS	PORCENTAJE RESPECTO TOTAL DEL CONTRATO O No. de SMMLV	VIGENCIA	JUSTIFICACIÓN
GARANTIA UNICA	**CUMPLIMENTO**	20% DEL TOTAL DEL CONTRATO*	A partir de la suscripción del contrato comprende el plazo del contrato y seis (6) meses más y/o hasta su liquidación	Cubre a la entidad de los perjuicios directos derivados del incumplimiento total o parcial de las obligaciones nacidas del contrato, así como su cumplimiento tardío o defectuoso, cuando ellos son imputables al contratista.
	CALIDAD DEL SERVICIO	20% DEL TOTAL DEL CONTRATO	A partir de la suscripción del contrato comprende el plazo del contrato, la vigencia de la garantía de soporte técnico y seis (6) meses más y/o hasta su liquidación **	Cubre a la entidad de los perjuicios, derivados del incumplimiento respecto a del servicio que implica la instalación y puesta en funcionamiento de la solución de ciberseguridad según ficha técnica y obligaciones específicas del contrato
	CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES	20% DEL TOTAL DEL CONTRATO	A partir de la suscripción del contrato comprende el plazo del contrato, la vigencia de la garantía del producto ofrecido y seis (6) meses más. ***	Cubre a la entidad de los perjuicios, derivados de la mala calidad de los bienes o deficiencias técnicas de los bienes, de acuerdo con las especificaciones técnicas establecidas en el contrato, o por incumplimiento de los parámetros o normas establecidos para el respectivo servicio.
	PAGO DE SALARIOS, PRESTACIONES SOCIALES LEGALES E	5% DEL TOTAL DEL CONTRATO	A partir de la suscripción del contrato comprende el plazo del contrato y	Cubre a la entidad de los perjuicios que se le ocasionen como consecuencia del incumplimiento de las obligaciones

	INDEMNIZACIONES LABORALES		tres (03) años más.	laborales del contratista, derivadas de la contratación del personal utilizado para la ejecución del contrato amparado

NOTA: Cuando la oferta es presentada por un proponente plural, como unión temporal, consorcio o promesa de sociedad futura, la garantía debe ser otorgada por todos sus integrantes.

PARÁGRAFO PRIMERO: La garantía exigida deberá ser constituida por EL CONTRATISTA dentro de los cinco (5) días hábiles siguientes a la suscripción del contrato. El CONTRATISTA deberá realizar el cargue por medio de la plataforma SECOP, de las garantías que constituya con ocasión del contrato e informar por escrito a la UAERMV de tal hecho.

PARÁGRAFO SEGUNDO: La vigencia de todos los amparos deberá ajustarse una vez se suscriba la respectiva acta de inicio. El hecho de la constitución de estos amparos no exonera al CONTRATISTA de sus responsabilidades legales en relación con los riesgos asegurados.

PARÁGRAFO TERCERO: EL CONTRATISTA deberá restablecer el valor de la garantía cuando éste se haya visto reducido por razón de las reclamaciones efectuadas por la UAERMV de acuerdo con el artículo 2.2.1.2.3.1.18 del Decreto 1082 de 2015. De igual manera, en cualquier evento en que se aumente o adicione el valor del contrato o se prorrogue su término, EL CONTRATISTA deberá ampliar el valor de la garantía otorgada o ampliar su vigencia, según sea el caso, dentro de los cinco (5) días hábiles siguientes a la entrega del documento que así lo soporte.

PARÁGRAFO CUARTO: En el evento en que la entidad que expide la garantía del contrato sea intervenida, tomado su control o liquidada por el Gobierno Nacional a través de entidad competente y con ello se genere incertidumbre sobre el pago o efectividad de la garantía aportada, EL CONTRATISTA deberá de manera inmediata presentar nueva póliza o reemplazar la expedida por la compañía de seguros intervenida, sujeta a toma de control o proceso de liquidación.

PARÁGRAFO QUINTO: La garantía requiere de aprobación de la UAERMV para la ejecución del contrato.

PARÁGRAFO SEXTO: En caso de incumplimiento del CONTRATISTA de la obligación de obtener la ampliación de la garantía o de la obligación de obtener su renovación o de la obligación de restablecer su valor o de aquella de otorgar una nueva garantía que ampare el cumplimiento de las obligaciones que surjan por razón de la celebración, ejecución y liquidación del contrato, la UAERMV podrá declarar la caducidad de este.

PARÁGRAFO SÉPTIMO: En el evento en que, por incumplimiento del CONTRATISTA garantizado, el asegurador resolviera continuar, como cesionario, con la ejecución del contrato y la UAERMV estuviese de acuerdo con ello, el CONTRATISTA garantizado aceptará desde el momento de la contratación de la póliza la cesión del contrato a favor del asegurador. En este caso, el asegurador cesionario deberá constituir una nueva garantía para amparar el cumplimiento de las obligaciones que ha asumido por virtud de la cesión.

PARÁGRAFO OCTAVO: El CONTRATISTA acepta que en el evento que el valor a pagar por los amparos tenga centavos, estos se ajustan o aproximen al peso, ya sea por exceso o por defecto si la suma es mayor o menor a 50 centavos respectivamente.

9. INDICACIÓN DE SI EL PROCESO DE CONTRATACIÓN ESTÁ COBIJADO POR UN ACUERDO COMERCIAL.

De acuerdo con el análisis realizado y conforme a lo señalado en el artículo 2.2.1.1.1.5.1 del Decreto 1082 de 2015, se verificó que el objeto del contrato –relacionado con el Fortalecimiento de capacidades, soporte y licenciamiento de las plataforma de seguridad endpoint de nueva generación (EDR) para la UAEMRV – no excede los umbrales establecidos para la aplicación de los Acuerdos Comerciales suscritos por Colombia ni se

trata de un bien o servicio incluido en los anexos de dichos tratados, ni se prevé la participación de oferentes extranjeros de países con los cuales Colombia tiene suscritos Tratados de Libre Comercio (TLC) con compromisos en materia de compras públicas.

Por lo tanto, no le son aplicables las obligaciones derivadas de los Acuerdos Comerciales vigentes.

Teniendo en cuenta que La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial UAERMV hace parte de la lista de "Entidades del nivel Subcentral del Gobierno, el cual incluye todas las demás entidades subcentrales", una vez revisado uno de los tres parámetros establecidos en el Manual explicativo de los capítulos de contratación pública de los acuerdos comerciales negociados por Colombia para entidades contratantes emitido por el Ministerio de Comercio, Industria y Turismo y el Departamento Nacional de Planeación, se evidencia lo siguiente:

ACUERDO COMERCIAL		**Entidad Estatal cubierta**	**Valor del Proceso superior al umbral del Acuerdo**	**Excepción aplicable al Proceso**	**Proceso cubierto por el Acuerdo Comercial**
		Si/No	**Si/No**	**Si/No**	**Si/No**
Alianza Pacífico	Chile	NO	NO	NO	NO
	Perú	NO	NO	NO	NO
	México	NO	NO	NO	NO
Canadá		NO	NO	NO	NO
Chile		SI	NO	NO	NO
Corea		NO	NO	NO	NO
Costa Rica		NO	NO	NO	NO
Estados Unidos		NO	NO	NO	NO
Estados AELC		NO	NO	NO	NO
México		NO	NO	NO	NO
Triángulo Norte	El Salvador	SI	SI	NO	SI
	Guatemala	SI	SI	NO	SI
	Honduras	NO	NO	NO	NO
Unión Europea		SI	NO	NO	NO
Comunidad Andina		SI	SI	NO	SI

10. ANEXOS

- ✓ *Estudio de Sector, Tabulación, Cotizaciones*
- ✓ *Formulación de Estudios del Sector*
- ✓ *Certificación Técnica del Oferente*
- ✓ *Matriz de Riesgos*
- ✓ *CDP 1297*

11. RESPONSABLES

Responsable de la Dependencia generadora de la necesidad:
NOMBRE: YENNY HASLEY YAZO LOZADA
CARGO: Jefe (e) de la Oficina de Tecnologías de la información
Resolución No. 547 de 2026

Profesional que proyecta:
NOMBRE: DANIELA ALEJANDRA AVILA MONTENEGRO
CARGO: Contratista Oficina de Tecnologías de la Información

Profesionales que revisan:
NOMBRE: FRANCISCO ANDRES RODRIGUEZ ERASO
CARGO: Contratista Secretaria General

NOMBRE: CARLOS ABEL BASTIDAS CUBILLOS
CARGO: Contratista Oficina de Tecnologías de la Información

NOMBRE: MARINO MIGUEL MORENO RHENALS
CARGO: Contratista Oficina de Tecnologías de la Información

NOMBRE: ANGEL LEONARDO JEREZ CARVAJAL
CARGO: Contratista Gerencia de Contratación

NOMBRE: NELSON EFRAIN MEDINA PINZON
CARGO: Contratista Gerencia de Contratación

NOMBRE: RAFAEL EDUARDO VARGAS CASTRO
CARGO: Contratista Gerencia de Contratación

Gerente del Proyecto:
NOMBRE: YENNY HASLEY YAZO LOZADA
CARGO: Jefe (e) de la Oficina de Tecnologías de la información

ESTE FORMATO CONTIENE LA INFORMACIÓN MÍNIMA REQUERIDA PARA CADA UNO DE LOS PROCEDIMIENTOS O TRÁMITES PARA LOS CUALES SE HAN ESTABLECIDO, NO SE PUEDE ELIMINAR NI PARCIAL NI TOTALMENTE LA INFORMACIÓN AQUÍ CONTENIDA; SÍ ALGÚN ESPACIO NO APLICA ESCRIBIR QUE N/A; AL DILIGENCIARLAS NO DEBEN QUEDAR ESPACIOS EN BLANCO. EL ESPACIO DE LAS FIRMAS HACE PARTE INTEGRAL DEL ACTA, RAZÓN POR LA CUAL NO DEBE QUEDAR EN UNA HOJA SEPARADA. DEBEN SER DILIGENCIADOS Y REMPLAZADOS LOS ESPACIOS MARCADOS CON GRIS Y TODO DOCUMENTO.

METADATOS: MODALIDAD, ESTUDIO PREVIO - "OBJETO A CONTRATAR", ÍTEM PLAN DE ADQUISICIONES
DISPONER EN: 110.100 CONTRATOS / SECRETARÍA GENERAL

Documento 20261140312213 firmado electrónicamente por:	
YENNY HASLEY YAZO LOZADA	JEFE OFICINA DE TECNOLOGIAS DE LA INFORMACION OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN yenny.yazo@umv.gov.co Fecha firma: 08-10-2026 16:15:01
DANIELA ALEJANDRA AVILA MONTENEGRO	Contratista OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN daniela.montenegro@umv.gov.co Fecha firma: 08-10-2026 16:21:44
NELSON EFRAIN MEDINA PINZON	Contratista GERENCIA DE CONTRATACIÓN nelson.medina@umv.gov.co Fecha firma: 08-10-2026 16:21:44

93e31d7be15176fa56c287ba68b9fd2c25c3da3bbfcf9be9907f06f736bd7026
Codigo de Verificación CV: 1e1cc Comprobar desde: https://www.umv.gov.co/portal/verificar/