ESTUDIO DE SECTOR
UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACIÓN Y MANTENIMIENTO VIAL

OBJETO PARA CONTRATAR:

"8089-053 SUSCRIPCION, IMPLEMENTACION Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACION PARA LA PROTECCION INTEGRAL DE LOS ACTIVOS DIGITALES DE LA UAERMV, ORIENTADA A LA PREVENCION, DETECCION Y RESPUESTA AVANZADA ANTE AMENAZAS EN ENDPOINTS Y PREVENCION DE PERDIDAS DE DATOS"

NOVIEMBRE DE 2026

Contenido

INTRODUCCIÓN.....3

1. DEFINICIÓN DE LA NECESIDAD.....3

2. ASPECTOS GENERALES DEL SECTOR.....20

3. ANÁLISIS DE LA OFERTA.....33

4. ANALISIS DE LA DEMANDA.....40

5. ANÁLISIS DEL SECTOR PARA DETERMINAR OTROS CRITERIOS DIFERENCIALES Y APLICACIÓN DE NORMATIVIDAD QUE LE APLIQUE.....42

6. FUNDAMENTO TEÓRICO Y METODOLOGIA UTILIZADA PARA ANÁLISIS DE PRECIOS.....54

7. CONCLUSIONES Y/O RECOMENDACIONES.....57

8. FUENTES DE INFORMACIÓN.....59

9. ANEXOS.....59

INTRODUCCIÓN

Para una adecuada gestión de las compras públicas, las Entidades Estatales deben contar con elementos de análisis que les permitan identificar y satisfacer sus necesidades de bienes y/o servicios, procurando la optimización de los recursos públicos y la selección de alternativas que respondan de manera eficiente, eficaz y oportuna a los requerimientos institucionales.

En este sentido, el presente documento tiene como propósito dar cumplimiento a lo establecido en el Decreto 1082 de 2015, particularmente a lo dispuesto en su artículo 2.2.1.1.1.6.1, que establece el deber de las Entidades Estatales de analizar el sector relativo al objeto del proceso de contratación que se pretenda adelantar, desde las perspectivas legal, comercial, financiera, organizacional, técnica y de análisis de riesgos. Este ejercicio permite, además, conocer las condiciones y características del mercado, identificar potenciales proveedores y establecer criterios que contribuyan a una adecuada planeación y estructuración del proceso de contratación.

En atención a lo anterior, se adelanta el análisis del sector relacionado con la contratación cuyo objeto corresponde a la **"8089-053 SUSCRIPCIÓN, IMPLEMENTACIÓN Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACIÓN PARA LA 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"**, mediante el cual la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial – UAERMV busca garantizar la disponibilidad, continuidad y adecuada operación de las herramientas tecnológicas requeridas para la protección de sus activos digitales y el fortalecimiento de sus capacidades de prevención, detección y respuesta frente a posibles amenazas de seguridad de la información.

El presente estudio tiene como finalidad reunir los elementos técnicos, económicos, legales, comerciales, financieros, organizacionales y de riesgo necesarios para que la UAERMV cuente con información suficiente y pertinente para la toma de decisiones durante la estructuración del proceso de contratación, contribuyendo al fortalecimiento de los procesos y procedimientos institucionales y a la adecuada administración de los recursos públicos.

Para la estructuración del presente análisis se tuvieron en cuenta las disposiciones normativas aplicables, así como las guías, manuales y lineamientos establecidos por la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, particularmente aquellos orientados a la adecuada elaboración de los estudios del sector, la determinación de las condiciones del mercado y la definición de requisitos y criterios que permitan promover la participación y pluralidad de oferentes, garantizando condiciones objetivas, proporcionales y acordes con las características y necesidades de la Entidad.

De igual manera, se consideraron los principios y disposiciones aplicables a la contratación estatal, con el propósito de que las condiciones previstas para el proceso respondan a las necesidades reales de la UAERMV, a las características del mercado de soluciones de ciberseguridad y a las condiciones técnicas requeridas para garantizar la protección integral de los activos digitales de la Entidad.

1. DEFINICIÓN DE LA NECESIDAD[1]

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial 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

[1] Tomado de FM 022 FORMULACIÓN DEL ESTUDIO DE SECTOR, generado por el área técnica de la necesidad.

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:

> ***a)*** *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.*
>
> ***b)*** *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.*
>
> ***c)*** *Atender la construcción y desarrollo de obras específicas que se requieran para complementar la acción de otros organismos y entidades del Distrito.*
>
> ***d)*** *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.*
>
> ***e)*** *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.*
>
> ***f)*** *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 UAERMV 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 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 significativa 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:

- 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).
- Identificación, evaluación y mitigación de vulnerabilidades (incluyendo detalle de códigos CVE aplicables, recomendaciones de remediación y aplicación de parches virtuales / Virtual Patching) para sistemas operativos Windows, macOS y Linux, sin exigir la distribución o instalación directa de actualizaciones sobre los sistemas operativos.

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.
15. Puntero no válido.
16. Inyección de kernel.
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.

31. Prevención automatizada en tiempo real encriptación de Ransomware.

Funcionalidades de Remediación.

La Solución de EDR propuesta debe orquestar operaciones de respuesta a incidentes utilizando playbooks predefinidos en la solución, optimizando sí 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 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).

- Debe contar con una Gestión Unificada.
- Debe contar con la funcionalidad de identificación de incidentes entre productos.
- Debe contar con la funcionalidad de investigación impulsada por inteligencia artificial.
- 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 compatible con los sistemas operativos y entornos con los que cuenta la Entidad (estaciones de trabajo, portátiles y servidores que conforman los 450 endpoints), en las arquitecturas (32 y/o 64 bits según corresponda a cada sistema operativo) oficialmente soportadas por el fabricante: Windows (incluyendo Windows 11), macOS (Ventura 13 y superior), Windows Server (2019, 2022 y superior) y Linux (Oracle Linux, Ubuntu Server LTS y CentOS/RHEL en las versiones soportadas oficialmente en la hoja de datos del fabricante).

En cuanto al hardware, debe ser un agente ligero, el cual no debe requerir más de 350 MB de memoria RAM y 1 GB de espacio en disco, de acuerdo con la documentación oficial del fabricante, garantizando una operación eficiente y mínima afectación al rendimiento de los equipos protegidos

Las referencias incluidas corresponden exclusivamente a los equipos de cómputo y servidores con los que actualmente cuenta la entidad, información de mercado y tendencias tecnológicas, sin que constituyan preferencia, direccionamiento o exigencia de fabricante específico.

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

Generalidades:

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:

1. Correlacionador de Eventos (FortiSIEM).
2. Analizador (Fortianalyzer)
3. 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 ligero en software compatible con sistemas operativos Windows, macOS y Linux, acreditado conforme a las versiones,

distribuciones y arquitecturas oficialmente soportadas en la documentación técnica o matriz de compatibilidad oficial del fabricante para los endpoints objeto de protección.

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

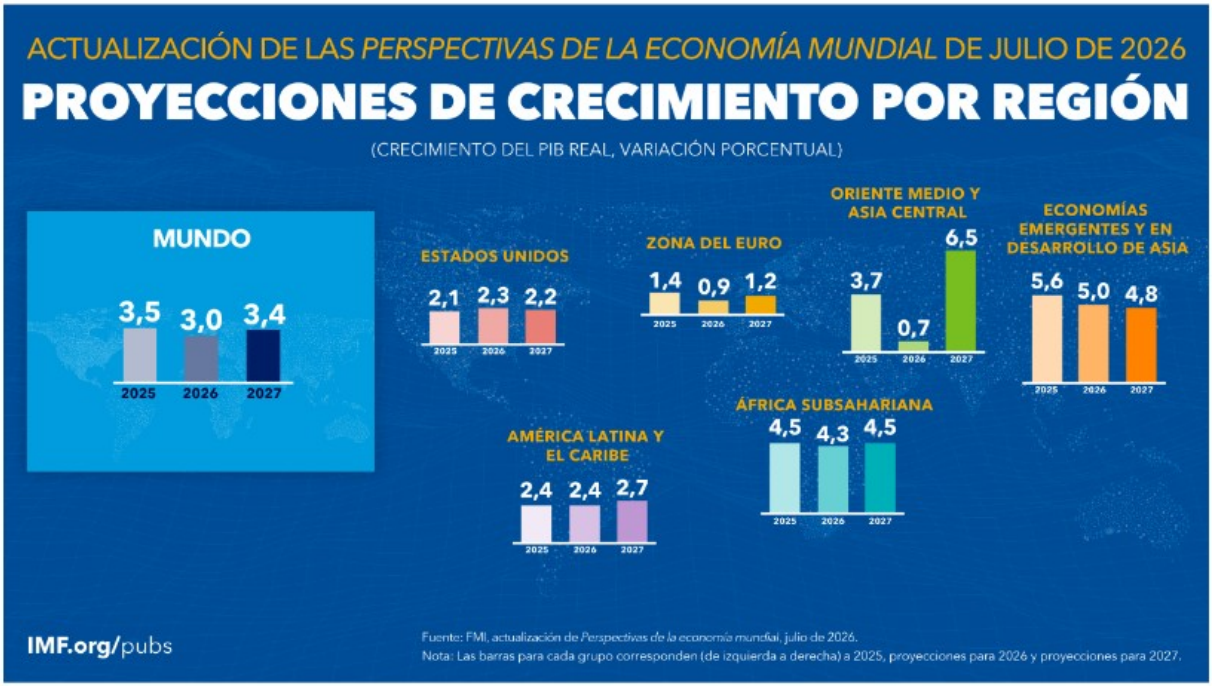
a. Aspectos de Tipo Económico (Macroeconómico y Microeconómico)

Contexto mundial[2].

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.

[2] Tomado de https://www.imf.org/es/publications/weo/issues/2026/07/08/world-economic-outlook-update-july-2026

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[3], 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.

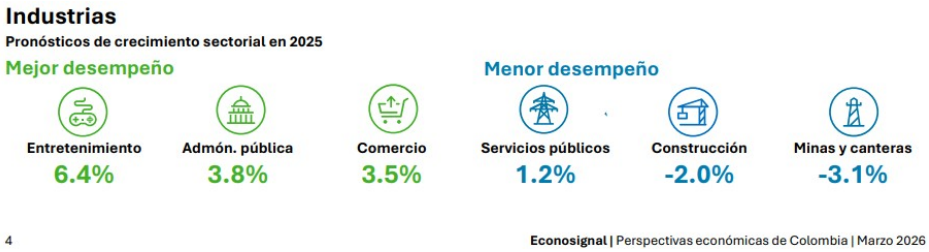
La inversión apenas creció 1.3% en 2025, reflejando una recuperación moderada, mientras que la baja ejecución del gasto público en capital continúa limitando una expansión más sólida de la formación bruta de capital fijo.

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.



[3] Tomado de https://www.deloitte.com/content/dam/assets-zone4/latam/es/docs/services/financial-advisory/2026/Perspectivas-economicas-de-Colombia.pdf



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 [4],

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.

[4] *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[5]

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%).

[5] 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[6]

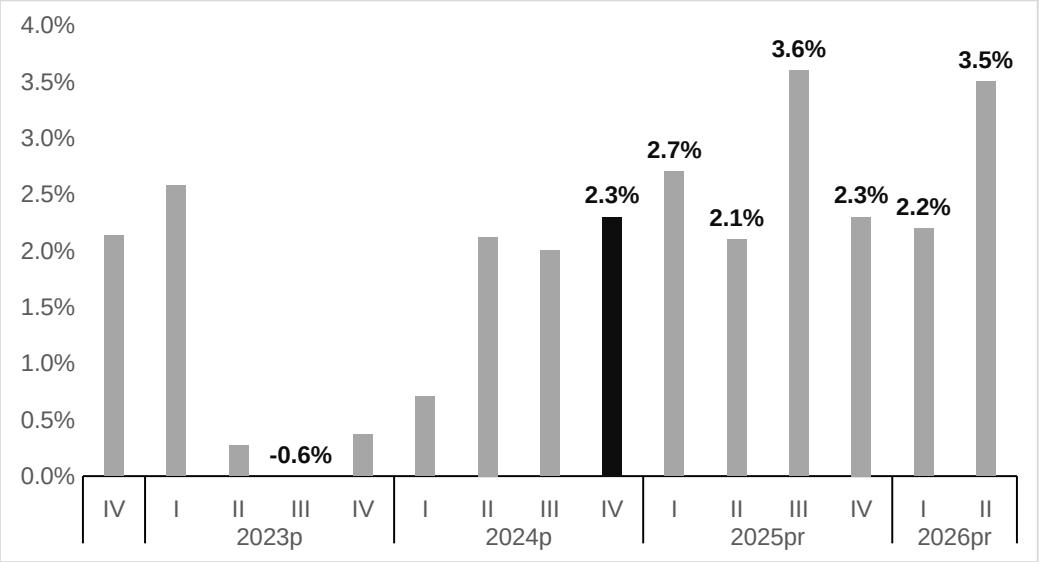
En el segundo trimestre de 2026pr, el Producto Interno Bruto en su serie original, crece 3,5% respecto al mismo periodo de 2025pr. Las actividades económicas que más contribuyen a la dinámica del valor agregado son:

- 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 agregado son:

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

- 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).

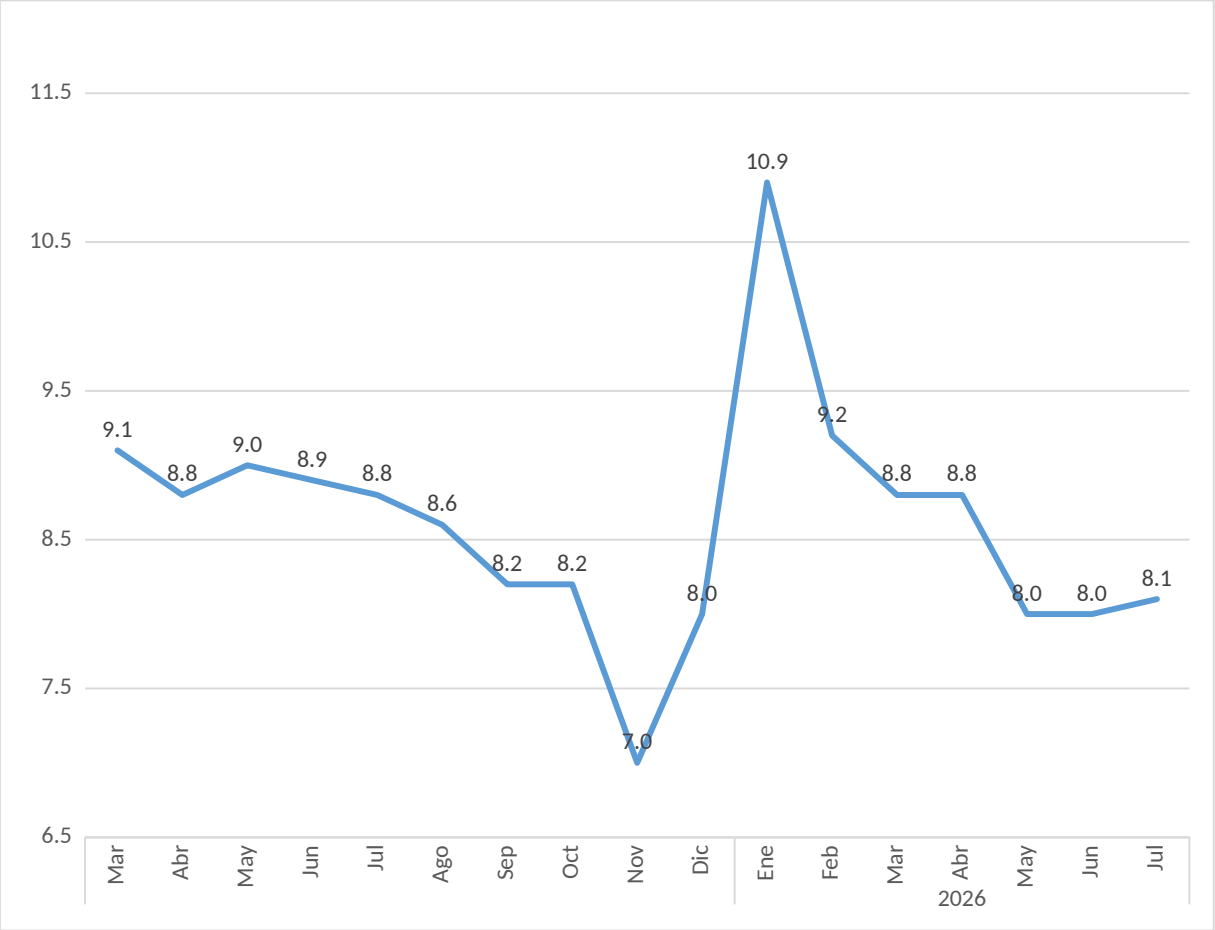


Fuente: DANE (2026).

Indicadores Macroeconómicos: EMPLEO[7]

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.

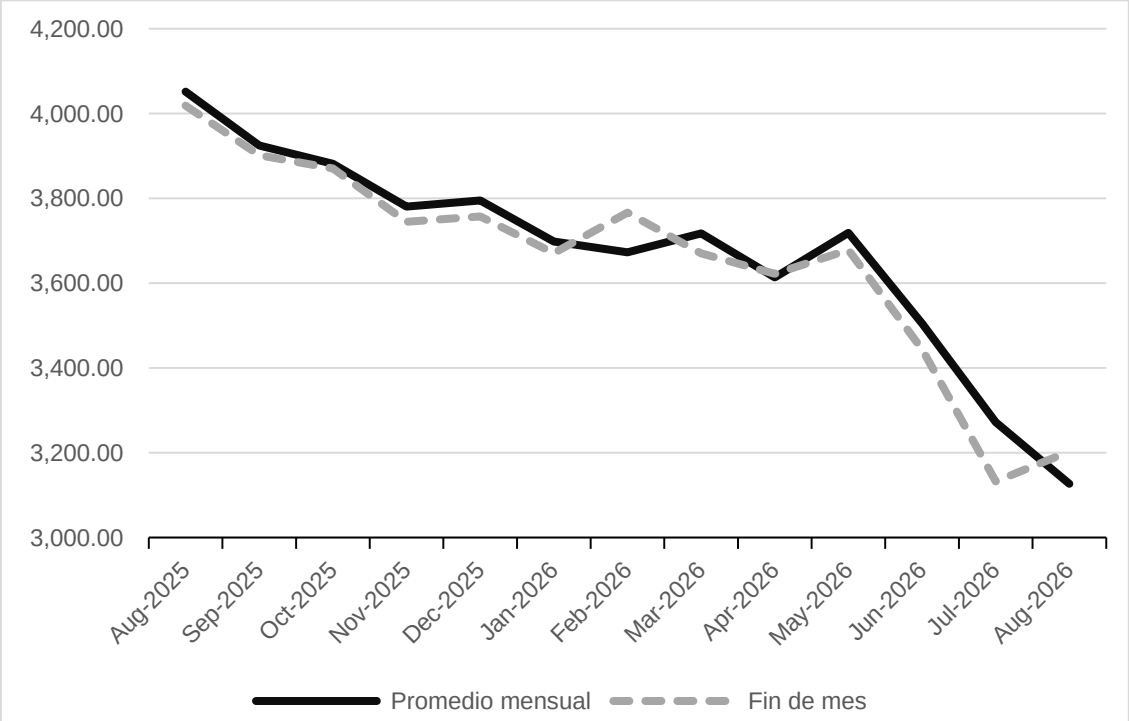
[7] Tomado de: https://www.dane.gov.co/index.php/estadisticas-por-tema/mercado-laboral/empleo-y-desempleo



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)[8].

[8] https://usbcali.edu.co/perspectivas-usd-cop-2026/

- 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%[9]. 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[10].

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[11].

- 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.

Codificación de bienes y servicios.

Conforme a lo establecido en el Decreto 1082 de 2015 “Por medio del cual se expide el decreto único reglamentario del sector administrativo de planeación nacional”, los elementos o bienes a adquirir por la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial se enmarcan en la siguiente clasificación UNSPSC:

Clasificación	Segmento	Familia	Clase	Productos

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

UNSPSC				
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) 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	[43222502] 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

Localización y Área de Influencia.

Ver lo dispuesto en el Anexo 1. GCON FM 022 Formulación Estudio del Sector y Condiciones Técnicas de la Necesidad, numeral Lugar de ejecución o entrega.

Plazo Definido para el Proceso Contractual.

El plazo de ejecución del contrato es de DOS (2) MESES, 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), previo cumplimiento de los requisitos de perfeccionamiento y ejecución establecidos en el artículo 41 de la Ley 80 de 1993.

Nota Aclaratoria: El término de cobertura de las suscripciones y soporte de la misma debe ser por DOCE (12) meses, contados a partir de la firma del acta de inicio, con esquema de soporte 7x24 con fabricante y soporte local por parte del Contratista.

c. Aspectos de Tipo Ambiental y Social

Guía para la Implementación de Compras Públicas Sostenibles.
Teniendo en cuenta, la Guía para la Implementación de Compras Públicas Sostenibles de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., la normatividad aplicable para este proceso en mención es:

Norma	Descripción
Decreto 1076 de 2015	“Por medio del cual se expide el Decreto Único Reglamentario del Sector Ambiente y Desarrollo Sostenible”.
Decreto 317 de 2021	“Por medio del cual se reglamenta el Acuerdo Distrital No. 808 del 2021 y se establecen medidas para reducir progresivamente la adquisición y consumo de plásticos de un solo uso en las Entidades del Distrito Capital”.
Resolución 1295 de 2006	“Por la cual se crea el Comité Interno del Sello Ambiental Colombiano y se adopta su reglamento operativo”.
Resolución 1555 de 2005	“Por medio de la cual se reglamenta el uso del Sello Ambiental Colombiano”.
Resolución 718 de 2023	“Por medio de la cual se adopta la Política Cero Papel en la Secretaría General”.
Resolución 3179 de 2023	“Por la cual se adopta la guía técnica para la formulación del Plan Institucional de Gestión Ambiental (PIGA), y se dictan lineamientos para su concertación, “implementación, evaluación, control y seguimiento, y otras disposiciones”.
Acuerdo 540 de 2013	“Por medio del cual se establecen los lineamientos del programa distrital de compras verdes y se dictan otras disposiciones”.

3. ANÁLISIS DE LA OFERTA

a. Reseña del Sector.

Las plataformas de ciberseguridad de nueva generación representan un cambio de paradigma en la defensa digital, pasando de un modelo reactivo basado en firmas (el antivirus tradicional) a un modelo proactivo basado en el análisis de comportamiento y la identidad. En esencia, estas tecnologías no buscan únicamente un "virus" conocido, sino que monitorean constantemente cualquier actividad inusual en el sistema. El EDR se enfoca en proteger cada dispositivo individual, lo que permite que las organizaciones modernas mantengan una visibilidad total sobre lo que sucede en su red.

El funcionamiento de estas herramientas se basa en un ciclo continuo de visibilidad, detección y respuesta asistida por inteligencia artificial. El EDR instala agentes ligeros que actúan como "sensores" en los equipos, recolectando telemetría sobre procesos, conexiones de red y cambios en archivos. Cuando ocurre un evento sospechoso, como un intento de cifrado masivo de datos (Ransomware), el sistema puede aislar automáticamente el equipo afectado de la red para evitar que la amenaza se propague.

La importancia de estas plataformas radica en la sofisticación de los ataques actuales, los cuales son capaces de evadir las defensas convencionales en cuestión de segundos. El uso principal de estas tecnologías es la reducción del "Dwell Time" o tiempo de permanencia, que es el periodo que un atacante pasa oculto dentro de una red antes de ser detectado; estas herramientas de nueva generación reducen ese tiempo de meses a solo minutos. Son fundamentales para la continuidad del negocio porque no solo detectan el problema, sino que ofrecen capacidades de remediación, como revertir

cambios maliciosos o restaurar configuraciones previas, lo que permite que una organización se recupere de un incidente con el menor impacto operativo y financiero posible.



A nivel global, el mercado de seguridad en el endpoint y plataformas de detección extendida está experimentando una consolidación hacia ecosistemas unificados. Según proyecciones de firmas como Fortune Business Insights, el valor del mercado global de seguridad de endpoints alcanzará aproximadamente los **USD 17,79 mil millones en 2026**, impulsado principalmente por la adopción masiva de modelos de trabajo híbridos y el aumento de ataques de ransomware.

Gartner e IDC coinciden en que los líderes indiscutibles del sector, como CrowdStrike y Microsoft, han logrado esta posición mediante la integración de Inteligencia Artificial Agéntica, que permite la remediación autónoma de incidentes sin intervención humana directa[12].

Las soluciones modernas ya no solo gestionan el acceso, sino que incorporan capacidades de ITDR (Identity Threat Detection and Response) para detectar comportamientos anómalos en las credenciales de los usuarios en tiempo real. Este enfoque de Confianza Cero (Zero Trust) es ahora el estándar exigido por regulaciones internacionales, lo que ha generado una tasa de crecimiento anual compuesta cercana al **8.6%** globalmente para este tipo de soluciones hacia el final de la década.

Dinámica del Mercado Local en Colombia

En el contexto colombiano, el mercado de ciberseguridad para 2026 se estima en un valor cercano a los **USD 1,24 mil millones**, con una marcada maduración en la adopción de tecnologías avanzadas por parte de las PYMES, las cuales crecen a un ritmo del **11.84%** anual.

[12]ttps://www.fortunebusinessinsights.com/industry-reports/endpoint-security-market-100614#:~:text=KEY%20MARKET%20INSIGHTS.%20Listen%20to%20Audio%20Version.,CAGR%20of%208.60%25%20during%20the%20forecast%20period.

Según Mordor Intelligence, este crecimiento local está fuertemente vinculado a la aplicación de normativas de protección de datos más estrictas y a la necesidad de proteger la infraestructura crítica nacional tras incidentes de alto perfil en años anteriores. La realidad operativa en el país ha pasado de la compra de herramientas aisladas a la búsqueda de servicios gestionados (MDR), debido a la escasez de talento especializado en ciberseguridad que afecta a las empresas colombianas, lo que obliga a tercerizar el monitoreo 24/7 a través de partners locales o regionales[13].

El mercado colombiano presenta una alta sensibilidad a los costos iniciales, lo que ha favorecido modelos de consumo por suscripción (SaaS) que permiten flexibilidad frente a la volatilidad de la TRM. Los sectores financieros y gubernamental lideran la inversión, concentrando más del **60%** de los ingresos del sector. No obstante, persiste una brecha de implementación en zonas rurales y sectores menos digitalizados, donde la conectividad fragmentada sigue siendo una barrera para la adopción de plataformas de ciberseguridad basadas 100% en la nube[14].

Precios, Actores y Modelos de Adquisición

El ecosistema de actores está dividido entre fabricantes globales que proveen la tecnología y canales locales que ofrecen la implementación y el soporte. CrowdStrike, Microsoft, Sophos y SentinelOne dominan el cuadrante de líderes por su capacidad de ejecución y visión tecnológica.

En términos de costos, para 2026 los precios de licenciamiento anual por dispositivo o usuario para soluciones de **EDR** oscilan entre **USD 60 y USD 90.**

El modelo de negocio dominante es el de suscripción plurianual (a menudo por 3 años) que incluye actualizaciones constantes de firmas e inteligencia de amenazas. En Colombia, es común que los proveedores incluyan capas de servicio de valor agregado, como el "Threat Hunting" o la respuesta ante incidentes, lo que puede incrementar el valor del contrato en un **30% o 50%**, pero reduce significativamente el riesgo residual para la organización al garantizar que expertos humanos supervisen las alertas generadas por la inteligencia artificial de la plataforma[15].

b. Posibles Proveedores.

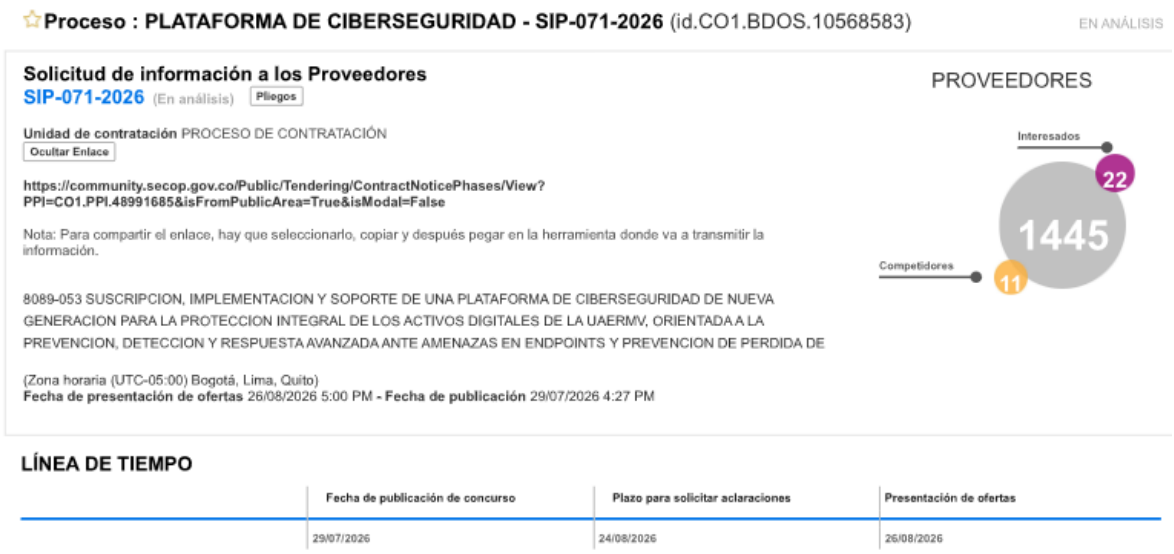
Los posibles proveedores son todas aquellas empresas y/o Uniones temporales que han sido oferentes y/o contratistas, en procesos relacionados con “8089-053 SUSCRIPCION, IMPLEMENTACION Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACION PARA LA PROTECCION INTEGRAL DE LOS ACTIVOS DIGITALES DE LA UAERMV, ORIENTADA A LA PREVENCION, DETECCION Y RESPUESTA AVANZADA ANTE AMENAZAS EN ENDPOINTS Y PREVENCION DE PERDIDAS DE DATOS.” y en otras entidades de tipo Estatal, también aquellas que están registradas en la plataforma de SECOP II y han mostrado interés en participar y también aquellas a las que se invitaron a cotizar la prestación del servicio.

Por tal razón, se abrió proceso de cotización, inicialmente, en la plataforma del SECOP II el día 29 de julio de 2026, con cierre previsto el 3 de agosto de 2026, se reabrió el 21 de agosto de 2026 para entregar las respuestas a las observaciones allegadas por los interesados (están son anexas al presente documentos: Observaciones SIP 071 2026) y dar a conocer el nuevo formato de cotización así como

[13] Ibidem.
[14] https://www.mordorintelligence.ar/industry-reports/colombia-cybersecurity-market.
[15] https://www.crowdstrike.com/en-us/resources/reports/gartner-mq/#:~:text=A%20six%2Dtime%20Leader.%20CrowdStrike%20has%20been%20named,Vision%20and%20highest%20for%20Ability%20to%20Execute.

las condiciones técnicas, entregándose un nuevo plazo de subsanación o entrega de nuevas cotizaciones el día 26 de agosto de 2026.

Se trata del SIP-071-2026 (Anexo 2a. SIP 071 2026 y 2b. SIP 071 2026 Mod. 21Ago26), cuyo objeto fueron el mismo: “8089-053 SUSCRIPCION, IMPLEMENTACION Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACION PARA LA PROTECCION INTEGRAL DE LOS ACTIVOS DIGITALES DE LA UAERMV, ORIENTADA A LA PREVENCION, DETECCION Y RESPUESTA AVANZADA ANTE AMENAZAS EN ENDPOINTS PREVENCION DE PERDIDAS DE DATOS.” y a través de este obtener un valor referente del mercado:



En esta se identificaron 1445 posibles proveedores registrados en SECOP II de acuerdo con los códigos UNSPSC definidos en el Plan Anual de Adquisiciones (PAA 2026), de los cuales ONCE (11) proponentes manifestaron interés y remitieron cotización en el plazo inicial, pero solo 4 proponentes allegaron cotizaciones nuevas tras el ajuste hecho por las observaciones allegadas: ALPHA TECNOLOGÍA SAS, SPECTRUM TECHNOLOGY S.A.S., HEIMCORE SAS y BIM LATINOAMÉRICA SAS.

No se gestionaron cotizaciones por correo electrónico y tampoco se tuvieron en cuenta compras de la entidad en otras vigencias porque el servicio es nuevo dentro de ella.

c. Información Financiera posibles proveedores.

Teniendo en cuenta que en el proceso de selección se deben incluir criterios de verificación financiera según lo establecido en los numerales 3. “Capacidad Financiera” y 4. “Capacidad Organizacional”, del artículo 2.2.1.1.1.5.3 del Decreto 1082 de 2015, y con el fin de que estos se ajusten al sector específico del servicio, bien u obra adquirir, estos indicadores se definen así:

> *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.

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.

Para efectos del análisis del sector económico al que se dirige el presente estudio, se usó la información estadística que produce el DANE conforme a la Clasificación Industrial Internacional Uniforme —CIIU— con base en la Resolución 2306 del 27 de diciembre de 2022 de la misma entidad, que modificó el documento denominado: "Clasificación Industrial Internacional Uniforme de todas las actividades económicas - CIIU Rev. 4 A.C.", y en el artículo 4 de dicha resolución señala que: "La CIIU Rev. 4 A.C. (2022) deberá utilizarse de manera obligatoria por todas las entidades de carácter público y privado que produzcan información estadística en materia de actividad económica, identificando la actividad económica principal para la asignación correcta del código", entonces para hacer el análisis del sector se hizo la verificación con el fin de homologar el Código Estándar de Productos y Servicios de Naciones Unidas con la CIIU.

De acuerdo con la base de datos del Sistema de Integrado de Información Societaria –SIIS, de la Superintendencia de Sociedades, y teniendo en cuenta la identificación de la actividad económica de quienes prestan el servicio, según Clasificación Industrial Internacional Uniforme revisión CIIU V 4 A.C., 6202: Actividades de consultoría informática y actividades de administración de instalaciones

informáticas; y 6201: Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas); se encontraron registros de 85 empresas en el archivo de Plenas individuales y de 298 en el de MIPYMES, con información financiera al 31 de diciembre de 2025.

NO MIPYMES (PLENAS)

Percentil	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA DE INTERÉS	ROE	ROA
20%	1,13	0,27	0,00	0,03	0,01
40%	1,41	0,47	0,82	0,09	0,03
60%	1,97	0,69	3,86	0,18	0,10
80%	4,33	0,80	20,23	0,34	0,17
100%	721,11	1,86	1116,24	0,61	0,33
Promedio	21,29	0,56	49,14	0,15	0,07
Mediana	1,69	0,53	2,84	0,15	0,07
Desviación estándar	107,03	0,33	207,13	0,22	0,12

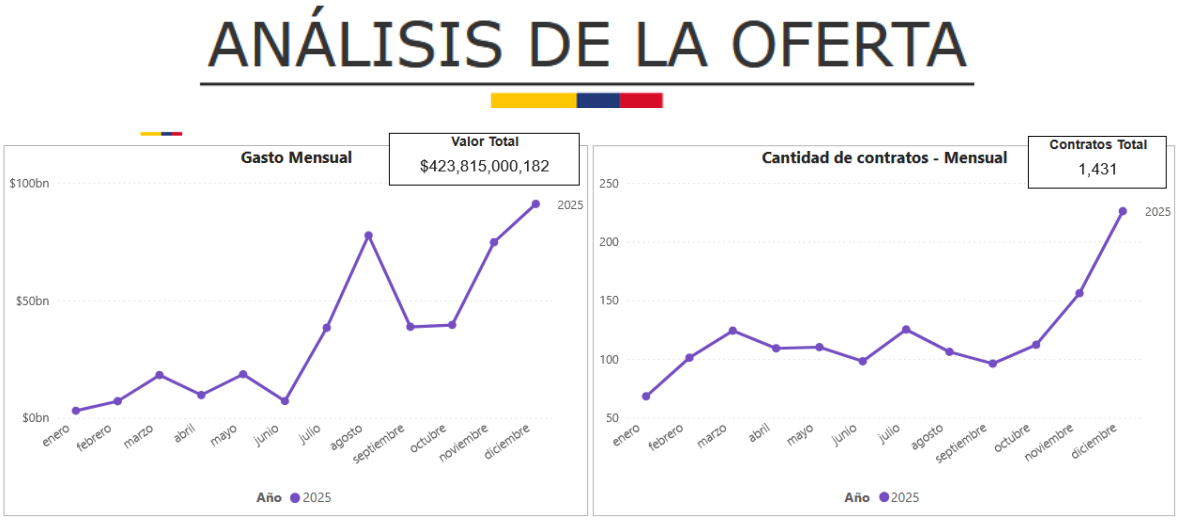
- Realizando un análisis integral de los datos estadísticos y los menores riesgos financieros para el presente proceso, se solicita a la entidad aplicar los siguientes indicadores a empresas NO MIPYMES:

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	
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

RENTABILIDAD DE ACTIVO - ROA	Utilidad Operacional/ Activo Total	Mayor o igual a 0,1	mínimos. Los indicadores se calculan de acuerdo con la participación porcentual de cada uno de los integrantes de consorcio o unión temporal.

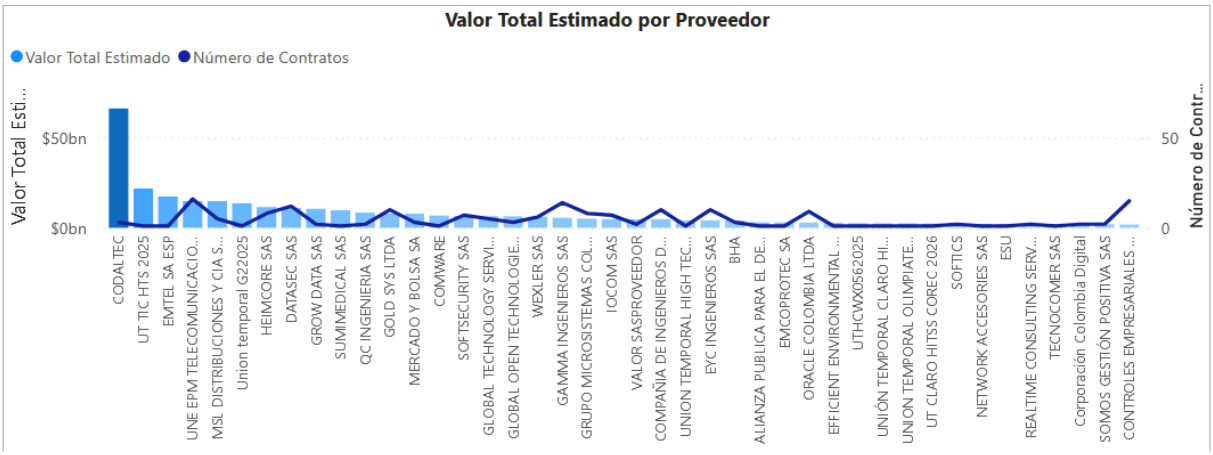
d. Análisis del Modelo de Abastecimiento Estratégico MAE- Colombia Compra Eficiente

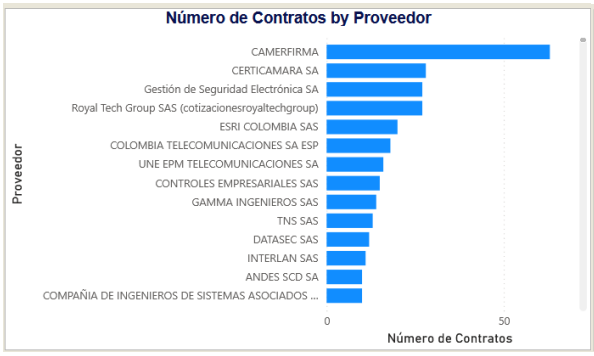
Al respecto, la entidad consultó en la herramienta de insumos de análisis estratégicos desarrollada por Colombia Compra Eficiente[16] la forma en la que los proveedores han ofertado el producto a comprar a través de este acuerdo. El comportamiento en 2025 ha sido para los 2 códigos de las Naciones Unidas definidas para el presente proceso (43222500 y 43233200), así:

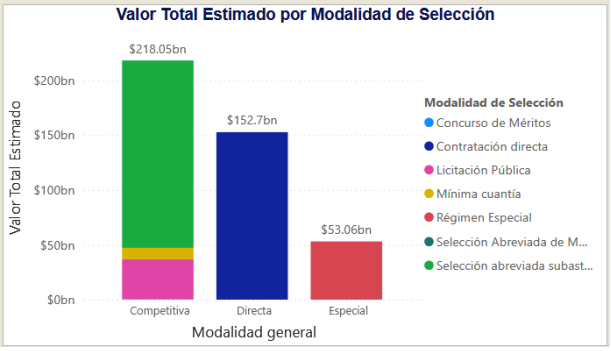


[16] En https://www.colombiacompra.gov.co/analisis-de-datos-de-compra-publica/modelo-de-abastecimiento-estrategico

Valor Contratación	Número de Proveedores	Número de Contratos
$423.82bn	664	1431







Los proponentes en 2025 firmaron contratos por valor de 423,82 billones de pesos. CAMERFIRMA es el proponente con mayor número de contratos, más de 50. La contratación directa y la subasta inversa son las modalidades más usadas para contratar estos servicios.

4. ANALISIS DE LA DEMANDA

a. Adquisiciones Propias de la Entidad

Con base en el historial que reposa en el área de OTI, esta manifiesta no haber contratado este servicio con anterioridad debido a la actualización de la tecnología.

b. Adquisiciones Otras Entidades

Con base en el historial registrado en SECOP, no se identificaron procesos con idéntico alcance funcional y técnico; sin embargo, se identificaron procesos con códigos UNSPSC equivalentes y objetos relacionados con ciberseguridad y protección de información, sin embargo, se trae a colación contratos que usaron los mismos códigos UNSPCS que ha determinado la entidad, con el propósito ilustrativo de que esta demanda existe en las entidades estatales pero cada una lo estructura a su necesidad:

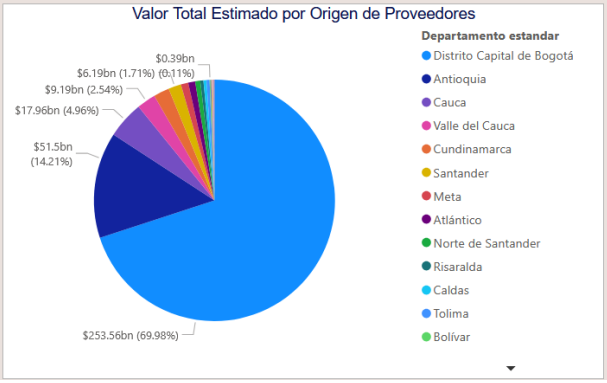
Año Clasificador de Bienes y Servicios - Familia
⊞ **4322 - Equipos o plataformas y accesorios de redes multimedia o de voz y datos**
⊟ **4323 - Software**
⊞ **432329 - Software para trabajo en redes**
⊟ **432332 - Software de seguridad y protección**
⊞ (INFO464) ADQUISICIÓN DE CERTIFICADOS DIGITALES SSL PARA PORTALES DE LA ENTIDAD
⊞ (SG241) ADQUISICIÓN DE FIRMAS DIGITALES PARA SERVIDORES Y COLABORADORES DEL IDEAM
⊞ 064ADQUISICION DE TRES (3) DISPOSITIVOS BIOMETRICOS PARA EL CONTROL DEL CUMPLIMIENTO DE HORARIO DEL PERSONAL DE PLANTA DE LA EMPRESA DE SERVICIOS PUBLICOS DE LA CALERA ESPUCAL ESP
⊞ 1 PLAN DE 1000 FIRMAS DE DOCUMENTOS ELECTRONICOS CON TECNOLOGIA BIOMETRICA CON VIGENCIA DE 1 AÑOPARA LA ENTIDAD
⊞ 1001410 Adquirir los componentes de Software de seguridad para punto final de TRENDMICRO para la protección y prevención del malware así como los servicios de instalación configuración migración y puesta en marcha en la plataforma tecnológica de la Autoridad Nacional de Licencias Ambientales ANLA
⊞ 1001415 ADQUIRIR EL LICENCIAMIENTO DE UNA SOLUCIÓN AVANZADA DE SEGURIDAD PARA LA PREVENCIÓN DE FUGA DE INFORMACIÓN Y CONTROL DE ACCESO (ZERO TRUST NETWORK ACCESS Y DATA LOSS PREVENTION) PARA USUARIOS APLICACIONES Y REDES ASÍ COMO SU IMPLEMENTACIÓN SOPORTE Y MANTENIMIENTO
⊞ 150076 Adquirir los Servicios de Conectividad a través de un enlace Dedicado a Internet para el Ministerio de Ambiente y Desarrollo Sostenible
⊞ 2025TI28 CONTRATAR LA PROVISIÓN DE 200 LICENCIAS DE SOFTWARE ANTIVIRUS POR 12 MESES PARA EQUIPOS DE CÓMPUTO SERVIDORES Y PROTECCIÓN DE LOS CORREOS INSTITUCIONALES AL IGUAL QUE LA INSTALACIÓN DE LA CONSOLA DE ADMINISTRACIÓN EN LA NUBE PARA LA GESTIÓN DE DICHO SERVICIO CON EL FIN DE GARANTIZAR LA PROTECCIÓN Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA ALCALDÍA DE SAN JOSÉ DE CÚCUTA
⊞ 4444 Renovación del soporte y garantía durante un (1) año de los APPLIANCE DE SEGURIDAD (FIREWALL) incluyendo los servicios de instalación configuración afinamiento monitoreo continuo soporte técnico actualizaciones de software reemplazo de componentes fallidos y mantenimiento preventivo y correctivo para asegurar la protección y seguridad de la infraestructura tecnológica de la Auditoría General de la RepúblicaHILLSTONE SG6000 E2860 SERIALES 28127141722009044 y 2812718172004245
⊞ 4448 Contratar la adquisición del servicio de software as a service (SaaS) de firma digital para el Sistema de Gestión de Documentos Electrónicos de Archivo SGDEA de la Auditoría General de la República así como la adquisición de firmas digitales certificadas con el fin de garantizar la autenticidad integridad disponibilidad y validez jurídica de los documentos electrónicos de archivo de la Entidad
⊞ 505Adquisición de la suscripción del licenciamiento de productos y servicios del antivirus Kaspersky para la Superintendencia de Transporte
⊞ 509Renovación del soporte mantenimiento y actualizaciones del licenciamiento de la herramienta Chilkat Crypt para la Superintendencia de Transporte
⊞ 58000C0735 ADQUIRIR LA SUSCRIPCIÓN A LAS LICENCIAS DE SEGURIDAD PERIMETRAL
⊞ 59A15 Adquirir los certificados de firma digital para el registro de información en el Sistema de Información Financiera SIIF Nación II el certificado de firma digital persona jurídica PJEE para validación de los pagos en línea certificado de firma digital persona jurídica para facturación electrónica y el certificado digital persona jurídica para registrar información en el RUNT

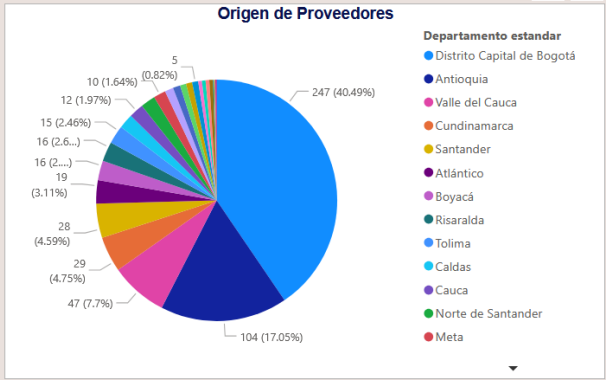
c. Análisis del Modelo de Abastecimiento Estratégico MAE- Colombia Compra Eficiente

Al respecto, la entidad consultó en la herramienta de insumos de análisis estratégicos desarrollada por Colombia Compra Eficiente la forma en la que las entidades estatales han demandado el producto a comprar a través de este acuerdo. El comportamiento en 2024 ha sido para los 2 códigos de las Naciones Unidas definidas para el presente proceso (43222500 y 43233200), así:

ANÁLISIS DE LA DEMANDA

Año	2024			Total		
Clasificador de Bienes y Servicios - Familia	Contratos	Valor	Participación	Contratos	Valor	Participación
⊟ **8111 - Servicios informáticos**	**974**	**$277,390,216,071**	**67.15%**	**974**	**$277,390,216,071**	**67.15%**
⊞ 811125 - Servicios de alquiler o arrendamiento de licencias de software de computador	974	$277,390,216,071	67.15%	**974**	**$277,390,216,071**	**67.15%**
⊟ **4323 - Software**	**423**	**$81,516,898,716**	**19.73%**	**423**	**$81,516,898,716**	**19.73%**
⊞ 432332 - Software de seguridad y protección	391	$72,112,546,997	17.46%	**391**	**$72,112,546,997**	**17.46%**
⊞ 432329 - Software para trabajo en redes	32	$9,404,351,719	2.28%	**32**	**$9,404,351,719**	**2.28%**
⊟ **4322 - Equipos o plataformas y accesorios de redes multimedia o de voz y datos**	**78**	**$54,161,579,540**	**13.11%**	**78**	**$54,161,579,540**	**13.11%**
⊞ 432225 - Equipo de seguridad de red	78	$54,161,579,540	13.11%	**78**	**$54,161,579,540**	**13.11%**
Total	**1475**	**$413,068,694,327**	**100.00%**	**1475**	**$413,068,694,327**	**100.00%**





Por lo que podemos ver, la mayoría de la demanda del servicio se da en la ciudad de Bogotá y los proveedores vienen de diferentes partes del país, siendo liderado por los propios que están ubicados en Bogotá. Finalmente, la mayoría de los proveedores se reconocen a través del Código UNSPCS 81112500.

5. ANÁLISIS DEL SECTOR PARA DETERMINAR OTROS CRITERIOS DIFERENCIALES Y APLICACIÓN DE NORMATIVIDAD QUE LE APLIQUE

Modalidad de Selección.

Por tratarse la contratación de bienes/servicios de características técnicas uniformes y de común utilización con especificaciones técnicas y patrones de desempeño y calidad iguales o similares que pueden ser ofertados por los proponentes en igualdad de condiciones, la UAERMV hará uso de la modalidad de Selección Abreviada prevista en el literal a) del numeral 2o. del artículo. 2 de la Ley 1150 de 2007, la cual describe 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.*
>
> *Para la adquisición de estos bienes y servicios las entidades deberán, siempre que el reglamento así lo señale, hacer uso de procedimientos de subasta inversa o de instrumentos de compra por catálogo derivados de la celebración de acuerdos marco de precios o de procedimientos de adquisición en bolsas de productos".*

Al respecto, el presente estudio del sector evaluará cuáles de las opciones será la más favorable para la entidad, partiendo que se deberá escoger entre SUBASTA INVERSA o BOLSA DE PRODUCTOS, ya que solo se tendrá en cuenta el factor de precio como criterio de selección, descartando así las demás modalidades.

Decreto 310 de 2021 "Sobre Aplicación de los Acuerdos Marco de Precios".

De acuerdo con el procedimiento establecido en el Decreto 310 de 2021 sobre la aplicación de los Acuerdos Marco de Precios —"Por el cual se reglamenta el artículo 41 de la Ley 1955 de 2019, sobre las condiciones para implementar la obligatoriedad y aplicación de los Acuerdos Marco de Precios y se modifican los artículos 2.2.1.2.1.2.7. y 2.2.1.2.1.2.12. del Decreto 1082 de 2015, Único Reglamentario

del Sector Administrativo de Planeación Nacional"—, se realizó una consulta en el portal de Colombia Compra Eficiente y se evidenció que:

Se realizó revisión de los catálogos de los Acuerdos Marco de Precios vigentes en la categoría de TECNOLOGÍA, que pudieran suplir la necesidad de la Entidad y que se encuentran publicados en la página https://www.colombiacompra.gov.co/archivos/portfolio-item/iad-sda-de-software-por-catalogo-ii:



De acuerdo con lo anterior, se verificó el catálogo del Instrumento de Agregación de Demanda / Sistema Dinámico de Adquisición (SDA) de Software por Catálogo II CCE-SNG-IAD-002-2024. Este mecanismo, al no constituir un Acuerdo Marco de Precios, carece de obligatoriedad y su utilización es potestativa para las entidades estatales.

En este contexto, la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial – UAERMV realizó la revisión del Instrumento de Agregación de Demanda – Sistema Dinámico de Adquisición de Software por Catálogo II, con el propósito de verificar la existencia de soluciones que cubrieran de manera integral el objeto de la presente contratación.

Como resultado de dicho análisis, se identificaron referencias asociadas a soluciones de **antivirus o antimalware de carácter tradicional**, así como funcionalidades puntuales orientadas a **protección básica o seguridad de endpoint específica**, las cuales no incorporan capacidades avanzadas de detección, análisis y respuesta ante incidentes de seguridad. En particular, dichas referencias no contemplan funcionalidades de EDR, ITDR, correlación de eventos, análisis comportamental, respuesta automatizada, investigación forense ni operación bajo un modelo de agente/sensor único, requeridas por la Entidad.

En consecuencia, se evidenció que las soluciones disponibles en el catálogo no cubren de manera integral el alcance funcional, técnico y operativo del objeto contractual, el cual incluye la suscripción y operación unificada de plataformas avanzadas de ciberseguridad para la protección de endpoints, identidades y activos críticos de información. Por lo anterior, el Instrumento de Agregación de Demanda analizado no resulta idóneo para atender las necesidades específicas de la UAERMV**,** haciendo necesario adelantar un proceso de contratación que permita garantizar el cumplimiento de los requerimientos definidos por la Entidad. La verificación quedó documentada mediante consulta

realizada durante la etapa de estructuración contractual y soportada mediante evidencia electrónica archivada en el expediente.

Teniendo en cuenta lo anterior, se concluye que, a la fecha de estructuración del presente Análisis del Sector y Estudio de Mercado (septiembre de 2026), no existe un mecanismo de compra aplicable para la suscripción de una solución de ciberseguridad con funcionalidades de DLP, ITDR y EDR para la UAERMV.

Ahora, atendiendo lo dispuesto en el "ARTÍCULO 2. Modificación del artículo 2.2.1.2.1.2.12. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional. Modifíquese el artículo 2.2.1.2.1.2.12. de la Subsección 2, de la Sección 1 del Capítulo 2, del Título 1, de la Parte 2, del Libro 2 del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional el cual quedará así:

> *"ARTÍCULO 2.2.1.2.1.2.12. Planeación de una adquisición en la bolsa de productos. Cuando no exista un Acuerdo Marco de Precios para el bien o servicio requerido, las entidades estatales deben estudiar, comparar e identificar las ventajas de utilizar la bolsa de productos para la adquisición respectiva frente a la subasta inversa o a la promoción de un nuevo Acuerdo Marco de Precios con la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente- para tales bienes o servicios, incluyendo el análisis del Proceso de Selección del comisionista, los costos asociados a la selección, el valor de la comisión y de las garantías".*

El análisis que realizó la entidad para dar cumplimiento a dicho artículo se expone a continuación[17].

Para el análisis cuantitativo la entidad tuvo en cuenta que el presente proceso se debe llevar a monto agotable y para el mismo ha dispuesto en su Plan Anual de Adquisiciones, de un presupuesto proyectado de **QUINIENTOS VEINTINUEVE MILLONES SETECIENTOS OCHENTA Y SEIS MIL OCHOCIENTOS CINCUENTA Y NUEVE PESOS M/CTE ($529.786.859,00).** Partiendo de este y teniendo en cuenta los costos inherentes al mecanismo de Bolsa de Productos (en Colombia lo ejerce la BOLSA MERCANTIL DE COLOMBIA S.A. o BMC), podemos discriminar los costos totales del proceso de la siguiente manera:

COSTOS TOTALES POR USO DEL MECANISMO DE BOLSA DE PRODUCTOS (BMC S.A.)			
OBJETO DE LA NEGOCIACIÓN	**PRECIOS SIN IVA**	**IVA**	**TOTAL**
8089-053 SUSCRIPCION, IMPLEMENTACION Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACION PARA LA PROTECCION INTEGRAL DE LOS ACTIVOS DIGITALES DE LA UAERMV, ORIENTADA A LA PREVENCION, DETECCION Y RESPUESTA AVANZADA ANTE AMENAZAS EN ENDPOINTS PREVENCION DE PERDIDAS DE DATOS.	$ 505.388.850,00	$ 18.263.598,00	$ 523.652.448,00

[17] De esta manera, la entidad da cumplimiento a lo dispuesto en la legislación, quien dispone que las Entidades Estatales que pretendan adquirir bienes y servicios de características técnicas uniformes mediante la Bolsa de Productos deben realizar un estudio de ventajas de este instrumento frente los Acuerdo Marco de Precios, teniendo en cuenta los aspectos cualitativos y cuantitativos, así como la obligación de incluir en el estudio de ventajas de acudir a la Bolsa de Productos el análisis del cumplimiento de los postulados de la función administrativa y de la Gestión Fiscal.

COSTOS DE BOLSA *(Se calculan teniendo como base el valor de la negociación antes de IVA)*	**%**	**PRECIOS SIN IVA**	**IVA**	**TOTAL**
REGISTRO BOLSA (%)	0,30	$1.516.167,00	$288.072,00	$1.804.239,00
COMPENSACIÓN BOLSA (%)	0,21	$1.061.317,00	$201.650,00	$1.262.967,00
COSTO SOCIEDAD COMISIONISTA COMPRADORA (%)	0,51	$2.577.483,00	$489.722,00	$3.067.205,00
TOTAL COSTOS DE BOLSA				$6.134.411,00

Notas:
1. El valor de la comisión de la sociedad comisionista compradora será el máximo a pagar, pero se espera que disminuya tras la rueda de selección realizada por la BMC S.A.
2. El dinero ahorrado por el menor costo de comisión de la sociedad comisionista compradora se añadirá al valor total del objeto de la negociación.
3. Los costos de registro y compensación podrán subir, toda vez que están en función del valor del objeto de la negociación antes de IVA.

$$Valor total del proceso = \$523.652.448,00 + \$6.134.411,00$$

$$Valor total del proceso = \$529.786.859,00$$

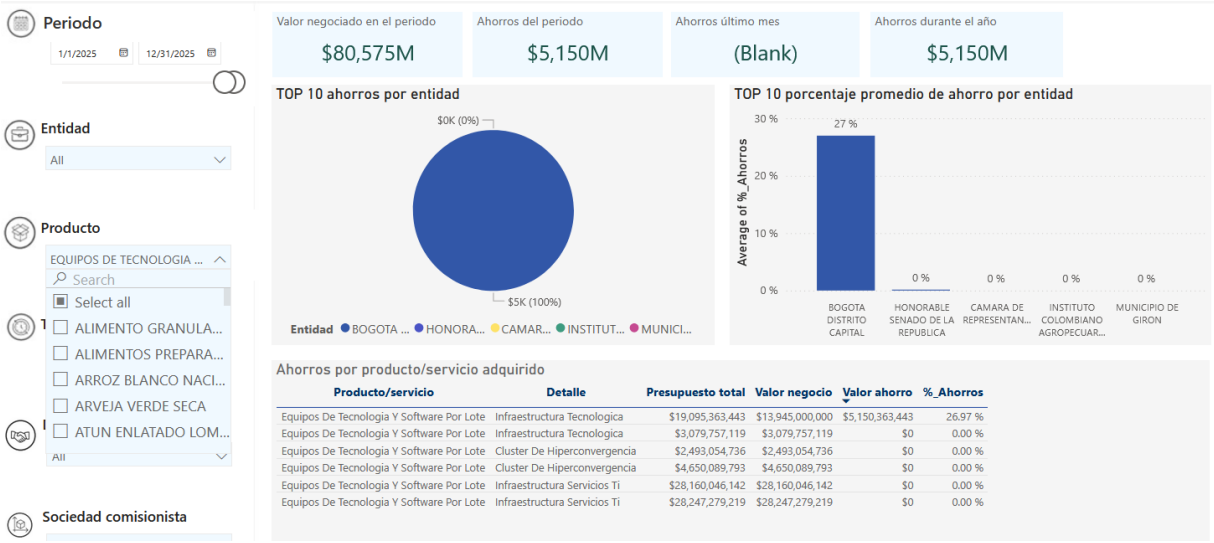
De manera comparativa, el valor por subasta inversa NUNCA podrá ser superior a:

POR SELECCIÓN ABREVIADA DE SUBASTA INVERSA	
	Valores
Presupuesto Oficial Estimado	$523.652.448

De manera concluyente y respecto del análisis cuantitativo, se puede evidenciar que para la entidad resulta mejor la compra de los elementos descritos en la necesidad ya que cuenta con mayor recurso financiero para satisfacer su necesidad al no pagar intermediarios.

Por otra parte, no es garante que, a través de la modalidad por Bolsa de Productos, la entidad logre algún tipo de ahorros, sobre todo para el monto por el cual la entidad espera negociar, lo anterior se basa en la gráfica que se muestra a continuación tomada directamente de la página web de la Bolsa Mercantil de Colombia S.A.[18]:

[18] https://www.bolsamercantil.com.co/mercado-de-compras-publicas



En ella se puede ver que, por negocios inclusive de mayor presupuesto al expuesto en el presente estudio del sector, las entidades que acudieron a este mecanismo no tuvieron ahorro alguno, por tanto, la UAERMV no puede correr el riesgo de llevar su proceso por este mecanismo, no encontrar pluralidad de oferentes y adjudicar a un precio interpuesto por el potencial único proponente.

Huelga mencionar que el mecanismo de subasta inversa permite una mayor concurrencia de oferentes especializados del sector TI y ciberseguridad, optimizando la competencia efectiva respecto al mecanismo de Bolsa Mercantil; si bien las entidades pueden elegir libremente cualquiera de las dos opciones, en términos de publicidad y optimización de costos administrativos, la subasta es el mecanismo más conveniente, además que, en virtud de lo normado en la Ley 1150 de 2007 y el Decreto 1082 de 2015, el mecanismo utilizado por regla general es el de selección abreviada a través de subasta inversa, atendiendo el tipo de bienes y servicios a adquirir, mientras que el mecanismo de adquisición a través de bolsa de productos opera más de manera excepcional.

Aplicación de Fichas Verdes.

Para el presente proceso “8089-053 SUSCRIPCION, IMPLEMENTACION Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACION PARA LA PROTECCION INTEGRAL DE LOS ACTIVOS DIGITALES DE LA UAERMV, ORIENTADA A LA PREVENCION, DETECCION Y RESPUESTA AVANZADA ANTE AMENAZAS EN ENDPOINTS PREVENCION DE PERDIDAS DE DATOS.” la entidad NO ha publicado FICHAS VERDES aplicables.

Decreto Único Sectorial 643 de 2025.

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.

Decreto 287 del 19 de marzo de 2026.

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 las Procesos de Contratación en favor de personas con discapacidad, las 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 Mipymes, emprendimientos de mujeres emprendimientos y empresas de 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 de plataformas de ciberseguridad (Endpoint Detection and Response y/o Data Loss Prevention) así:

Número de contratos con los cuales el proponente cumple la experiencia		**Valor mínimo a certificar (como % del Presupuesto Oficial expresado en SMMLV)**
MiPymes, emprendimiento de mujeres y emprendimiento de empresas de personas con discapacidad	**No MiPymes**	
Máximo 5	Máximo 3	100%

Nota 1: Para efectos de la verificación de la experiencia habilitante, la UAERMV considerará válidos los contratos aportados por el proponente que, de manera individual o conjunta, permitan acreditar las actividades relacionadas con (Endpoint Detection and Response y/o Data Loss Prevention),
Nota 2: No será obligatorio que las dos plataformas se encuentren acreditadas dentro de un mismo contrato. En consecuencia, el proponente podrá demostrar la experiencia requerida mediante la combinación de los contratos presentados, siempre que, en su conjunto, permitan verificar el cumplimiento de las actividades exigidas, respetando el número máximo de contratos establecido y las demás condiciones de experiencia habilitante previstas en el presente proceso.

Artículo 2.2.1.2.4.2.2 del Decreto 1082 de 2015 modificado por el artículo 5 del Decreto 1860 de 2021

De conformidad con lo dispuesto en el artículo 2.2.1.2.4.2.2 del Decreto 1082 de 2015, modificado por el Decreto 1860 de 2021, la posibilidad de limitar la participación en los procesos de contratación a MIPYMES procede únicamente cuando el valor del proceso sea inferior a ciento veinticinco mil dólares de los Estados Unidos de América (US$125.000)[19], liquidados con la tasa de cambio que para el efecto fija el Ministerio de Comercio, Industria y Turismo. Por lo tanto, para el presente proceso NO aplica lo descrito en el decreto 1082 de 2015, modificado por el decreto 1860 de 2021.

Decreto 1082 de 2015, Art 2.2.1.2.4.2.16 y Decreto 380 de 2015.

Exigir el cumplimiento del artículo 2.2.1.2.4.2.16 del Decreto 1082 de 2015 y del Decreto 380 de 2015, expedido por la Alcaldía Mayor de Bogotá el 28 de septiembre de 2015, adopta la Política Pública de Trabajo Decente y Digno en el Distrito Capital. Esta norma busca erradicar la segregación social, promoviendo empleo digno con garantías fundamentales, seguridad social y equidad para la población en edad de trabajar que habita en la ciudad, , sin embargo, dadas las características altamente especializadas del objeto contractual, los perfiles requeridos deberán acreditar las competencias técnicas definidas en el proceso, sin perjuicio del respeto de los principios de igualdad y no discriminación, esta contratación no da aplicación a lo establecido en dicha normativa.

Aplicación Artículo 2.2.1.2.4.2.19. del Decreto 1082 de 2015.

De conformidad con lo previsto en el artículo 2.2.1.2.4.2.19. del Decreto 1082 de 2015, se procedió a validar la pertinencia de dividir en lotes los bienes y servicios objeto de la necesidad manifestada por la entidad, verificando que NO ES VIABLE, dado que el servicio a proveer debe ser integral, por lo que una posible división haría más difícil la ejecución técnica del mismo.

Aplicación Artículo 2.2.1.2.4.2.15 y 2.2.1.2.4.2.18 del Decreto 1860 de 2021

De conformidad con el artículo 3º del decreto 1860 de 2021 que adicionó el artículo 2.2.1.2.4.2.14, 2.2.1.2.4.2.15 y 2.2.1.2.4.2.18 a la Subsección 2 de la Sección 4 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, con la finalidad de promover y facilitar la participación en los procedimientos de selección competitivos tanto de los emprendimientos y empresas de mujeres, así como de las Mipyme, se consagra que siempre que no se ponga en riesgo el cumplimiento adecuado

[19] Que en pesos colombianos corresponde a $511.708.497 según Radicado 2-2026-002760 del Ministerio de Comercio, Industria y Turismo del 3 de febrero de 2026.

del objeto contractual, con excepción de los procedimientos donde el menor precio ofrecido sea el único factor de evaluación, las Entidades deberán incorporar requisitos habilitantes diferenciales relacionados con alguno o algunos de los siguientes aspectos:

1. Tiempo de experiencia.
2. Número de contratos para la acreditación de la experiencia.
3. Índices de capacidad financiera.
4. Índices de capacidad organizacional.
5. Valor de la garantía de seriedad de la oferta.

Por lo tanto, para el presente proceso, la entidad ha determinado que aplicará los aspectos 2, 3 y 4. Con base al Artículo 3 del Decreto 1860 de 2021 que adiciono el 2.2.1.2.4.2.15 Criterios Diferenciales para **emprendimientos de mujeres en el sistema de compras públicas** (…) y el 2.2.1.2.4.2.18 del Decreto 1082 que señala - **Criterios diferenciales para MiPymes** en el sistema de compras públicas. Con el ánimo de establecer condiciones habilitantes diferenciales que promuevan y faciliten la participación en los procedimientos de selección competitivos de las **MiPymes** domiciliadas en Colombia en cumplimiento del numeral 2 se establecerán los siguientes criterios para la acreditación de la experiencia, cuyo Objeto o alcance se encuentre relacionado con la suscripción, implementación y soporte de soluciones de plataformas de ciberseguridad (Endpoint Detection and Response y/o Data Loss Prevention), así:

Número de contratos con los cuales el proponente cumple la experiencia		**Valor mínimo a certificar (como % del Presupuesto Oficial expresado en SMMLV)**
MiPymes, emprendimiento de mujeres y emprendimiento de empresas de personas con discapacidad	**No MiPymes**	
Máximo 5	Máximo 3	100%

Nota 1: Para efectos de la verificación de la experiencia habilitante, la UAERMV considerará válidos los contratos aportados por el proponente que, de manera individual o conjunta, permitan acreditar las actividades relacionadas con (Endpoint Detection and Response y/o Data Loss Prevention),
Nota 2: No será obligatorio que las dos plataformas se encuentren acreditadas dentro de un mismo contrato. En consecuencia, el proponente podrá demostrar la experiencia requerida mediante la combinación de los contratos presentados, siempre que, en su conjunto, permitan verificar el cumplimiento de las actividades exigidas, respetando el número máximo de contratos establecido y las demás condiciones de experiencia habilitante previstas en el presente proceso.

La verificación se hará con base en la sumatoria de los valores ejecutados de las actividades que cumplen la experiencia solicitada (incluido IVA) en SMMLV de los contratos que cumplan con los requisitos a establecer.

El proponente cumple el requisito de experiencia si la sumatoria de los valores totales ejecutados de las actividades que cumplen la experiencia solicitada (incluido IVA) expresados en SMMLV es mayor o igual al valor mínimo a certificar establecido en la tabla anterior.

Análisis de MiPymes.

"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"

Para una adecuada gestión de compras en las Entidades Estatales, es necesario contar con elementos que les permitan satisfacer sus necesidades de bienes y/o servicios obteniendo siempre la mayor optimización posible de los recursos públicos.

En este sentido, el Artículo No. 2.2.1.1.1.6.1. "Deber de análisis de las Entidades Estatales" del Decreto 1082 de 2015, dispone: "*La Entidad Estatal debe hacer, durante la etapa de planeación, el análisis necesario para conocer el sector relativo al objeto del Proceso de Contratación desde la perspectiva legal, comercial, financiera, organizacional, técnica, y de análisis de Riesgo*".

A través del análisis de sector se pretende orientar a la Entidad Estatal en la definición requisitos habilitantes y técnicos de su proceso, así como en la caracterización de su mercado e identificación de posibles riesgos del proceso de contratación. Aunado a lo anterior, el 31 de diciembre de 2020 se sancionó la Ley 2069 de 2020 con el propósito de impulsar el nacimiento de nuevas empresas que incentiven la generación de empleo en país. En aras de dar cumplimiento a lo dispuesto en el artículo 33 de la Ley 2069 de 2020 referente a la "Promoción del acceso de las MiPymes al mercado de compras públicas":

> *"(…) Artículo 12. Promoción del acceso de las MIPYMES al mercado de Compras Públicas. Con el fin de promover el acceso de las MIPYMES al mercado de Compras Públicas, las Entidades Estatales indistintamente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos:*
>
> 1. *Deberán en el Análisis de Sector identificar las MIPYMES que podrían ser potenciales proveedoras directas o indirectas, con el fin de definir reglas que promuevan y faciliten su participación en el Proceso de Contratación. (…)"*
>
> Según la Ley 590 del 2000 "*Se entiende por micro, pequeña y mediana empresa, toda unidad de explotación económica, realizada por persona natural o jurídica, en actividades empresariales, agropecuarias, industriales, comerciales o de servicios, rural o urbana que cumpla con algunos requisitos*".

Las pequeñas, medianas y grandes empresas cumplen un importante papel en la economía de todos los países. Los países de la OCDE suelen tener entre el 70% y el 90% de los empleados en este grupo de empresas. Las principales razones de su existencia son:

- Pueden realizar productos individualizados en contraposición con las grandes empresas que se enfocan más a productos más estandarizados.
- Sirven de tejido auxiliar a las grandes empresas. La mayor parte de las grandes empresas se valen de empresas subcontratadas menores para realizar servicios y operaciones que de estar incluidas en el tejido de la gran corporación redundaría en un aumento de coste.

- Existen actividades productivas donde es más apropiado trabajar con empresas pequeñas, como por ejemplo el caso de las cooperativas agrícolas.

El Gobierno Nacional expidió el Decreto 957 de 2019[20], mediante el cual se establece una nueva clasificación del tamaño empresarial basada en el criterio único de ingresos por actividades ordinarias.

El ministro de Comercio, Industria y Turismo afirmó que la nueva disposición es más cercana a la realidad del tejido empresarial ya que reconoce las diferencias sectoriales y por ello, define rangos de clasificación para tres macrosectores económicos: manufacturas, servicios y comercio.

A la fecha, las empresas en Colombia se han clasificado por medio de las variables “Número de empleados” y “Volumen de activos”. Sin embargo, dada la necesidad de contar con una clasificación que responda a las nuevas realidades de las empresas colombianas, el Gobierno Nacional decidió adoptar los ingresos como único criterio ya que aporta mejor información sobre el tamaño real de las empresas y permite tener presentes las particularidades de cada sector de la economía, como por ejemplo el comportamiento de firmas de servicios o tecnología.

La norma señala como criterio para la clasificación los ingresos de actividades ordinarias anuales y dicho nivel variará dependiendo del sector económico en el que las empresas desarrollen sus actividades y, además, del valor de la UVT para el año gravable anterior.

Teniendo en cuenta que la Resolución de la Dian número 000238 de 2025 estableció el valor de la UVT para el año gravable 2026 en $52.374, así quedan los valores en pesos que determinan la clasificación de las empresas para el año 2026 con ingresos a 31 de diciembre de 2025:

SECTOR	MICRO	PEQUEÑA	MEDIANA
Manufacturero	Iguales o inferiores a 23.563 UVT. Ingresos iguales o inferiores a $ 1.234.088.562,00	Mayores a 23.563 UVT y menores o iguales a 204.995 UVT. Ingresos mayores a $ 1.234.088.562,00 y menores o iguales a $10.736.408.130,00	Mayores a 204.995 UVT y menores o iguales a 1.736.565 UVT. Ingresos mayores a $10.736.408.130,00 y menores o iguales a $90.950.855.310,00
Servicios	Iguales o inferiores a 32.988 UVT. Ingresos iguales o inferiores a $1.727.713.512,00	Mayores a 32.988 UVT y menores o iguales a 131.951 UVT. Ingresos mayores a $1.727.713.512,00y menores o iguales a $6.910.801.674,00	Mayores a 131.951 UVT y menores o iguales a 483.034 UVT. Ingresos mayores que $6.910.801.674,00 y menores iguales a $25.298.422.716,00
Comercio	Iguales o inferiores a 44.769 UVT. Ingresos iguales o inferiores a $2.344.731.606,00	Mayores a 44.769 y menores o iguales a 431.196 UVT. Ingresos mayores a $2.344.731.606,00 y menores o iguales a $22.583.459.304,00	Mayores a 431.196 UVT y menores o iguales a 2.160.692 UVT. Ingresos mayores que $22.583.459.304,00 y menores o iguales a $113.164.082.808,00

Nota: Aquellas firmas que no clasifiquen en alguno de los tres sectores anteriores deberán usar los umbrales determinadores para el macro sector de manufactura.

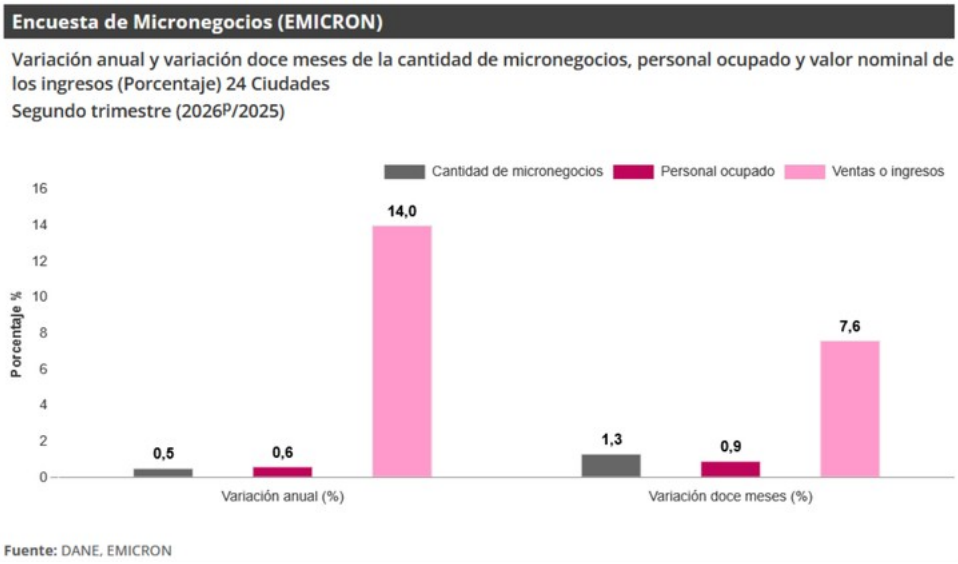
Caracterización de las MIPYMES

La Encuesta de Micronegocios - EMICRON[21], tiene el objetivo general de proporcionar información estadística sobre la estructura y evolución de las principales variables económicas de los micronegocios con hasta nueve (9) personas ocupadas y que desarrollan actividades de agricultura, ganadería, silvicultura y pesca, minería, industria manufacturera, comercio, construcción, transporte y demás servicios. Asimismo, provee estadísticas e indicadores que permiten conocer las formas de operación

[20] https://www.mincit.gov.co/prensa/noticias/industria/gobierno-expide-nueva-clasificacion-de-empresas-a
[21] https://www.dane.gov.co/index.php/estadisticas-por-tema/mercado-laboral/micronegocios (publicación más reciente)

de las unidades económicas de pequeña escala: su actividad económica, emprendimiento, sitio o ubicación, características del personal ocupado, uso de las Tecnologías de la Información y las Comunicaciones (TIC), inclusión financiera, costos, gastos y activos, ventas o ingresos y capital social.

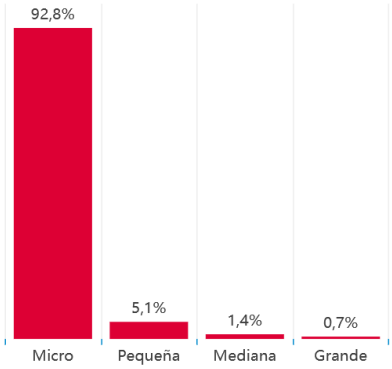
En el segundo trimestre de 2026, la cantidad de micronegocios aumentó 0,5% en comparación con el mismo periodo de 2025. Respecto al personal ocupado por estas unidades económicas aumentó 0,6%. De la misma manera, los ingresos de los micronegocios aumentaron 14,0% en este mismo intervalo de tiempo.



Las actividades económicas que tuvieron contribución positiva a la variación total de la cantidad de micronegocios fueron: Actividades inmobiliarias, profesionales y comunicaciones con 1,1 p.p.; Transporte y almacenamiento con 1,0 p.p.; Otras actividades de servicios con 0,4 p.p.; Alojamiento y servicios de comida con 0,3 p.p. e Industria manufacturera con 0,05 p.p. Por su parte, las actividades que contribuyeron negativamente a la variación fueron: Comercio y reparación de vehículos automotores y motocicletas con -1,7 p.p. y Construcción con -0,6 p.p.

Empresas activas 2025 por tamaño.[22]

[22] https://www.ccb.org.co/informacion-especializada/observatorio/dinamica-empresarial/empresas-activas (publicación más reciente).



Fuente: Registro Mercantil, CCB para Bogotá, enero – diciembre 2025.

Indicadores financieros y de capacidad organizacional para MIPYMES

Para efectos del análisis del sector económico al que se dirige el presente estudio, se usó la información estadística que produce el DANE conforme a la Clasificación Industrial Internacional Uniforme —CIIU— con base en la Resolución 2306 del 27 de diciembre de 2022 de la misma entidad, que modificó el documento denominado: "Clasificación Industrial Internacional Uniforme de todas las actividades económicas - CIIU Rev. 4 A.C.", y en el artículo 4 de dicha resolución señala que: "La CIIU Rev. 4 A.C. (2022) deberá utilizarse de manera obligatoria por todas las entidades de carácter público y privado que produzcan información estadística en materia de actividad económica, identificando la actividad económica principal para la asignación correcta del código", entonces para hacer el análisis del sector se hizo la verificación con el fin de homologar el Código Estándar de Productos y Servicios de Naciones Unidas con la CIIU. De acuerdo con la base de datos del Sistema de Integrado de Información Societaria –SIIS, de la Superintendencia de Sociedades[23], y teniendo en cuenta la identificación de la actividad económica de quienes prestan el servicio, según Clasificación Industrial Internacional Uniforme revisión CIIU V 4 A.C.: De acuerdo con la base de datos del Sistema de Integrado de Información Societaria – SIIS, de la Superintendencia de Sociedades, y teniendo en cuenta la identificación de la actividad económica de quienes prestan el servicio, según Clasificación Industrial Internacional Uniforme revisión CIIU V 4 A.C., 6202: Actividades de consultoría informática y actividades de administración de instalaciones informáticas; y 6201: Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas); se encontraron registros de 85 empresas en el archivo de Plenas individuales y de 298 en el de MIPYMES, con información financiera al 31 de diciembre de 2025.

MIPYMES

Percentil	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA DE INTERÉS	ROE	ROA
20%	1,12	0,25	0,00	-0,01	-0,02
40%	1,45	0,38	0,14	0,07	0,03
60%	1,90	0,56	2,10	0,21	0,08

[23] https://siis.ia.supersociedades.gov.co/#/massivereports

80%	3,34	0,72	8,29	0,37	0,16
100%	721,11	6,45	1116,24	0,87	0,64
Promedio	11,58	0,57	-455,69	-0,24	-0,03
Mediana	1,69	0,47	0,62	0,15	0,07
Desviación estándar	78,13	0,71	4427,39	3,18	0,60

Realizando un análisis integral de los datos estadísticos y los menores riesgos financieros para el presente proceso, se solicita a la entidad aplicar los siguientes indicadores a empresas 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 0,80	
RAZON COBERTURA DE INTERES	Utilidad Operacional/ Gastos de intereses	Mayor o igual 1	
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	

6. FUNDAMENTO TEÓRICO Y METODOLOGIA UTILIZADA PARA ANÁLISIS DE PRECIOS

a. Base Fundamento Teórico

Para el análisis de precios nos apoyamos en las siguientes herramientas de estadística descriptiva:

- PROMEDIO: El promedio o también media aritmética es la sumatoria de los valores de la muestra, que para este caso es la sumatoria de los precios obtenidos, sin incluir el valor del IVA

dividido por el número de observaciones o para este caso el número de precios que se cotizan por ítem. Es una aproximación a un número entre los precios que tenemos.

- DESVIACIÓN ESTÁNDAR: La desviación estándar o desviación típica, es una medida de centralización o dispersión para variables de razón y de intervalo, de gran utilidad en la estadística descriptiva. Se define como la raíz cuadrada de la varianza. Junto con este valor, la desviación típica es una medida (cuadrática) que informa la distancia que tienen los precios respecto de su media aritmética, expresada en las mismas unidades que la variable. Para conocer los precios de las diferentes cotizaciones, no basta con conocer las medidas de tendencia central, sino que necesitamos conocer la desviación de los precios respecto de la media aritmética de la misma, para tener una visión acorde con la realidad al describirlos e interpretarlos para tomar decisiones en la unidad y ver si está sobre los rangos normales.
- COEFICIENTE DE VARIACIÓN: En estadística, cuando se desea hacer referencia a la relación entre el tamaño de la media y la variabilidad de la variable, se utiliza el coeficiente de variación. Su fórmula expresa la desviación estándar como porcentaje de la media aritmética, mostrando una mejor interpretación porcentual del grado de variabilidad que la desviación típica o estándar. Por ello es importante hacer su uso en el análisis de precios del estudio de mercado, puesto que permite dar un porcentaje de error que pueden tener los precios sobre el valor promedio y el mercado. A mayor valor del coeficiente de variación mayor heterogeneidad de los valores de la variable; y a menor valor, mayor homogeneidad en los valores de la variable.
- MARGEN DE CONFIABILIDAD: El nivel de confianza se indica por 1-α y habitualmente se da en porcentaje (1-α) %. Ya que, una vez extraídas las demás ayudas estadísticas, nos permite saber qué tan confiable son los precios de mercado y qué margen de error pueden tener. Los valores que se suelen utilizar para el nivel de confianza son el 95%, 99% y 99,9%. Pero para fines de calidad del estudio se utiliza mayor al 70%.

b. Metodología utilizada para el análisis de precios

Uno de los elementos dentro de la gestión de estudios de sector, es el análisis de los precios de referencia que se logren para el propósito del estudio, estos precios de referencia son:

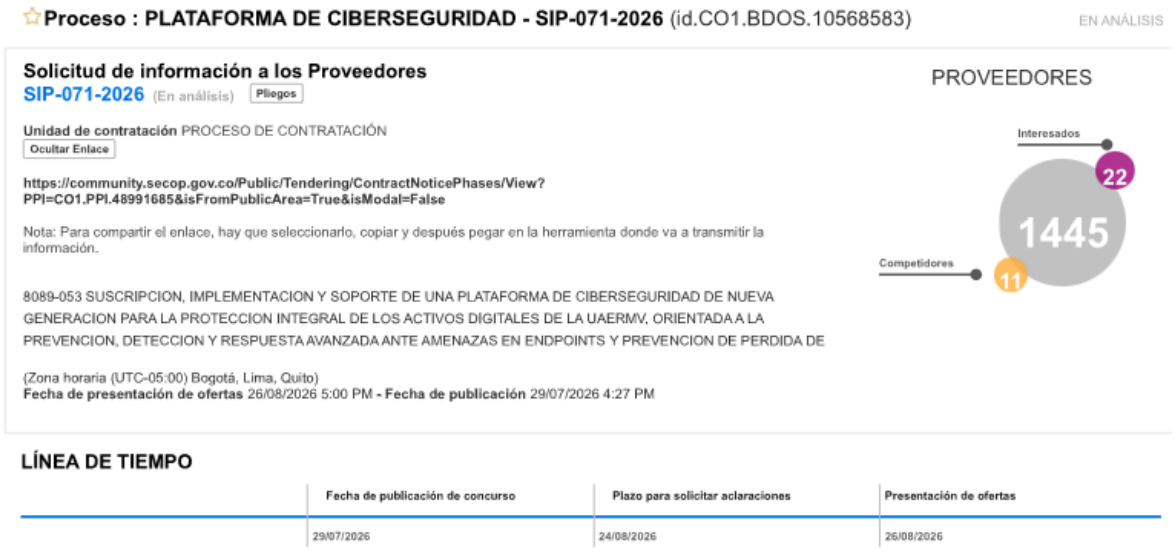
- Los obtenidos mediante cotizaciones.
  Los precios históricos de los mismos bienes y/o servicios que haya demandado la entidad, generalmente de las últimas vigencias, cabe resaltar que para el presente análisis, se utilizaron procesos que incluyen ítems con características técnicas equivalentes o similares, validadas por un profesional técnico de la Gerencia de Contratación, garantizando la idoneidad y pertinencia de los elementos evaluados.

Estos precios son sometidos a:

- A un procesamiento de datos y a análisis mediante herramientas de estadística descriptiva, tales como la media aritmética, la desviación estándar, el coeficiente de variación y el nivel de confianza. Estas herramientas, nos permiten determinar si hay un nivel de confiabilidad adecuado entre los precios de referencia logrados, lo cual se determina por el nivel de dispersión de estos con respecto al promedio; entre menor sea el nivel de dispersión, mayor confiabilidad hay en la muestra.
- Por lo tanto y finalmente para depurar la base de precios trabajada, se descartan los precios de referencia logrados que se encuentran por fuera de la tendencia de la mayoría de los otros precios, por afectar el nivel de dispersión y por lo tanto impactar el nivel de confiabilidad de los datos; una vez descartados se toma el promedio final obtenido.

Para la construcción del Presupuesto final se incluyen las diferentes columnas con los valores discriminados de los ítems que intervienen para configurar el presupuesto final y el plazo de ejecución del contrato. Por tal razón, se abrió proceso de cotización, inicialmente, en la plataforma del SECOP II el día 29 de julio de 2026, con cierre previsto el 3 de agosto de 2026, se reabrió el 21 de agosto de 2026 para entregar las respuestas a las observaciones allegadas por los interesados (están son anexas al presente documentos: Observaciones SIP 071 2026) y dar a conocer el nuevo formato de cotización así como las condiciones técnicas, entregándose un nuevo plazo de subsanación o entrega de nuevas cotizaciones el día 26 de agosto de 2026.

Se trata del SIP-071-2026 (Anexo 2a. SIP 071 2026 y 2b. SIP 071 2026 Mod. 21Ago26), cuyo objeto fueron el mismo: “8089-053 SUSCRIPCIÓN, IMPLEMENTACIÓN Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACIÓN PARA LA 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.” y a través de este obtener un valor referente del mercado:



En esta se identificaron 1445 posibles proveedores registrados en SECOP II de acuerdo con los códigos UNSPSC definidos en el Plan Anual de Adquisiciones (PAA 2026), de los cuales ONCE (11) proponentes manifestaron interés y remitieron cotización en el plazo inicial, pero solo 4 proponentes allegaron cotizaciones nuevas tras el ajuste hecho por las observaciones allegadas: ALPHA TECNOLOGÍA SAS, SPECTRUM TECHNOLOGY S.A.S., HEIMCORE SAS y BIM LATINOAMÉRICA SAS.

No se gestionaron cotizaciones por correo electrónico y tampoco se tuvieron en cuenta compras de la entidad en otras vigencias porque el servicio es nuevo dentro de ella.

De acuerdo con las cotizaciones obtenidas se determinó la desviación estándar, se estableció el coeficiente de variación de las cotizaciones, se eliminaron valores máximos y mínimos que estuvieran por fuera del rango e igualmente se estableció un margen de confiabilidad de los datos por encima del 70%.

Lo anterior, se evidencia en Anexo GCON-FM-029 Cuadro de Tabulación de Precios, con base en el análisis de dispersión y el nivel de confiabilidad de los datos se determinó que el valor del Presupuesto Oficial Estimado (POE) para el presente proceso 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%).

Los precios unitarios máximos para pagar son:

	PRECIOS MÁXIMOS A PAGAR 8089-053 SUSCRIPCION, IMPLEMENTACION Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACION PARA LA PROTECCION INTEGRAL DE LOS ACTIVOS DIGITALES DE LA UAERMV, ORIENTADA A LA PREVENCION, DETECCION Y RESPUESTA AVANZADA ANTE AMENAZAS EN ENDPOINTS PREVENCION DE PERDIDAS DE DATOS						
ÍTEM	**DESCRIPCIÓN**	**UND**	**Cant.**	**VALOR UNITARIO MÁXIMO A PAGAR ANTES DE IVA**	**IVA APLICABLE**	**VALOR UNITARIO MÁXIMO A PAGAR CON IVA**	**VALOR UNITARIO TOTAL A PAGAR CON IVA**
1	Solución EDR Avanzada	Endpoints	450	$ 441.285	$ -	$ 441.285	$198.578.250,00
2	Solución DLP Avanzada	Endpoints	450	$ 468.192	$ -	$ 468.192	$210.686.400,00
3	Servicios de instalación, configuración, pruebas, puesta en marcha, estabilización y soporte	Servicio	1	$ 96.124.200	$ 18.263.598	$ 114.387.798	$114.387.798,00
						PRESUPUESTO OFICIAL ESTIMADO	$523.652.448,00
						SMMLV 2026	$299,08
						UVT 2026	$9.998,33

7. CONCLUSIONES Y/O RECOMENDACIONES

a. Recomendaciones para requisitos de tipo financiero

Modalidad de Selección.

Por tratarse la contratación de bienes/servicios de características técnicas uniformes y de común utilización con especificaciones técnicas y patrones de desempeño y calidad iguales o similares que pueden ser ofertados por los proponentes en igualdad de condiciones, la UAERMV hará uso de la modalidad de Selección Abreviada prevista en el literal a) del numeral 2o. del artículo. 2 de la Ley 1150 de 2007, la cual describe 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.*
>
> *Para la adquisición de estos bienes y servicios las entidades deberán, siempre que el reglamento así lo señale, hacer uso de procedimientos de subasta inversa o de instrumentos de compra por catálogo derivados de la celebración de acuerdos marco de precios o de procedimientos de adquisición en bolsas de productos".*

Al respecto, el presente estudio del sector evaluó y determinó que se deberá escoger la SUBASTA INVERSA.

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%).

Los precios máximos a pagar por cada uno de los ítems descritos en la necesidad son:

	PRECIOS MÁXIMOS A PAGAR 8089-053 SUSCRIPCION, IMPLEMENTACION Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACION PARA LA PROTECCION INTEGRAL DE LOS ACTIVOS DIGITALES DE LA UAERMV, ORIENTADA A LA PREVENCION, DETECCION Y RESPUESTA AVANZADA ANTE AMENAZAS EN ENDPOINTS PREVENCION DE PERDIDAS DE DATOS						
ÍTEM	**DESCRIPCIÓN**	**UND**	**Cant.**	**VALOR UNITARIO MÁXIMO A PAGAR ANTES DE IVA**	**IVA APLICABLE**	**VALOR UNITARIO MÁXIMO A PAGAR CON IVA**	**VALOR UNITARIO TOTAL A PAGAR CON IVA**

1	Solución EDR Avanzada	Endpoints	450	$ 441.285	$ -	$ 441.285	$198.578.250,00
2	Solución DLP Avanzada	Endpoints	450	$ 468.192	$ -	$ 468.192	$210.686.400,00
3	Servicios de instalación, configuración, pruebas, puesta en marcha, estabilización y soporte	Servicio	1	$ 96.124.200	$ 18.263.598	$ 114.387.798	$114.387.798,00
						PRESUPUESTO OFICIAL ESTIMADO	$523.652.448,00
						SMMLV 2026	$299,08
						UVT 2026	$9.998,33

b. Recomendaciones para requisitos de tipo técnico

Dar cumplimiento a los requisitos técnicos se describen detalladamente en el 1. GCON FM 022 Formulación Estudio del Sector y Condiciones Técnicas de la Necesidad.

8. FUENTES DE INFORMACIÓN

a. Fuentes de Información Primaria

Las fuentes de información primarias corresponden a la investigación de campo que se desarrolle mediante cotizaciones, entrevistas y encuestas. Para el caso particular de este estudio, no se realizó visita a alguna empresa de la muestra, pero se obtuvieron cotizaciones de posibles proveedores por medios electrónicos

b. Fuentes de Información Secundaria

Las fuentes de información secundaria corresponden a toda la información escrita existente. Para el presente estudio, se han tenido en cuenta las siguientes fuentes:

- https://www.secop.gov.co
- https://www.dane.gov.co
- https://www.banrep.gov.co
- Ficha Técnica - Requerimientos y especificaciones mínimas
- GCON-FM-022 - Formato de formulación de estudio del sector

9. ANEXOS

1. GCON FM 022 Formulación Estudio del Sector y Condiciones Técnicas de la Necesidad

2a. SIP 071 2026
2b. SIP 071 2026 Mod. 21Ago26
3a. Cotización Ciberseguridad Spectrum 26Ago26
3b. Cotizacion Ciberseguridad V21Ago26 Alphatech
3c. Cotizacion Ciberseguridad V21Ago26 Heimcore
3d. Cotizacion Ciberseguridad V21Ago26_BIMLATINOAMERICA
4. GCON FM 029 Tabulación v27Ago26
6. Cálculo Costos BMC

Documento 20261140350593 firmado electrónicamente por:	
DANIELA ALEJANDRA AVILA MONTENEGRO	Contratista OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN daniela.montenegro@umv.gov.co Fecha firma: 18-11-2026 14:42:38
ANGEL LEONARDO JEREZ CARVAJAL	Contratista GERENCIA DE CONTRATACIÓN angel.jerez@umv.gov.co Fecha firma: 18-11-2026 15:06:33
NELSON EFRAIN MEDINA PINZON	Contratista GERENCIA DE CONTRATACIÓN nelson.medina@umv.gov.co Fecha firma: 18-11-2026 15:07:43
Revisó:	CARLOS ABEL BASTIDAS CUBILLOS - Contratista – Líder de Infraestructura y Servicios - OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - carlos.bastidas@umv.gov.co
	MARINO MIGUEL MORENO RHENALS - Contratista - OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - marino.moreno@umv.gov.co
Proyectó:	BERNARDO ALFONSO DUQUE FORERO - Contratista - OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - bernardo.duque@umv.gov.co

54d1f7da98042c1bdea99bd0e54d7384153227a4b9ac99f9a3d99c01db93ac5a
Codigo de Verificación CV: 10692 Comprobar desde: https://www.umv.gov.co/portal/verificar/