

1. NECESIDAD

La Agencia Nacional de Defensa Jurídica del Estado (en adelante, "Agencia") es una Unidad Administrativa Especial descentralizada del orden nacional, con personería jurídica, autonomía administrativa y financiera, y patrimonio propio, adscrita al Ministerio de Justicia y del Derecho, creada mediante el parágrafo del artículo 5 de la Ley 1444 de 2011.

A través del Decreto Ley 4085 de 2011, modificado parcialmente por los Decretos 915 de 2017, 1698 y 2269 de 2019, y 1244 de 2021, el Gobierno Nacional estableció los objetivos y la estructura de la Agencia Nacional de Defensa Jurídica del Estado.

En el artículo 2 Decreto Ley 4085 de 2011 se establece como objetivo de la Agencia *"El diseño de estrategias, planes y acciones dirigidos a dar cumplimiento a las políticas de defensa jurídica de la Nación y del Estado definidas por el Gobierno Nacional; la formulación, evaluación y difusión de las políticas en materia de prevención de las conductas antijurídicas por parte de servidores y entidades públicas, del daño antijurídico y la extensión de sus efectos, y la dirección, coordinación y ejecución de las acciones que aseguren la adecuada implementación de las mismas, para la defensa de los intereses litigiosos de la Nación."*

Mediante el numeral 2.4 del artículo 2 del Decreto 1244 de 2021, "Por el cual se modifican parcialmente las funciones y la estructura de la Unidad Administrativa Especial Agencia Nacional de Defensa Jurídica del Estado", se creó la Oficina Asesora de Sistemas de Tecnologías de la Información (OASTI). En consecuencia, a través del artículo 3 del mismo decreto se adicionó el artículo 15A al Decreto 4085 de 2011, estableciendo, entre otras, las siguientes funciones asignadas a dicha Oficina en materia de gestión y soporte tecnológico institucional:

"4. Administrar y realizar los procesos de soporte informático y tecnológico que la gestión de la Agencia Nacional de Defensa Jurídica del Estado requiera".

"7. Realizar las gestiones necesarias para garantizar la operación y sostenibilidad de los sistemas de información de la Agencia Nacional de Defensa Jurídica del Estado".

"8. Coordinar el desarrollo, uso e implementación de los sistemas y tecnologías de Información y comunicaciones que requiera la Agencia Nacional de Defensa Jurídica del Estado."

"10. Definir lineamientos tecnológicos y velar por su implementación, para el cumplimiento de estándares y buenas prácticas de seguridad y privacidad de la información y en especial la interoperabilidad de los sistemas que la soportan."

"13. Diseñar los protocolos de seguridad de la información para la Agencia Nacional de Defensa Jurídica del Estado."

"14. Administrar la infraestructura de seguridad para la protección de la información y datos magnéticos y físicos, en la Agencia Nacional de Defensa Jurídica del Estado."

"16. Proponer al Director General de la Agencia Nacional de Defensa Jurídica del Estado las políticas para garantizar la calidad de los datos, y el manejo adecuado de los sistemas de información y el aseguramiento de la información."

En el marco de las funciones referidas, la OASTI requiere llevar a cabo la renovación del licenciamiento de soporte y garantía de los equipos de seguridad perimetral para la Agencia, teniendo en cuenta que:

- Mediante el contrato No 085-2022, la Entidad adquirió la renovación del licenciamiento de dos (2) equipos de seguridad perimetral marca Fortinet modelo FortiGate 200E con soporte y garantía de tres (3) años, el cual finalizó el 24 de agosto de 2025.
- Mediante contrato BID OC 051-2022, la Entidad adquirió (3) equipos de seguridad perimetral marca Fortinet modelos FortiGate 200E y FortiWeb 400E con soporte y garantía de 3 años, los cuales tuvieron soporte y garantía hasta el 4 y 7 de diciembre de 2025 respectivamente.
- Mediante contrato 158-2023, la Entidad adquirió el licenciamiento en renovación, soporte y garantía de la plataforma FortiSIEM con soporte y garantía de 3 años, los cuales tienen soporte y garantía hasta el 17 de diciembre de 2026 respectivamente.
- En el año 2025, mediante contrato 190-2025, la Entidad adquirió la renovación de infraestructura, soporte y garantía de licenciamiento de equipos de seguridad perimetral hasta el 17 de diciembre de 2026.

Estos equipos y plataforma desempeñan un rol esencial en la protección de la red institucional, el resguardo de los servicios digitales y la salvaguarda de la información sensible, todos ellos activos críticos para la continuidad operativa y el cumplimiento de las funciones misionales de la Agencia.

Los equipos FortiGate son dispositivos que protegen la red de la Agencia contra accesos no autorizados, ataques informáticos y programas maliciosos. Actúan como una barrera que revisa toda la información que entra y sale, permitiendo solo lo que es seguro y bloqueando lo que representa un riesgo. Además, permiten

establecer conexiones seguras para el trabajo remoto y ayudan a garantizar que el uso de internet y las aplicaciones institucionales sea controlado y confiable.

Por su parte, el equipo FortiWeb está diseñado específicamente para proteger las páginas web y aplicaciones en línea de la Agencia. Este equipo evita que personas malintencionadas puedan aprovechar errores o debilidades en los sitios web para robar información, alterar contenidos o afectar su funcionamiento. Gracias a este sistema, se brinda mayor seguridad a los servicios que los ciudadanos y funcionarios utilizan desde internet, como formularios, plataformas o portales institucionales.

Así mismo, la plataforma FortiSIEM está diseñada para monitorear de manera centralizada los eventos de seguridad generados por los diferentes sistemas tecnológicos de la Agencia. Este equipo permite identificar oportunamente comportamientos inusuales, posibles incidentes de seguridad y fallas en la infraestructura tecnológica, facilitando su análisis y atención antes de que afecten la operación. Gracias a este sistema, se fortalece la capacidad de vigilancia, respuesta y gestión de la seguridad de la información, contribuyendo a la continuidad y protección de los servicios tecnológicos de la Entidad.

La necesidad de renovar el soporte y la garantía de estos equipos se fundamenta en garantizar el acceso continuo a actualizaciones de software, firmware y parches de seguridad desarrollados por el fabricante, sin costos adicionales, permitiendo que los dispositivos se mantengan protegidos frente a nuevas amenazas y vulnerabilidades. Además, contar con soporte vigente nos brinda acceso a asistencia técnica especializada y garantía de fabricante, aspectos fundamentales para atender fallas operativas o incidentes críticos sin afectar la continuidad de los servicios tecnológicos.

Considerando la utilidad y funcionalidad de estas soluciones, y que su período de soporte y garantía está próximo a vencer, se requiere realizar la renovación del licenciamiento y el fortalecimiento de la infraestructura de seguridad Fortinet con la que ya se cuenta, para asegurar que la Agencia mantenga la protección activa de sus sistemas, se garantice la operación de los componentes tecnológicos de la seguridad perimetral, opere de forma segura en entornos híbridos y cumpla con los más altos estándares de seguridad informática.

Por lo tanto, se requiere la renovación del licenciamiento y soporte de los equipos de seguridad perimetral FortiGate-200E (dos equipos), FortiGate-100E (dos equipos), FortiWeb-400E (un equipo) y la plataforma FortiSIEM, los cuales se encuentran instalados en los centros de datos institucionales y cumplen un papel

esencial en la protección de los sistemas de información.

La información contenida en los sistemas misionales y de soporte constituye un activo crítico para el cumplimiento de los fines institucionales, por lo que se hace necesario mantener soluciones robustas de seguridad informática. La renovación objeto de este proceso permite fortalecer y mantener el sistema de ciberseguridad institucional, identificar, detectar, prevenir y gestionar ataques a los servicios expuestos y mejorar la infraestructura de red, mediante funcionalidades como filtrado web, prevención de intrusos (IPS), filtrado de aplicaciones y análisis de tráfico, entre otros.

Actualmente, no se encuentra disponible un Instrumento de Agregación de Demanda (IAD) ni un Acuerdo Marco de Precios vigente en la Tienda Virtual del Estado Colombiano.

Bajo este marco y dado que los bienes requeridos presentan características técnicas objetivas, uniformes y de común utilización en el mercado, se considera que la presente contratación cumple con las condiciones previstas en el inciso 2º del literal a) del numeral 2 del artículo 2º de la Ley 1150 de 2007, razón por la cual y no siendo posible la adquisición a través de un instrumento de agregación de demanda o acuerdo marco de precios, se adelantará el proceso bajo la modalidad de Selección Abreviada mediante Subasta Inversa Electrónica de acuerdo con el procedimiento establecido en el artículo 2.2.1.2.1.2.2 y siguientes del Decreto 1082 de 2025.

La presente contratación se encuentra incluida en el ítem 16 del Plan Anual de Adquisiciones para el año 2026.

2. OBJETO

Renovación de infraestructura, soporte y garantía de licenciamiento de equipos de seguridad perimetral.

3. CLASIFICACIÓN UNSPSC

CLASIFICADOR	SEGMENTO	FAMILIA	CLASES	PRODUCTO
Código UNSPSC 81112208 Mantenimiento y soporte de software	[81] Servicios Basados en Ingeniería, Investigación y Tecnología	[11] Servicios informáticos	[22] Mantenimiento y soporte de software	[08] Mantenimiento de software de protección y seguridad

CLASIFICADOR	SEGMENTO	FAMILIA	CLASES	PRODUCTO
Código UNSPSC 43222501 Equipo de seguridad de red cortafuegos (firewall)	[43] Difusión de tecnologías de la información y las comunicaciones	[22] Equipos o plataformas y accesorios de redes multimedia o de voz y de datos	[25] Equipo de seguridad de red	[01] Equipo de seguridad de red cortafuegos (firewall)
Código UNSPSC 43233205 Software de seguridad de transacciones y de protección contra virus	[43] Difusión de tecnologías de la información y las comunicaciones	[23] Software	[32] Software de seguridad y control de acceso	[05] Software de seguridad de transacciones y de protección contra virus

4. ASPECTOS GENERALES¹

El sector de Tecnologías de la Información y las Comunicaciones (TIC) en Colombia constituye uno de los pilares estratégicos para el desarrollo económico, la innovación y la transformación digital de las entidades públicas y privadas. En los últimos años, el país ha avanzado significativamente en la adopción de tecnologías digitales, impulsando una creciente demanda de servicios de infraestructura tecnológica, virtualización, almacenamiento, ciberseguridad y servicios en la nube.

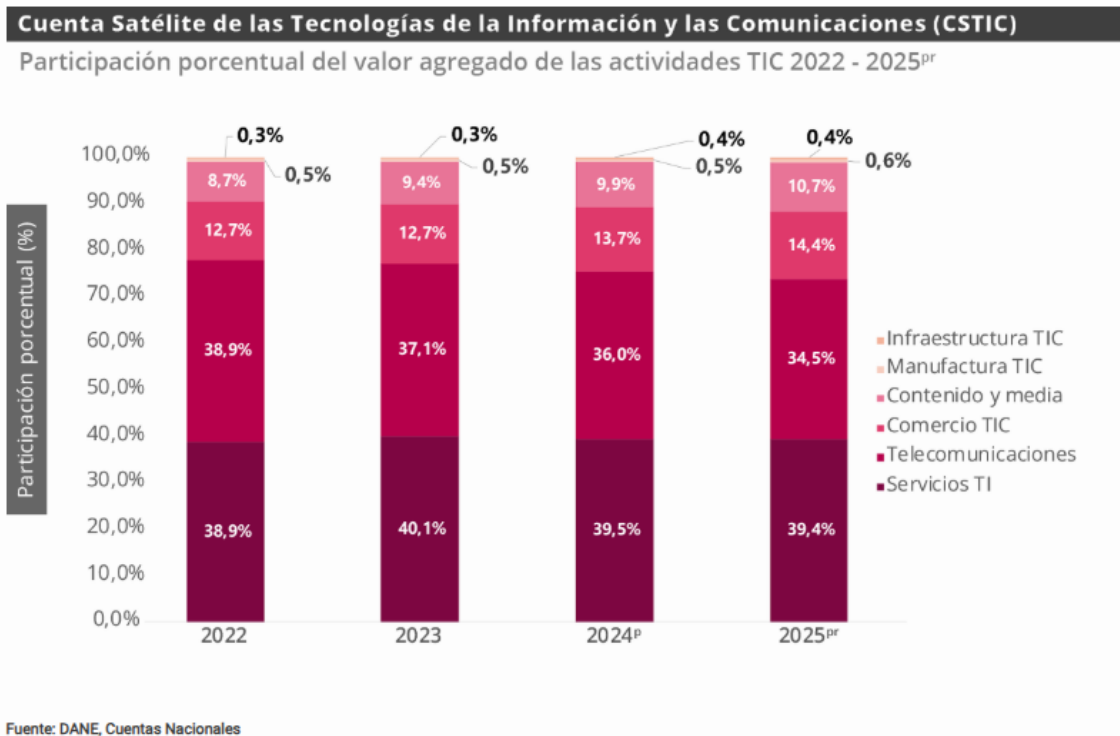
Esta evolución ha sido promovida tanto por políticas públicas del Gobierno Nacional, como la Estrategia de Gobierno Digital y los lineamientos de transformación digital del Estado, como por las necesidades de modernización tecnológica, continuidad operativa, interoperabilidad y fortalecimiento de la seguridad de la información en las organizaciones públicas y privadas.

De acuerdo con información publicada por el Departamento Administrativo Nacional de Estadística (DANE)², el valor agregado bruto del sector TIC en Colombia alcanzó aproximadamente \$55,1 billones en 2024, registrando un crecimiento de 5,3% frente al año 2023 y una participación cercana al 3,55% del valor agregado nacional. Estos resultados evidencian la relevancia económica del sector y su crecimiento sostenido dentro de la estructura productiva del país.

¹ www.colombiacompra.gov.co/sites/cce_public/files/cce_documents/cce_guia_elaboracion_estudios.pdf

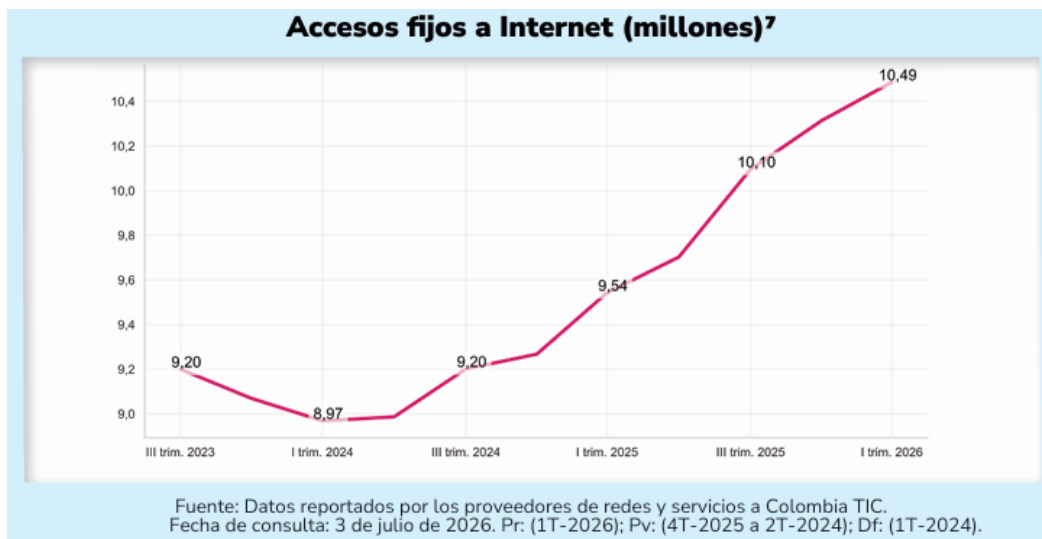
² <https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-satelite/cuenta-satelite-de-las-tecnologias-de-la-informacion-y-las-comunicaciones-cstic>

El sector comprende un amplio conjunto de actividades relacionadas con las tecnologías de información, las comunicaciones, el desarrollo y soporte de sistemas informáticos, la administración de infraestructura tecnológica, el procesamiento de información, el suministro de equipos y soluciones tecnológicas, entre otras. En este sentido, la clasificación CIIU Rev. 4 A.C. del DANE contempla, entre otras, las actividades de consultoría informática y administración de instalaciones informáticas (CIIU 6202), dentro de las cuales se incluyen servicios asociados con la integración de sistemas, soporte tecnológico y seguridad informática. Asimismo, contempla actividades relacionadas con el comercio mayorista de computadores, equipos periféricos y programas informáticos (CIIU 4651), así como el comercio mayorista de equipos, partes y componentes electrónicos y de telecomunicaciones (CIIU 4652).



De manera complementaria, el DANE reconoce dentro de la Clasificación Central de Productos los servicios de consultoría en tecnologías de la información, incluyendo expresamente la seguridad informática, así como los servicios de soporte en tecnologías de la información, que comprenden actividades como actualización y suministro de parches informáticos y soporte técnico de soluciones de hardware y software. Igualmente, se identifican servicios de administración de redes que incluyen actividades de monitoreo, diagnóstico y asistencia a los sistemas de seguridad.

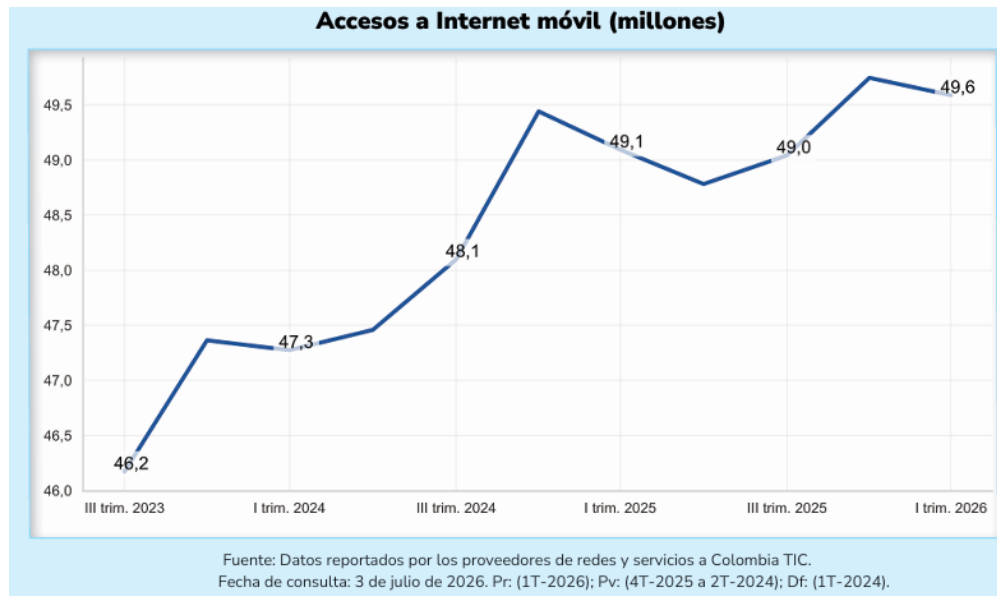
En cuanto a los servicios de telecomunicaciones, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), con base en los reportes periódicos presentados por los Proveedores de Redes y Servicios de Telecomunicaciones (PRST), informó que al término del primer trimestre de 2026 el total de accesos fijos a internet en Colombia alcanzó los 10,49 millones. Esta cifra representa un incremento aproximado de 950 mil de accesos frente al mismo periodo del año inmediatamente anterior, cuando se registraron 9,54 millones de accesos³.



Además, se evidenció un incremento en la demanda de servicios móviles y en la adopción de tecnologías emergentes como la computación en la nube, la inteligencia artificial y el análisis de grandes volúmenes de datos (big data), lo que ha impulsado una mayor inversión en infraestructura tecnológica para el almacenamiento, procesamiento y gestión de la información.

En este contexto, el total de accesos a internet móvil alcanzó los 49,6 millones al cierre del mismo periodo, cifra que representa cerca de 500 mil accesos adicionales frente a los registrados en el mismo trimestre del año inmediatamente anterior.

³ https://ontic.mintic.gov.co/857/articles-440020_boletin.pdf



Estos factores han generado un entorno favorable para el crecimiento del mercado de infraestructura tecnológica, impulsado por la creciente demanda de servicios digitales y de soluciones que garanticen disponibilidad, seguridad, eficiencia energética, continuidad operativa y cumplimiento normativo. Esta transformación digital, a su vez, incrementa los requerimientos de protección de las redes, sistemas de información, aplicaciones, infraestructura tecnológica y datos. En este contexto, la seguridad digital constituye un componente transversal de la modernización tecnológica y un elemento esencial para fortalecer la confianza en los servicios digitales y proteger los activos de información de las organizaciones.

Organismos internacionales como la Comisión Económica para América Latina y el Caribe han señalado que la transformación digital y la adopción de tecnologías emergentes representan una oportunidad estratégica para impulsar la productividad, la competitividad y el cierre de brechas económicas y sociales en América Latina y el Caribe. En este contexto, Colombia ha venido fortaleciendo su ecosistema TIC mediante la ejecución de políticas de transformación digital, el impulso a la conectividad, la modernización de los marcos regulatorios y el incremento de inversiones públicas y privadas orientadas al fortalecimiento de infraestructura tecnológica, servicios en la nube, gestión segura de la información y la prestación confiable de los servicios digitales.

En este sentido, el Ministerio TIC actualizó en 2025 el Modelo de Seguridad y Privacidad de la Información – MSPI mediante la Resolución 02277 de 2025, alineándolo con la norma ISO/IEC 27001:2022 y fortaleciendo los lineamientos

aplicables a las entidades públicas para la protección de sus activos de información y la continuidad de los servicios esenciales.

La necesidad de fortalecer las capacidades de seguridad digital también responde a la evolución del riesgo cibernético. De acuerdo con el Ministerio TIC, durante 2024 Colombia registró aproximadamente 36.000 millones de intentos de afectación, mientras que el Informe de Tendencias de Amenazas Cibernéticas 2025 del ColCERT⁴ reportó 697 incidentes de seguridad digital gestionados durante 2025. Aunque esta última cifra representó una disminución frente a 2024, el Ministerio advierte sobre la mayor sofisticación de las amenazas, incluyendo el incremento de amenazas persistentes avanzadas (APT) y el uso de inteligencia artificial para la ejecución de ataques.

Clase de Incidente	Incidentes 2024	Incidentes 2025	Total	% del Total
Fraude	1,222	475	1,697	87.29%
Intrusión	91	89	180	9.26%
Vulnerable	69	45	114	5.86%
Compromiso de Información	17	59	76	4.42%
Contenido Dañino	14	26	40	2.06%
Disponibilidad	3	3	6	0.31%
Contenido Abusivo	5	0	5	0.26%
Intento de Intrusión	4	0	4	0.21%
Obtención de Información	1	0	1	0.05%

En este escenario, la protección de la infraestructura de red adquiere especial importancia, dado que las organizaciones requieren mecanismos que permitan prevenir, detectar, analizar y mitigar accesos no autorizados, tráfico malicioso, explotación de vulnerabilidades y otras amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de la información y de los servicios tecnológicos.

En el Informe Balance 2025 y Perspectivas 2026⁵, elaborado por la Asociación Nacional de Empresarios de Colombia - ANDI, se destaca que la economía colombiana continúa enfrentando un entorno caracterizado por alta incertidumbre, presiones fiscales, bajo dinamismo de la inversión y desafíos estructurales en

⁴ https://www.colcert.gov.co/800/articles-433510_recurso_1.pdf

⁵ https://www.andi.com.co/Uploads/Balance%202025%20y%20Perspectivas%202026%20_639056474172585923.pdf

materia de competitividad y productividad. No obstante, el informe señala que Colombia mantiene condiciones estratégicas que le permiten conservar su potencial como destino de inversión y como uno de los mercados más relevantes de América Latina para el desarrollo empresarial y tecnológico.

La ANDI advierte que, aunque durante 2025 la economía presentó una recuperación moderada con crecimientos cercanos al 3%, este comportamiento continúa siendo insuficiente frente a las necesidades de generación de empleo, fortalecimiento productivo y crecimiento sostenible del país. Asimismo, el gremio resalta que gran parte del crecimiento reciente ha estado impulsado por el consumo y el gasto público, mientras que la inversión privada continúa mostrando señales de desaceleración debido a factores asociados con incertidumbre regulatoria, sostenibilidad fiscal y estabilidad institucional.

En este escenario, la transformación digital y la seguridad de la información adquieren especial relevancia para la sostenibilidad y competitividad empresarial. La ANDI ha reconocido la ciberseguridad como un elemento necesario para incorporar las tecnologías digitales de manera estratégica y sostenible, junto con factores como la cultura organizacional, la tecnología, el liderazgo, el talento y la regulación. Asimismo, ha resaltado la necesidad de fortalecer la gestión del riesgo cibernético, la capacidad de respuesta ante incidentes y la disponibilidad de talento especializado, aspectos que incrementan la necesidad de contar con infraestructura tecnológica segura y mecanismos adecuados para proteger las redes, sistemas de información y activos digitales de las organizaciones.

En consecuencia, el sector objeto de análisis presenta una oferta conformada no solamente por fabricantes y comercializadores de equipos tecnológicos, sino también por proveedores especializados en licenciamiento, soporte, mantenimiento, actualización, consultoría, administración de redes, seguridad informática y servicios asociados. Esta característica resulta particularmente relevante para el presente proceso, toda vez que las necesidades de la Agencia no se limitan a la adquisición de componentes tecnológicos, sino que comprenden la renovación del licenciamiento, soporte, garantía, actualización, mantenimiento y atención especializada de las soluciones de seguridad perimetral existentes, de manera que se garantice su disponibilidad, funcionamiento y capacidad de respuesta frente a las amenazas de seguridad digital.

En este sentido, el comportamiento y evolución del sector TIC, junto con el incremento de la dependencia de las organizaciones respecto de los servicios digitales y la necesidad de gestionar los riesgos asociados al entorno cibernético,

sustentan la importancia de mantener actualizadas y soportadas las tecnologías destinadas a la protección de la infraestructura de red de la Agencia.

CONTEXTO ECONÓMICO

De acuerdo con las más recientes proyecciones de organismos multilaterales como el Banco Mundial⁶ y el Fondo Monetario Internacional⁷, la economía global mantiene una senda de recuperación moderada para el periodo 2025–2026, aunque todavía por debajo de los niveles promedio observados antes de la pandemia de COVID-19. Las estimaciones más recientes indican que el crecimiento económico mundial se ubicaría alrededor del 2,7 % en 2025 y cerca del 2,8 % en 2026, reflejando un entorno internacional marcado por desaceleración del comercio, tensiones geopolíticas, altos niveles de endeudamiento y condiciones financieras restrictivas.

En las economías avanzadas, el crecimiento continuaría siendo moderado, con tasas cercanas al 1,5 %–1,7 %, debido principalmente a la persistencia de altas tasas de interés, menores niveles de consumo y desaceleración de la inversión productiva. Por su parte, las economías emergentes y en desarrollo mantendrían perspectivas de crecimiento superiores, cercanas al 4 %, impulsadas por procesos de transformación digital, recuperación parcial del comercio internacional y expansión de sectores asociados a servicios, tecnología e infraestructura digital.

No obstante, los organismos internacionales advierten que persisten riesgos importantes asociados con la sostenibilidad fiscal, el elevado costo del servicio de la deuda, la volatilidad financiera internacional, las presiones inflacionarias y los efectos derivados de conflictos geopolíticos y fenómenos climáticos extremos. En particular, los países de ingresos bajos continúan enfrentando limitaciones estructurales relacionadas con acceso al financiamiento, inversión en infraestructura, cobertura educativa y fortalecimiento institucional, lo que podría afectar su capacidad de crecimiento sostenido en el mediano plazo.

En materia inflacionaria, se proyecta que la inflación mundial continúe moderándose gradualmente durante 2025 y 2026, ubicándose alrededor del 3 % en promedio. Sin embargo, el descenso de la inflación ha sido más lento de lo inicialmente previsto, razón por la cual varios bancos centrales han mantenido políticas monetarias restrictivas y una reducción cautelosa de las tasas de interés. En consecuencia, se estima que las tasas de interés internacionales permanecerán

⁶ <https://www.worldbank.org/en/publication/global-economic-prospects>

⁷ <https://www.imf.org/en/publications/weo>

relativamente elevadas frente a los promedios históricos observados entre 2000 y 2019, generando impactos sobre el costo del financiamiento, la inversión tecnológica y la ejecución de proyectos de modernización digital.

En este escenario económico global, el sector de Tecnologías de la Información y las Comunicaciones (TIC) continúa posicionándose como uno de los principales motores de productividad, transformación digital y modernización institucional. La creciente dependencia de infraestructura tecnológica, servicios digitales, computación en la nube, virtualización, inteligencia artificial y analítica de datos ha incrementado significativamente la necesidad de plataformas robustas, seguras y escalables que garanticen continuidad operativa y resiliencia tecnológica⁸.

Particularmente, la industria de la ciberseguridad atraviesa una etapa de expansión acelerada como consecuencia del incremento en la frecuencia, sofisticación e impacto de las amenazas cibernéticas a nivel mundial. Ataques de ransomware, phishing, fuga de información, explotación de vulnerabilidades y afectaciones a infraestructura crítica han llevado a que las organizaciones incrementen sus inversiones en soluciones avanzadas de seguridad digital, monitoreo, protección de datos y gestión de riesgos tecnológicos.

Asimismo, la consolidación de esquemas de trabajo híbrido, servicios en la nube, ambientes multicloud y procesos de transformación digital ha incrementado la necesidad de contar con infraestructuras tecnológicas altamente seguras y resilientes. Tecnologías emergentes como la inteligencia artificial, el aprendizaje automático y el análisis avanzado de datos están siendo incorporadas progresivamente en las soluciones de ciberseguridad, permitiendo fortalecer capacidades de detección temprana, respuesta automatizada y análisis predictivo de amenazas.

De acuerdo con estudios recientes de mercado, se estima que el mercado global de ciberseguridad alcanzará valores superiores a los USD 230 mil millones en 2025 y podría superar los USD 420 mil millones hacia 2030, con tasas de crecimiento anual compuestas cercanas al 12 %. Paralelamente, el impacto económico del ciberdelito continúa aumentando significativamente; diversas proyecciones internacionales estiman que los costos globales asociados a incidentes de ciberseguridad podrían superar los USD 10 billones anuales durante los próximos años, consolidando la seguridad digital como una prioridad estratégica para gobiernos, entidades públicas y organizaciones privadas⁹.

⁸ <https://www.cepal.org/es/temas/agenda-digital>

⁹ <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025>

En este contexto, las inversiones en infraestructura tecnológica, continuidad operativa, protección de redes y plataformas especializadas de seguridad adquieren una importancia estratégica para garantizar la disponibilidad, estabilidad, integridad y eficiencia de los servicios institucionales. En particular, las soluciones de seguridad perimetral se constituyen en componentes fundamentales de la infraestructura tecnológica de las organizaciones públicas y privadas, al permitir controlar y monitorear el tráfico de red, prevenir accesos no autorizados, detectar y mitigar amenazas y proteger los servicios y sistemas expuestos a redes externas. Su adecuada operación, actualización y mantenimiento resultan esenciales para fortalecer la capacidad de las organizaciones frente a un entorno de amenazas cibernéticas en constante evolución.

Región de América Latina y el Caribe

El mercado de seguridad informática y protección de infraestructura de red en América Latina y el Caribe viene experimentando una evolución acelerada, impulsada por los procesos de transformación digital, el crecimiento de los servicios en línea, la expansión de las infraestructuras de conectividad y la adopción de arquitecturas híbridas y multicloud. Tanto las entidades públicas como las organizaciones privadas han incrementado progresivamente sus inversiones en soluciones orientadas a prevenir, detectar, analizar y responder ante amenazas que puedan comprometer la disponibilidad, integridad y confidencialidad de sus sistemas y servicios tecnológicos.

La creciente dependencia de las organizaciones respecto de las redes y plataformas digitales ha generado una mayor necesidad de fortalecer los mecanismos de protección de la infraestructura tecnológica. En particular, las soluciones de seguridad perimetral han adquirido un papel estratégico al permitir controlar y monitorear el tráfico de red, gestionar accesos, prevenir intrusiones, detectar actividades maliciosas y proteger los servicios expuestos a Internet. Estas capacidades resultan especialmente relevantes en sectores como gobierno, servicios financieros, telecomunicaciones, salud, comercio electrónico y otras actividades que gestionan información y servicios de carácter crítico.

La expansión de los servicios en la nube, el trabajo remoto, la interconexión de múltiples plataformas y el uso creciente de aplicaciones y servicios digitales han transformado el concepto tradicional de perímetro de red. En consecuencia, las organizaciones requieren soluciones capaces de proporcionar protección tanto para sus redes locales como para ambientes distribuidos, híbridos y multicloud, incorporando mecanismos de inspección avanzada del tráfico, control de

aplicaciones, protección de servicios web, gestión de vulnerabilidades, monitoreo de eventos y respuesta ante incidentes de seguridad.

De manera paralela, el crecimiento y sofisticación de las amenazas cibernéticas ha incrementado la demanda de tecnologías especializadas de protección. Las organizaciones enfrentan riesgos asociados, entre otros, con malware, ransomware, explotación de vulnerabilidades, ataques de denegación de servicio, accesos no autorizados, amenazas persistentes avanzadas y compromisos de aplicaciones y servicios expuestos a Internet. Este escenario ha impulsado la evolución de las soluciones de seguridad perimetral hacia plataformas integradas que combinan capacidades de firewall de nueva generación (NGFW), protección de aplicaciones web (WAF), prevención y detección de intrusiones, filtrado de contenidos, inteligencia de amenazas, análisis de eventos y gestión centralizada de la seguridad.

Asimismo, las estrategias modernas de ciberseguridad requieren una capacidad permanente de monitoreo, correlación y análisis de eventos provenientes de diferentes componentes de la infraestructura tecnológica. En este contexto, las plataformas de gestión de información y eventos de seguridad (SIEM) han adquirido relevancia como herramientas para centralizar registros, identificar comportamientos anómalos, correlacionar eventos y facilitar la detección y atención oportuna de incidentes. La integración de estas capacidades con las soluciones de seguridad perimetral permite fortalecer la visibilidad sobre el estado de la infraestructura y mejorar la capacidad de respuesta de las organizaciones frente a eventos de seguridad.

La evolución del mercado también ha generado una mayor demanda de servicios asociados al ciclo de vida de las soluciones de seguridad, incluyendo licenciamiento, actualizaciones de software y firmware, bases de datos de amenazas, soporte técnico especializado, mantenimiento, garantía, atención de incidentes y acompañamiento en la implementación de buenas prácticas. En consecuencia, la adquisición de tecnologías de seguridad perimetral no se limita a la obtención de un componente de hardware o software, sino que requiere esquemas integrales que permitan mantener las capacidades de protección actualizadas durante toda la vida útil de la solución.

En materia de talento especializado, la creciente complejidad de las amenazas y de las arquitecturas tecnológicas ha incrementado la necesidad de contar con profesionales capacitados en seguridad informática, administración de redes, gestión de incidentes y operación de plataformas especializadas. La disponibilidad

de personal con conocimientos y certificaciones otorgadas por los fabricantes constituye un factor relevante para garantizar una adecuada implementación, configuración, actualización, mantenimiento y atención de incidentes asociados a las tecnologías de seguridad.

De igual manera, los fabricantes de soluciones de ciberseguridad han fortalecido sus modelos de atención y soporte mediante esquemas que combinan asistencia especializada, actualización permanente de las plataformas, acceso a bases de datos de amenazas, gestión de vulnerabilidades y escalamiento de incidentes hacia niveles avanzados de soporte. Estos mecanismos permiten que las organizaciones mantengan sus tecnologías alineadas con la evolución de las amenazas y accedan oportunamente a correcciones, parches de seguridad y mejoras funcionales.

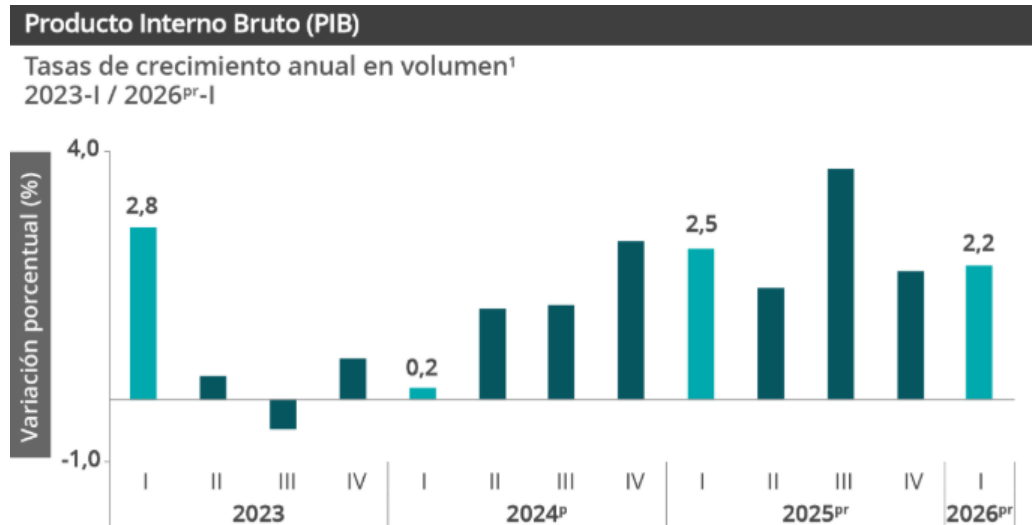
En este contexto, las organizaciones públicas y privadas requieren mantener actualizadas sus plataformas de seguridad perimetral y garantizar su adecuada operación, particularmente aquellas que soportan servicios institucionales, sistemas de información y aplicaciones accesibles desde Internet. La continuidad del licenciamiento y de los servicios de soporte y garantía permite preservar las capacidades de protección existentes, reducir la exposición frente a vulnerabilidades conocidas y garantizar el acceso a las actualizaciones y mecanismos de seguridad desarrollados por los fabricantes.

En consecuencia, el mercado de seguridad perimetral se caracteriza actualmente por una oferta de soluciones integrales que combina componentes tecnológicos, licenciamiento, soporte especializado, mantenimiento, actualización continua, inteligencia de amenazas y servicios asociados a la gestión del ciclo de vida de las plataformas. Esta dinámica evidencia la importancia de contar con esquemas de renovación que permitan garantizar la disponibilidad, estabilidad, seguridad y capacidad de respuesta de las infraestructuras tecnológicas frente a un entorno de amenazas cibernéticas en constante evolución.

4.1.1 Aspectos Económicos Generales

La tecnología en Colombia ha venido creciendo en los últimos años, tanto así que actualmente este sector ocupa una parte importante en el producto interno bruto (PIB) y en el mercado laboral del país.

En el primer trimestre de 2026, el Producto Interno Bruto en su serie original, crece 2,2% respecto al mismo periodo de 2025¹⁰.



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 5,7% (contribuye 0,9 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 2,9% (contribuye 0,6 puntos porcentuales a la variación anual).
- Industrias manufactureras crece 2,9% (contribuye 0,3 puntos porcentuales a la variación anual).

4.1.2 Tasa Representativa del Mercado (TRM – Peso por dólar)

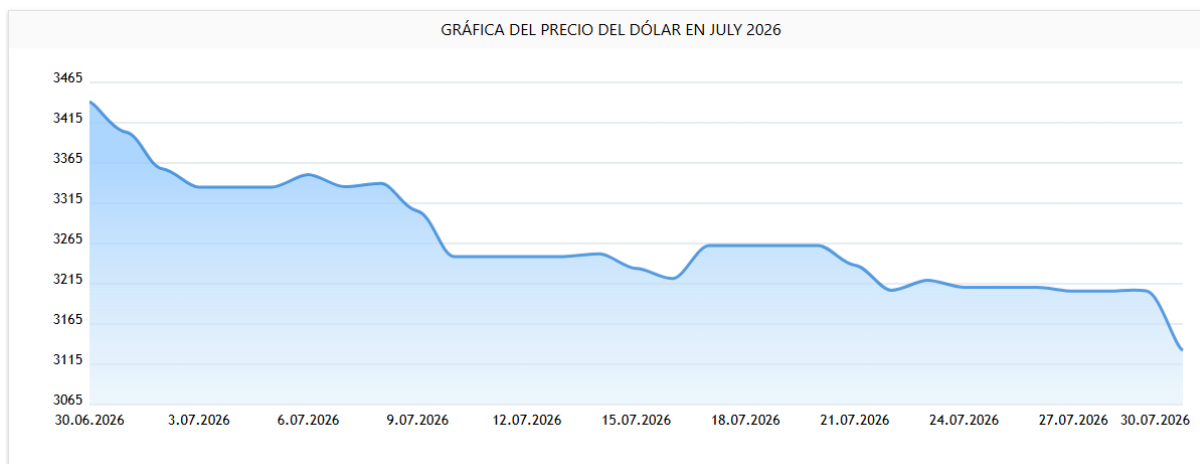
La TRM es la cantidad de pesos colombianos por un dólar de los Estados Unidos. La TRM se calcula con base en las operaciones de compra y venta de divisas entre intermediarios financieros que transan en el mercado cambiario colombiano, con cumplimiento el mismo día cuando se realiza la negociación de las divisas.

¹⁰ <https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-nacionales-trimestrales/pib-informacion-tecnica>

➤ Valor histórico del dólar en Colombia de los últimos tres meses (resumen).



➤ Valor histórico del dólar en Colombia para julio de 2026



El precio del dólar en Colombia lo determina un mercado libre, sin intervención por parte del Estado. Sin embargo, existe un sistema de control establecido por el Banco de la República a través de la llamada banda cambiaria dentro de la cual el precio de la divisa se mueve y es casi que imposible controlarlo, ya que es un factor global que afecta todas las economías mundiales.

En el sector TIC, cuando ese precio baja los importadores son los beneficiados, pues por cada dólar que pagan por la compra de sus productos en el exterior invierten menos pesos a cambio. Mientras los importadores ganan con la baja de la divisa, los exportadores pierden pues las ventas que realizan en el exterior les resultan menos rentables pues reciben menos pesos.

Para este proceso la TRM es un indicador relevante dado que los servicios que requieren repuestos la gran mayoría están soportados en compras que se hacen en dólares.

4.1.3 Índice de Precios al Consumidor (IPC)

Cuando se hace referencia al Índice de Precios al Consumidor (IPC) se debe tener en cuenta que este mide la evolución del costo promedio de una canasta de bienes y servicios representativa del consumo final de los hogares, expresado en relación con un período base. La variación porcentual del IPC entre dos periodos de tiempo representa la inflación observada en dicho lapso. El cálculo del IPC para Colombia se hace mensualmente en el Departamento Administrativo Nacional de Estadística (DANE). Este índice es constantemente frecuentado porque participa como base fundamental para el ajuste de otras variables económicas como es el caso ya expuesto del valor del salario mínimo.

Es tarea fundamental del Banco Central, utilizar las herramientas necesarias con el fin de mantener tasas de inflación de un dígito, lo que permite a la economía generar confianza tanto a nivel interno como externo.

La inflación controlada no solo permite a los consumidores mantener niveles aceptables de poder adquisitivo, sino que, además, genera una atmósfera positiva a la inversión lo que repercute en productividad.

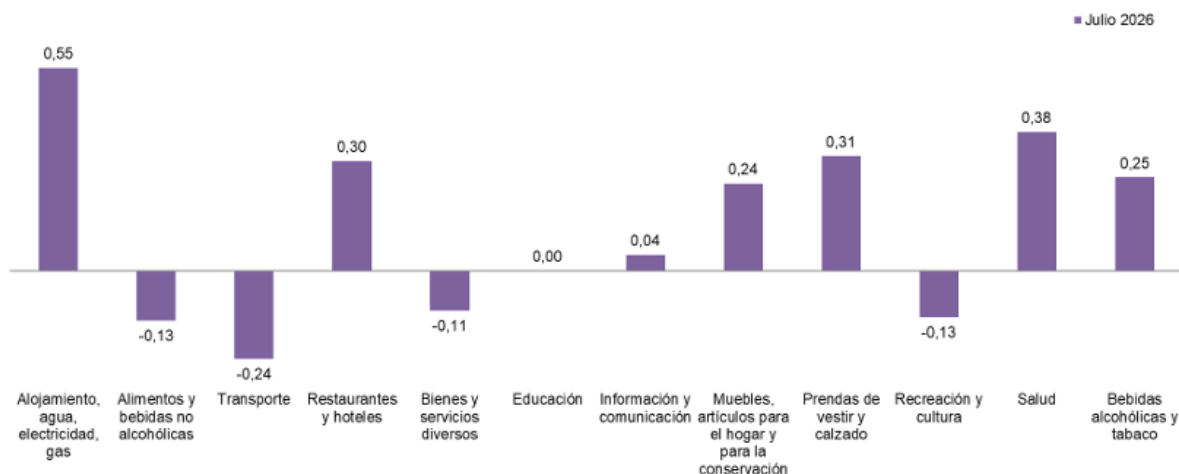
Variación mensual, año corrido y anual
Total nacional
2025 - 2026 (julio)

IPC	Julio					
	Variación mensual		Variación año corrido		Variación anual	
	2025	2026	2025	2026	2025	2026
IPC total	0,28	0,17	4,02	4,94	4,90	6,03

Fuente: DANE, IPC

En julio de 2026 la variación mensual del IPC fue 0,17%, la variación año corrido fue 4,94% y la anual 6,03%. 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%).¹¹

Variación mensual del Índice de Precios al Consumidor (IPC) Por Divisiones 2026 (julio)



Fuente: DANE, IPC

Nota: el orden de las divisiones responde a su ponderación dentro de la canasta del IPC (izq – der).

En julio de 2026 las mayores contribuciones a la variación mensual en las doce divisiones del IPC Total se registraron en las siguientes subclases: electricidad con 0,08 puntos porcentuales, servicios relacionados con la copropiedad con 0,04 puntos porcentuales y arriendo imputado con 0,03 puntos porcentuales. Las subclases con las menores contribuciones fueron: plátanos con -0,03 puntos porcentuales, frutas frescas con -0,02 puntos porcentuales y vehículo particular nuevo o usado con -0,02 puntos porcentuales.

Para el presente proceso es fundamental involucrar el indicador del Índice de Precios al Consumidor, por cuanto es una variable macroeconómica que se emplea para actualizar los valores de los bienes y servicios del país, para nuestro caso el valor del IPC tiene un efecto directo en la estructuración del presupuesto de cada uno de los elementos que lo integran (salarios, prestaciones, tasas y contribuciones, insumos para la producción y otros).

¹¹ <https://www.dane.gov.co/files/operaciones/IPC/jul2026/cp-IPC-jul2026.pdf>

4.1.4 Identificación del sector económico al cual pertenece la necesidad.

El sector de las Tecnologías de la Información y las Comunicaciones (TIC) continúa consolidándose como uno de los sectores estratégicos para el crecimiento económico, la transformación digital y el fortalecimiento de la competitividad institucional en Colombia. Su evolución ha impulsado cambios significativos en los ámbitos económico, social, cultural y gubernamental, facilitando la modernización de procesos, la automatización de servicios y la adopción de nuevas tecnologías digitales.

Desde el punto de vista económico, el sector TIC mantiene una dinámica de crecimiento sostenida, impulsada por la expansión de los servicios digitales, la adopción de soluciones en la nube, el fortalecimiento de la conectividad y la creciente necesidad de modernización tecnológica tanto en el sector público como privado. En este contexto, las organizaciones continúan orientando sus inversiones hacia iniciativas de transformación digital, automatización, innovación, continuidad operativa y fortalecimiento de la seguridad de la información.

En materia de conectividad, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha reportado un crecimiento sostenido de los accesos a Internet en Colombia, acompañado de una expansión de las redes de banda ancha y de las tecnologías móviles de cuarta y quinta generación. Esta evolución refleja el crecimiento del ecosistema digital del país y la mayor dependencia de las entidades públicas y organizaciones privadas respecto de las redes y servicios tecnológicos para el desarrollo de sus actividades y la prestación de servicios a ciudadanos, usuarios y demás grupos de interés.

En paralelo, el incremento y la sofisticación de las amenazas cibernéticas, incluidos los ataques de ransomware, explotación de vulnerabilidades, accesos no autorizados y demás incidentes dirigidos contra sistemas y servicios expuestos a Internet, han incrementado la necesidad de fortalecer las capacidades de prevención, detección, monitoreo y respuesta de las organizaciones. En consecuencia, la ciberseguridad se ha consolidado como un componente estratégico de la gestión tecnológica y de la continuidad operativa, generando una mayor demanda de soluciones especializadas para la protección de redes, aplicaciones, sistemas de información e infraestructura crítica.

Adicionalmente, la creciente adopción de tecnologías como la computación en la nube, la inteligencia artificial, la analítica de datos, el trabajo remoto y las arquitecturas híbridas y multicloud ha ampliado la superficie de exposición de las organizaciones y ha generado nuevos desafíos para la protección de los recursos

tecnológicos. Este escenario requiere mecanismos de seguridad capaces de operar en ambientes distribuidos, proporcionar visibilidad sobre el tráfico y los eventos de red y mantener actualizadas las capacidades de protección frente a nuevas amenazas y vulnerabilidades.

En este escenario, también se evidencian transformaciones relevantes en el mercado de seguridad de red y perimetral, caracterizadas por la evolución de los dispositivos tradicionales de filtrado hacia plataformas integrales de seguridad que incorporan capacidades como firewall de nueva generación (NGFW), prevención y detección de intrusiones, control de aplicaciones, filtrado avanzado, inteligencia de amenazas, protección de servicios web y gestión centralizada de eventos de seguridad. De manera complementaria, los fabricantes han fortalecido los esquemas de licenciamiento y servicios asociados, incorporando actualizaciones permanentes de software y firmware, bases de datos de amenazas, parches de seguridad, soporte técnico especializado, mantenimiento y servicios de garantía.

Esta evolución implica que las organizaciones no solo requieren disponer de soluciones tecnológicas de seguridad, sino garantizar su actualización, soporte y adecuada operación durante todo su ciclo de vida. La continuidad del licenciamiento y el acceso a las actualizaciones y servicios de soporte del fabricante permiten mantener vigentes las capacidades de protección, atender vulnerabilidades identificadas y responder oportunamente ante incidentes de seguridad, contribuyendo a reducir los riesgos asociados a la indisponibilidad o afectación de los servicios tecnológicos.

Por lo anterior, la inversión en infraestructura digital, conectividad y soluciones de ciberseguridad se consolida como un componente estratégico para garantizar la continuidad de los sistemas de información misionales y de apoyo, la disponibilidad de los servicios tecnológicos y el fortalecimiento de las capacidades institucionales frente a los retos derivados de la transformación digital y la evolución permanente del panorama de amenazas cibernéticas.

4.1. CONTEXTO TÉCNICO

Como se ha señalado anteriormente, las Tecnologías de la Información y las Comunicaciones (TIC) constituyen actualmente un componente estratégico para el funcionamiento y desarrollo de las organizaciones, al facilitar la gestión y protección de la información, la prestación de servicios digitales, la comunicación con los grupos de interés y la articulación de los procesos institucionales. La creciente dependencia de las organizaciones respecto de las redes, sistemas de

información y servicios tecnológicos ha generado, a su vez, una mayor necesidad de implementar mecanismos que permitan proteger estos recursos frente a accesos no autorizados, vulnerabilidades, amenazas cibernéticas y demás riesgos que puedan afectar su disponibilidad, integridad y confidencialidad.

En este contexto, el sector de servicios informáticos y de tecnologías de seguridad ha adquirido una importancia creciente, al proporcionar soluciones de infraestructura, conectividad, ciberseguridad, soporte técnico, mantenimiento y administración de plataformas tecnológicas a organizaciones de diferentes sectores de la economía. La evolución de las tecnologías digitales, la expansión de los servicios en línea, la adopción de ambientes híbridos y multicloud y el incremento de las amenazas cibernéticas han impulsado la demanda de soluciones especializadas que permitan fortalecer las capacidades de prevención, detección, monitoreo y respuesta ante incidentes de seguridad.

Dentro de este mercado, la seguridad perimetral de red comprende un conjunto de soluciones tecnológicas destinadas a controlar y supervisar el tráfico entre redes internas y externas, aplicar políticas de seguridad, prevenir accesos no autorizados, detectar y bloquear actividades maliciosas y proteger los servicios y aplicaciones expuestos a Internet. Estas soluciones pueden incorporar componentes de hardware y software, licenciamiento, actualizaciones, bases de datos de amenazas, soporte especializado, mantenimiento, garantía y mecanismos de monitoreo y gestión centralizada, cuya integración permite fortalecer la protección de la infraestructura tecnológica de las organizaciones.

En consecuencia, la adquisición o renovación de soluciones de seguridad perimetral debe considerar no solamente las características técnicas de los componentes tecnológicos, sino también los servicios asociados a su ciclo de vida, tales como la renovación del licenciamiento, actualización de software y firmware, aplicación de parches de seguridad, acceso a bases de datos de amenazas, soporte técnico especializado, atención de incidentes, mantenimiento preventivo y correctivo y garantía. Estos elementos resultan fundamentales para conservar las capacidades de protección de la infraestructura y mantenerla alineada con la evolución de las amenazas y las recomendaciones de los fabricantes.

Los aspectos técnicos del presente proceso se estructuraron a partir de las necesidades identificadas por la Agencia y de las condiciones de operación de las soluciones de seguridad actualmente implementadas y en producción. En este sentido, las especificaciones técnicas establecen las condiciones y requerimientos mínimos que deberán cumplir los bienes y servicios objeto del proceso,

permitiendo a los proponentes estructurar sus ofertas de acuerdo con las condiciones establecidas en el estudio previo y sus anexos.

Las condiciones técnicas definidas responden, además, a la necesidad de garantizar la continuidad, disponibilidad, estabilidad y seguridad de los servicios tecnológicos de la Agencia, procurando que las actividades de renovación, actualización, soporte, mantenimiento y garantía sean compatibles con la infraestructura actualmente implementada. No obstante, durante el desarrollo del proceso podrán analizarse las observaciones y recomendaciones formuladas por los interesados y proponentes, siempre que estas resulten técnica y jurídicamente procedentes y no afecten los principios de pluralidad de oferentes, selección objetiva y satisfacción de la necesidad de la Entidad.

El siguiente cuadro indica el licenciamiento tecnológico del cual se requiere la renovación del soporte y garantía de fabrica (Fortinet):

Numero Serial	Nombre Del Producto	Vigencia Actual Licenciamiento	Servicios	Renovación Fecha Inicial	Renovación Fecha Final
FG200ETK19902207	FortiGate 200E	17/12/2026	UTP + Elite Service	18/12/2026	17/12/2027
FG200ETK19902482	FortiGate 200E	17/12/2026	UTP + Elite Service	18/12/2026	17/12/2027
FG100FTK21055016	FortiGate 100F	17/12/2026	UTP	18/12/2026	17/12/2027
FG100FTK21055108	FortiGate 100F	17/12/2026	UTP	18/12/2026	17/12/2027
FV400ETA22000156	FortiWeb 400E	17/12/2026	Estándar Bundle	18/12/2026	17/12/2027
FSMP000000000521	FortiSIEM	17/12/2026	90 activos	18/12/2026	17/12/2027

En virtud de las funciones asignadas a la Oficina de Sistemas y Tecnologías de la Información, resulta fundamental garantizar la disponibilidad, continuidad, soporte y adecuado funcionamiento de las soluciones tecnológicas que conforman la infraestructura de seguridad de la Agencia Nacional de Defensa Jurídica del Estado.

En este contexto, la renovación del licenciamiento, soporte y garantía de la plataforma de seguridad Fortinet constituye una medida necesaria para preservar las capacidades de protección de la infraestructura tecnológica y contribuir a la continuidad y seguridad de los servicios institucionales.

A continuación, se presentan las principales razones que sustentan la necesidad de adelantar la presente contratación:

1. Garantizar la continuidad y disponibilidad de la plataforma de seguridad perimetral, la cual constituye un componente fundamental para la protección de las redes, sistemas de información, servicios institucionales y aplicaciones de la Agencia frente a accesos no autorizados, tráfico malicioso y demás amenazas provenientes de redes externas.
2. Mantener vigente el licenciamiento, soporte y garantía del fabricante, permitiendo a la Agencia acceder durante la vigencia contratada a las actualizaciones de software y firmware, parches de seguridad, bases de datos de amenazas, mejoras funcionales y demás recursos oficiales necesarios para mantener las capacidades de protección de la plataforma.
3. Contar con soporte técnico especializado y atención oportuna de incidentes, que permita gestionar fallas, vulnerabilidades, eventos de seguridad, requerimientos de configuración y demás situaciones que puedan afectar la operación de la plataforma, incluyendo el escalamiento al fabricante cuando se requiera soporte de tercer nivel.
4. Mantener actualizada y adecuadamente configurada la infraestructura de seguridad, mediante la aplicación de actualizaciones, buenas prácticas, actividades de mantenimiento, revisión de configuraciones y procedimientos de aseguramiento y hardening, con el propósito de optimizar su funcionamiento y reducir posibles vulnerabilidades o configuraciones que puedan incrementar la superficie de exposición de la Agencia.
5. Fortalecer las capacidades institucionales de prevención, detección y respuesta frente a amenazas cibernéticas, mediante la disponibilidad de herramientas y servicios especializados que permitan proteger la información, las redes y los servicios tecnológicos de la Entidad frente a incidentes que puedan comprometer su confidencialidad, integridad o disponibilidad.
6. Reducir los riesgos asociados a la obsolescencia, pérdida de soporte o falta de actualización de las soluciones de seguridad, garantizando la continuidad del ciclo de vida tecnológico de los productos implementados y el acceso a los servicios oficiales del fabricante durante la vigencia contractual.

En consecuencia, contar con el licenciamiento, soporte y garantía vigentes de la plataforma de seguridad permite mantener las soluciones Fortinet en condiciones adecuadas de operación, disponer oportunamente de actualizaciones, parches de seguridad y bases de datos de amenazas, acceder al acompañamiento técnico especializado y fortalecer la capacidad de la Agencia para prevenir y atender eventos que puedan afectar la seguridad y continuidad de sus servicios tecnológicos. Lo anterior contribuye a preservar la disponibilidad, integridad y

confidencialidad de la información institucional y a garantizar la continuidad de la operación de los servicios que dependen de la infraestructura de seguridad perimetral.

CONTEXTO REGULATORIO O LEGAL

Las normas que regulan el proceso de contratación son la Constitución Política de Colombia, la Ley 80 de 1993, la Ley 489 de 1998 (Capítulo I, II, III, VIII, X), la Ley 1952 de 2019 modificada por la Ley 2094 de 2021, la Ley 1150 de 2007, la Ley 1474 de 2011, el Decreto 1082 de 2015, la Ley 1882 de 2018, y demás disposiciones aplicables a la materia. La modalidad de selección aplicable a la presente contratación corresponde a la contenida en el literal a) numeral 2 del artículo 2 de la Ley 1150 de 2007, que corresponde a la Selección Abreviada bajo la causal “adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades”, toda vez que, el objeto y las especificaciones técnicas a ejecutar, 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. Así mismo el suministro de servicios es de común utilización por parte de las entidades.

5. ESTUDIO DE LA OFERTA

Para efectos de la presente contratación y con el fin de determinar el presupuesto oficial, la Entidad realizó el correspondiente análisis técnico y económico con base en el estudio de mercado adelantado mediante las cotizaciones presentadas por firmas especializadas, en el marco de la solicitud de información publicada en el SECOP con No. SIP-ANDJE-042-2026. Dichas cotizaciones, las cuales se anexan al presente documento, permitieron identificar las variables técnicas y financieras consideradas para la estimación del presupuesto de la presente contratación.

El licenciamiento, soporte técnico y garantía requeridos para las soluciones de seguridad objeto del presente proceso son comercializados en Colombia a través de fabricantes y canales autorizados, entre los cuales se encuentran distribuidores, integradores y partners certificados. Estos actores participan en la comercialización, renovación y prestación de servicios asociados a las soluciones tecnológicas, de acuerdo con las condiciones y esquemas de distribución establecidos por los respectivos fabricantes.

Para el presente estudio de sector se identificaron empresas con capacidad técnica, operativa y comercial para atender los requerimientos establecidos en el Anexo 1 – Especificaciones Técnicas, incluyendo las actividades de renovación y activación

del licenciamiento, soporte especializado, garantía, actualización de software y firmware, atención de incidentes, mantenimiento y demás servicios asociados durante el periodo de vigencia requerido por la Agencia.

La identificación de estos proveedores permite evidenciar la existencia de oferta en el mercado nacional para atender la necesidad de la Entidad y garantizar la continuidad de las soluciones de seguridad actualmente implementadas, bajo las condiciones técnicas y de servicio establecidas en el presente proceso de contratación.

Proveedores	NIT	Tamaño de la empresa
GAMMA INGENIEROS SAS	891501783	Mediana
TSG THE IT EXPERTS SAS	900994724	Grande
WEXLER SAS	900390198	Mediana
DATASEC SAS	901223827	Mediana
ROYAL TECH GROUP SAS	901394655	Pequeña
ECOMIL SAS	830133271	Mediana
EYC INGENIEROS SAS	900024202	Mediana
STS SAS	830505521	Mediana
OPEN GROUP SAS	900249043	Mediana
MCO GLOBAL SAS	9007498203	Pequeña
SUMINISTROS OBRAS Y SISTEMAS	900261209	Pequeña
SERVERS & SOFTWARE SAS	900130300	Pequeña
IMPORTAREX SAS	805031667	Pequeña
KNOX IT	901157678	Pequeña
CORE IP SAS	900945968	Mediana
IOGESTION SAS	900554321	Pequeña
SECURITY TECH CONTROL SAS	900118932	Microempresa

Estas empresas cuentan en su portafolio y certificación directamente del fabricante con los servicios requeridos, con el fin de ofrecer a sus clientes en forma oportuna, eficaz, con calidad y tiempos de entrega los mejores servicios. La información de proveedores fue previamente consultada por la Agencia en el histórico de adquisiciones con el mismo objeto, en listas de referencia de proveedores de tecnología y la Agencia Nacional de Contratación Estatal – Colombia Compra Eficiente.

6. ESTUDIO DE LA DEMANDA

Con el objeto de realizar el análisis de la demanda del sector para el objeto del presente proceso de selección, se realizó la búsqueda en SECOP II y a nivel interno

de los principales contratos con características similares con el fin de tener una perspectiva desde el punto de vista del valor de los servicios como también de los esquemas de contratación utilizados, que se relacionan a continuación:

PROCESOS EN SECOP II

ENTIDAD	OBJETO	TIPO PROCESO	NÚMERO DEL PROCESO O NÚMERO DEL CONTRATO	AÑO	VALOR DEL CONTRATO
INSTITUTO DISTRITAL DE PROTECCION Y BIENESTAR	CONTRATAR LA RENOVACIÓN DE LAS SUSCRIPCIÓN DE SOPORTE TÉCNICO Y ACTUALIZACIÓN DE LOS EQUIPOS FORTINET QUE SOPORTAN LA SEGURIDAD INFOMÁTICA DEL IDPYBA.	SELECCIÓN ABREVIADA SUBASTA INVERSA	SASI-007-2026	2026	\$ 108.375.281
AGENCIA ITRC	RENOVACIÓN DEL LICENCIAMIENTO, GARANTÍA, ACTUALIZACIÓN Y SOPORTE TÉCNICO, DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL - FORTINET	SELECCIÓN ABREVIADA SUBASTA INVERSA	ITRC-SASI-003-2026	2026	\$ 121.900.000
MUNICIPIO DE SAN JOSE DE CUCUTA	CONTRATAR LA RENOVACIÓN DEL LICENCIAMIENTO Y SOPORTE TIPO UTP DE 12 MESES FORTINET FG1801F PARA EL PROCESO DE CIBERSEGURIDAD DE LA ALCALDÍA DE SAN JOSÉ DE CÚCUTA	SELECCIÓN ABREVIADA SUBASTA INVERSA	TIC-SUB-001-2026	2026	\$349.169.000
FONDO DE PRESTACIONES ECONOMICAS CESANTIAS Y PENSIONES	CONTRATAR LA ADQUISICIÓN Y RENOVACIÓN DEL LICENCIAMIENTO, SOPORTE DE FÁBRICA FORTINET Y BOLSA DE HORAS PARA LA ADMINISTRACIÓN Y SOPORTE DE LA INFRAESTRUCTURA DE SEGURIDAD DEL FONDO DE PRESTACIONES ECONÓMICAS,	SELECCIÓN ABREVIADA SUBASTA INVERSA	SASI_001 DE 2026	2026	\$ 523.211.690

	CESANTÍAS Y PENSIONES - FONCEP				
SECRETARIA DISTRITAL DE GOBIERNO	ADQUIRIR Y RENOVAR EL LICENCIAMIENTO, SOPORTE Y GARANTÍA DE LA INFRAESTRUCTURA DE SEGURIDAD (FORTINET) Y FORTALECIMIENTO DE LA INFRAESTRUCTURA DE SEGURIDAD PARA EL TRABAJO INTELIGENTE DE LA SECRETARIA DISTRITAL DE GOBIERNO	SELECCIÓN ABREVIADA SUBASTA INVERSA	SDG-SASI- 1-2025	2025	\$ 2.489.167.600
DIRECCION GENERAL MARITIMA - SUBDIRECCION ADMINISTRATI VA Y FINANCIERA - SUBAFIN	ADQUIRIR EL LICENCIAMIENTO PARA EL SOFTWARE DE LA INFRAESTRUCTURA FORTINET DE LA DIRECCIÓN GENERAL MARÍTIMA - DIMAR	SELECCIÓN ABREVIADA MENOR CUANTÍA	181- GINREDCE- 2025	2025	\$ 424.168.500
UAE-CUERPO OFICIAL DE BOMBEROS DE BOGOTA	CONTRATAR LA RENOVACIÓN DEL LICENCIAMIENTO Y SOPORTE DE LAS PLATAFORMAS DE SEGURIDAD PERIMETRAL FORTINET, FIREWALLS Y WAF DEL EDIFICIO COMANDO Y ESTACIONES PARA LA U.A.E. CUERPO OFICIAL DE BOMBEROS DE BOGOTÁ - TIC	SELECCIÓN ABREVIADA SUBASTA INVERSA	UAECOB- SASI-002- 2025	2025	\$ 216.142.630
AREA METROPOLITAN A DEL VALLE DE ABURRA	ADQUISICION Y RENOVACION DEL LICENCIAMIENTO FORTINET PARA LA PROTECCION INFORMATICA DEL AREA METROPOLITANA DEL VALLE DE ABURRA	SELECCIÓN ABREVIADA SUBASTA INVERSA	SIE 001 DE 2025	2025	\$ 997.539.995

De igual manera, se relacionan los contratos celebrados por parte de la Agencia en las vigencias anteriores.

NÚMERO DE CTO	MODALIDAD DE CONTRATACIÓN	NOMBRE CONTRATISTA	OBJETO	VALOR DEL CONTRATO
160- 2019	SELECCIÓN ABREVIADA SUBASTA INVERSA	ADSUM SOLUCIONES TECNOLOGICAS S.A.S	ADQUIRIR UNA SOLUCIÓN DE UN SISTEMA DE SEGURIDAD INFORMÁTICA "FIREWALL" EN ALTA DISPONIBILIDAD CON SU	\$ 95.535.940

ANÁLISIS ECONÓMICO DEL SECTOR

			RESPECTIVA LICENCIA Y LOS SERVICIOS DE IMPLEMENTACIÓN Y PUESTA EN FUNCIONAMIENTO DE LA ENTIDAD SEGÚN ESPECIFICACIONES TÉCNICAS	
BID 051-2022	COMPARACIÓN DE PRECIOS	SOLUCIONES, TECNOLOGIA Y SERVICIOS SAS "STS SAS"	ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE EQUIPOS TECNOLÓGICOS DE SEGURIDAD PERIMETRAL, PARA LA PROTECCIÓN DE LA AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO, CONTRA AMENAZAS INFORMÁTICAS EXTERNAS"	\$ 342.999.998,67
085-2022	SELECCIÓN ABREVIADA SUBASTA INVERSA	ADSUM SOLUCIONES TECNOLOGICAS S.A.S	RENOVACIÓN LICENCIAMIENTO DE SOPORTE Y GARANTÍA DE LA SEGURIDAD PERIMETRAL FORTIGATE 200E PARA LA AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO.	\$ 75.707.100
158-2023	SELECCIÓN ABREVIADA SUBASTA INVERSA	B2B TIC S.A.S.	LICENCIAMIENTO EN RENOVACIÓN, SOPORTE Y GARANTÍA DE LA PLATAFORMA FORTISIEM.	\$ 142.400.000
190-2025	SELECCIÓN ABREVIADA SUBASTA INVERSA	EYC INGENIEROS SAS	RENOVACIÓN DE INFRAESTRUCTURA, SOPORTE Y GARANTÍA DE LICENCIAMIENTO DE EQUIPOS DE SEGURIDAD PERIMETRAL.	\$ 58.999.171,69

Por otra parte, de acuerdo con lo reportado por el grupo de Gestión Financiera de la Agencia Nacional de Defensa Jurídica del Estado, los indicadores financieros evaluados con respecto a las diferentes empresas dieron como resultado los siguientes datos:

Capacidad Financiera	
Liquidez	Mayor o igual a 1.2
Nivel de endeudamiento	Menor o igual a 68%
Razón de Cobertura de Intereses	Mayor o igual a 1.5 y/o indeterminada cuando su utilidad operacional sea positiva.
Capital de trabajo	Mayor o igual al 50% del presupuesto oficial

Capacidad Organizacional	
Rentabilidad del patrimonio	Mayor o igual a 1.6%
Rentabilidad del activo	Mayor o igual a 1.7%

7. ANÁLISIS MIPYMES:

Para identificar los proveedores del presente estudio, se tomó la base de datos de las empresas que cotizaron a la Entidad y se encontró que las cuatro (4) empresas son MIPYMES¹².

Proveedores	NIT	Tamaño de la empresa
EYC INGENIEROS SAS	900024202	Mediana
CORE IP SAS	900945968	Mediana
IOGESTION SAS	900554321	Pequeña
SECURITY TECH CONTROL SAS	900118932	Micro

Lo anterior, tiene como finalidad, permitir el acceso el mercado a este tipo de empresas para impulsar el emprendimiento colombiano, pues así lo establece la Ley 2069 de 2020: Artículo 33: "(...) 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 (...)*".

En virtud del análisis del sector económico y de los oferentes, este proceso corresponde a los servicios de "Renovación de infraestructura, soporte y garantía de licenciamiento de equipos de seguridad perimetral", servicio que, como se evidencia, es prestado en su mayoría por personas jurídicas, por lo que, se dará prevalencia a la industria nacional; sea importante mencionar así mismo, que los servicios son prestados por personal idóneo y capacitado nacional colombiano o residente en Colombia, siempre y cuando el personal extranjero cuente con la idoneidad y su situación esté regularizada en el territorio nacional.

8. ANÁLISIS CUMPLIMIENTO DECRETO 1860 DE 2021

Para el presente Análisis del sector, a través de SECOP II se identificaron las empresas que prestan los servicios objeto del presente proceso, en este sentido y a efectos de dar cumplimiento al Decreto 1860 de 2021 por el cual se busca

¹² MiPyme de acuerdo con la Ley 590 del 2000 se define como: "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".

incentivar entre otros aspectos, la participación de emprendimientos femeninos se solicitó a estas empresas que cotizaron, la siguiente información:

INDICADORES EMPRENDIMIENTO FEMENINO	Por favor indicar con una X si a su empresa le aplica alguna de las siguientes condiciones
1. Más del cincuenta por ciento (50%) de las acciones, partes de interés o cuotas de participación de su empresa pertenecen a mujeres y/o los derechos de propiedad pertenecieron a mujeres durante el último año.	
2. El cincuenta por ciento (50%) de los empleos del nivel directivo de su empresa son ejercidos por mujeres y éstas han estado vinculadas laboralmente a la empresa durante al menos el último año anterior en el mismo cargo u otro del mismo nivel.	
3. Usted participó como mujer, (persona natural) en actividades comerciales a través de un establecimiento de comercio durante al menos el último año anterior	
4. Participó en asociaciones y cooperativas en las que más del cincuenta por ciento (50%) de los asociados sean mujeres y su participación fue durante al menos el último año anterior.	

Al respecto se recibieron tres (3) respuestas que cumplieron con los requerimientos del evento de cotización, así:

INDICADORES EMPRENDIMIENTO FEMENINO	EYC INGENIEROS	SECURITY TECH CONTROL	CORE IP
1. Más del cincuenta por ciento (50%) de las acciones, partes de interés o cuotas de participación de su empresa pertenecen a mujeres y/o los derechos de propiedad pertenecieron a mujeres durante el último año	N/R	SI	N/R
2. El cincuenta por ciento (50%) de los empleos del nivel directivo de su empresa son ejercidos por mujeres y éstas han estado vinculadas laboralmente a la empresa durante al menos el último año anterior en el mismo cargo u otro del mismo nivel.	SI	N/R	N/R
3. Usted participó como mujer, (persona natural) en actividades comerciales a través de un establecimiento de comercio durante al menos el último año anterior	N/R	N/R	N/R

4. Participó en asociaciones y cooperativas en las que más del cincuenta por ciento (50%) de los asociados sean mujeres y su participación fue durante al menos el último año anterior.	N/R	N/R	N/R
---	-----	-----	-----

Como resultado del estudio realizado se encontró que dentro de las empresas del sector, SECURITY TECH CONTROL cumple con los requisitos para ser considerada como "EMPRENDIMIENTO DE MUJERES", puesto que marcó el indicador del numeral 1 (más del 50% de la propiedad en cabeza de mujeres).

Por otra parte, EYC INGENIEROS señaló cumplir con el indicador del numeral 2, referido a que el 50% de los cargos directivos están ejercidos por mujeres vinculadas laboralmente durante al menos el último año.

Conforme lo anterior, dos de los tres cotizantes se consideran empresas de mujeres, por lo cual, se establecerá criterios diferenciales de experiencia y valor de la garantía de seriedad, conforme lo señalado en el Decreto 1860 de 2021.

Nota: Se presentó una cuarta cotización por parte de la sociedad IO GESTION, la cual no fue tenida en cuenta porque se encuentra desfasada en el valor promedio aproximadamente un 27%.

9. ANÁLISIS CUMPLIMIENTO DECRETO No. 1860 DE 2021 FOMENTO PROVISIÓN DE BIENES O SERVICIOS POR PARTE DE POBLACIÓN EN POBREZA EXTREMA, DESPLAZADOS POR LA VIOLENCIA, PERSONAS EN PROCESO DE REINTEGRACIÓN O REINCORPORACIÓN Y SUJETOS DE ESPECIAL PROTECCIÓN CONSTITUCIONAL.

En cumplimiento de lo establecido en el artículo 2.2.1.2.4.2.16 "Fomento a la ejecución de contratos estatales por parte de población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional" del Decreto No. 1860 de 2021, la Entidad realizó el análisis de oportunidad y conveniencia de la participación de los sujetos antes mencionados para este proceso de contratación, teniendo en cuenta el objeto contractual y el alcance de las obligaciones.

De dicho análisis se tiene en primer término que, el contrato resultado del presente proceso se ejecutará a través de la Renovación de infraestructura, soporte y garantía de licenciamiento de equipos de seguridad perimetral, la cual estará a disposición de la Agencia una vez suscrita el acta de inicio.

En segundo lugar, en lo relacionado con exigencias de personal, se establece que el contratista NO pondrá a disposición de la Agencia personal humano debido a las características propias del contrato.

Ahora bien, la norma en mención también establece:

“Esta provisión se establecerá en un porcentaje que no será superior al diez por ciento (10%) ni inferior al cinco por ciento (5%) de los bienes o servicios requeridos para la ejecución del contrato, de manera que no se ponga en riesgo su cumplimiento adecuado”.

Por tanto, una vez analizada la descripción del objeto contractual y las condiciones técnicas para su desarrollo, se concluye que no es posible que el contratista asegure el porcentaje exigido durante la ejecución del contrato mediante la provisión de bienes o servicios por parte de población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional, ya que la renovación del soporte y garantía se perfeccionará con la entrega de las mismas.

Por lo anterior, no se incorporará la obligación descrita en el Decreto No. 1860 de 2021.

10. CONCEPTOS ESTADÍSTICOS

10.1. TAMAÑO DE LA MUESTRA - MUESTRA PARA EL ESTUDIO DE MERCADO - ANÁLISIS ECONÓMICO QUE SOPORTA EL VALOR ESTIMADO DEL CONTRATO.

Como resultado del presente análisis, y tomando como referencia la muestra de los contratos que se han celebrado el sector público para la renovación de los servicios de soporte de los equipos de Infraestructura Tecnológica, se evidencia la necesidad de garantizar la operatividad de los mismos a través del respaldo del propio fabricante.

Teniendo en cuenta que la AGENCIA no cuenta con el personal, infraestructura y logística para brindar el soporte que garantice el mantenimiento correctivo e incluso el cambio y suministro de partes, se requiere contratar.

Bajo los anteriores presupuestos, la Oficina Asesora de Sistemas y Tecnologías de Información de la Agencia, en cumplimiento de su función de direccionamiento y orientación en la adquisición, mantenimiento y mejoramiento de los bienes tecnológicos de la Agencia, los cuales son necesarios para el normal

funcionamiento y con el fin de mantener en producción y sin inconvenientes la infraestructura tecnológica que soporta los procesos Misionales y de Apoyo, requiere contratar la Renovación de infraestructura, soporte y garantía de licenciamiento de equipos de seguridad perimetral, que hacen parte de la infraestructura tecnológica misional y de apoyo de la Agencia Nacional de Defensa Jurídica del Estado, de conformidad a las condiciones técnicas mínimas requeridas.

10.2. ANÁLISIS ESTADÍSTICO

La Agencia Nacional de Defensa Jurídica del Estado, realizó el análisis económico con base en el estudio de mercado realizado a través de cotizaciones presentadas por diferentes proveedores de servicios requeridos por la entidad, el cual se anexa al presente documento, lo cual permitió determinar las variables consideradas para calcular el presupuesto de la presente contratación.

Dentro de este ejercicio mediante la Solicitud de Información a Proveedores a través de SECOP II identificado como SIP-ANDJE-042-2026, se logró identificar a cuatro (4) proveedores, así:



En concordancia con lo anterior, para el presente proceso de selección la Agencia determinó que el presupuesto oficial se establecerá con base en el promedio simple de las tres (3) cotizaciones de menor valor presentadas por las empresas

ANÁLISIS ECONÓMICO DEL SECTOR

CORE IP, EYC INGENIEROS y SECURITY TECH CONTROL, por cuanto corresponden a ofertas con condiciones técnicas y económicas comparables.

La cotización de la empresa IO GESTION (\$154.257.829,98) no fue considerada para el cálculo del presupuesto por ser un valor atípico, toda vez que su valor es 27,64% superior al promedio de las demás cotizaciones, lo que evidencia una desviación significativa que podría distorsionar la estimación del presupuesto oficial.

Ítem	Producto	COTIZANTE			PROMEDIO PROPUESTAS MENOR VALOR
		CORE IP	EYC INGENIEROS	SECURITY TECH CONTROL	
1	FortiGate 200E Serial: FG200ETK19902207 Periodo Licencia: 18/12/2026 a 17/12/2027	\$11.548.264,00	\$11.369.882,72	\$11.231.111,11	\$11.383.085,94
2	FortiGate 200E Serial: FG200ETK19902482 Periodo Licencia: 18/12/2026 a 17/12/2027	\$11.548.264,00	\$11.369.882,72	\$11.231.111,11	\$11.383.085,94
3	FortiGate 100F Serial: FG100FTK21055016 Periodo Licencia: 18/12/2026 a 17/12/2027	\$12.092.088,00	\$11.905.306,56	\$11.760.000,00	\$11.919.131,52
4	FortiGate 100F Serial: FG100FTK21055108 Periodo Licencia: 18/12/2026 a 17/12/2027	\$12.092.088,00	\$11.905.306,56	\$11.760.000,00	\$11.919.131,52
5	FortiWeb 400E Serial: FV400ETA22000156 Periodo Licencia: 18/12/2026 a 17/12/2027	\$47.440.655,00	\$46.707.856,16	\$46.137.777,78	\$46.762.096,31
6	FortiSIEM Serial: FSMP000000000521 Periodo Licencia: 18/12/2026 a 17/12/2027	\$27.889.645,00	\$27.458.844,19	\$27.123.703,70	\$27.490.730,96
VALOR TOTAL		\$122.611.004,00	\$120.717.078,91	\$119.243.703,70	\$120.857.262,19

De esta manera se establece como presupuesto oficial estimado la suma de hasta **CIENTO VEINTE MILLONES OCHOCIENTOS CINCUENTA Y SIETE MIL DOSCIENTOS SESENTA Y DOS PESOS CON DIECINUEVE CENTAVOS M/CTE (\$120.857.262,19)** incluido el IVA y demás impuestos a que haya lugar, para la para la Renovación de infraestructura, soporte y garantía de licenciamiento de equipos de seguridad perimetral, descritos en el **ANEXO 1. ESPECIFICACIONES TÉCNICAS**.

Teniendo en cuenta que el proceso se adelantará mediante la modalidad de selección abreviada por subasta inversa electrónica, cuyo criterio de adjudicación corresponde al menor precio, se considera procedente adoptar el valor anteriormente indicado como base para el presupuesto oficial, por cuanto representa un valor competitivo, técnicamente viable y dentro del comportamiento general del mercado.

En este sentido, el valor definitivo del contrato será ajustado acorde con el valor resultante en la selección abreviada por subasta inversa electrónica, el cual tiene tendencia a la baja.

CONCLUSIONES

Como resultado del presente análisis y tomando como referencia la muestra de contratos celebrados por entidades del sector público para la renovación de licenciamiento, soporte y garantía de soluciones de seguridad perimetral, se evidencia la necesidad de garantizar la continuidad operativa de la infraestructura tecnológica de la Agencia mediante la vigencia del licenciamiento y el acceso al soporte oficial del fabricante. Lo anterior permite disponer de actualizaciones de software y firmware, parches de seguridad, bases de datos de amenazas, mejoras funcionales y servicios de asistencia técnica especializada, así como disponer de las condiciones necesarias para atender oportunamente fallas, vulnerabilidades e incidentes que puedan afectar la operación de la infraestructura de seguridad.

Asimismo, el análisis realizado permite establecer que existe pluralidad de proveedores con capacidad técnica, operativa y comercial para atender los requerimientos definidos por la Agencia, incluyendo la renovación de las licencias, soporte especializado, garantía, mantenimiento y demás servicios asociados. De igual manera, la participación de canales autorizados y el respaldo de los respectivos fabricantes permiten garantizar la disponibilidad de los servicios y el acceso a los recursos oficiales requeridos durante la vigencia contractual.

En consecuencia, se determina que existe oferta suficiente en el mercado para atender la necesidad identificada por la Agencia, por lo que resulta técnica,

operativa y comercialmente viable adelantar el proceso de contratación bajo las condiciones establecidas en el presente estudio y sus anexos.

11. FUENTES DE INFORMACIÓN

Desde el punto técnico y de precios se realizó el sondeo de mercado mediante cotizaciones directas a los proveedores o canales directos que suministran los respectivos servicios en mención, como también el portal SECOP II en su plataforma transaccional donde las Entidades Estatales pueden hacer revisión de Procesos Históricos de Contratación en línea.

1. www.colombiacompra.gov.co/sites/cce_public/files/cce_documents/cce_guia_elaboracion_estudios.pdf
2. <https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-satelite/cuenta-satelite-de-las-tecnologias-de-la-informacion-y-las-comunicaciones-cstic>
3. https://ontic.mintic.gov.co/857/articles-440020_boletin.pdf
4. https://www.colcert.gov.co/800/articles-433510_recurso_1.pdf
5. https://www.andi.com.co/Uploads/Balance%202025%20y%20Perspectivas%202026%20_639056474172585923.pdf
6. <https://www.worldbank.org/en/publication/global-economic-prospects>
7. <https://www.imf.org/en/publications/weo>
8. <https://www.cepal.org/es/temas/agenda-digital>
9. <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025>
10. <https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-nacionales-trimestrales/pib-informacion-tecnica>
11. <https://www.dane.gov.co/files/operaciones/IPC/jul2026/cp-IPC-jul2026.pdf>

Cordialmente,



JENNY YASMIN PINZON PERILLA

Jefe Oficina Asesora de Sistemas y Tecnologías de Información (E)

Proyectó: Jeison Yamit Gómez Camacho
Luis Marcelo Rentería Asprilla