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 de la suscripción y/o licenciamiento de la solución de protección de datos que permite realizar copias de seguridad, recuperación y replicación en entornos físicos, virtuales y en la nube para la Agencia.

A continuación, se presenta el antecedente de las adquisiciones realizadas por la Agencia en materia de licenciamiento y soporte, así como la evolución cronológica de los contratos suscritos para las renovaciones y contrataciones de soporte asociadas a dicha solución de protección de datos:

NÚMERO DE CONTRATO	NOMBRE CONTRATISTA	OBJETO
216-2019	REDCOMPUTO LIMITADA	Adquirir una Solución de Sistema de Backup y Sistema de Almacenamiento que incluya su respectivo licenciamiento y los Servicios de Implementación y puesta en funcionamiento en la Entidad según especificaciones técnicas
098-2022	COLOMBIANA DE SERVICIOS TECNOLOGICOS S.A.S	Renovación de los Servicios de Soporte y Garantía de los Productos de Licencias de Backups y Equipos de Infraestructura Tecnológica.

151-2023	COLOMBIANA DE SERVICIOS TECNOLÓGICOS S.A.S.	Renovación de soporte y garantía de equipo de infraestructura y renovación de soporte y garantía de licenciamiento de software de Backups.
250-2025	SUMINISTROS OBRAS Y SISTEMAS	Renovación de soporte y garantía de licenciamiento de la herramienta Veeam Backups de la Agencia Nacional de Defensa Jurídica del Estado.

Es así, como a través de este último contrato la Agencia adquirió la renovación del soporte y garantía para equipos de infraestructura marca Dell, así como la renovación del soporte y garantía del licenciamiento del software de respaldo Veeam hasta el 30 de diciembre de 2026.

Estas suscripciones son esenciales para garantizar la continuidad del negocio, la resiliencia operativa y la disponibilidad de la información institucional, ya que permiten la protección integral, recuperación oportuna y trazabilidad de los datos críticos que soportan los sistemas misionales, estratégicos y de apoyo de la Agencia. La solución Veeam constituye un componente fundamental dentro de la arquitectura de respaldo y recuperación ante desastres (DRP) definida por la OASTI, asegurando la integridad, confidencialidad y disponibilidad de los activos de información conforme a los principios de la Política de Seguridad Digital del Estado (CONPES 3975 de 2019) y las directrices establecidas en el Modelo de Seguridad y Privacidad de la Información – MSPI del MinTIC.

En concordancia con los lineamientos del Decreto 620 de 2020, que establece la necesidad de implementar mecanismos que garanticen la continuidad de la operación ante eventos de indisponibilidad tecnológica, la renovación del soporte y garantía de la herramienta Veeam Backup & Replication se constituye en una medida preventiva indispensable para mitigar riesgos de pérdida de información, asegurar la recuperación rápida de entornos virtualizados, y mantener la interoperabilidad de los sistemas institucionales en entornos físicos, virtuales y en la nube híbrida de la Entidad.

La OASTI, como responsable de la administración, soporte y operación de los servicios tecnológicos de la Agencia, ha identificado que la solución de respaldo Veeam permite ejecutar estrategias de copias de seguridad incrementales, replicación entre nodos de almacenamiento y restauración granular de máquinas virtuales, archivos y bases de datos, lo cual resulta crítico para mantener la disponibilidad continua de los servicios institucionales tales como el Sistema de Gestión de la Defensa Jurídica (SGDEA), las plataformas de correo electrónico, bases de datos administrativas y los sistemas que soportan la defensa jurídica del Estado.

Asimismo, la renovación del soporte y garantía garantiza el acceso a actualizaciones, parches de seguridad, soporte técnico especializado y acompañamiento del fabricante, condiciones indispensables para mantener la solución en cumplimiento con los estándares internacionales de gestión de continuidad (ISO 22301) y de seguridad de la información (ISO/IEC 27001 y 27002). El no contar con dicho soporte podría exponer a la Agencia a riesgos operativos y reputacionales derivados de fallas no atendidas, vulnerabilidades sin corregir o demoras en la restauración de información crítica.

En este sentido, la necesidad que se pretende satisfacer con el presente proceso de contratación es garantizar la operación continua y segura de los servicios tecnológicos institucionales, mediante la renovación del soporte y garantía de la herramienta Veeam Backup & Replication, asegurando la gestión eficiente de los respaldos, la recuperación ante incidentes y el cumplimiento normativo en materia de seguridad digital y protección de datos, en armonía con los objetivos estratégicos de la Agencia Nacional de Defensa Jurídica del Estado y las políticas nacionales de transformación digital y seguridad de la información.

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 dedicado al soporte y garantía de la herramienta Veeam Backup.

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 2° del literal a) del numeral 2 del artículo 2° de la Ley 1150 de 2007 y en los artículos 2.2.1.2.1.2.11 y siguientes del Decreto 1082 de 2015, razón por la cual se adelantará el proceso bajo la modalidad de Selección Abreviada mediante Subasta Inversa Electrónica.

La presente contratación se encuentra incluida en el ítem 31 del Plan Anual de Adquisiciones para el año 2026.

2. OBJETO

Renovación de soporte y garantía de licenciamiento de la herramienta VEEAM BACKUPS de la Agencia Nacional de Defensa Jurídica del Estado.

3. CLASIFICACIÓN UNSPSC

CLASIFICADOR	SEGMENTO	FAMILIA	CLASES
Código UNSPSC **43233700** Software de administración de sistemas.	[43] Tecnología de la información, telecomunicaciones.	[23] Software.	[37] Software de administración de sistemas
Código UNSPSC **43232900** Software para trabajo en redes.	[43] Difusión de Tecnologías de información y telecomunicaciones.	[23] Software.	[29] Software para trabajo en redes.
Código UNSPS **43233400** Software de controladores de dispositivos y utilidades.	[43] Difusión de Tecnologías de información y telecomunicaciones.	[23] Software.	[34] Software de controladores de dispositivos y utilidades
Código UNSPS **81111800** Servicios de Sistemas Administración de Componentes de Sistemas.	[81] Servicios basados en Ingeniería, Investigación y Tecnología.	[11] Servicios Informáticos	[18] Servicios de Sistemas Administración de Componentes de Sistemas.

4. ASPECTOS GENERALES[1]

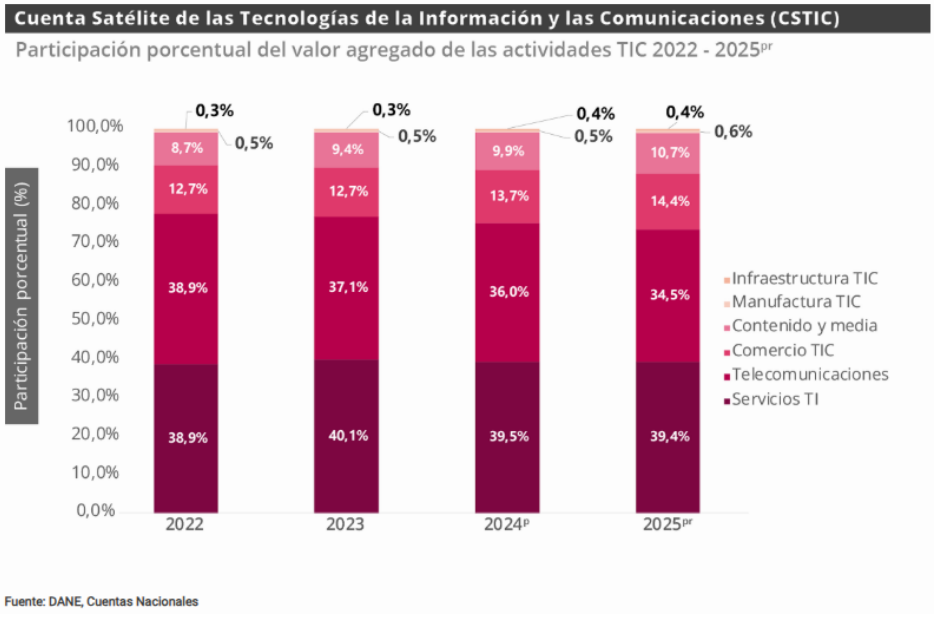
El sector de Tecnologías de la Información y las Comunicaciones (TIC) en Colombia constituye uno de los pilares estratégicos para el desarrollo económico, la innovación y la transformación digital de las entidades públicas y privadas. En los últimos años, el país ha avanzado significativamente en la 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.

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

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.

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).



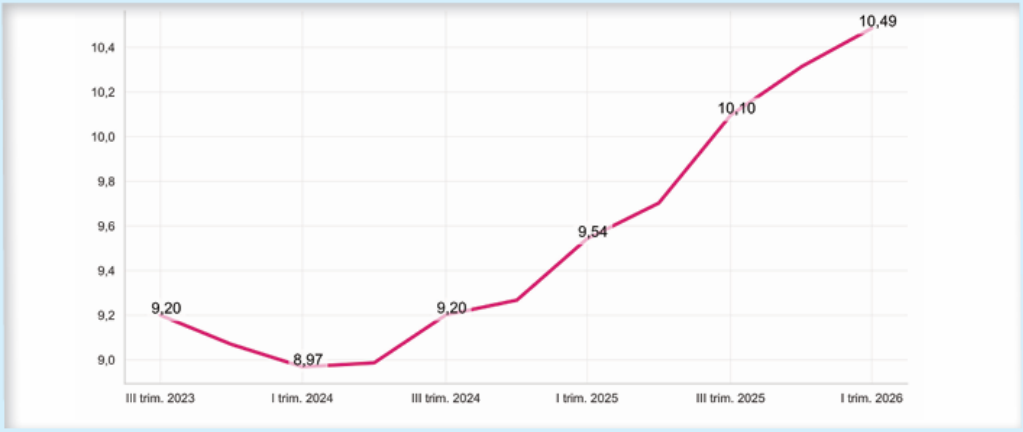
De manera complementaria, el DANE reconoce dentro de la Clasificación Central de Productos los servicios de consultoría en tecnologías de la información,

[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

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 accesos [3].

Accesos fijos a Internet (millones)[7]

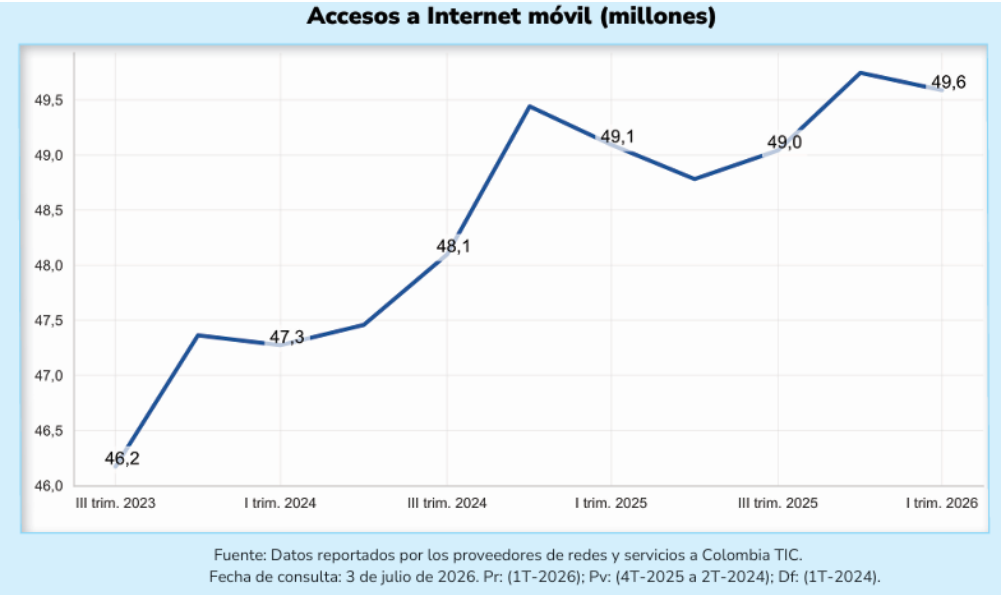


Fuente: Datos reportados por los proveedores de redes y servicios a Colombia TIC.
Fecha de consulta: 3 de julio de 2026. Pr: (1T-2026); Pv: (4T-2025 a 2T-2024); Df: (1T-2024).

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



Fuente: Datos reportados por los proveedores de redes y servicios a Colombia TIC.
Fecha de consulta: 3 de julio de 2026. Pr: (1T-2026); Pv: (4T-2025 a 2T-2024); Df: (1T-2024).

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 ColCERT[4] 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 2026[5], 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 de soporte y garantía de licenciamiento de la herramienta VEEAM BACKUPS, 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 Mundial[6] y el Fondo Monetario Internacional[7], 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 tecnológica[8].

La industria de la ciberseguridad se encuentra en un momento crucial, lo que refleja la evolución general de los sectores de TI y tecnología. Esta transformación está impulsada por la creciente dependencia de la infraestructura digital y la apremiante necesidad de contrarrestar ciberamenazas sofisticadas, en línea con las tendencias actuales de ciberseguridad. Tecnologías emergentes como la inteligencia artificial, el aprendizaje automático y el análisis de big data se encuentran entre las tendencias emergentes en ciberseguridad que no solo mejoran las capacidades de las soluciones de ciberseguridad, sino que también introducen nuevas complejidades. Las organizaciones se adaptan a este panorama dinámico para proteger sus activos digitales y garantizar una seguridad robusta de los datos. A medida que la transformación digital se acelera en las industrias y los gobiernos, la necesidad de contar con medidas de seguridad robustas y adaptables, en línea con las tendencias de la industria de la ciberseguridad, nunca ha sido tan crucial[9].

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

[8] https://www.cepal.org/es/temas/agenda-digital

[9] https://www.mordorintelligence.com/industry-reports/cyber-security-market

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 privadas[10].

En este contexto, las inversiones en infraestructura tecnológica, continuidad operativa, protección de la información y soluciones especializadas de seguridad adquieren una importancia estratégica para garantizar la disponibilidad, integridad, confidencialidad y eficiencia de los servicios institucionales. En particular, las soluciones de licenciamiento de la herramienta Veeam Backup & Replication permite proteger datos críticos de empresas mediante copias de seguridad rápidas y confiables, restauraciones instantáneas y replicación eficiente de sistemas completos o archivos individuales. Su plataforma centralizada facilita la gestión de backups, asegurando que los datos estén disponibles y recuperables ante fallos, errores humanos, ataques de ransomware y otras amenazas cibernéticas. Su adecuada operación, actualización, mantenimiento y soporte resultan esenciales para fortalecer las capacidades de prevención, detección y respuesta de la Entidad frente a un entorno de amenazas cibernéticas en constante evolución, contribuyendo a la protección de los activos de información y a la continuidad de los servicios institucionales.

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 los sistemas de información, dispositivos tecnológicos, servidores, aplicaciones y plataformas

[10] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025

digitales ha generado una mayor necesidad de fortalecer los mecanismos de protección de los activos tecnológicos y de la información institucional. En particular, las soluciones de Veeam Backup & Replication han adquirido un papel estratégico como solución integral de respaldo, recuperación y replicación de datos para entornos virtuales, físicos y en la nube. Estas capacidades resultan especialmente relevantes en entidades públicas y privadas que gestionan información sensible, confidencial o crítica para el desarrollo de sus actividades.

La expansión de los servicios en la nube, el trabajo remoto, la utilización de dispositivos móviles y equipos portátiles, la interconexión de múltiples plataformas y el crecimiento de los servicios y aplicaciones digitales han transformado los modelos tradicionales de gestión y protección de la información. En consecuencia, las organizaciones requieren soluciones capaces de garantizar la disponibilidad, integridad y recuperación de la información alojada en ambientes locales, distribuidos, híbridos y basados en la nube, mediante mecanismos centralizados que permitan administrar las políticas de respaldo, monitorear el estado de las copias de seguridad, identificar eventos que puedan comprometer la información y responder oportunamente ante incidentes que afecten la continuidad de los servicios tecnológicos.

De manera paralela, el crecimiento y sofisticación de las amenazas cibernéticas ha incrementado los riesgos asociados con la pérdida, corrupción, cifrado, alteración o indisponibilidad de la información institucional. Las organizaciones enfrentan escenarios relacionados, entre otros, con ransomware, malware, errores humanos, eliminación accidental de información, fallas de hardware, indisponibilidad de infraestructura, vulnerabilidades de software, ataques dirigidos y otros eventos que pueden comprometer los sistemas de información y los datos que soportan los procesos institucionales. Este escenario ha impulsado la evolución de las estrategias tradicionales de respaldo hacia plataformas especializadas que incorporan capacidades avanzadas de protección de datos, recuperación ante incidentes, administración centralizada, automatización, monitoreo, verificación de copias y recuperación ante desastres.

Asimismo, la creciente generación, procesamiento, almacenamiento y transferencia de información digital ha incrementado la necesidad de implementar mecanismos que permitan garantizar su disponibilidad y recuperación ante eventos que puedan ocasionar pérdida o indisponibilidad. En este contexto, las soluciones de respaldo y recuperación permiten establecer políticas y controles sobre la protección de la información, mediante la generación, administración, conservación y recuperación de copias de seguridad de servidores, máquinas

virtuales, aplicaciones, bases de datos, estaciones de trabajo y demás activos tecnológicos. La implementación de mecanismos adecuados de respaldo contribuye a fortalecer la resiliencia tecnológica de la Agencia y a reducir los riesgos asociados con incidentes de seguridad, fallas operativas, errores humanos y eventos que puedan afectar la continuidad de los servicios.

De igual manera, las estrategias modernas de protección de datos requieren capacidades permanentes de monitoreo, análisis y recuperación frente a eventos que puedan afectar los equipos de cómputo, servidores, máquinas virtuales y demás activos tecnológicos. En este contexto, las soluciones de backup han evolucionado hacia plataformas que permiten centralizar la administración de políticas de respaldo, recopilar información sobre los trabajos ejecutados, verificar el estado de las copias, identificar fallas o comportamientos anómalos, generar alertas y facilitar la recuperación de la información ante diferentes escenarios de pérdida o indisponibilidad.

La incorporación de mecanismos especializados de protección frente a ransomware y recuperación ante incidentes permite, adicionalmente, fortalecer las capacidades institucionales para restablecer oportunamente los servicios tecnológicos y la información afectada. En este sentido, resulta fundamental disponer de esquemas de respaldo que contemplen mecanismos de protección de las copias, control de acceso, administración de repositorios y capacidades de recuperación que permitan reducir el impacto de eventos que puedan comprometer la disponibilidad o integridad de los datos institucionales.

La evolución del mercado también ha generado una mayor demanda de servicios asociados al ciclo de vida de las soluciones de respaldo y recuperación, incluyendo licenciamiento o suscripción, actualizaciones de software, mantenimiento, soporte técnico especializado, asistencia, administración de la solución, monitoreo, servicios de recuperación, protección de repositorios, transferencia de conocimientos y acompañamiento técnico. En consecuencia, la adquisición o renovación de soluciones de backup no se limita a disponer de un software instalado en los equipos o servidores, sino que requiere mantener vigentes las capacidades de respaldo, recuperación, actualización, monitoreo y soporte durante el periodo contratado, con el fin de responder adecuadamente a los riesgos asociados con la pérdida o indisponibilidad de la información.

En este sentido, la continuidad del licenciamiento y de los servicios asociados a la solución Veeam Backup resulta fundamental para mantener los mecanismos de protección de datos implementados por la Entidad, reducir la exposición frente a

eventos que puedan ocasionar pérdida o indisponibilidad de información, fortalecer las capacidades de recuperación y contribuir a la continuidad de los servicios tecnológicos que soportan los procesos misionales y administrativos.

En materia de talento especializado, la creciente complejidad de las infraestructuras tecnológicas, los ambientes virtualizados, los servicios en la nube y las estrategias de protección de datos han incrementado la necesidad de contar con profesionales capacitados en administración de plataformas de backup, virtualización, almacenamiento, recuperación ante desastres y gestión de incidentes tecnológicos. La disponibilidad de personal con conocimientos y certificaciones otorgadas por los fabricantes constituye un factor relevante para garantizar una adecuada implementación, configuración, actualización, mantenimiento, monitoreo y recuperación de la información protegida.

De igual manera, los fabricantes de soluciones de protección de datos han fortalecido sus modelos de atención y soporte mediante esquemas que combinan asistencia especializada, actualización permanente de las plataformas, acceso a nuevas funcionalidades, mejoras de seguridad, mecanismos de monitoreo, herramientas de diagnóstico y escalamiento de incidentes hacia niveles avanzados de soporte. Estos mecanismos permiten que las organizaciones mantengan sus tecnologías de respaldo alineadas con la evolución de sus infraestructuras y dispongan oportunamente de nuevas versiones, actualizaciones de seguridad, mejoras funcionales y mecanismos de protección desarrollados por los fabricantes.

En este contexto, las organizaciones públicas y privadas requieren mantener actualizadas sus soluciones de respaldo y recuperación de información y garantizar su adecuada operación, particularmente aquellas destinadas a proteger servidores, máquinas virtuales, bases de datos, aplicaciones y demás activos tecnológicos que soportan servicios institucionales y sistemas de información. La continuidad del licenciamiento y de los servicios asociados de soporte, actualización y asistencia técnica permite preservar las capacidades de protección y recuperación implementadas, reducir la exposición frente a fallas y eventos que puedan comprometer la información y garantizar el acceso a las actualizaciones, funcionalidades de protección, herramientas de administración, mecanismos de recuperación y demás capacidades desarrolladas por el fabricante.

En consecuencia, el mercado de soluciones de backup y recuperación se caracteriza actualmente por una oferta de servicios integrales que combina licenciamiento o suscripción, protección de ambientes físicos, virtuales y en la nube, respaldo de servidores y aplicaciones, administración centralizada,

monitoreo continuo, protección frente a ransomware, verificación de copias, recuperación ante desastres, soporte especializado, asistencia técnica y servicios asociados a la gestión del ciclo de vida de las soluciones. Esta dinámica evidencia la importancia de contar con esquemas de renovación y soporte que permitan garantizar la continuidad de las capacidades de respaldo, protección y recuperación de la información institucional frente a un entorno tecnológico y de amenazas en constante evolución.

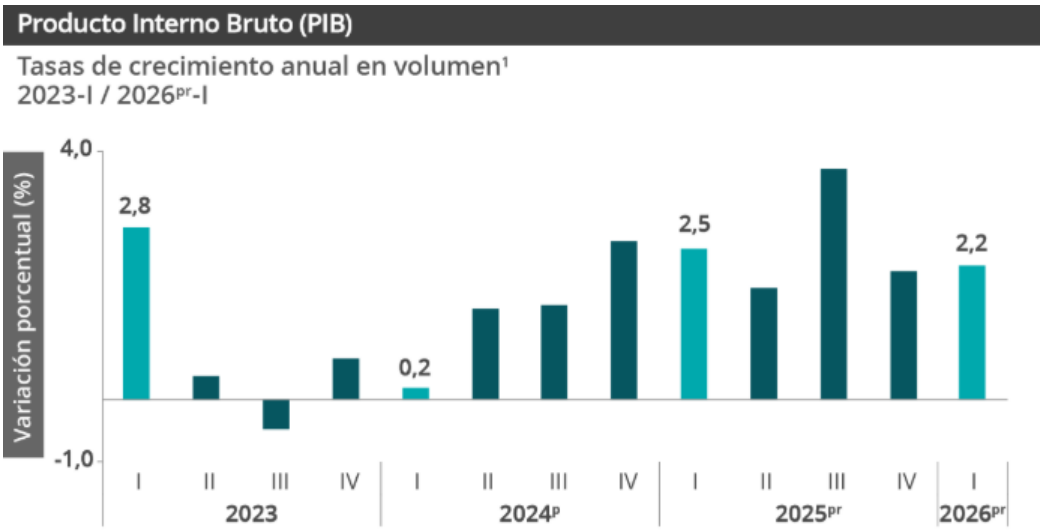
Por lo anterior, la renovación del licenciamiento y de los servicios asociados a Veeam Backup permite mantener operativas las capacidades institucionales de respaldo y recuperación, asegurar la protección de la información crítica y fortalecer la continuidad de los servicios tecnológicos, reduciendo el impacto potencial derivado de fallas de infraestructura, errores humanos, ataques de ransomware, pérdida de información, indisponibilidad de sistemas y demás eventos que puedan afectar los activos de información de la Entidad.

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 2025[11].

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



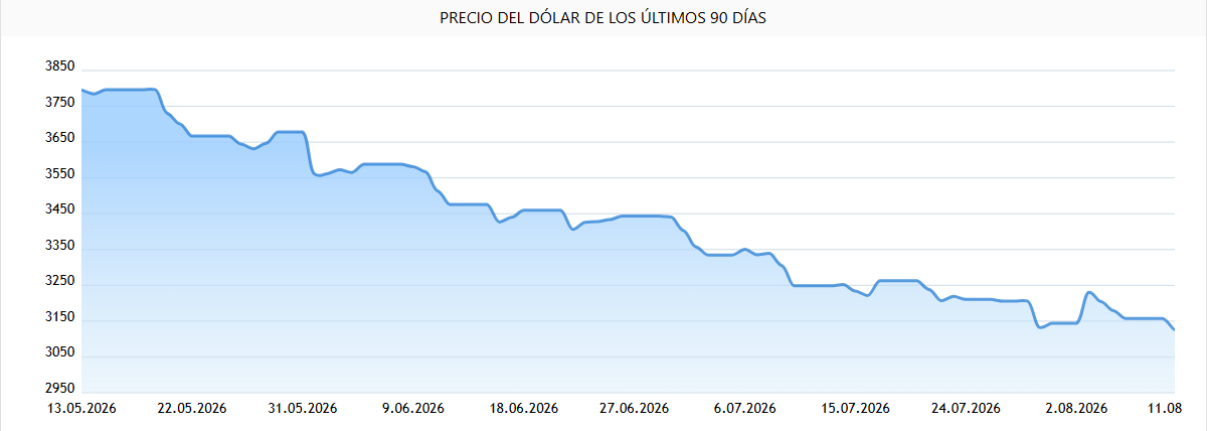
Las actividades económicas que más contribuyen a la dinámica del valor agregado son:

- 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).

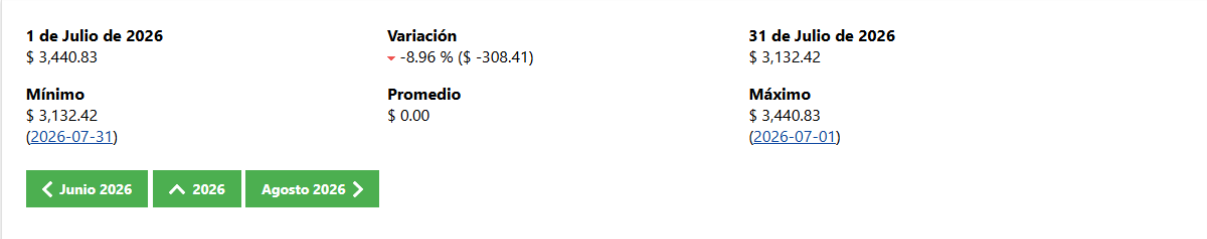
4.1.2 Tasa Representativa del Mercado (TRM – Peso por dólar)

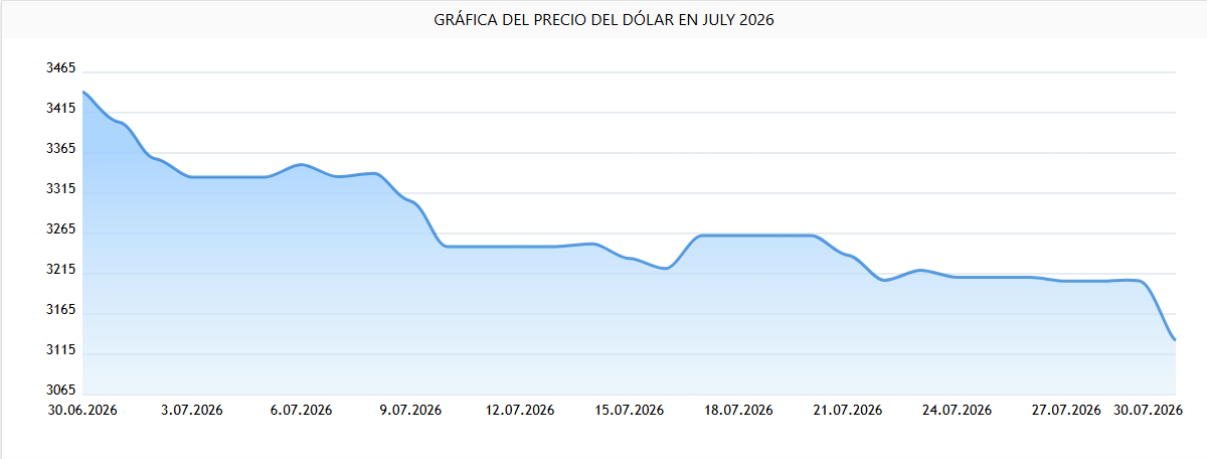
La TRM es la cantidad de pesos colombianos por un dólar de los Estados Unidos. La TRM se calcula con base en las operaciones de compra y venta de divisas entre intermediarios financieros que transan en el mercado cambiario colombiano, con cumplimiento el mismo día cuando se realiza la negociación de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

➢ 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.

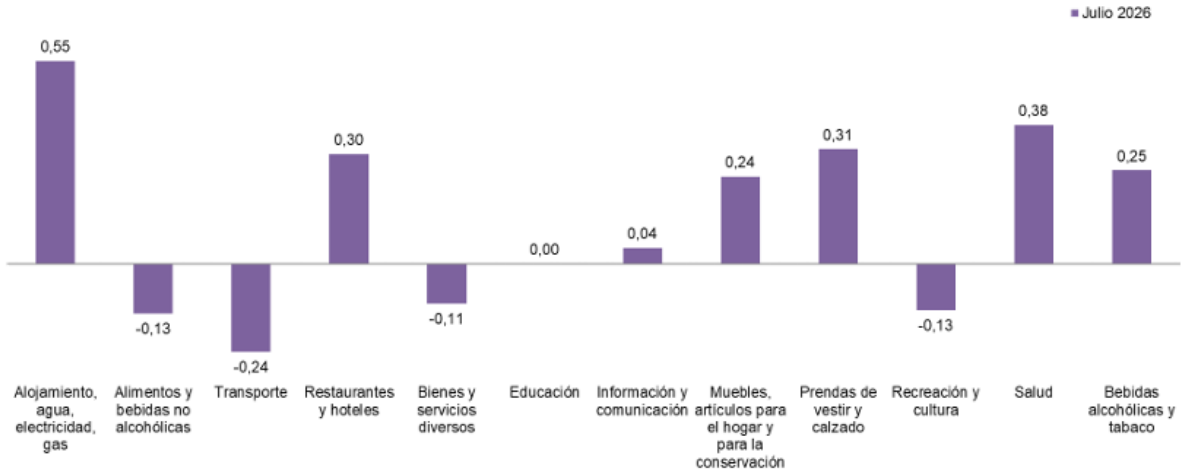
Variación mensual, año corrido y anual
Total nacional
2025 - 2026 (julio)

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%).[12]

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).

[12] 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 implementar mecanismos que permitan garantizar su disponibilidad y recuperación ante eventos que puedan ocasionar pérdida o indisponibilidad. 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 generado nuevos desafíos para la protección de los activos tecnológicos y de la información. Este escenario requiere mecanismos de seguridad capaces de operar en ambientes distribuidos, proporcionar visibilidad sobre los dispositivos, servidores y eventos de seguridad, 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 soluciones de respaldo y recuperación de información, caracterizadas por la evolución de los mecanismos tradicionales de backup hacia plataformas integrales que incorporan capacidades de protección de ambientes físicos, virtuales y en la nube, administración centralizada, automatización de tareas de respaldo, monitoreo, verificación de copias, recuperación granular y protección frente a eventos como ransomware, fallas de infraestructura, errores humanos y pérdida o corrupción de información. De manera complementaria, los fabricantes han fortalecido los esquemas de licenciamiento o suscripción y los servicios asociados, incorporando actualizaciones permanentes de las plataformas, nuevas funcionalidades, mecanismos de protección de los repositorios, soporte técnico especializado, asistencia, monitoreo y servicios de recuperación.

Esta evolución implica que las organizaciones no solo requieren disponer de soluciones tecnológicas de respaldo, sino garantizar su actualización, soporte y adecuada operación durante todo su ciclo de vida. La continuidad del licenciamiento y el acceso a las actualizaciones, funcionalidades de protección y servicios de soporte del fabricante permiten mantener vigentes las capacidades de respaldo y recuperación, atender oportunamente fallas o eventos que puedan comprometer la información, fortalecer la protección de las copias de seguridad y facilitar la recuperación ante incidentes, contribuyendo a reducir los riesgos asociados con la pérdida, alteración o indisponibilidad de la información y de los servicios tecnológicos.

Por lo anterior, la inversión en infraestructura digital, protección de la información y soluciones especializadas de respaldo y recuperación 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 de los riesgos tecnológicos y de ciberseguridad. En este contexto, la renovación de la solución Veeam Backup, junto con los servicios de soporte y asistencia requeridos, constituye un mecanismo necesario para preservar las capacidades de protección, respaldo y

recuperación implementadas por la Entidad y mantener un nivel adecuado de disponibilidad, integridad y resiliencia sobre sus activos tecnológicos y de información.

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 tecnológica, ciberseguridad, protección de la información, 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, el trabajo remoto y el incremento y sofisticación 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, las soluciones de respaldo y recuperación de información comprenden un conjunto de tecnologías destinadas a proteger servidores, máquinas virtuales, aplicaciones, bases de datos, estaciones de trabajo y demás activos tecnológicos frente a eventos que puedan ocasionar pérdida, corrupción, alteración o indisponibilidad de la información. Estas soluciones han evolucionado desde mecanismos tradicionales de generación de copias de seguridad hacia plataformas integrales que incorporan capacidades de administración centralizada, automatización de respaldos, monitoreo continuo, verificación de copias, recuperación granular, protección de repositorios y recuperación ante incidentes como ransomware, fallas de infraestructura y errores humanos.

En consecuencia, la adquisición o renovación de soluciones de respaldo y recuperación debe considerar no solamente las funcionalidades técnicas de protección de datos, sino también los servicios asociados a su ciclo de vida, tales como la renovación del licenciamiento o suscripción, actualización de la plataforma, acceso a nuevas funcionalidades, aplicación de actualizaciones y parches de seguridad, soporte técnico especializado, asistencia, monitoreo, administración, verificación de respaldos, recuperación ante incidentes y transferencia de conocimientos. Estos elementos resultan fundamentales para conservar las capacidades de protección y recuperación de los activos tecnológicos y de información de la Entidad, mantenerlas alineadas con la evolución de la infraestructura tecnológica y de los riesgos de seguridad, y aprovechar las mejoras y mecanismos de protección desarrollados por 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 la solución de Veeam Backup actualmente implementada 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 y servicios de asistencia y soporte:

Producto	Cantidad	Tiempo de renovación
Vend Part No: P-ADVVUL-0I-SU1AR-00 **Support ID:** 03886533 (70 instancias) **Fecha de finalización vigente:** 31/12/2026 **Detalle:** Veeam Data Platform Advanced Universal Subscription License. Includes Enterprise Plus Edition features. 1 Year Renewal	1	1 año

Subscription Upfront Billing & Production (24/7) Support. 10 instance pack. Public Sector.		
Vend Part No: V-ADVPLS-VS-PP1AR-00 **Support ID:** 03886533 (20 sockets) **Fecha de finalización del soporte vigente:** 30/12/2026 **Detalle:** 1 Year of Production (24/7) maintenance renewal for Veeam Data Platform Advanced Enterprise Plus	1	1 año

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 servicios asociados a la solución Veeam Backup constituye una medida necesaria para preservar las capacidades de respaldo, protección y recuperación de los activos tecnológicos y de información de la Agencia, así como para contribuir a la continuidad, disponibilidad, integridad y adecuada operación de los servicios institucionales.

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

1. Garantizar la continuidad de las capacidades de respaldo y recuperación de los servidores, máquinas virtuales, aplicaciones, bases de datos y demás activos tecnológicos de la Agencia, mediante la permanencia de la solución Veeam Backup, como componente fundamental para proteger la información frente a eventos que puedan ocasionar su pérdida, corrupción, alteración o indisponibilidad.
2. Mantener vigente el licenciamiento y los servicios de soporte del fabricante, permitiendo a la Agencia acceder durante la vigencia contratada a las actualizaciones de software, nuevas funcionalidades, mejoras de seguridad, herramientas de administración y demás recursos oficiales necesarios para mantener actualizadas las capacidades de respaldo y recuperación.
3. Contar con soporte técnico especializado y atención oportuna de incidentes, que permita gestionar fallas, alertas, errores en los procesos de respaldo y recuperación, requerimientos de configuración y demás situaciones que puedan afectar la operación de la solución, incluyendo el escalamiento al fabricante o a los niveles especializados de soporte cuando se requiera.
4. Mantener actualizada y adecuadamente configurada la solución de respaldo, mediante la aplicación de actualizaciones, políticas y buenas prácticas, revisión de configuraciones, verificación de los trabajos de backup y demás

actividades de aseguramiento que contribuyan a optimizar su funcionamiento y reducir los riesgos asociados con fallas en los procesos de respaldo o recuperación.

5. Fortalecer las capacidades institucionales de protección y recuperación frente a incidentes tecnológicos y de ciberseguridad, mediante la disponibilidad de herramientas y servicios especializados que permitan realizar copias de seguridad, monitorear su ejecución, verificar su integridad y facilitar la recuperación de la información ante eventos como ransomware, fallas de infraestructura, errores humanos, eliminación accidental de información u otros incidentes que puedan comprometer los activos tecnológicos.
6. Fortalecer la protección de las copias de seguridad y la resiliencia de la información, mediante mecanismos que permitan administrar y controlar los repositorios de respaldo, verificar la disponibilidad de las copias y establecer condiciones adecuadas para su recuperación, reduciendo el riesgo de pérdida o indisponibilidad de la información institucional ante eventos que afecten la infraestructura tecnológica.
7. Reducir los riesgos asociados a la obsolescencia, pérdida de soporte o falta de actualización de la solución, garantizando la continuidad de su ciclo de vida tecnológico y el acceso a los servicios, actualizaciones, mejoras y mecanismos de protección proporcionados por el fabricante durante la vigencia contractual.

En consecuencia, contar con el licenciamiento y los servicios de soporte vigentes de la solución Veeam Backup permite mantener las capacidades institucionales de respaldo y recuperación de la información, disponer oportunamente de actualizaciones y nuevas funcionalidades, acceder al acompañamiento técnico especializado y fortalecer la capacidad de la Agencia para prevenir y atender eventos que puedan afectar la disponibilidad e integridad de la información y la continuidad de los servicios tecnológicos.

Lo anterior contribuye a preservar la confidencialidad, integridad y disponibilidad de la información institucional, así como a reducir la exposición de la Agencia frente a riesgos asociados con la pérdida, corrupción, alteración o indisponibilidad de la información y de los activos tecnológicos que soportan su operación.

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-043-2026. 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.

La renovación del soporte, mantenimiento y actualización del licenciamiento perpetuo de la plataforma Veeam Backup & Replication objeto del presente proceso se adquieren a través de proveedores en Colombia en razón a que los fabricantes realizan su distribución a través de los denominados partners que actúan como distribuidores autorizados por los mismos para prestar el servicio de venta y soporte de software, en este caso de los productos solicitados en el anexo técnico.

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 la renovación del soporte, mantenimiento y actualización del licenciamiento 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 la solución actualmente implementada, bajo las condiciones técnicas y de servicio establecidas en el presente proceso de contratación.

No.	PROVEEDOR	NIT
1	COLSISTEC SAS	800249315
2	EYC INGENIEROS SAS	900024202
3	NETMASK SAS	900590270
4	SUMINISTROS OBRAS Y SISTEMAS	900261209
5	REDCOMPUTO	830016004
6	GLOBAL TECHNOLOGY SERVICES GTS S.A.	830060020
7	UT B2B GLOBAL	901238826
8	LATTITUDE CORP SAS	900818856
9	INTER MILLENIUM SAS	830049538
10	C&S TECNOLOGIA S.A	811000242
11	ROYAL TECH GROUP SAS	901394655
12	EXPERTOS TECNOLOGICOS SAS	900428395
13	ELECTROCOM SAS	800229279
14	IDEALOGIC SAS	901157921
15	INNATEL S.A.S BIC	900171749
16	INFORMACION LOCALIZADA S.A.S	830062674

Estas empresas cuentan con la capacidad y experiencia para prestar los servicios requeridos de renovación del licenciamiento de la plataforma Veeam Backup & Replication, ofreciendo soluciones oportunas, eficaces y de calidad, de acuerdo con las necesidades y requerimientos técnicos de sus clientes.

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 GESTIÓN DE RIESGOS Y CAMBIO CLIMÁTICO - IDIGER	ADQUIRIR LA RENOVACIÓN DE LICENCIAMIENTO VEEAM BACKUP PARA LOS EQUIPOS QUE RESGUARDAN LA INFORMACIÓN NECESARIA PARA EL CUMPLIMIENTO DE LAS METAS DEL IDIGER	SELECCIÓN ABREVIADA SUBASTA INVERSA	IDIGER-SA-SI-003-2026	2026	$208.918.599
FABRICA DE LICORES Y ALCOHOLES DE ANTIOQUIA	RENOVACIÓN DE LA SUSCRIPCIÓN DE LICENCIAS DE MICROSOFT 365 Y VEEAM BACKUP CON SOPORTE INCLUIDO, PARA LA FÁBRICA DE LICORES Y ALCOHOLES DE ANTIOQUIA EICE	RÉGIMEN ESPECIAL	101112	2026	$225.846.695
INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA	CONTRATAR EL ARRENDAMIENTO DE LICENCIAS DEL SOFTWARE VEEAM BACKUP, CON EL FIN DE GARANTIZAR LA DISPONIBILIDAD, INTEGRIDAD, SEGURIDAD Y RESPALDO DE LA INFORMACIÓN CRÍTICA DE LA INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA, CONTRIBUYENDO A LA CONTINUIDAD OPERATIVA DE SUS SERVICIOS TECNOLÓGICOS.	MÍNIMA CUANTÍA	SMC2026015	2026	$9.758.000
SUPERVIGILANCIA - MD	ADQUIRIR EL LICENCIAMIENTO Y SOPORTE TÉCNICO DE LA HERRAMIENTA DE RESPALDO, RECUPERACIÓN Y REPLICACIÓN VEEAM BACKUP PARA LA SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA, EN EL MARCO DEL PROYECTO DE INVERSIÓN	MÍNIMA CUANTÍA	MC-005-2026	2026	$ 33.462.800
FONDO NACIONAL AMBIENTAL - ANLA	FORTALECER LA PLATAFORMA DE GESTIÓN DE COPIAS DE RESPALDO VEEAM BACKUP MEDIANTE	SELECCIÓN ABREVIADA SUBASTA INVERSA	SUBASTA INVERSA NO. 031 DE 2025	2025	$ 889.040.000

	ADQUISICIÓN Y RENOVACIÓN DEL LICENCIAMIENTO POR SUSCRIPCIÓN DE VEEAM BACKUP, ADEMÁS DE RENOVACIÓN DE LA GARANTÍA DE FABRICA DEL EQUIPO DE ALMACENAMIENTO DE RESPALDOS Y LA PROVISIÓN DE SERVICIOS DE SOPORTE ESPECIALIZADO DE LA HERRAMIENTA DE ALMACENAMIENTO DE BACKUPS DE LA AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES - ANLA				
INSTITUTO DISTRITAL PARA LA PROTECCIÓN DE LA NIÑEZ Y LA JUVENTUD - IDIPRON*	ADQUIRIR LA SUSCRIPCIÓN Y SOPORTE DEL LICENCIAMIENTO PARA RESPALDO DE MÁQUINAS FÍSICAS Y VIRTUALES (VEEAM BACKUP) DEL IDIPRON.	SELECCIÓN ABREVIADA SUBASTA INVERSA	SASI-IDIPRON-2024-0009	2024	$ 37.268.090
UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACIÓN Y MANTENIMIENTO VIAL	RENOVACIÓN DEL SOPORTE Y ACTUALIZACIÓN DE LAS LICENCIAS DE VEEAM BACKUP PARA EJECUTAR COPIAS DE RESPALDO DE LA INFORMACIÓN DE LAS HERRAMIENTAS DE MICROSOFT 365 Y VEAM DATA PLATAFORM ESSEMTIALS PARA RESPALDAR LA INFORMACIÓN LA UAERMV	SELECCIÓN ABREVIADA SUBASTA INVERSA	UMV-SASI-014-2024	2024	$357.710.332
FONDO NACIONAL AMBIENTAL - ANLA	ADQUIRIR LICENCIAMIENTO POR SUSCRIPCIÓN PARA LA AMPLIACIÓN DE LA SOLUCIÓN DE GESTIÓN DE COPIAS DE RESPALDO VEEAM BACKUP, QUE INCLUYA UN SISTEMA DE PROPÓSITO ESPECÍFICO Y SEGURO PARA ALMACENAR LOS BACKUPS PARA LA AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES - ANLA	SELECCIÓN ABREVIADA SUBASTA INVERSA	SUBASTA INVERSA ELECTRONICA NO. 031 DE 2024	2024	$1.099.559.888

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

216-2019	SUBASTA INVERSA	REDCOMPUTO LIMITADA	Adquirir una Solución de Sistema de Backup y Sistema de Almacenamiento que incluya su respectivo licenciamiento y los Servicios de Implementación y puesta en funcionamiento en la Entidad según especificaciones técnicas	$ 799.308.228,36
098-2022	SUBASTA INVERSA ELECTRONICA	COLOMBIANA DE SERVICIOS TECNOLOGICOS S.A.S	Renovación de los Servicios de Soporte y Garantía de los Productos de Licencias de Backups y Equipos de Infraestructura Tecnológica.	$ 462.453.180
151-2023	SUBASTA INVERSA ELECTRONICA	COLOMBIANA DE SERVICIOS TECNOLÓGICOS S.A.S.	Renovación de soporte y garantía de equipo de infraestructura y renovación de soporte y garantía de licenciamiento de software de Backups.	$ 315.423.019
250-2025	SUBASTA INVERSA ELECTRONICA	SUMINISTROS OBRAS Y SISTEMAS	Renovación de soporte y garantía de licenciamiento de la herramienta Veeam Backups de la Agencia Nacional de Defensa Jurídica del Estado.	$166.285.320,05

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 70%
Razón de Cobertura de Intereses	Mayor o igual a 1.2 y/o indeterminada cuando su utilidad operacional sea positiva.
Capital de trabajo	Mayor o igual al 30% del presupuesto oficial

Capacidad Organizacional	
Rentabilidad del patrimonio	Mayor o igual a 2%
Rentabilidad del activo	Mayor o igual a 2%

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 MIPYMES[13].

Proveedores	NIT	Tamaño de la empresa
COLSISTEC SAS	800249315	Pequeña
EYC INGENIEROS SAS	900024202	Pequeña
NETMASK SAS	900590270	Mediana
SUMINISTROS OBRAS Y SISTEMAS	900261209	Mediana

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 soporte y garantía de licenciamiento de la herramienta VEEAM BACKUPS", 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 CUMPLIMENTO 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 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

[13] 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".

	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 recibió solo una (1) respuesta, así:

INDICADORES EMPRENDIMIENTO FEMENINO	SUMINISTROS OBRAS Y SISTEMAS
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
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
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
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

Como resultado del estudio realizado se encontró que dentro de las empresas del sector, solo SUMINISTROS OBRAS Y SISTEMAS señalo 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, una de los cuatro 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.

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 soporte y garantía de licenciamiento de la herramienta VEEAM BACKUPS, el 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 soporte y garantía de licenciamiento de la herramienta VEEAM BACKUPS, 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-043-2026, se logró identificar a cuatro (4) proveedores, así:



☆**Proceso : renovación del soporte del licenciamiento Veeam ...** (id.CO1.BDOS.10456463) EN ANÁLISIS

Solicitud de información a los Proveedores
SIP-ANDJE-043-2026 (En análisis) Pliegos

Unidad de contratación GRUPO DE GESTIÓN CONTRACTUAL
Ver Enlace

Contratar la renovación del soporte, mantenimiento y actualización del licenciamiento perpetuo de la plataforma Veeam Backup & Replication de la Agencia Nacional de Defensa Jurídica del Estado, garantizando la continuidad del soporte oficial del fabricante, el acceso a actualizaciones, parches de seguridad y asistencia técnica especializada durante la vigencia contractual.

(Zona horaria (UTC-05:00) Bogotá, Lima, Quito)
Fecha de presentación de ofertas 14/08/2026 11:59 PM - **Fecha de publicación** 10/07/2026 3:10 PM

PROVEEDORES

Interesados 10
2171
Competidores 4

LÍNEA DE TIEMPO

Fecha de publicación de concurso 10/07/2026
Plazo para solicitar aclaraciones 06/08/2026
Presentación de ofertas 14/08/2026

LISTA DE OFERTAS

Opciones

Referencia de oferta	Entidad	Presentada	Oferta
oferta Netmask SIP-ANDJE-043-2026	Netmask S.A.S	12/08/2026 5:34 PM	205.896.501,3
EYC ING - SIP-ANDJE-043-2026	eyc ingenieros SAS	11/08/2026 11:20 AM	196.225.605,4
RENOVACION LICENCIA VEEAM	COLSISTEC	4/08/2026 2:01 PM	215.615.125
OFERTA SIP-ANDJE-043-2026	SUMINISTROS OBRAS Y SISTEMAS	24/07/2026 12:31 PM	201.996.948

OBSERVACIONES AL PLIEGO DE CONDICIONES Contestar
No tiene ninguna observación a los documentos del proceso

MENSAJES Crear
Sin mensajes

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 cuatro (4) cotizaciones que cumplen con la totalidad de productos requeridos por la Agencia, presentadas por las empresas EYC INGENIEROS, SUMINISTROS OBRAS Y SISTEMAS, NETMASK y COLSISTEC, por cuanto corresponden a ofertas con condiciones técnicas y económicas comparables.

Nombre del Producto	Cantidad	PROPONENTE				PROMEDIO
		EYC INGENIEROS	SUMINISTROS OBRAS Y SISTEMAS	NETMASK	COLSISTEC	
Vend Part No: P-ADVVUL-0I-SU1AR-00 Contrato: 3210398 (70 instancias) Fecha de Fin de soporte: 30/12/2026 Detalle: Veeam Data Platform Advanced Universal Subscription License. Includes Enterprise Plus Edition features. 1 Year Renewal Subscription Upfront Billing & Production (24/7) Support. 10 instance pack. Public Sector.	1	$64.272.058,63	$66.162.414,00	$67.439.680,00	$75.711.228,00	$68.396.345,16

Vend Part No: V-ADVPLS-VS-PP1AR-00 Contrato: 3210399 (20 sockets) Detalle: 1 Year of Production (24/7) maintenance renewal for Veeam Data Platform Advanced Enterprise Plus Fecha de Fin: 31/12/2026	1	$131.953.546,63	$135.834.534,00	$138.456.821,30	$139.903.897,00	$136.537.199,73
VALOR TOTAL INCLUIDO IMPUESTOS		**$196.225.605,25**	**201.996.948,00**	**$205.896.501,30**	**$215.615.125,00**	**$204.933.544,89**

De esta manera se establece como presupuesto oficial estimado la suma de hasta **DOSCIENTOS CUATRO MILLONES NOVECIENTOS TREINTA Y TRES MIL QUINIENTOS CUARENTA Y CUATRO PESOS CON OCHENTA Y NUEVE CENTAVOS M/CTE ($ 204.933.544,89)** incluido el IVA y demás impuestos a que haya lugar, para la Renovación de soporte y garantía de licenciamiento de la herramienta VEEAM BACKUPS, 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 adquisición y renovación de licenciamiento, soporte y servicios asociados a soluciones de respaldo y recuperación de información, se evidencia la necesidad de garantizar la continuidad de las capacidades de protección, respaldo y recuperación de los activos tecnológicos y de información de la Agencia mediante la vigencia del licenciamiento y el acceso al soporte oficial del fabricante. Lo anterior permite disponer de actualizaciones de software, nuevas funcionalidades, mejoras de seguridad y servicios de asistencia técnica especializada, así como contar con mecanismos para atender oportunamente fallas, alertas, errores en los procesos de respaldo y recuperación e incidentes que puedan afectar la disponibilidad e integridad de la información institucional.

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 del licenciamiento de Veeam Backup, soporte especializado, actualización, asistencia técnica, configuración, monitoreo, administración y demás servicios asociados a la protección y recuperación de información. De igual manera, la participación de fabricantes y canales autorizados permite garantizar el acceso a los servicios, actualizaciones, recursos técnicos y mecanismos oficiales requeridos para mantener la solución en condiciones adecuadas de operación 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, con el propósito de garantizar la continuidad de las capacidades institucionales de respaldo, protección y recuperación de información, fortalecer la resiliencia tecnológica y contribuir a la continuidad de los servicios y sistemas de información que soportan la operación de la Entidad.

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://www.mordorintelligence.com/industry-reports/cyber-security-market

10. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025
11. https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-nacionales-trimestrales/pib-informacion-tecnica
12. https://www.dane.gov.co/files/operaciones/IPC/jul2026/cp-IPC-jul2026.pdf

Cordialmente,

Diana Betty Clavijo Vargas
Jefe Oficina Asesora de Sistemas y Tecnologías de Información (E)

Proyectó: Jeison Yamit Gómez Camacho