Conforme lo establece el artículo 2.2.1.2.1.5.1 del Decreto 1082 de 2015, que desarrolla el numeral 12 del Artículo 25 de la Ley 80 de 1993 modificado por el Articulo 87 de la Ley 1474 de 2011, se elaboran los presentes **ESTUDIOS Y DOCUMENTOS PREVIOS** con el fin de adelantar el correspondiente proceso de selección **DE MÍNIMA CUANTÍA**, rigiéndose por las siguientes consideraciones:

1. DESCRIPCIÓN DE LA NECESIDAD

El Consejo Profesional Nacional de Arquitectura y sus Profesiones Auxiliares – CPNAA es un órgano estatal creado mediante la Ley 435 de 1998, reglamentado por el Decreto 932 de 1998, la Ley 1768 de 2015 y la Ley 1796 de 2016, al cual se le asignaron funciones de fomento, promoción, control y vigilancia del ejercicio de la profesión de la arquitectura y sus profesiones auxiliares, dentro del marco de los principios y postulados de la ética profesional.

El CPNAA es una entidad de naturaleza sui generis, especial e independiente del orden nacional, que no hace parte de la Rama Ejecutiva del Poder Público ni se encuentra adscrita o vinculada al Ministerio de Vivienda, Ciudad y Territorio de Colombia, razón por la cual ejerce sus funciones de manera autónoma, conforme a las competencias conferidas por la ley.

La entidad cuenta con una sede en la ciudad de Bogotá D. C., desde donde presta servicios a nivel nacional e internacional, apoyándose en herramientas tecnológicas y canales virtuales, entre ellos su sitio web institucional, con el fin de garantizar una atención oportuna, eficiente y segura a los usuarios. En cumplimiento de los principios de la función administrativa y las disposiciones normativas relacionadas con atención al ciudadano, transparencia, acceso a la información pública y eficiencia administrativa (Ley 1437 de 2011, Ley 1712 de 2014, entre otras), el CPNAA debe garantizar la continuidad, calidad y seguridad en la prestación de sus servicios.

Para el cumplimiento de sus funciones y la protección de los activos de información institucionales, la Entidad ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI), soportado en políticas y procedimientos orientados a garantizar la confidencialidad, integridad y disponibilidad de la información. Dichas políticas regulan aspectos relacionados con el control de acceso, la gestión de activos de información, las copias de seguridad, el uso de servicios en la nube, la protección de datos personales y la utilización de recursos tecnológicos, entre otros.

La adecuada implementación de estas políticas requiere mantener actualizada y protegida la infraestructura tecnológica de la Entidad, así como disponer de herramientas especializadas que permitan prevenir, detectar y mitigar riesgos asociados a la seguridad de la información. En este contexto, resulta indispensable contar con soluciones de protección informática que contribuyan a la aplicación efectiva de los controles de seguridad definidos por la Entidad y a la reducción de vulnerabilidades que puedan afectar la operación institucional.

Actualmente, las organizaciones se enfrentan a un entorno digital caracterizado por amenazas informáticas cada vez más sofisticadas y cambiantes, las cuales exceden los riesgos asociados a los virus informáticos tradicionales. Entre estas amenazas se encuentran el malware, ransomware, phishing, spyware, troyanos, gusanos informáticos y otras modalidades de software malicioso que pueden comprometer la seguridad de los sistemas de información. Estos ataques tienen la capacidad de ejecutar código no autorizado, afectar la disponibilidad de los servicios tecnológicos, ocasionar la pérdida, alteración o secuestro de información, así como comprometer la integridad de los sistemas y las comunicaciones de red de la Entidad.

En este sentido, el CPNAA dispone de una infraestructura tecnológica compuesta, entre otros recursos, por un servidor HP DL380P Gen8, sobre el cual operan ambientes con sistemas operativos Windows Server 2012 y Windows Server 2016, configurados mediante máquinas virtuales que soportan servicios críticos para la operación institucional, tales como el Directorio Activo, la administración de políticas de seguridad, el direccionamiento IP interno, la conectividad de la red local y el acceso a internet.

Adicionalmente, dicho servidor cuenta con componentes de hardware redundantes, como fuentes de alimentación, que contribuyen a garantizar la continuidad y disponibilidad de los servicios tecnológicos.

Teniendo en cuenta la criticidad de esta infraestructura y la necesidad de proteger los activos de información institucionales frente a amenazas cibernéticas, se requiere la adquisición, renovación y configuración de licencias de antivirus que permitan fortalecer los mecanismos de seguridad existentes, mantener actualizada la protección de los equipos y servidores de la Entidad, reducir la exposición a riesgos de seguridad informática y asegurar la continuidad de los servicios tecnológicos que soportan el cumplimiento de las funciones misionales y administrativas del CPNAA.

Por lo tanto, el CPNAA debe mantener una política de actualización y apropiación de tecnologías de la información y telecomunicaciones que le permita ser cada vez más competitivo ofreciendo trámites de una manera ágil, segura y confiable y así optimizar los servicios, para lo cual ha implementado un SGSI – Sistema de Gestión de Seguridad de la Información, a través de las políticas de seguridad en lo referente a:

- Control de acceso a la información.
- Desarrollo seguro.
- Escritorio limpio y pantalla limpia.
- Protección de datos personales.
- Protección de dispositivo propio (BYOD).
- Relaciones con proveedores.
- Respaldo de la información.
- Servicios de computación en la nube.
- Transferencia o intercambio de información.
- Uso aceptable de activos de información.
- Uso de controles criptográficos y gestión de llaves criptográficas.
- Uso de servicio de acceso a internet.
- Uso de servicios de correo electrónico.

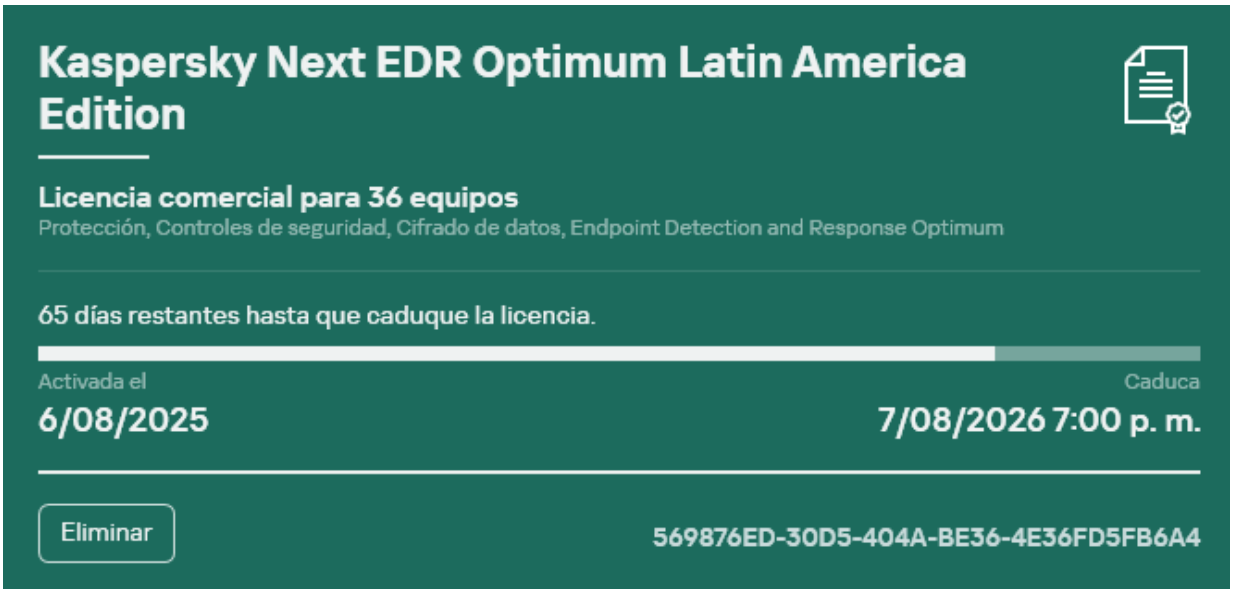
Estas políticas tienen el objetivo de implementar un lenguaje común en lo referente a la seguridad de la información, que es apoyado directamente con el óptimo desempeño de todos sus equipos en software, hardware, recurso humano y una plataforma robusta de antivirus, es así que la solución de Kaspersky Next EDR Optimum licenciada para uso del CPNAA, ha permitido a través de su consola, salvaguardar los parámetros de seguridad informática, los computadores, servidores e información de la red interna del CPNAA.

Con base en lo anterior, el área y personal de tecnología del CPNAA, cuenta con el conocimiento, capacitación y manejo en la administración de la plataforma de antivirus, es por esto que el producto Kaspersky Next EDR Optimum ha demostrado durante su vigencia: Efectividad, eficiencia y eficacia a la hora de proteger los sistemas de información y los equipos de cómputo; la formación, experiencia y conocimiento del CPNAA, en esta plataforma ha permitido la reducción de costos y operatividad, agilizando su implementación y tiempos de capacitación y respuesta.

La renovación de la licencia actual del antivirus Kaspersky Next EDR Optimum para uso en dispositivos concurrentes de computadores, servidores y máquinas virtuales, permite la protección contra ataques cibernéticos recurrentes en la red de internet, así mismo garantiza la protección de dispositivos de almacenamiento extraíble (pen drive, discos duros portables, memorias USB, entre otros).

Por otro lado, la renovación de una licencia de antivirus cuenta con un costo y servicio especial, en comparación con los valores inherentes a un nuevo licenciamiento y prevé un ahorro significativo ante nuevas implementaciones y procesos de desinstalación del software actual para la integración de nuevas herramientas ajenas para el CPNAA, sus usuarios, aplicaciones equipos móviles, computadores y sistemas operativos actuales.

Licencia Actual Kaspersky – CPNAA.



Por lo expuesto, para que el Consejo Profesional Nacional de Arquitectura y sus Profesiones Auxiliares, garantice y pueda ejercer mecanismos de control en archivos electrónicos, digitales, herramientas informáticas, correo electrónico, navegación en internet y la protección y seguridad de los sistemas e información que se encuentran en el servidor y los equipos de cómputo del CPNAA, es necesario contratar el servicio para la renovación de la licencia, junto con la consola de administración en la nube por un (1) año más, del antivirus Kaspersky Next EDR Optimum para treinta y nueve (39) usuarios concurrentes.

La contratación requerida se encuentra alineada con los principios de planeación, economía y responsabilidad, en la medida en que busca preservar la seguridad de la información institucional, prevenir afectaciones operativas derivadas de incidentes de ciberseguridad y garantizar la continuidad de los servicios tecnológicos que soportan el cumplimiento de las funciones legales y misionales del CPNAA.

Una vez sustentada la necesidad, la modalidad de selección aplicable corresponde a la mínima cuantía, de conformidad con lo previsto en el numeral 5 del artículo 2 de la Ley 1150 de 2007, la cual aplica para aquellos procesos cuyo valor no excede el diez por ciento (10%) de la menor cuantía de la entidad, independientemente de su objeto. El presupuesto oficial estimado y respaldado mediante el amparo presupuestal (CDP) para la ejecución de este contrato asciende de manera exacta a la suma de Ocho millones seiscientos cuarenta mil trescientos cuarenta y seis pesos M/CTE ($8.640.346,00).

Finalmente, la presente contratación se encuentra incluida en el Plan Anual de Adquisiciones -PAA de la vigencia fiscal 2026, conforme a lo establecido en el artículo 2.2.1.1.1.4.1 del Decreto 1082 de 2015, bajo los códigos de las Naciones Unidas (UNSPSC) 43233205 y 81112501.

2. OBJETO A CONTRATAR

Suministrar la licencia de antivirus en la nube para el servidor y los equipos de cómputo del CPNAA.

3. TIPO DE CONTRATO

El contrato que se pretende celebrar es de Compraventa.

El proceso de selección a que se refiere éste Estudio Previo se encuentra sometido al Estatuto General de Contratación de la Administración Pública contenido en las leyes 80 de 1993, 1150 de 2007, 1450 de 2011, 1474 de 2011, el Decreto – Ley 019 de 2012, Decreto 1082 de 2015 y las disposiciones que modifiquen o reglamenten aquellas, por virtud de las cuales, la selección se realizará de manera objetiva, a efecto de adjudicar la propuesta más favorable para los intereses del CPNAA y los fines que ella persigue.

La modalidad de selección aplicable para la celebración del contrato objeto del presente estudio previo corresponde a la de mínima cuantía, de conformidad con lo dispuesto en el numeral 5 del artículo 2 de la Ley 1150 de 2007, el artículo 274 de la Ley 1450 de 2011 y los artículos 2.2.1.2.1.5.1 y 2.2.1.2.1.5.2 del Decreto 1082 de 2015.

La escogencia recaerá sobre aquella oferta que contenga el precio más bajo, siempre que cumpla los requisitos mínimos habilitantes establecidos por el CPNAA.

Los requisitos mínimos habilitantes serán verificados únicamente en el oferente con el precio más bajo, de acuerdo con lo establecido por el artículo 2.2.1.2.1.5.2 del Decreto 1082 de 2015 el cual señala: *"Procedimiento para la contratación de mínima cuantía. Las siguientes reglas son aplicables a la contratación cuyo valor no excede del 10% de la menor cuantía de la Entidad Estatal, independientemente de su objeto. (…) 4. La Entidad Estatal debe revisar las ofertas económicas y verificar que la de menor precio cumple con las condiciones de la invitación. Si ésta no cumple con las condiciones de la invitación, la Entidad Estatal debe verificar el cumplimento de los requisitos de la invitación de la oferta con el segundo mejor precio, y así sucesivamente (…)".*

Lo anterior, dado que la menor cuantía del **CPNAA** se encuentra hasta los 280 salarios mínimos mensuales legales vigentes, siendo el diez por ciento (10%) de esta, la suma de **CUARENTA Y NUEVE MILLONES VEINTICINCO MIL TRESCIENTOS CUARENTA PESOS M/CTE ($49.025.340),** suma dentro de la cual se encuentra el prepuesto oficial del presente proceso de selección, que corresponde a **OCHO MILLONES SEISCIENTOS CUARENTA MIL TRESCIENTOS CUARENTA Y SEIS PESOS M/CTE ($8.640.346)**

4. IDENTIFICACIÓN DEL NIVEL DEL CLASIFICADOR DE BIENES Y SERVICIOS

CLASIFICACIÓN UNSPSC:

SEGMENTO	FAMILIA	CLASE	PRODUCTO
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	**43230000** Software	**43233200** Software de seguridad y protección	**43233205** Software de seguridad de transacciones y de protección contra virus
81000000 Servicios basados en Ingeniería, Investigación y Tecnología	**81110000** Servicios Informáticos	**81112500** Servicios de alquiler o arrendamiento de licencias de software de computador	**81112501** Servicio de Licencias del software del computador

Clasificación Central de Productos
47829 - Paquetes de software de otras aplicaciones

5. PRESUPUESTO OFICIAL

De acuerdo con el análisis y estudio de mercado realizado por el **CPNAA,** el presupuesto oficial de la presente contratación IVA incluido es de hasta **OCHO MILLONES SEISCIENTOS CUARENTA MIL TRESCIENTOS CUARENTA Y SEIS PESOS M/CTE ($8.640.346),** incluida la totalidad de los costos directos e indirectos, fijos y variables, tales como gastos de administración impuestos, imprevistos, tasas, margen de utilidad, prestaciones sociales y salarios del personal ofrecido, y demás conceptos que el cumplimiento del respectivo contrato conlleve.

6. CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL

El valor de la presente contratación está respaldado con el Certificado de Disponibilidad Presupuestal N°. 176 del 1 de julio de 2026, expedido por el Jefe de la Oficina Administrativa y Financiera, así:

RUBRO	DESCRIPCIÓN	VALOR
2.1.2.01.01.005.02.03.01.01	Paquetes de Software	$8.640.346

7. ANÁLISIS Y JUSTIFICACIÓN DEL VALOR DEL CONTRATO

El Consejo Profesional Nacional de Arquitectura y sus Profesiones Auxiliares – CPNAA, en cumplimiento de los principios de planeación, economía y selección objetiva que orientan la contratación estatal, realizó un estudio de mercado con el fin de identificar las condiciones comerciales vigentes y determinar el valor estimado para la adquisición de la licencia de antivirus requerida por la Entidad.

Para ello, se solicitaron cotizaciones a diferentes proveedores del mercado nacional especializados en el suministro de licencias de antivirus, teniendo en cuenta las especificaciones técnicas definidas por el CPNAA. Lo anterior, con el propósito de obtener información suficiente, pertinente y comparable que permitiera establecer el presupuesto oficial del proceso de contratación y verificar las condiciones del mercado en términos de calidad, cobertura y precio.

Como resultado del estudio de mercado, se recibieron cuatro (4) cotizaciones. Sin embargo, para efectos del análisis comparativo y la determinación del valor estimado del contrato, únicamente se tuvieron en cuenta dos (2) de ellas, debido a que dos de las cotizaciones presentaban condiciones económicas que no permitían una comparación homogénea y objetiva frente a las demás ofertas recibidas.

En consecuencia, se realizó validación del valor en la tienda de Kaspersky en línea, el análisis comparativo de las tres (3) cotizaciones habilitadas, evaluando los valores ofertados y las condiciones comerciales presentadas por cada proveedor y la tienda en línea de Kaspersky, obteniéndose el siguiente resultado:

OBJETO	*"Suministrar la licencia de antivirus en la nube para el servidor y los equipos de cómputo del CPNAA."*						
DESCRIPCIÓN DE LA NECESIDAD		**COTIZACIÓN 3 – Tienda en línea Kaspersky**		**COTIZACIÓN 2 – APROVISIONAR SOLUCIONES S.A.S - 20261200147372**		**COTIZACIÓN 1 – CREAR IMAGEN DISEÑO WEB Y MULTIMEDIA SAS - 20261200148212**	
ITEM	**CANTIDAD**	**VALOR UNITARIO**	**VALOR TOTAL**	**VALOR UNITARIO**	**VALOR TOTAL**	**VALOR UNITARIO**	**VALOR TOTAL**
Solución de seguridad digital, antivirus y protección endpoint Un (1) año (12 meses) a partir de su correcta activación y/o instalación. Comercial, 100% original, con modalidad de entrega y gestión 100% digital.	Licenciamiento para 39 equipos concurrentes	$ 220.434	$8.596.926	$ 164.208	$ 6.404.112	$ 280.000	$ 10.920.000

Multiplataforma. Compatible con los sistemas operativos Windows (Windows 10, 11, server 2012, server 2016), macOS, iOS y Android.							
Valor promedio del estudio de mercado:				**$8.640.346**			

ANÁLISIS DE MERCADO

El crecimiento de ciberataques impulsa a empresas en América Latina a adoptar centros especializados de ciberseguridad - *14 de abril de 2026*

Según un estudio de Kaspersky, casi la mitad de las organizaciones de la región planea implementar estos centros, llamados SOC, para fortalecer su capacidad de detección y respuesta frente a las amenazas actuales.

En un entorno donde las amenazas digitales evolucionan con mayor velocidad y profesionalización, cada vez más empresas deciden reforzar su estrategia de defensa con urgencia. Un estudio de Kaspersky revela que casi la mitad (49%) de las organizaciones de América Latina planea establecer un Centro de Operaciones de Seguridad (SOC) para fortalecer su postura de ciberseguridad, mientras que un 42% busca mejorar su capacidad de respuesta frente a ataques cada vez más complejos y persistentes.

Un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) es una unidad especializada dentro de las empresas encargada de monitorear de forma continua los sistemas y proteger la infraestructura tecnológica. En la práctica, funciona como un "centro de control" desde donde expertos en ciberseguridad vigilan redes, detectan actividades sospechosas, analizan incidentes y responden de forma proactiva a posibles ataques digitales.

Para identificar los factores determinantes, prioridades estratégicas y desafíos potenciales en la planificación e implementación de SOC, Kaspersky realizó un estudio global con especialistas senior en seguridad de TI, gerentes y directores de empresas con 500 o más empleados. Todos los participantes operan actualmente sin un SOC, pero planean establecer uno en el corto plazo. El estudio, que abarca 16 países de APAC, META, LATAM y Europa, ofrece información valiosa sobre tendencias emergentes y mejores prácticas en el desarrollo de SOC a nivel mundial.

Los encuestados expusieron las principales razones para establecer un SOC, entre ellas el fortalecimiento de la postura de ciberseguridad de la organización, la posibilidad de detectar amenazas con mayor rapidez y mejorar la capacidad de respuesta ante incidentes. Además, muchas empresas consideran que contar con este tipo de centros puede representar una ventaja competitiva, al permitir una gestión más eficiente de los riesgos digitales y una mayor capacidad para enfrentar un panorama de amenazas cada vez más complejo.

Otros factores incluyen la optimización del presupuesto, la necesidad de una detección y respuesta más rápidas, y la expansión del software, los endpoints y los dispositivos de usuario, lo que exige medidas de seguridad más integrales y por capas. Estos factores son citados por el 41% de las organizaciones. Además, el 40% busca una mejor protección de la información confidencial, el 39% pretende cumplir con requisitos regulatorios y un 33% espera que las capacidades de un SOC proporcionen una ventaja competitiva. Las empresas de mayor tamaño tienden a mencionar cada una de estas razones con mayor frecuencia, lo que refleja las mayores presiones operativas y regulatorias que enfrentan.

El monitoreo continuo se convierte en el principal requisito

Entre las funciones clave que las organizaciones planean delegar, el monitoreo de seguridad 24/7 encabeza la lista con un 54%. Esta vigilancia permanente permite detectar anomalías de forma temprana, prevenir la escalada de incidentes y mantener la resiliencia cibernética en tiempo real. Esta demanda pone de relieve la necesidad estratégica de una gestión proactiva de riesgos, ya que las organizaciones buscan defenderse de amenazas persistentes que pueden atacar en cualquier momento.

Las empresas que planean externalizar por completo las operaciones del SOC muestran un mayor interés en aplicar metodologías de "lecciones aprendidas", mientras que aquellas que desarrollan SOC internos se enfocan más en la gestión de accesos para mantener un control más estricto.

"Para construir con éxito un SOC, las empresas deben priorizar no solo la combinación adecuada de tecnologías, sino también la planificación cuidadosa de los procesos, el establecimiento claro de objetivos y una distribución eficiente de los recursos. Los flujos de trabajo bien definidos y la mejora continua son fundamentales para garantizar que los analistas humanos puedan concentrarse en tareas críticas, convirtiendo al SOC en un componente proactivo y adaptable dentro de la estrategia de ciberseguridad", comenta ***Claudio Martinelli, director general para Américas en Kaspersky****.*

El ejecutivo explicó que: "al tercerizar la estructura SOC, es posible involucrar a proveedores competentes que van contribuir con sus conocimientos y experiencia al manejar este concepto en varias organizaciones. Sin embargo, es importante considerar que lo que se terceriza es la operación, no la responsabilidad. Es decir, los Acuerdos de Nivel de Servicio, las reglas de confidencialidad, las políticas, etc. lo define el dueño del dato, no el operador. Es importante tener en cuenta los 'derechos y deberes' antes de partir para la opción externa".

Otra recomendación es incorporar inteligencia de amenazas para fortalecer la eficiencia del SOC, ya que permite anticipar riesgos y ajustar las políticas de ciberseguridad con base en amenazas que ya están impactando a otras organizaciones, especialmente aquellas del mismo sector.

Para instalar y mantener un SOC de manera exitosa, Kaspersky recomienda:

- *Involucrar a Kaspersky SOC Consulting durante la fase inicial de implementación o al fortalecer sus operaciones de seguridad existentes. Nuestros servicios integrales de consultoría están diseñados para ayudar a las empresas a construir un SOC sólido y optimizar sus procesos.*
- *Impulsa el desempeño de tu seguridad con Kaspersky SIEM, impulsado por capacidades avanzadas de inteligencia artificial. Esta solución recopila, analiza y almacena datos de registro en toda su infraestructura de TI, proporcionando enriquecimiento contextual e información accionable de inteligencia de amenazas.*
- *Protege a tu empresa* ***frente a una amplia gama de amenazas con las soluciones de la línea*** *Kaspersky Next****,*** *que ofrecen protección en tiempo real, visibilidad de amenazas y capacidades de investigación y respuesta EDR y XDR para organizaciones de cualquier tamaño e industria.*
- *Habilita a tu* ***equipo de ciberseguridad con una visibilidad profunda de las amenazas que apuntan a su organización.*** *La más reciente Kaspersky Threat Intelligence proporciona información contextual enriquecida a lo largo de todo el ciclo de gestión de incidentes, facilitando la identificación oportuna de riesgos cibernéticos.*

Para minimizar las consecuencias negativas de la escasez de personal de ciberseguridad, los expertos de Kaspersky recomiendan:

- *Adoptar servicios de seguridad gestionados como Kaspersky Managed Detection and Response (MDR) o/y Incident Response para obtener experiencia extra sin necesidad de contrataciones adicionales. Esto ayuda a protegerse contra ciberataques e investigar incidentes incluso si la empresa carece de trabajadores de seguridad.*

- *Invertir en cursos de ciberseguridad para el personal de la empresa con el objetivo de mantenerlos al día con los conocimientos más recientes. Con la formación de Kaspersky Expert, los profesionales de InfoSec pueden avanzar en sus habilidades y ser capaces de defender a las compañías frente a los ataques.*
- *Utilizar simuladores interactivos para poner a prueba los conocimientos y evaluar la forma de pensar en situaciones críticas. Por ejemplo, con el nuevo juego interactivo de Kaspersky sobre ransomware se puede observar la forma en que el departamento de TI de la empresa despliega, investiga y responde frente a un ataque y toma decisiones con el personaje principal del juego.*
- *Utilizar soluciones centralizadas y automatizadas como Kaspersky Extended Detection and Response (XDR) para reducir la carga del equipo de seguridad de TI y minimizar la posibilidad de cometer errores. Al agregar y correlacionar datos de múltiples fuentes en un solo lugar y utilizar tecnologías de aprendizaje automático, estas soluciones proporcionan una detección eficaz de amenazas y una rápida respuesta automatizada.*

Fuente*:* https://latam.kaspersky.com/about/press-releases/el-crecimiento-de-ciberataques-impulsa-a-empresas-en-america-latina-a-adoptar-centros-especializados-de-ciberseguridad

Sector Económico – Servicios

La contratación se enmarca en el Sector Terciario de la Economía, específicamente en el ámbito de los servicios. Este sector abarca todas aquellas actividades económicas destinadas a ofrecer y poner a disposición distintos tipos de servicios a individuos, hogares y empresas, según sus necesidades.

Es crucial considerar dos características esenciales de los servicios:

1. No pueden almacenarse ni transportarse, lo que implica que su comercialización está directamente ligada a su producción.
2. No generan un traslado de propiedad; en su lugar, el proveedor otorga al consumidor el derecho a utilizarlos según su demanda.

El sector de licenciamiento y antivirus en Colombia ha experimentado un crecimiento significativo en los últimos años, impulsado por la creciente digitalización de las empresas y la necesidad de proteger la información frente a amenazas cibernéticas. Este mercado se caracteriza por la presencia de múltiples proveedores y distribuidores autorizados que ofrecen soluciones adaptadas a las necesidades de diferentes sectores, desde pequeñas y medianas empresas hasta grandes corporaciones.

En cuanto al marco legal, Colombia ha establecido normativas claras para regular el uso de software y garantizar la protección de los derechos de autor. La Ley 603 de 2000 obliga a las empresas a reportar en sus informes anuales de gestión el cumplimiento de las normas de propiedad intelectual y derechos de autor, incluyendo la legalidad del software utilizado. El incumplimiento de esta ley puede acarrear sanciones administrativas y penales, como multas de hasta 200 salarios mínimos legales mensuales vigentes y penas de prisión de 2 a 5 años.[1]

A pesar de estas regulaciones, la piratería de software sigue siendo un desafío en el país. Se estima que el índice de piratería en Colombia es del 53%, lo que representa pérdidas significativas para la economía nacional y afecta la competitividad del país en el ámbito internacional.

En respuesta a esta situación, el gobierno colombiano ha implementado medidas adicionales para fortalecer la seguridad digital. La Resolución 746 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establece lineamientos para la gestión de la seguridad de la información

[1] https://softimiza.co/blog/ley-sobre-software-legal-en-colombia

en las relaciones con proveedores, incluyendo la implementación de controles para mitigar riesgos asociados a la adquisición de productos y servicios de seguridad digital[2] .

En el mercado colombiano, existen diversas opciones de licenciamiento de antivirus ofrecidas por distribuidores autorizados. Empresas como Warescolombia y Aplicaciones Dinámicas brindan asesoría y distribución de licencias de antivirus de marcas reconocidas como Kaspersky, ESET NOD32, Symantec y Bitdefender, adaptándose a las necesidades específicas de cada cliente.

En resumen, el sector de licenciamiento y antivirus en Colombia está en constante evolución, con un enfoque creciente en la legalidad del software y la protección contra amenazas cibernéticas. Las empresas deben mantenerse informadas sobre las regulaciones vigentes y considerar la implementación de soluciones de seguridad adecuadas para proteger sus activos digitales y cumplir con las normativas legales.

ENCUESTA MENSUAL DE SERVICIOS (EMS)[3]

Variación anual de los ingresos nominales y contribución por tipo de ingresos, según subsector de servicios (abril 2026p / abril 2025)

En abril de 2026, quince de los dieciocho subsectores de servicios presentaron variación positiva en los ingresos totales, en comparación con abril de 2025.

[2] https://normograma.invima.gov.co/compilacion/docs/resolucion_mintic_0746_2022.htm?

[3] https://www.dane.gov.co/files/operaciones/EMS/bol-EMS-abr2026.pdf

Tabla 1. Variación anual de los ingresos y contribución por tipo de ingresos, según subsector de servicios
Total nacional
Abril 2026P / abril 2025

Clasificación CIIU Rev. 4 A.C.			Ingresos nominales	Ingresos por servicios	Venta de Mercancías	Otros Ingresos
Sección	División	Descripción	Variación (%)	Contribución (PP)		
H	División 52	Almacenamiento y actividades complementarias al transporte	-0,4	-0,9	-0,1	0,6
H	División 53	Correo y servicios de mensajería	7,4	7,2	-0,0	0,2
I	División 56	Restaurantes, catering y bares	8,1	6,9	1,4	-0,3
J	División 58	Actividades de edición	21,0	8,1	1,1	11,7
J	División 59, excepto Clase 5920	Producción de películas cinematográficas y programas de televisión	63,2	37,7	21,8	3,6
J	División 60 y Clase 6391	Actividades de programación y transmisión, agencias de noticias	8,6	4,2	0,0	4,4
J	División 61	Telecomunicaciones	1,4	2,1	-0,7	0,0
J	División 62, División 63, excepto Clase 6391	Desarrollo de sistemas informáticos y procesamiento de datos	8,2	7,4	0,9	-0,1
L,N	Sección L, División 68 Sección N, Divisiones 7710, 7729 y 7730	Inmobiliarias, alquiler de maquinaria y equipo	11,4	13,4	-1,8	-0,2
M	Divisiones 69, 70, 71, 72, Clase 7320, División 74	Actividades profesionales científicas y técnicas	12,9	13,2	-0,3	-0,0
M	Clase 7310	Publicidad	8,5	8,4	-0,0	0,0
N	Divisiones 78, 80 y 81, excepto Clase 8130	Actividades de empleo, seguridad e investigación privada, servicios a edificios	17,0	17,1	-0,1	-0,0
N	Clase 8220	Actividades de centros de llamadas (Call center)	-9,5	-9,6	0,0	0,1
N	División 82 excepto Clase 8220	Actividades administrativas y de apoyo de oficina y otras actividades, excepto Call center	-3,0	-3,2	0,0	0,1
P	Grupo 854	Educación superior privada	6,7	5,6	0,1	1,0
Q	Clase 8610	Salud humana privada con internación	5,6	5,7	-0,1	0,1
Q	División 86 excepto Clase 8610	Salud humana privada sin internación	11,4	11,5	0,1	-0,1
S	Divisiones 90, 92, 93, 95 y 96	Otros servicios de entretenimiento y otros servicios	16,7	15,7	-0,5	1,5

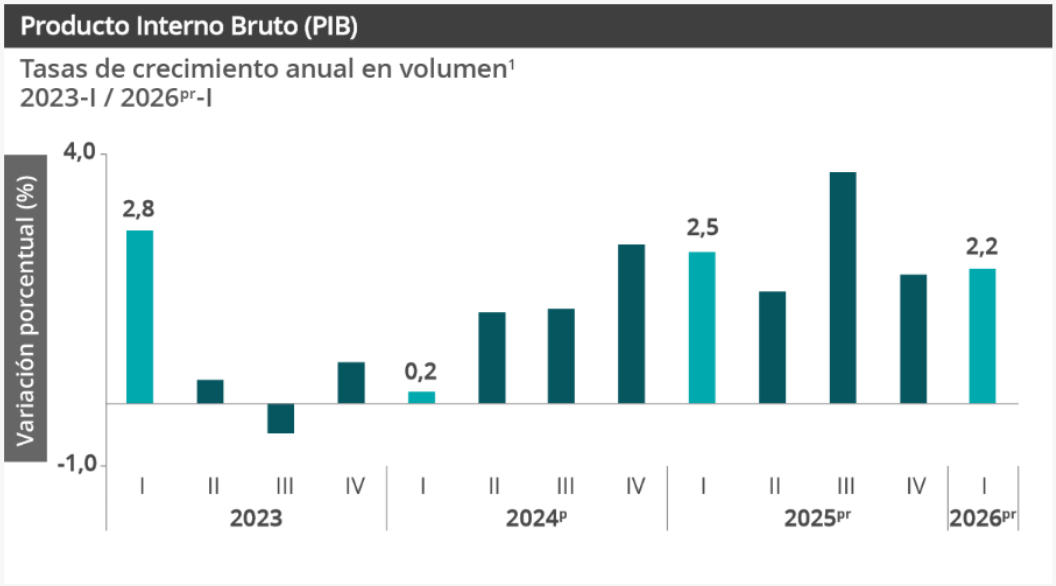
Fuente: DANE, EMS.
P Cifra provisional
(PP) Puntos porcentuales
Nota: por aproximación decimal, se puede presentar diferencia en la suma de las contribuciones frente a la variación total.

PRODUCTO INTERNO BRUTO (PIB) NACIONAL TRIMESTRAL[4]

Información primer trimestre 2026pr

En el primer trimestre de 2026pr, el Producto Interno Bruto en su serie original, crece 2,2% respecto al mismo periodo de 2025pr.

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



Fuente: DANE, PIB_T
[1]: Series originales encadenadas de volumen con año de referencia 2015
Pr: preliminar
P: provisional

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).

Respecto al trimestre inmediatamente anterior, el Producto Interno Bruto en su serie ajustada por efecto estacional y calendario crece 0,6%. Cuando se observa el comportamiento de las actividades económicas relacionadas:

- Industrias manufactureras crece 2,3%.
- Actividades financieras y de seguros crece 2,2%.
- Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios; Actividades de los hogares individuales en calidad de empleadores; actividades no diferenciadas de los hogares individuales como productores de bienes y servicios para uso propio crece 1,4%.

Enfoque del gasto[5]

En el tercer trimestre de 2025pr, el Producto Interno Bruto en su serie original crece 3,6% respecto al mismo periodo de 2024pr. Esta dinámica se explica por los siguientes comportamientos del componente del gasto (ver tabla 2):

[5] https://www.dane.gov.co/files/operaciones/PIB/cp-PIB-IIItrim2025.pdf

Tabla 2. Producto Interno Bruto (PIB)
Enfoque del gasto
Tasas de crecimiento (%) anual y trimestral en volumen[1] por componentes del gasto
Cuarto trimestre 2025[Pr]

Componente del gasto	Serie original		Serie ajustada por efecto estacional y calendario
	Anual		Trimestral
	2024[P] - IV / 2023 - IV	2025[Pr] - IV / 2024[P] - IV	2025[Pr] - IV / 2025[Pr]- III
Demanda final interna[2]	3,7	2,3	-1,0
Gasto de consumo final[3]	3,5	3,8	0,4
Formación bruta de capital[4]	4,7	-9,3	-8,9
Exportaciones	2,2	1,2	1,2
Importaciones	7,6	1,4	-4,5
Producto Interno Bruto	**2,4**	**2,3**	**0,1**

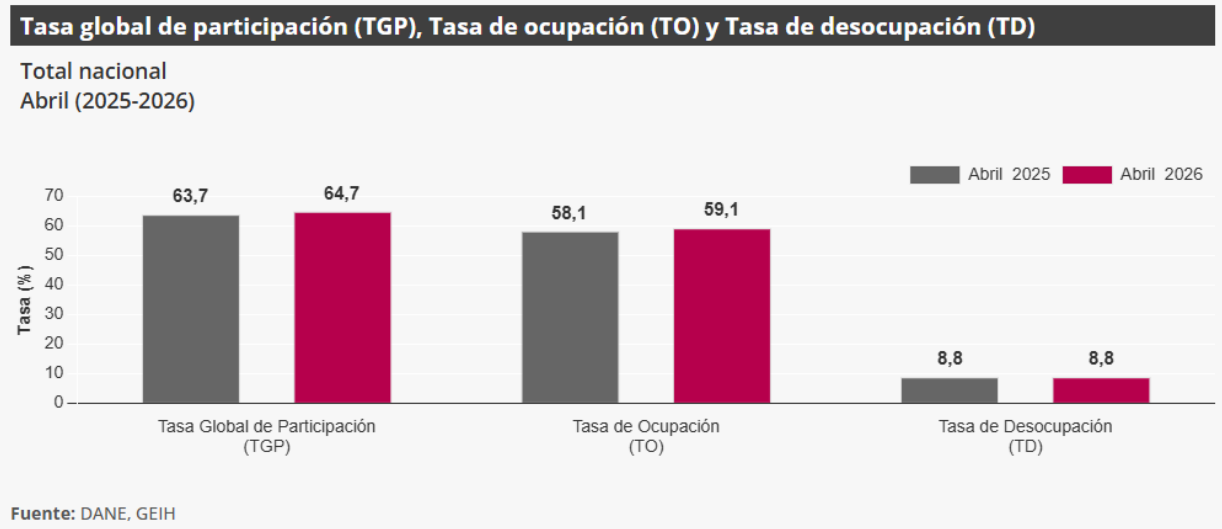
Fuente: DANE, PIB_T
[Pr]preliminar
[P]provisional
[1]Series encadenadas de volumen con año de referencia 2015.
[2]La demanda final interna incluye el gasto de consumo final y la formación bruta de capital.
[3]Incluye consumo final de los hogares, consumo final de gobierno y las instituciones sin fines de lucro que sirven a los hogares.
[4]La formación bruta de capital incluye la formación bruta de capital fijo, la variación de existencias y la adquisición menos disposición de objetos valiosos.

- **MERCADO LABORAL**[6]

Información abril de 2026

Para abril de 2026, la tasa de desocupación del total nacional fue 8,8%, siendo similar a la registrada en el mismo mes de 2025. La tasa global de participación se ubicó en 64,7%, lo que significó un aumento de 1,0 puntos porcentuales frente a abril de 2025 (63,7%). Finalmente, la tasa de ocupación fue 59,1%, lo que representó un aumento de 0,9 puntos porcentuales respecto al mismo mes del año anterior (58,1%).

[6] DANE. Gran encuesta Integrada de Hogares. https://www.dane.gov.co/index.php/estadisticas-por-tema/mercado-laboral/empleo-y-desempleo



En abril de 2026, la tasa de desocupación en el total de las 13 ciudades y áreas metropolitanas fue 8,8%, mientras que en el mismo mes de 2025 fue 8,7%. La tasa global de participación se ubicó en 66,6% y la tasa de ocupación en 60,7%, en abril de 2025 estas tasas fueron 65,9% y 60,1%, respectivamente.

VARIABLES ECONÓMICAS A CONSIDERAR EN EL PRESENTE PROCESO

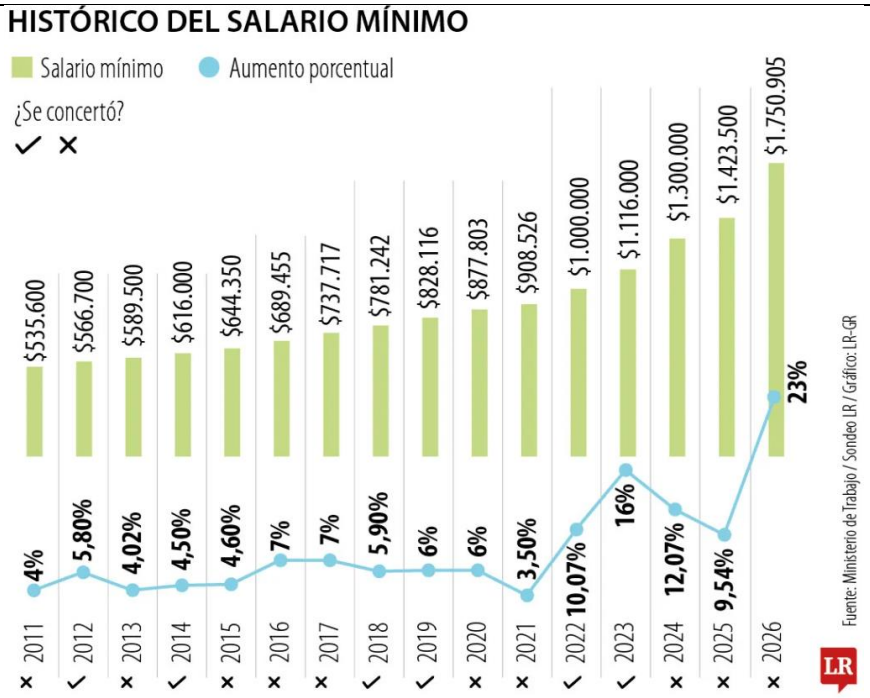
Las variables económicas que afectan el sector se encuentran referidas a la variación del salario mínimo - SMMLV y el índice de precios al consumidor - IPC.

SALARIO MÍNIMO MENSUAL LEGAL VIGENTE

El salario mínimo mensual legal vigente (SMMLV) en Colombia se fija para períodos de un (1) año y su periodicidad de pago es mensual. Dicho salario constituye la base para la estimación de los costos asociados al personal requerido para la ejecución de los trabajos objeto del presente proceso.

Para el año 2026, mediante el Decreto 1469 del 29 de diciembre de 2025, se estableció un incremento nominal de trescientos veintisiete mil cuatrocientos cinco pesos ($327.405), equivalente a un aumento del veintitrés por ciento (23 %), fijando el salario mínimo mensual legal vigente, a partir del 1 de enero de 2026, en la suma de un millón setecientos cincuenta mil novecientos cinco pesos ($1.750.905).

Así mismo, mediante el Decreto 1470 del 29 de diciembre de 2025, se incrementó el auxilio de transporte en cuarenta y nueve mil noventa y cinco pesos ($49.095), quedando establecido para el año 2026 en la suma de doscientos cuarenta y nueve mil noventa y cinco pesos ($249.095).



INDICE DE PRECIOS AL CONSUMIDOR (IPC) [7]

Información mayo 2026

Índice de Precios al Consumidor (IPC)

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

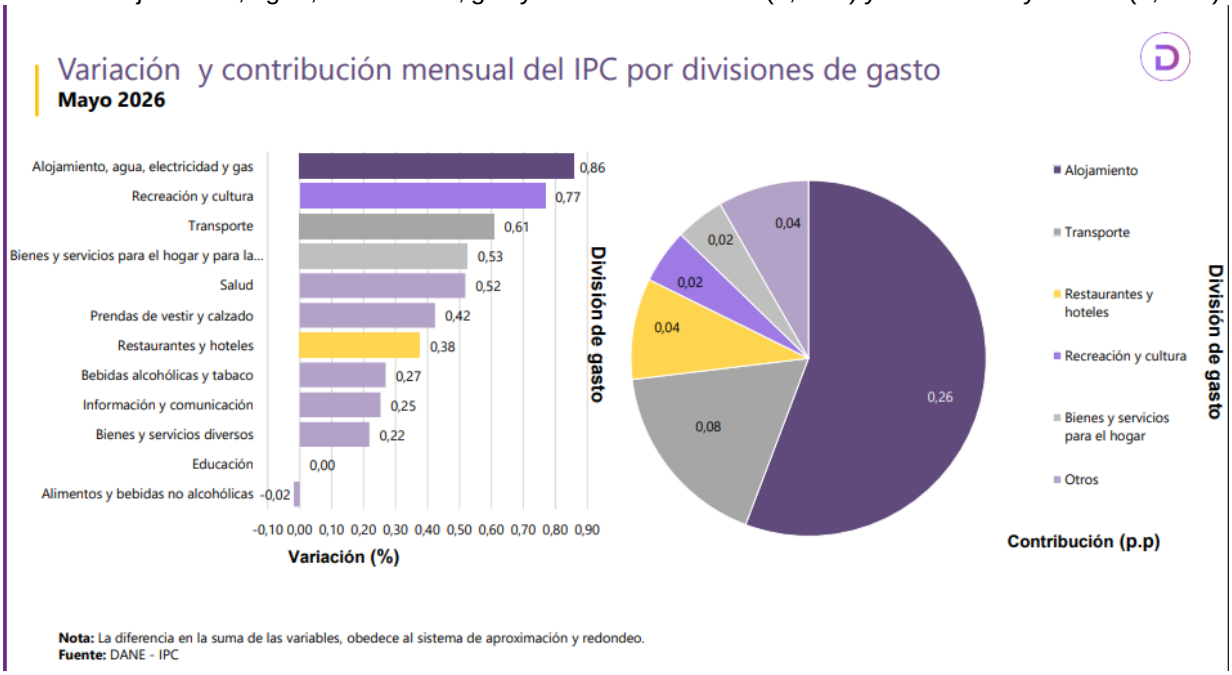
IPC	Mayo					
	Variación mensual		Variación año corrido		Variación anual	
	2025	2026	2025	2026	2025	2026
IPC total	0,32	**0,47**	3,63	**4,36**	5,05	**5,84**

Fuente: DANE, IPC

- En mayo de 2026 la variación mensual del IPC fue 0,47%, la variación año corrido fue 4,36% y la anual 5,84%.
- En mayo de 2026 la variación anual del IPC fue 5,84%, es decir, 0,79 puntos porcentuales mayor que la reportada en el mismo periodo del año anterior, cuando fue de 5,05%.

[7] https://www.dane.gov.co/index.php/estadisticas-por-tema/precios-y-costos/indice-de-precios-al-consumidor-ipc/ipc-informacion-tecnica?highlight=WyJpcGMiLCJcdTAwZWRwYyIsMjAxNiwiZGFuZSIsImRhbiJd

- El comportamiento mensual del IPC total en mayo de 2026 (0,47%) se explicó principalmente por la variación mensual de las divisiones Alojamiento, agua, electricidad, gas y otros combustibles y Transporte. Las mayores variaciones se presentaron en las divisiones Alojamiento, agua, electricidad, gas y otros combustibles (0,86%) y Recreación y cultura (0,77%).



Según un estudio realizado por Gartner, se espera un incremento de 11,5 % en el uso de herramientas de software empresarial

Las empresas, sin importar su tamaño, se han mantenido a la vanguardia en tendencias de software y transformación digital. Entre los temas prioritarios para las compañías destacan el fortalecimiento de la seguridad, la creciente adopción de plataformas low-code por parte de los desarrolladores, el uso de soluciones nativas en la nube y una mayor colaboración entre diseñadores y programadores para optimizar la ejecución de proyectos.

Según un informe entregado por Fedesoft, en Colombia se ha desarrollado un ecosistema digital, lo que ha permitido la dinamización de la industria de software y el desarrollo tecnológico en diferentes sectores de la economía y la sociedad. Sin embargo, aún persisten grandes desafíos en materia de conectividad, apropiación, productividad, internacionalización, talento, entre otros retos.[8]

Sector Digital en Colombia[9]

El primer trimestre de 2026 ha marcado un hito sin precedentes para el ecosistema digital en Colombia. Según los datos revelados en el Primer Informe público trimestral de comercio electrónico 2026, las transacciones en línea alcanzaron la cifra histórica de 186,35 millones, lo que representa un crecimiento del 22,2% en comparación con el mismo periodo del año anterior. Este volumen de operaciones no es un fenómeno aislado, sino la consolidación de una tendencia que ha transformado la arquitectura del consumo en el país. En términos de valor, las ventas corrientes sumaron un total de 39,72 billones de pesos, un incremento del 14,5% frente a los 34,38 billones reportados en el primer trimestre de 2025.

[8] https://www.larepublica.co/internet-economy/la-industria-del-software-representa-alrededor-de-us-10-000-millones-en-colombia-3330546

[9] https://brainitnews.com/comercio-electronico-en-colombia-alcanza-cifras-record-en-2026/

Para los directivos y tomadores de decisión, estas cifras no solo representan un aumento en las ventas, sino un cambio en la estructura misma del mercado, que se ha multiplicado por ocho desde 2019, pasando de 23,3 millones de transacciones a los actuales 186,4 millones. Este crecimiento exponencial sugiere que el comercio electrónico ha dejado de ser un canal secundario para convertirse en el eje central de la estrategia comercial de las grandes compañías y pymes en el territorio nacional.

La madurez del mercado colombiano se evidencia en la estabilidad de su crecimiento. A diferencia de los picos volátiles observados durante la crisis sanitaria de 2020, el dinamismo actual responde a una adopción estructural. “El comercio electrónico en Colombia está entrando en una etapa de madurez. Más que crecimientos episódicos, vemos una adopción estructural y progresiva del canal digital”, afirmó María Fernanda Quiñones, presidenta ejecutiva de la Cámara Colombiana de Comercio Electrónico (CCCE), en el apartado de conclusiones del estudio Informe del primer trimestre económico de 2026. Esta declaración subraya que el consumidor colombiano ya no acude a internet únicamente por necesidad o por ofertas temporales, sino por hábito y conveniencia.

Desde una perspectiva corporativa, este cambio implica que las inversiones en infraestructura digital ya no pueden ser vistas como un gasto opcional de mercadeo, sino como una inversión crítica en activos operativos. La recurrencia de compra es el nuevo motor del sector; los usuarios están realizando transacciones con mayor frecuencia, integrando el canal digital en sus necesidades diarias, desde servicios financieros hasta la compra de bienes básicos.

ANÁLISIS DE LA DEMANDA:

Para el análisis de la demanda se consultó SECOP, identificando procesos de contratación cuyo objeto tuviese elementos y software cercanos o semejantes al del presente proceso, las contrataciones referentes corresponden tanto a las realizadas al interior de la Entidad como a las adelantadas en otras Entidades Estatales.

Se pueden tener en cuenta los siguientes procesos similares en la plataforma de SECOP II:

ENTIDAD	PROCESO	DESCRIPCION	CUANTIA	PROVEEDOR
MUNICIPIO DE LA CEJA	2026.10.05.05.495	RENOVACIÓN DE LICENCIAS DE SOFTWARE (ANTIVIRUS) PARA LAS DEPENDENCIAS DE LA ADMINISTRACIÓN MUNICIPAL.	$29.878.050	NETWORK-TICS
CONTRALORIA DISTRITAL DE BUENAVENTURA	IP-04-033-2026	ADQUISICION LICENCIAS ANTIVIRUS	$7.500.000	Giovanni Enrique Balanta
FONDO ADAPTACIÓN	FA-PS-278-2026	Renovación del licenciamiento de antivirus ESET-ENDPOINT PROTECTION STANDARD.	$20.443.384	Kavantic S.A.S
EMPRESA DE RENOVACION Y DESARROLLO URBANO DE BOGOTA D.C	RENOBO-CD-002-2025	Licenciamiento de Antivirus - DATASEC S.A.S.	$280.058.849	DATASEC S.A.S.
INSTITUTO DISTRITAL DE TURISMO	IDT-MC-004-2024	ADQUISICIÓN DE RENOVACIÓN SOPORTE Y ACTUALIZACION DEL LICENCIAMIENTO DEL	$15.452.700	STAR SOLUTIONS TI S.A.S.

		ANTIVIRUS BITDEFENDER GRAVITIZONE EN LA VERSION ELITE SECURITY		
FONDO ADAPTACIÓN	FA-MC-F-S-002-2024	Renovación del licenciamiento de antivirus ESET-ENDPOINT PROTECTION STANDARD	$415.503.269	Kavantic S.A.S.

En relación con la demanda en entidades Públicas de este servicio en Colombia el **CPNAA** identificó los procesos que se señalan a continuación:

- **ADQUISICIONES PREVIAS DE LA ENTIDAD ESTATAL:**

Según revisión de la información previa consultada en las carpetas contentivas de los contratos celebrados y en el archivo documental de la entidad, el Consejo Profesional Nacional de Arquitectura y sus Profesiones Auxiliares ha celebrado los siguientes contratos:

Proceso de Selección y N° Contrato	Contratista	Objeto	Plazo de Ejecución	Valor
Proceso Mínima Cuantía Contrato de Suministro N° 32 de 2025	Royal Tech Group SAS	Suministrar la licencia de antivirus en la nube para el servidor y los equipos de cómputo del CPNAA.	12 meses	$ 6.050.000
Proceso Mínima Cuantía Contrato N° 24 de 2024.	APROVISIONAR SOLUCIONES S.A.S.	"Suministrar la licencia de antivirus en la nube para el servidor y los equipos de cómputo del CPNAA".	12 meses	$3.961.370
Mínima Cuantía Contrato N° 14 de 2023.	ITO SOFTWARE S.A.S.	"Realizar la Instalación, actualización, renovación y configuración 100% operativa de la licencia de antivirus en la nube para el servidor y los equipos de cómputo del CPNAA".	12 meses	$3.500.000
Mínima Cuantía Contrato N° 19 de 2022.	BIM LATINOAMERICA SAS	Realizar la Instalación, actualización, renovación y configuración 100% operativa de la licencia de antivirus en la nube para el servidor y los equipos de cómputo del CPNAA	12 meses	$2.584.800
Mínima Cuantía Contrato N° 17 de 2021.	ITSEC S.A.S.	Instalación, actualización, renovación y configuración 100% operativa de la licencia de antivirus en la nube para el servidor y los equipos de cómputo del CPNAA.	12 meses	$2.078.490

ESTUDIO DE LA OFERTA

Teniendo en cuenta que el **CPNAA** debe identificar los proveedores en el mercado nacional del bien o servicio y a quienes han participado como oferentes y contratistas en procesos de contratación con entidades estatales, a continuación, para identificar los posibles proveedores, se consultó la página de https://community.secop.gov.co, en el directorio de SECOP, obteniendo los siguientes proveedores que ofrecen servicios similares al objeto de contratación:

NIT	NOMBRE
900480656-4	TEK SOLUCIONES TECNOLOGICAS S.A.S.
900080073-4	CLUSTER DE SERVICIOS SAS
900987336-1	BIM LATINOAMERICA SAS
900306068	SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S

ANÁLISIS DE RIESGO Y FORMA DE MITIGARLO

En razón al tipo de contrato a celebrar y a la actividad a ejecutar, se prevén los siguientes riesgos:

De acuerdo con lo previsto en el artículo 4º de la Ley 1150 de 2007 y los lineamientos del manual de riesgos expedido por Colombia Compra Eficiente, respecto de la presente contratación, el **CPNAA** ha tipificado, estimado y asignado provisionalmente, los siguientes riesgos:

No.	Clase	Fuente	Etapa	Tipo	DESCRIPCIÓN (Qué puede pasar y cómo puede ocurrir)	Consecuencia de la ocurrencia de laevento	Probabilidad	Impacto	Calificación Total	Prioridad
1	General	Interno	Ejecución	Operacional	Ocurre cuando se presentan demoras por parte del CPNAA en las aprobaciones previas de la información generada o solicitada por el proveedor.	Afecta el cumplimiento de las obligaciones del contratante a cargo del supervisor del contrato, relacionadas con la aprobación de la información, generando retrasos en la entrega de las licencias solicitadas.	Improbable	Moderado	Medio	Media
2	General	Externa	Ejecución	Regulatorio	Se presenta por la expedición de normas que impongan nuevos tributos, impuestos o cargas parafiscales, que pueden afectar el equilibrio económico del contrato.	Genera una carga adicional a las previstas, que puede afectar a cualquiera o a las dos partes del contrato.	Improbable	Menor	Bajo	Baja
3	General	Externa	Contratación	Económico	Afectación del estudio de mercado por fluctuación de la moneda cambiaria, en los casos que las licencias dependan de la TRM cambiaria.	Incumplimiento del objeto contractual.	Improbable	Alto	Alto	Alto
4	General	Interno	Ejecución	Operacional	Ocurre cuando se presta el servicio de baja calidad, por falta de experticia del personal del proveedor.	Afecta el servicio prestado por la Entidad y el óptimo funcionamiento de las licencias.	Improbable	Moderado	Medio	Media
5	Específico	Externo	Ejecución	Operacionales	Equipo humano o técnico inadecuados o insuficientes	Baja calidad del servicio, demoras en la prestación del servicio de entrega y configuración de las licencias.	Raro	Alto	Alto	Alto

FORMA DE MITIGARLO:

No.	¿A quién se le asigna?	Tratamiento/Controles a ser implementados	Impacto después del tratamiento			¿Afecta el equilibrio	Persona responsable porimplementar el tratamiento	Monitoreo y revisión	
			Probabilidad	Impacto	Calificación Total			¿Cómo se realizael monitoreoo?	Periodicidad

1	CPNAA	Aplicación y ajuste de los procesos internos de la entidad.	Raro	Insignificante	Baja	No	CPNAA	Cumplimiento de procedimientos y fechas pactadas de entrega.	Permanente
2	CONTRATISTA	El contratista deberá prever esta situación al momento de realizar la oferta.	Raro	Insignificante	Baja	No	Contratista	Validación régimen de impuestos.	Al elaborar la propuesta
3	CONTRATISTA	El contratista deberá prever esta situación al momento de realizar la oferta.	Medio	Alto	Medio	Si	Contratista	Al término de validación de las propuestas	Acto de adjudicación
4	CONTRATISTA	El contratista deberá prever esta situación al momento de realizar la oferta.	Raro	Alto	Alto	No	Contratista	Al término de validación de laspropuestas.	Al elaborar la propuesta
5	CONTRATISTA	El contratista deberá prever esta situación al momento de realizar la oferta.	Raro	Insignificante	Baja	Si	Contratista	Al término de validación de las propuestas	Acto de adjudicación

Probabilidad	Insignificante (1)	Moderado (2)	Mayor (3)	Catastrófico (4)
Raro (1)	2	3	4	5
Posible (2)	3	4	5	6
Probable (3)	4	5	6	7
Casi cierto (4)	5	6	7	8

CATEGORIA	RIESGO
2-3	RIESGO BAJO
4-5	RIESGO MEDIO
6	RIESGO ALTO
7-8	RIESGO EXTREMO

Nota: *En aras de reducir la exposición del Proceso de Contratación frente a los diferentes Riesgos que se pueden presentar, debe estructurarse un sistema de administración de Riesgos teniendo en cuenta, entre otros los siguientes aspectos: (a) los eventos que impiden la adjudicación y firma del contrato como resultado del Proceso de Contratación; (b) los eventos que alteren la ejecución del contrato; (c) el equilibrio económico del contrato; (d) la eficacia del Proceso de Contratación, es decir, que la Entidad Estatal pueda satisfacer la necesidad que motivó el Proceso de Contratación; y (e) la reputación y legitimidad de la Entidad Estatal encargada de prestar el bien o servicio.*

Un manejo adecuado del Riesgo permite a las Entidades estatales: (i) proporcionar un mayor nivel de certeza y conocimiento para la toma de decisiones relacionadas con el Proceso de Contratación; (ii) mejorar la planeación de contingencias del Proceso de Contratación; (iii) incrementar el grado de confianza entre las partes del Proceso de Contratación; (iv) reducir la posibilidad de litigios; entre otros.[10]

[10] Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación M-ICR-01 Colombia Compra Eficiente

En virtud de lo expuesto la Matriz de Riesgo que se plantea en este formato identifica, clasifica, evalúa, califica, asigna tratamiento y establece las actividades posibles para monitorear algunos de los posibles riesgos, luego es un elemento orientador sujeta a ajustes de acuerdo en cada caso en particular.

8. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será por **DOCE (12) MESES,** contados a partir de la suscripción del acta de inicio, una vez se hayan cumplido los requisitos de perfeccionamiento y ejecución del contrato.

9. FORMA DE PAGO

El valor del contrato se cancelará en las fechas establecidas en el calendario de pagos del **CPNAA,** mediante transferencia electrónica, de la siguiente manera:

EJECUCIÓN DE PAGOS	CONTENIDO DEL INFORME
Un (1) pago correspondiente al 100% del valor total del contrato.	Una vez la licencia de la Solución de seguridad digital, antivirus y protección endpoint sea activada y renovada y se encuentre 100% operativa en los equipos de cómputo y servidores del **CPNAA**, en cumplimiento del objeto contractual y cumplido el primer mes vencido de firma del acta de inicio.

El **CPNAA** realizará el pago del contrato conforme al calendario establecido en su sitio web https://www.cpnaa.gov.co/calendario-de-pagos-a-proveedores-y-trabajadores/. Para ello, el **CONTRATISTA** deberá radicar la factura o documento equivalente en la ventanilla única del CPNAA, atendiendo los parámetros y directrices de Colombia Compra Eficiente, enviarla al correo electrónico info@cpnaa.gov.co y cargarla en el proceso contractual del SECOP II. La factura debe estar acompañada de la certificación del supervisor sobre la correcta ejecución del contrato y de los comprobantes de pago de aportes al Sistema de Seguridad Social Integral, en cumplimiento de lo dispuesto en el artículo 23 de la Ley 1150 de 2007, Ley 1607 de 2012, Ley 1753 de 2015, Decreto 1828 de 2013, Decreto 1273 de 2018 y demás normas reglamentarias aplicables.

Para los desembolsos, el **CONTRATISTA** deberá acreditar su afiliación y pago al Sistema de Seguridad Social Integral conforme a la normatividad vigente.

PARÁGRAFO: El **CONTRATISTA** deberá asumir los costos derivados de los servicios que requiera tales como equipos de computación, impresiones, digitalización de información, papelería y demás implementos y servicios necesarios para la ejecución del contrato, sin perjuicio de la obligación de acompañamiento que asume la entidad para el cumplimiento de las obligaciones a cargo del **CPNAA.** Si la factura o documento equivalente no ha sido correctamente elaborada o no se acompañan de los documentos requeridos para el pago, el término para éste solamente empezará a contarse desde la fecha en que se presenten en debida forma o se haya aportado el último de los documentos. Las demoras que se presenten por estos conceptos serán responsabilidad del **CONTRATISTA** y no tendrá por ello derecho al pago de intereses o compensación de ninguna naturaleza. Los pagos se efectuarán a través de la consignación en la cuenta corriente o de ahorros que indique el **CONTRATISTA** previos los descuentos de Ley si a ello hubiere lugar. El valor establecido en el presente numeral, contempla los gastos, descuentos e impuestos que se generan para la suscripción y legalización del contrato y en los pagos.

10. CARACTERÍSTICAS TÉCNICAS DEL BIEN O SERVICIO O FICHA TÉCNICA

Las especificaciones técnicas corresponden a las condiciones mínimas obligatorias que integran el requerimiento del **CPNAA** y que deben ser tenidas en cuenta por los interesados en el proceso. Estas especificaciones tienen carácter habilitante, en la medida en que constituyen aspectos esenciales para garantizar el adecuado suministro de los bienes requeridos.

En atención a lo anterior, se deben contemplar las siguientes especificaciones técnicas:

FICHA TÉCNICA DE SERVICIOS
DESCRIPCIÓN DE REQUERIMIENTOS MÍNIMOS

ITEM	DESCRIPCIÓN
Licenciamiento para 39 equipos en línea.	*Renovación, activación, actualización de plataforma Kaspersky Next EDR, para equipos de cómputo con sistemas operativos: Windows 10,11 Pro y servidor de propiedad de CPNAA.*

11. MECANISMOS DE COBERTURA

De conformidad con lo establecido en el artículo 7 de la Ley 1150 de 2007 y 2.2.1.2.3.1.1 y ss. Del Decreto 1082 de 2015, una vez aprobada la aceptación de la oferta, el **CONTRATISTA** deberá constituir en un plazo no mayor a un (1) día hábil a favor del **CPNAA,** una garantía única que avalará el cumplimiento de las obligaciones surgidas del contrato, la cual contendrá el siguiente amparo:

***De cumplimiento:** En cuantía equivalente al diez por ciento (10%) del valor total del contrato y con una vigencia igual al término de la duración del mismo y cuatro (4) meses más*
***De calidad del servicio**: En cuantía equivalente al diez por ciento (10%) del valor total del contrato y con una vigencia igual al término de duración del mismo y cuatro (4) meses más.*
***De salarios, prestaciones sociales e indemnizaciones:** En cuantía equivalente al cinco por ciento (5%) del valor total del contrato y con una vigencia igual al término de duración del mismo y tres (3) años más.*

El **CONTRATISTA** deberá reponer la garantía cuando el valor de la misma se vea afectada por razón de siniestros. De igual manera en cualquier evento en que se aumente el valor del contrato o se prorrogue su vigencia debe ampliar o prorrogar la correspondiente garantía, de acuerdo con las normas legales vigentes y sin ningún costo adicional para el **CPNAA.**

12. OBLIGACIONES DEL CONTRATISTA

Además de las obligaciones inherentes a la naturaleza del contrato, el **CONTRATISTA** se obliga a:

DE CARÁCTER ESPECIAL.

1. Cumplir con el objeto del contrato en las condiciones y plazos pactados y con los requerimientos técnicos señalados en la **FICHA TÉCNICA DE SERVICIOS - DESCRIPCIÓN DE REQUERIMIENTOS MÍNIMOS.**
2. Renovar, activar y entregar la licencia del antivirus Kaspersky Next EDR, la cual debe continuar siendo compatible y operativa con sistemas Windows 10 Pro, 11 Pro de 64 bits y Windows Server 2016, cuya fecha de vencimiento actual es 07/08/2026.
3. Proveer y realizar la instalación en sitio y de manera remota, cuando se presenten fallas técnicas en la consola de Kaspersky y en cualquiera de las 39 licencias requeridas, en las oficinas de la carrera 6 No. 26 B-85, en la ciudad de Bogotá D. C., cuando el **CPNAA** así lo requiera.

Los servicios de instalación deben incluir:

- *Implementación de la consola de administración de antivirus en la nube para: Servidor y equipos de cómputo de propiedad del **CPNAA**.*
- *Transferencia y apoyo de conocimiento en el manejo de la plataforma de antivirus.*
- *Brindar soporte y servicio a través de personal experto en las herramientas contratadas, referente a la corrección de fallas en los sistemas ofrecidos, entendiendo por falla la degradación o pérdida de una funcionalidad previamente configurada.*
- *Servicio de atención pos instalación en las oficinas del **CPNAA**, en caso que no lograr solucionar el incidente de manera telefónica, vía email o remotamente.*
- *Reconfiguración en caso de pérdida de datos en la configuración inicial y las estaciones de trabajo para la plataforma antivirus.*
- *El horario de atención para la prestación del servicio de soporte ilimitado deberá ser de lunes a viernes, en horario de oficina del **CPNAA**, durante la vigencia del contrato.*
- *Entrega de licencias de uso y los medios necesarios para instalar las versiones Server y Cliente de las licencias objeto de este proceso contractual.*
- *El soporte remoto deberá prestarse mediante las herramientas de diagnóstico o de soporte remoto comprendidas por el proveedor.*

4. Garantizar y prestar el soporte técnico al **CPNAA,** ante las fallas de los programas, licencias y la consola de administración instaladas, que surjan durante el tiempo de ejecución del contrato y durante el periodo de la renovación, cuya solución debe generarse en un tiempo no mayor a 6 horas hábiles, de manera presencial y virtual a través de acceso remoto, una vez reportada la falla vía correo electrónico por parte del **CPNAA.**

5. El **CONTRATISTA** deberá estar certificado como proveedor o distribuidor autorizado o partner registrado por el fabricante Kaspersky.

6. Ante la materialización de un ataque informático por virus o falla de la consola de antivirus a la red y equipos del **CPNAA,** garantizar el apoyo y soporte por parte del proveedor, en la plataforma antivirus, en un tiempo no mayor a seis (6) horas hábiles de forma telefónica, presencial o a través de conexión remota, todo esto a fin de estabilizar nuevamente la red, detección y análisis de causa raíz y asegurar la eliminación del ataque informático y virus en el equipo o los equipos afectados.

7. La solución de antivirus debe continuar siendo efectiva ante posibles ataques de virus, entre otros de las siguientes clases: prevención de malware, protección contra ransomware y análisis de vulnerabilidades.

8. Garantizar la calidad y buen funcionamiento del producto licenciado en el periodo establecido y en caso tal cambiar y reinstalar a todo costo y sin perjuicio alguno para el **CPNAA,** el servicio defectuoso, entendiéndose esto como aquel que habiéndose recibido e instalado a satisfacción del **CPNAA,** a través de la supervisión, presente defectos y fallas con posterioridad a su entrega, durante la vigencia del contrato.

9. Responder por las pérdidas y daños que durante y en ejercicio de sus actividades para el cumplimiento de las obligaciones del contrato, el personal a su cargo ocasione a los equipos objeto de instalación de la licencia, las personas o bienes del **CPNAA.**

10. Las demás que el **CPNAA** considere pertinentes de acuerdo con las necesidades que se deriven del contrato.

DE CARÁCTER GENERAL:

1. Cumplir a cabalidad con lo establecido en el objeto y alcance descritos en el presente documento en los términos y condiciones aquí pactadas y a lo señalado en su propuesta, observando en todo momento la constitución política, las leyes colombianas y el régimen de contratación pública. Por ningún motivo suspenderá o abandonará el cumplimiento del contrato, sin previa justificación aceptada por la Entidad contratante. El **CONTRATISTA** no podrá subcontratar ni ceder el contrato sin el consentimiento previo y escrito del **CPNAA**.

2. Cumplir con los pagos correspondientes al Sistema General de Salud y de Seguridad Social Integral, de conformidad con lo establecido por la normatividad vigente conforme el artículo 23 de la Ley 1150 de 2007, Ley 1607 de 2012, Ley 1753 de 2015, Decreto 1828 del 27 de agosto de 2014 y Decreto 1273 de Julio de 2018, y demás normas reglamentarias y complementarias con la materia.
3. Cumplir con las normas vigentes en materia del Sistema de Gestión de Seguridad y Salud en el Trabajo en el marco del Decreto 1443 del 31 de julio de 2014 que fuera compilado por el Decreto 1072 del 26 de mayo de 2015 y demás normas reglamentarias y complementarias con la materia.
4. Obrar con lealtad, responsabilidad, idoneidad en desarrollo del objeto contractual.
5. Realizar por su cuenta y riesgo todas las diligencias que se requieran para cumplir el objeto del contrato a celebrar, las cuales quedarán bajo su responsabilidad.
6. Pagar oportunamente los salarios, prestaciones e indemnizaciones de carácter laboral del personal que contrate para la ejecución del contrato, lo mismo que el pago de honorarios, los impuestos, gravámenes, aportes y servicios de cualquier género que establezcan las leyes colombianas y demás erogaciones necesarias para la ejecución del contrato. Es entendido que todos estos gastos han sido estimados por el proponente e incluido en el precio de su oferta.
7. Presentar al supervisor del contrato los informes y los soportes que sean requeridos sobre la ejecución del objeto y las obligaciones contractuales cuando sea solicitado por el mismo.
8. Responder por los bienes muebles, equipos y elementos de oficina que le sean entregados para la correcta ejecución de las actividades encomendadas. A la terminación del contrato devolverá debidamente inventariados dichos bienes (Si a ello hubiere lugar).
9. TELEPRESTRACION: Cuando el **CPNAA** así lo determine, el **CONTRATISTA** podrá ejecutar las actividades contractuales que le sean asignadas por el supervisor previamente, haciendo uso de las tecnologías de la información y comunicaciones como medio para cumplir con la actividad contractual. Para ello deberá disponer de los recursos tecnológicos necesarios y entregar el producto de la actividad encomendada en el tiempo solicitado por el supervisor. Parágrafo: Si para tal efecto el **CPNAA** pone a disposición del **CONTRATISTA** equipos, softwares o cualquier clase de herramientas, el **CONTRATISTA** será la única responsable del cuidado, buen uso y control de los mismos. En todo caso, el **CONTRATISTA** responderá por la integridad, seguridad y confidencialidad de la información del **CPNAA** de la que pueda hacer uso en ejecución de cualquier actividad desarrollada bajo el esquema de tele prestación. (Si a ello hubiere lugar)
10. Mantener confidencialidad y seguridad en el manejo de la información con ocasión del objeto contratado.
11. Abstenerse de hacer uso de la información a la que accede con ocasión al objeto contractual para cualquier objetivo diferente al mismo.
12. Hacer buen uso de los recursos suministrados por el **CPNAA** para el cumplimiento del objeto contractual.
13. Responder civil y penalmente tanto por el cumplimiento de las obligaciones derivadas del contrato, como por hechos u omisiones que le fueren imputables y que causen daño o perjuicio a la entidad de conformidad con lo establecido en el artículo 52 de la Ley 80 de 1993 y sus normas complementarias.
14. Será obligación exclusiva del **CONTRATISTA** mantener al **CPNAA** indemne de cualquier reclamación proveniente de terceros que tenga como causa las actuaciones del **CONTRATISTA.**
15. Constituir la garantía única que avala el cumplimiento de las obligaciones surgidas del contrato. así como ampliar o modificar la vigencia de las pólizas en los eventos en que conforme a la Ley se lo solicite el **CPNAA.** (Si a ello hubiere lugar).
16. Mantener actualizado su lugar de residencia durante la vigencia del contrato y cuatro (4) meses más y presentarse al Consejo en el momento en que sea requerida por el mismo para la suscripción de la correspondiente Acta de Liquidación, si a ello hubiere lugar.
17. Mantener los precios ofrecidos durante la ejecución del contrato.
18. Constituyen derechos y deberes para efectos del contrato a celebrar los contenidos en el artículo 5 de la Ley 80 de 1993.
19. Las demás que le indique el Supervisor del Contrato y que se relacionen con el objeto del contrato.

13. SUPERVISIÓN

El **CPNAA** ejercerá la supervisión del contrato a través del **Profesional Especializado Código 02 Grado 04 de la Oficina Administrativa y Financiera** o quien designe el Director Ejecutivo del **CPNAA,** quien será responsable de cumplir con lo establecido en el Manual de Contratación y Supervisión del Consejo Profesional Nacional de Arquitectura y sus Profesiones Auxiliares y la Ley 80 de 1993, la Ley 1150 de 2007, la Ley 1474 de 2011 y demás normas y decretos que le sean aplicables.



Emil Andrés Mena Palacios
Profesional Especializado Código 02 Grado 04
Oficina Administrativa y Financiera