

OBJETO PROCESO:

Contratar la renovación de la solución de antivirus Trellix Endpoint Security Suite (TRXE1), Suite Cloud Workload Security - Essentials - (CWS-E) existentes en la entidad, y adquisición del licenciamiento adicional con soporte técnico por 1 año, de acuerdo con las características y condiciones técnicas definidas.

ASPECTOS GENERALES

El objeto del presente proceso tiene relación con servicios de licencias de software y servicios de soporte técnico.

La cadena de valor del sector TIC en Colombia se compone de cinco grandes dimensiones, (1) la infraestructura que soporta la utilización de los servicios y productos, (2) la fabricación y/o venta de los bienes TIC, (3) la producción de los servicios de telecomunicaciones, donde el servicio de Internet comienza a ser el punto de surgimiento de una nueva industria, (4) la industria de las plataformas digitales. Toda la cadena de valor (Gráfica 1) tiene como componente transversal el conjunto de actividades de (5) investigación, desarrollo e innovación necesarias para la continua evolución del sector.¹

ECONÓMICO


Fuente: Autor, Guide to Measuring the Information Society (2011). OECD; Clasificación Central de Productos – CPC Vers. 2 A.C. DANE; CRC (2010). Análisis del sector TIC en Colombia: Evolución y Desafíos; RAÚL KATZ (2015). El ecosistema y la economía digital en América Latina.

Figura 1. Cadena de valor sector tics

Las Tecnologías de la Información (TI) han sido claves en el cambio de los modelos de los negocios a nivel mundial donde el manejo y transmisión de grandes cantidades de información en tiempos cada vez más cortos son fundamentales, su utilización y desarrollo han promovido cambios estructurales en los modos de producción y la forma en que se articulan, permitiendo que las diferentes partes de un proceso productivo se lleven a cabo desde diferentes lugares del mundo desde donde se transmiten sus componentes a gran velocidad.

Entre los agentes que componen el sector de software se tienen: entidades gubernamentales, empresas nacionales de software, empresas internacionales de software, academia, entidades de integración, industrias conexas y ciencias administrativas de soporte.

¹ Ministerio de Tecnologías de la Información y las Comunicaciones. Panorama TIC – diciembre 2015, https://colombiatic.mintic.gov.co/679/articles-73994_recurso_1.pdf

La industria de software y las tecnologías de la información se sigue consolidando en Colombia.

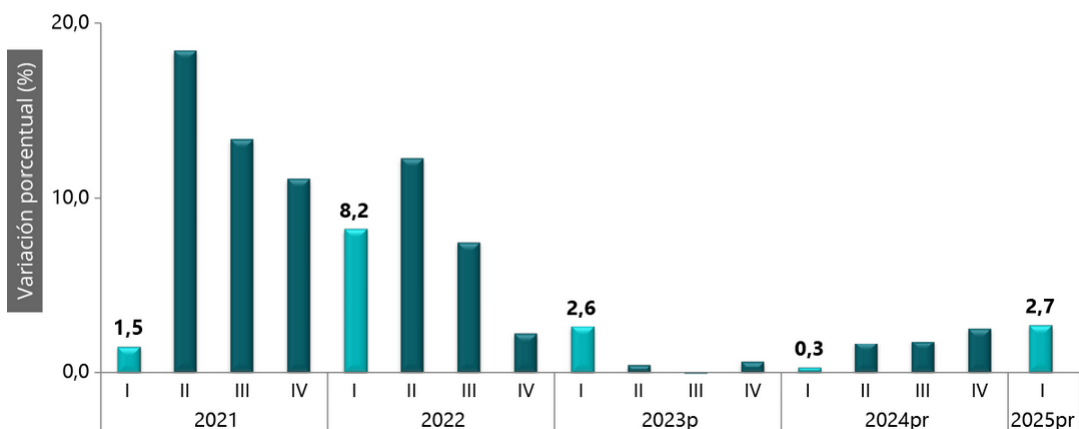
El presente proceso se enmarca en el sector terciario o de servicios y específicamente de las tecnologías de la información y la comunicación – TICS, en la dimensión de Producción de Servicios TIC.

Este sector es vital para la economía, especialmente en países desarrollados, y ha experimentado un crecimiento significativo en las últimas décadas. Este aumento se debe a varios factores, como la automatización, la globalización, y un incremento en la demanda debido a la subida de los ingresos y el crecimiento de la población. Como resultado, el sector terciario se ha convertido en una parte esencial del Producto Interno Bruto (PIB) de muchos países, tanto desarrollados como en desarrollo.²

REPORTE DE LAS ESTADÍSTICAS DEL PRIMER TRIMESTRE 2025 PRELIMINAR DEL PRODUCTO INTERNO BRUTO (PIB)³:

Producto Interno Bruto (PIB)

Tasas de crecimiento anual en volumen¹
2020-I / 2025^{pr} - I



En el primer trimestre de 2025^{pr}, el Producto Interno Bruto en su serie original, crece 2,7% respecto al mismo periodo de 2024^{pr}

1. PRODUCTO INTERNO BRUTO (PIB) SERIES ENCADENADAS DE VOLUMEN CON AÑO DE REFERENCIA 2015

1.1 PIB desde el enfoque de la producción

En el primer trimestre de 2025^{pr}, el Producto Interno Bruto en su serie original, crece 2,7% respecto al mismo periodo de 2024^{pr} (ver tabla 1). Las actividades económicas que más contribuyen a la dinámica del valor agregado son:

² <https://economipedia.com/definiciones/sector-terciario-servicios.html>

³ <https://www.dane.gov.co/files/operaciones/PIB/bol-PIB-Itrim2025.pdf>



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

- Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida crece 3,9% (contribuye 0,8 puntos porcentuales a la variación anual).
- Agricultura, ganadería, caza, silvicultura y pesca crece 7,1% (contribuye 0,7 puntos porcentuales a la variación anual).
- Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios; Actividades de los hogares individuales en calidad de empleadores; actividades no diferenciadas de los hogares individuales como productores de bienes y servicios para uso propio crece 15,5% (contribuye 0,6 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 0,8%. Cuando se observa el comportamiento de las actividades económicas relacionadas:

- 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 4,1%.
- Actividades financieras y de seguros crece 1,0%.
- Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales crece 0,6%.

**Tabla 1. Valor agregado por actividad económica
Tasas de crecimiento en volumen¹
Primer trimestre 2025^{Pr}**

Actividad económica	Tasas de crecimiento (%)	
	Serie original	Serie ajustada por efecto estacional y calendario
		Trimestral
	2025 ^{Pr} -I / 2024 ^{Pr} -I	2025 ^{Pr} -I / 2024 ^{Pr} -IV
Agricultura, ganadería, caza, silvicultura y pesca	7,1	-0,2
Explotación de minas y canteras	-5,0	0,2
Industrias manufactureras	1,4	0,2
Suministro de electricidad, gas, vapor y aire acondicionado ²	-1,2	0,3
Construcción	-3,5	-1,8
Comercio al por mayor y al por menor ³	3,9	0,4
Información y comunicaciones	0,7	-1,0
Actividades financieras y de seguros	3,3	1,0
Actividades inmobiliarias	2,1	0,5
Actividades profesionales, científicas y técnicas ⁴	1,0	0,6
Administración pública, defensa, educación y salud ⁵	3,5	0,6
Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios ⁶	15,5	4,1
Valor agregado bruto	2,7	0,6
Impuestos menos subvenciones sobre los productos	2,2	-0,3
Producto Interno Bruto	2,7	0,8

Fuente: DANE, PIB_T

^{Pr} preliminar

¹Series encadenadas de volumen con año de referencia 2015.

²Suministro de electricidad, gas, vapor y aire acondicionado; Distribución de agua; evacuación y tratamiento de aguas residuales, gestión de desechos y actividades de saneamiento ambiental.

³Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida.

⁴Actividades profesionales, científicas y técnicas; Actividades de servicios administrativos y de apoyo.

⁵Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales.

⁶Actividades 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.

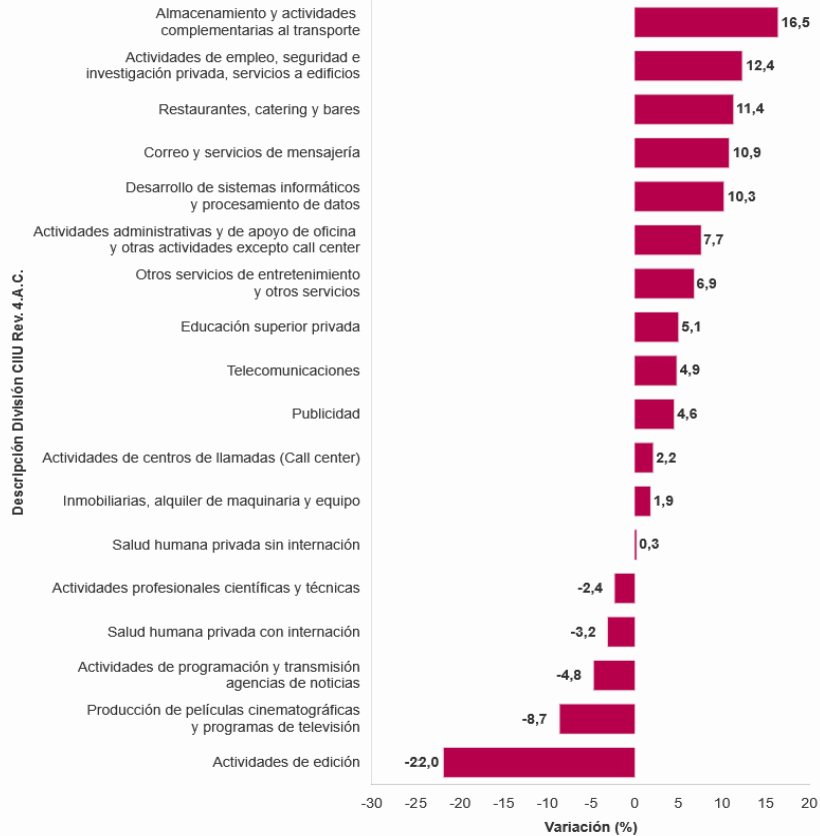
Fuente: Boletín técnico del PIB del primer trimestre de 2025 - DANE

En abril de 2025, trece de los dieciocho subsectores de servicios presentaron variación positiva en los ingresos totales, en comparación con abril de 2024.⁴

⁴ <https://www.dane.gov.co/files/operaciones/EMS/bol-EMS-abr2025.pdf>

Encuesta Mensual de Servicios (EMS)

Variación anual de los ingresos nominales
Total Nacional
Abril (2025P - 2024)



Fuente: DANE - EMS
P Cifra provisional

Por otra parte, en el boletín técnico de Cuenta Satélite de las Tecnologías de la Información y las Comunicaciones (CSTIC) 2022 – 2024pr, publicado por el DANE el 28 de marzo de 2025⁵, se presentan los principales agregados macroeconómicos del sector TIC 2022 - 2024pr relacionados a continuación:

Cuenta de producción y generación del ingreso

⁵ <https://www.dane.gov.co/files/operaciones/CSTIC/bol-CSTIC-2024pr.pdf>

La cuenta de producción permite medir el valor agregado generado en el proceso productivo de las actividades económicas características del sector. El valor agregado se obtiene de la diferencia entre la producción y el consumo intermedio.

La cuenta de generación del ingreso registra la remuneración de los asalariados, los impuestos menos subvenciones sobre la producción y el saldo de la cuenta, que corresponde al excedente de explotación bruto e ingreso mixto bruto.

Tabla 1. Cuenta de producción y generación del ingreso del sector TIC (millones de pesos)

Valores a precios corrientes

Total nacional

2022 - 2024^{Pr}

Concepto	2022	2023^P	2024^{Pr}
Producción	98.216.502	104.319.039	106.767.791
(-) Consumo Intermedio	49.067.026	52.270.418	53.138.822
(=) Valor Agregado	49.149.476	52.048.621	53.628.969
(-) Remuneración de los asalariados	19.740.714	22.467.788	23.785.475
(-) Impuestos menos subvenciones sobre la producción y las importaciones	1.710.830	1.979.277	1.998.041
(=) Excedente de explotación bruto e ingreso mixto bruto	27.697.932	27.601.556	27.845.453

Fuente: DANE - Ministerio de Tecnologías de la Información y Comunicaciones. Cuenta Satélite TIC

^P provisional

^{Pr} preliminar

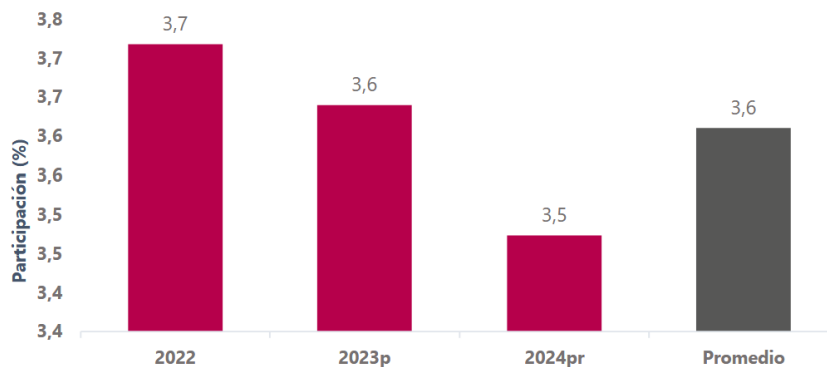
En 2024^{pr} el valor agregado del sector TIC ascendió a 53,6 billones de pesos presentando un crecimiento de 3,0% respecto a 2023^p; mientras que en 2023^p el valor agregado fue de 52,0 billones de pesos, con un crecimiento de 5,9% al compararlo con el año 2022.

El excedente de explotación bruto e ingreso mixto bruto de la cuenta satélite TIC presentó un crecimiento de 0,9% en 2024^{pr}, mientras que en 2023^p presentó un decrecimiento de 0,3% respecto a 2022.

Participación del valor agregado del sector TIC en el valor agregado nacional

El sector TIC para 2024^{pr} registró una participación de 3,5% con relación al valor agregado nacional; en 2023^p esta participación fue de 3,6%, mientras que para el período 2022 – 2024^{pr} en promedio su participación fue de 3,6% respecto al total del valor agregado nacional.

Gráfico 2. Participación porcentual del valor agregado del sector TIC en el valor agregado nacional Total nacional 2022 - 2024^{Pr}



Fuente: DANE - Ministerio de Tecnologías de la Información y las Comunicaciones. Cuenta Satélite TIC
^P provisional
^{Pr} preliminar

Participación del valor agregado de las actividades económicas características en el sector TIC

En 2024^{pr} la actividad económica TIC que registró la mayor participación dentro del valor agregado del sector TIC fue servicios TI con un 40,1%; seguido de telecomunicaciones con 36,6%; comercio TIC con 12,8%; contenido y media con 9,6%; manufactura TIC con 0,5%, e infraestructura TIC con 0,4%.

Tabla 2. Participación porcentual del valor agregado de las actividades económicas características en el sector TIC

Total nacional 2022 – 2024^{Pr}

Actividad característica TIC	2022	2023 ^P	2024 ^{Pr}
Servicios TI	38,9	39,9	40,1
Telecomunicaciones	38,9	37,2	36,6
Comercio TIC	12,7	12,6	12,8
Contenido y Media	8,7	9,5	9,6
Manufactura TIC	0,5	0,5	0,5
Infraestructura TIC	0,3	0,3	0,4
Total sector TIC	100,0	100,0	100,0

Fuente: DANE – Ministerio de Tecnologías de la Información y Comunicaciones. Cuenta Satélite TIC
^P provisional
^{Pr} preliminar

Teniendo en cuenta lo anterior, la actividad económica TIC- Servicios de TI tuvo una participación importante en los últimos tres años.

Por otro lado, En cuanto al licenciamiento requerido para el presente proceso, el siguiente artículo presenta un panorama de la ciberseguridad en el país.

Tendencias de ciberataques en Colombia 2025: ¿Qué sectores están en la mira?⁶

Colombia enfrenta una situación alarmante en el ámbito de la ciberseguridad, con cifras que evidencian un incremento sin precedentes en los ataques digitales. Entre enero y noviembre de 2024, el país fue víctima de 36 mil millones de intentos de ciberataques, mientras que las denuncias por delitos informáticos alcanzaron 77.866 casos, representando un aumento del 23% respecto al año anterior. Este panorama posiciona a Colombia como el cuarto país más atacado en Latinoamérica según el Informe Ransomware 2024, generando preocupación tanto en el sector público como privado. A continuación, analizamos los sectores más vulnerables, las amenazas predominantes y las estrategias de respuesta que están surgiendo en este contexto.

La escalada de ciberataques en Colombia

El incremento de ciberataques en Colombia ha sido exponencial en los últimos años. De acuerdo con los datos disponibles, el país experimentó un salto de 12.000 millones de intentos de ciberataques en 2023 a 20.000 millones en los primeros meses de 2024, lo que refleja un incremento cercano al 70% en menos de un año. Esta tendencia ha continuado a lo largo de 2024, convirtiendo a Colombia en un punto focal de la cibercriminalidad en América Latina.

La sofisticación de estas amenazas es otro factor preocupante. Los ataques ya no se limitan a intentos masivos de phishing o malware genérico, sino que ahora incluyen ataques dirigidos que explotan vulnerabilidades específicas y son ejecutados por actores cada vez más organizados y tecnificados. Esta evolución en las técnicas de ataque ha superado en muchos casos la capacidad de respuesta tanto del sector público como privado.

Ante este panorama, se prevé que para 2025 la inversión en ciberseguridad en Colombia crezca un 19%, una respuesta necesaria pero que requerirá estrategias coordinadas y efectivas para contrarrestar la creciente amenaza.

Amenazas predominantes en el escenario colombiano**El reinado del ransomware**

El ransomware continúa siendo la modalidad de ataque preferida por los ciberdelincuentes en Colombia. Solo en la primera mitad de 2023, el país experimentó más de 1.000 millones de ataques de este tipo, una tendencia que ha continuado durante 2024 y 2025. La preferencia por este tipo de ataque se debe a su alto índice de éxito y al potencial de ganancias financieras rápidas mediante la extorsión a las víctimas.

Las organizaciones afectadas se enfrentan a un dilema difícil: pagar el rescate para recuperar sus datos o intentar restaurar sus sistemas por otros medios, frecuentemente costosos y con resultados inciertos. Además, incluso el pago del rescate no garantiza la recuperación completa de la información o la ausencia de filtraciones posteriores.

Phishing y ataques dirigidos

Los ataques de phishing y otras técnicas de ingeniería social han evolucionado hacia estrategias más sofisticadas y dirigidas. En lugar de campañas masivas con mensajes genéricos, los ciberdelincuentes

⁶ <https://pralogy.co/wp/2025/05/12/tendencias-de-ciberataques-en-colombia-2025-que-sectores-estan-en-la-mira/>

están realizando ataques altamente personalizados (spear phishing) contra objetivos específicos dentro de las organizaciones, particularmente aquellos con acceso a información sensible o capacidad para autorizar transferencias financieras.

Estos ataques explotan el factor humano como el eslabón más débil de la cadena de seguridad, utilizando técnicas psicológicas avanzadas para manipular a las víctimas y obtener credenciales, información confidencial o provocar acciones que comprometan la seguridad.

Explotación de vulnerabilidades técnicas

Los cibercriminales continúan aprovechando vulnerabilidades en sistemas desactualizados y procesos mal protegidos para infiltrarse en las redes corporativas y gubernamentales. La falta de parches de seguridad oportunos, configuraciones inadecuadas y la ausencia de monitoreo continuo facilitan estas intrusiones, que pueden pasar desapercibidas durante meses mientras los atacantes extraen información valiosa o preparan ataques más devastadores.

Estrategias y respuestas ante el panorama de amenazas**Iniciativas gubernamentales para fortalecer la ciberseguridad**

El gobierno colombiano ha reconocido la gravedad de la situación y ha tomado medidas para fortalecer la postura de ciberseguridad del país. Una de las iniciativas más destacadas es la actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) por parte del Ministerio TIC, basándose en la norma internacional ISO/IEC 27001:2022. Esta actualización busca garantizar la integridad, confidencialidad y disponibilidad de la información en las entidades públicas, así como construir un entorno digital confiable para la interacción entre ciudadanos e instituciones estatales. Paralelamente, desde hace tres años se debate en Colombia la creación de una agencia nacional para la ciberseguridad, propuesta promovida por Saúl Kattan, consejero presidencial para la Transformación Digital. Esta iniciativa busca centralizar y coordinar los esfuerzos nacionales en materia de ciberseguridad, proporcionando capacidades avanzadas de respuesta ante incidentes.

Recomendaciones para organizaciones

Frente al creciente riesgo, los expertos recomiendan que las organizaciones adopten un enfoque proactivo en su ciberseguridad. "Los ataques cibernéticos no solo representan una amenaza para la reputación empresarial, sino que también pueden causar una parálisis operativa significativa. Es crucial que las empresas inviertan en tecnologías de predicción y prevención de riesgos, y establezcan procesos y procedimientos sólidos para la detección y recuperación ante incidentes de ciberseguridad", indica Ricardo Pulgarín, director de productos y servicios en ciberseguridad de Olimpia.

Las recomendaciones específicas incluyen:

- Implementar sistemas de autenticación multifactor
- Mantener actualizados todos los sistemas operativos y aplicaciones
- Realizar copias de seguridad periódicas y almacenarlas fuera de línea
- Capacitar constantemente al personal sobre amenazas de ingeniería social
- Desarrollar y probar planes de respuesta a incidentes cibernéticos
- Considerar la contratación de seguros específicos contra riesgos cibernéticos

Para concluir el panorama de ciberataques en Colombia para 2025 muestra un claro incremento tanto en la cantidad como en la sofisticación de las amenazas. Los sectores financieros, salud,

educación y gobierno continuarán siendo blancos prioritarios, lo que exigirá estrategias defensivas cada vez más robustas y adaptativas.

El ransomware seguirá siendo la amenaza predominante, complementado por ataques de phishing dirigido y la explotación de vulnerabilidades técnicas. Ante este escenario, es fundamental que tanto el sector público como el privado aumenten su inversión en ciberseguridad, mejoren sus capacidades de detección y respuesta, y fomenten una cultura de seguridad digital en todos los niveles organizacionales.

La colaboración entre sectores será clave para enfrentar las amenazas de manera efectiva. El intercambio de información sobre amenazas, la coordinación de respuestas ante incidentes y el desarrollo de capacidades conjuntas mejorarán la postura de seguridad digital del país, permitiendo una mayor resiliencia frente al cambiante panorama de ciberamenazas que enfrentamos.

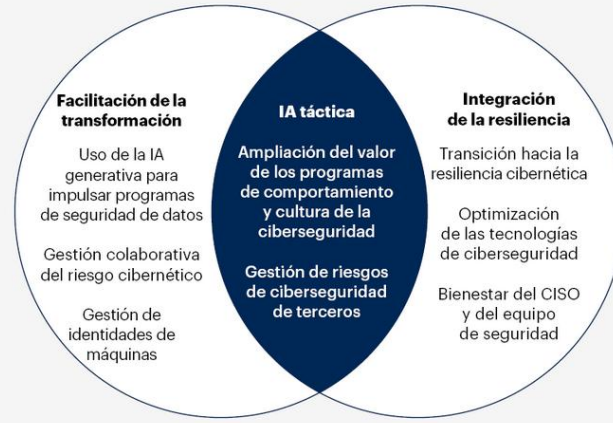
Teniendo en cuenta la perspectiva de la ciberseguridad, la entidad busca fortalecer la seguridad de la información a través de las diferentes soluciones del mercado y actualmente se tiene implementada en la entidad la solución de antivirus Trellix MVISION Protect Plus EDR for Endpoint y la Suite Cloud Workload Security - Essentials - (CWS-E) y con el presente proceso se efectuará la renovación y ampliación del licenciamiento de la solución de antivirus que nos permita el fortalecimiento, la resiliencia organizacional, personal y del equipo, con el fin de brindar la seguridad de la información.

Las principales tendencias en ciberseguridad para 2025 se centran en la resiliencia y la transformación⁷

Estas son las tendencias clave para los responsables de ciberseguridad: educar, colaborar y prevenir el agotamiento para integrar la resiliencia en los programas de ciberseguridad.

⁷ <https://www.gartner.es/es/ciberseguridad/temas/tendencias-ciberseguridad#:~:text=Las%20principales%20tendencias%20en%20ciberseguridad%20para%202025%20se%20centran%20en,en%20los%20programas%20de%20ciberseguridad.>

Principales tendencias en ciberseguridad para 2025



Fuente: Gartner
© 2025 Gartner, Inc. o sus filiales. Todos los derechos reservados. 3363616

Gartner

Un entorno de amenazas en constante evolución obliga a modificar el enfoque de la ciberseguridad

“¿Qué es la ciberseguridad?”: es la práctica de destinar personal, procesos, políticas y tecnologías a proteger las organizaciones, sus sistemas esenciales y su información confidencial frente a los ataques digitales.

Estas prácticas están cambiando radicalmente en las organizaciones.

Los responsables de ciberseguridad deben mantenerse al día de las tendencias y buenas prácticas en su área si quieren gestionar eficazmente las amenazas y exposiciones diarias en constante cambio a las que se enfrenta la organización sin limitar las aspiraciones empresariales.

La encuesta de Gartner sobre las principales tendencias en ciberseguridad para 2025 revela nuevas presiones derivadas de:

- El crecimiento constante de los casos de uso (y riesgos) asociados a la IA generativa.
- El agotamiento causado por la continua brecha entre la oferta y la demanda de talento experto en seguridad.
- El crecimiento incesante de la adopción de la nube, que está alterando la composición de los ecosistemas digitales.
- El incremento en las obligaciones reglamentarias y la supervisión de los gobiernos en temas de ciberseguridad, privacidad y localización de datos.
- La constante descentralización de las capacidades digitales en todo el conjunto de la empresa.
- El reto de integrar una cultura de gestión colaborativa del riesgo.
- La exigencia de estabilidad/seguridad empresarial en un entorno de amenazas en constante evolución.

- El bienestar del CISO y del equipo de seguridad.
- La gestión colaborativa del riesgo cibernético.
- La gestión de identidades de máquinas.
- Como respuesta, los responsables de ciberseguridad trabajan para dotar a sus departamentos de capacidades ágiles y adaptables. El informe de tendencias de 2025 revela que los responsables de ciberseguridad están enfocando sus medidas y prioridades en nueve prácticas, capacidades técnicas y reformas estructurales que les permiten avanzar hacia:
- Una transformación empresarial segura e impulsada por la IA, mediante la formalización de la responsabilidad de los riesgos de ciberseguridad, el fomento del juicio cibernético, la revitalización de los programas de gestión de seguridad de datos y la ampliación de las estrategias de IAM para incluir identidades de máquinas.
- La resiliencia a través de la planificación y revisión periódica de las capacidades tecnológicas y humanas, mediante la optimización de la inversión y el uso de tecnología, la incorporación de la IA en los flujos de trabajo y la prevención del agotamiento en los equipos de seguridad.
- Una transformación empresarial segura mediante el desarrollo de políticas de gestión de riesgos de terceros claras y aplicables, además de fomentar compromisos de colaboración específicos entre TI y la empresa.

QUE ES UN ANTIVIRUS Y CÓMO FUNCIONA?⁸

Los virus informáticos han avanzado a pasos agigantados, siendo cada vez más difícil detectarlos.

Más allá del sistema operativo que utilicemos en nuestra computadora o dispositivo móvil, es fundamental que tengamos instalado un buen antivirus, y bien actualizado con las últimas definiciones.

Un antivirus en la realidad es una herramienta de seguridad muy compleja, tanto en su funcionamiento como en su desarrollo. Si entendemos cómo funcionan y cuáles son los distintos tipos de antivirus que existen, podremos salir airosos de cualquier problema que podamos llegar a tener en el caso de contagiarnos con un virus informático.

TÉCNICO

Por definición: los antivirus son programas de computadora cuyo principal objetivo es **detectar y protegernos de las amenazas informáticas** a las cuales estamos expuestos cuando usamos la computadora para llevar a cabo nuestras tareas.

Mantienen a raya todo tipo de software malicioso y amenazas como, por ejemplo:

- Virus informáticos
- caballos de troya o troyanos
- worms o gusanos
- rootkit
- spyware (programas espías)

Para mantenernos seguros de los peligros y amenazas, **una app antivirus analiza en tiempo real las operaciones que realizamos con nuestra computadora** intentando identificar si los archivos

⁸ <https://www.tecnologia-informatica.com/tipos-de-antivirus/>

que descargamos o almacenamos contienen porciones de código incrustado, llamados "Firmas", que los identifiquen con alguno de los códigos de virus informáticos conocidos.

Cada virus conocido tiene un patrón de código que se puede identificar, lo que le da la identidad apropiada a cada amenaza. Este código se denomina "**Firma**", y podríamos decir que se trata del ADN mismo del virus. Si el antivirus identifica en un archivo una firma compatible con cualquiera de las firmas que tiene almacenadas, inmediatamente tomará medidas para evitar que el mismo se propague.

Por ello es tan importante que el antivirus se encuentre actualizado, ya que si lo está, la base de datos con cientos de miles de firmas de virus que contiene también estará actualizado, lo que nos ofrece mejores chances de estar protegidos.

Más allá de tener un antivirus instalado en el sistema, es muy importan tener hábitos de navegación seguros, es decir no meternos en cualquier lado y abrir cualquier archivo que caiga en nuestras manos, son puntos más que importantes a la hora de estar seguros.

Técnicas de detección de virus



La técnica de detección virus más utilizadas por los antivirus son la llamada "Técnica de verificación de firmas", la cual es una estrategia que implica la comprobación de uno o más archivos en búsqueda de determinados patrones, la llamada "Firma" detallada más arriba en este post.

Lamentablemente, este tipo de detección no siempre puede ser segura, ya que depende de que nuestros antivirus tengan su base datos actualizada al momento.

El otro tipo de análisis más conocido se llama "Técnica de Verificación Heurística" y consiste básicamente en la anticipación del descubrimiento del virus informático en base a comportamientos aprendidos. Este tipo de técnica no es uno de las más adecuados o seguras, ya que además de ser mucho más lento el procedimiento, pueden llegar a generar un alto número de falsos positivos, es decir señalar a un archivo como virus cuando en realidad no lo es.

El tercer método para la detección de virus informáticos es la llamada "Técnica de Bloqueo de Comportamiento", la cual básicamente consiste en analizar las acciones realizadas por los programas que tenemos instalados en la computadora en búsqueda de cualquiera que pudiera representar un peligro, como por ejemplo, intentar quitar un bloqueo de firewall o acceder a determinados archivos del sistema, ambas acciones que deben ser consideradas como sospechosas.

Dependiendo del tipo de sistema antivirus que se trate, se utilizará alguno de estos métodos. Es posible que se utilice una combinación de los tres, con el fin de obtener un mejor resultado a la hora de detectar y descontaminar el sistema de cualquier tipo de amenaza.

Tipos de antivirus



Al igual que con otras categorías de software, podemos encontrar aplicaciones antivirus que se ajusten a cualquiera de las necesidades que pueda tener el usuario, es por ello que podemos contar hasta incluso con antivirus online, los cuales son gratuitos, y cuyos servicios podemos usar sin tener que descargar ni instalar ningún software a nuestra PC.

Sin embargo, este tipo de antivirus en la nube no es el más adecuado para proteger nuestro sistema, ya que depende de una conexión a Internet, y si esta se pierde nos quedamos sin protección.

Los antivirus online tienen el beneficio, además de encontrarse siempre actualizados, de permitirnos analizar, encontrar y eliminar programas infecciosos de nuestra computadora luego de que hayamos comprobado la infección, es decir en un punto en donde instalar un antivirus puede no ser posible, o que la propia acción de los virus no permita el accionar del antivirus.

Es por el ello que la mejor manera de permanecer seguros es instalar en la computadora un buen antivirus y siempre actualizado, pero también prestarle atención a las indicaciones que este nos ofrece cuando detecta movimientos sospechosos, ya que, si hacemos caso omiso de estas notificaciones, podemos vernos rápidamente envueltos en problemas.

Otra forma de categorizar los antivirus es con relación a su precio. En el mercado actual, lo cierto es que tener un antivirus caro no significa para nada estar perfectamente protegidos contra todo riesgo, ya que el dinero que pagamos por el software lo más probable es que sea debido a su servicio post-venta, y no debido a alguna capacidad mágica de detección.

Hoy en día podemos encontrar antivirus gratuitos de primer nivel, como por ejemplo el integrado con Windows 10, o incluso alguna de las versiones "Lite" de reconocidos softwares antivirus como AVG o Avast pueden ofrecernos un alto grado de seguridad.

No existen tantas diferencias entre un buen antivirus gratuito como Microsoft Defender y otros de pago, ya que ambos nos ofrecerán un alto grado de seguridad, básico, pero lo necesario para el normal desenvolvimiento de las actividades de los usuarios, es decir aquellas personas que no requieren que su antivirus provea de VPN, firewall integrado, sandbox y otras utilidades más orientadas a powerusers.

Ahora, los antivirus no sólo se pueden diferenciar por su precio o por estar en la nube o ser instalables. Los antivirus también se pueden diferenciar según su finalidad. Esto significa que los antivirus no son capaces de analizar y eliminar todos los tipos de malware existentes, es decir virus, troyanos, gusanos y demás tipos de amenazas. Por este motivo los antivirus se diferencian en las siguientes categorías.

Tipos de antivirus según su finalidad

Las tres columnas sobre las que se basan los antivirus para cumplir con su tarea son la prevención, la identificación, y la eliminación.

En el mercado existen tres modelos diferentes de antivirus:

Antivirus preventores

Este tipo de antivirus se caracteriza por su capacidad de evitar que cualquier amenaza pueda acceder a nuestro sistema basándose en la anticipación. Una de las principales desventajas de este tipo de antivirus es el uso de los recursos. Este software en funcionamiento se aloja en la memoria principal de la computadora, por lo cual resta recursos utilizables para otros procesos del sistema, lo que puede llegar a ralentizar su funcionamiento.

Antivirus identificadores

Este tipo de antivirus cumple con la función de identificar cualquier tipo de amenaza que quiera acceder a nuestro sistema, o que ya se encuentre agazapado de antes. Para cumplir con su tarea, este tipo de antivirus constantemente analizan el sistema de nuestra computadora con el fin de encontrar secuencias de códigos compatibles con malwares y otras amenazas.

Antivirus descontaminadores

Como último tipo de antivirus tenemos aquellos antivirus diseñados con el objetivo de eliminar cualquiera de las amenazas que pudieran haber sido detectadas en el sistema. Muchos de ellos, incluso pueden llegar a intentar recuperar el estado en que se encontraba nuestro sistema antes de la infección.

Para conocer más en profundidad acerca de la finalidad de este tipo de antivirus, al final del presente post encontrarás más información al respecto.

Tipos de antivirus según su objetivo específico

Entre los programas malignos más conocidos, nos encontramos con:

- los llamados spywares, también conocidos como programas espía,
- virus que facilitan el llamado spam,
- las ventanas emergentes,
- el cambio de las páginas de inicio de nuestro navegador,
- malware específico para el robo de información,
- sitios webs que contienen código malicioso,
- phishing
- rootkits
- y muchas otras técnicas más

Existen herramientas específicas que nos permiten tener un cierto grado de seguridad frente a cada una de estas amenazas y prevenir su accionar. Generalmente un buen antivirus es capaz de proveer de todas ellas en un mismo paquete, lo que se recomienda para la mayoría de los usuarios.

Sin embargo, es posible obtener estas herramientas de manera separada, lo que puede ser beneficioso para el usuario, ya que puede elegir cuál de estas opciones de protección en el mercado es la más adecuada a sus necesidades.

Estas herramientas de protección son las siguientes:

Antispyware

Básicamente, el software antispyware son programas desarrollados específicamente con el objetivo de analizar, detectar y eliminar todos los programas de tipo spyware, los cuales son aquellas aplicaciones que se han instalado en nuestra computadora sin permiso, es decir que están ocultos a nuestros ojos, y que hemos instalado sin darnos cuenta a través de otros softwares. Esta es una práctica habitual con la cual debemos tener cuidado.

Estos programas se instalan en nuestro equipo con el fin de recolectar y enviar información de nuestros hábitos de consumo y navegación hacia servidores externos, datos que luego son vendidos a otras empresas que los usan con fines de mejorar estrategias publicitarias, en el mejor de los casos.

Si quieres conocer cuáles son las mejores aplicaciones antispyware, te recomendamos la lectura de este post muy interesante sobre el tema, pulsando sobre este enlace.

Antimalware

Las aplicaciones de tipo antimalware son desarrolladas con el objetivo de bloquear y eliminar cualquier malware que quiera acceder a nuestra computadora. Como sabemos, se denomina "Malware" a todo aquel software con código malicioso que ingresa furtivamente a nuestra computadora con el fin de producir daños al sistema operativo, a las aplicaciones o a los documentos que podemos tener almacenados en el dispositivo.

En el mercado existen múltiples herramientas de este tipo, cada una de ellas desarrollada con un objetivo particular. Sin embargo, una de estas apps, Malwarebytes Anti-malware es una de las más utilizadas ya que es capaz de ofrecernos una solución efectiva en muchos escenarios.

Antiadware

También conocidos como "Antipop-ups", este tipo de antivirus fue desarrollado con el fin de poder identificar y eliminar la aparición de las ventanas emergentes cuando navegamos por Internet con nuestro browser favorito. Si bien en la actualidad la mayoría de los navegadores modernos incluyen una forma propia de evitar estos pop-ups, lo cierto es que todavía las aplicaciones antiadware siguen siendo muy útiles a la hora de eliminar ventanas emergentes específicas.

Si quieres saber más acerca de los adware y las diferentes formas de eliminarlo de nuestro sistema, te recomendamos la lectura de este interesante artículo, al cual podrás acceder pulsando sobre este enlace.

Antispam

Las aplicaciones del tipo Antispam son las encargadas de conseguir que leer nuestro correo electrónico sea una cosa sencilla, ya que estas herramientas son utilizadas para que ningún correo spam, también conocidos como correos basura, alcance nuestra bandeja de entrada. Si estas apps no estuvieran controlando el tráfico de correos electrónicos, una tarea tan sencilla como leer nuestros emails sería una verdadera pesadilla, ya que tendríamos que filtrar entre miles de correos que no nos importan para nada.

En la actualidad, los servicios de mail cuentan con estos servicios en sus propios servidores, realizando toda esta tarea de forma automática, lo que permite que a nuestra bandeja de entrada

no llegue ningún correo no deseado, ya que es el propio sistema el que los envía directamente a la papelera.

Firewall

Si bien específicamente no es un antivirus, el Firewall, también conocido por muchos como cortafuegos, puede ser considerado como una herramienta de este tipo también, ya que cumple con una tarea de prevención que nos permite tener una contención contra cualquier amenaza que intente llegar a los puertos de nuestra computadora.

El uso de un Firewall es extremadamente recomendable en aquellos equipos que están conectados a una red o a Internet de forma constante, ya que la principal función del Firewall es la gestionar y analizar el tráfico entrante y saliente de las redes, y cuando encuentra alguna actividad sospechosa, bloquearla.

Tipos de antivirus según su función

Las aplicaciones antivirus pueden actuar de diferentes maneras y con diferentes metodologías con el fin de controlar las amenazas que puedan surgir llevando a cabo nuestras tareas diarias. A pesar de esta diversidad de comportamiento, los antivirus también pueden clasificarse en categorías que nos permitan tener bien en claro para qué sirve cada uno de estos antivirus.

Las categorías de antivirus según su función son las siguientes:

Antivirus eliminadores y reparadores

El propósito específico de este tipo de antivirus no es otro que centrarse en eliminar cualquier de las amenazas que puedan haber accedido al sistema, pero además cuentan con la posibilidad de poder volver el mismo al estado en que se encontraba antes del momento del ataque, una función muy importante ya que nos permite ganar algo de tiempo al momento de volver a trabajar con nuestras cosas.

Antivirus detectores

Los antivirus de este tipo cumplen con la misión de analizar y detectar la presencia de una amenaza informática en cualquiera de sus formas, informándole al usuario mediante una notificación. El usuario tendrá que decidir cuál será la estrategia adecuada para la eliminación del virus que el antivirus detector ha encontrado. En la mayoría de los casos se deberá pasar a la acción mediante el uso de antivirus inmunizadores.

Inmunizadores

Por regla general, este tipo de antivirus son considerados como uno de los más seguros, ya que fueron desarrollados con el objetivo de anticiparse a cualquier infección. Son también conocidos como antivirus protectores, y para cumplir con su tarea con mejores resultados suelen instalarse en la memoria del equipo, desde donde analizan y detectan cualquier alteración sospechosa de los procesos que allí acontecen, como por ejemplo la copia de archivos, la ejecución de aplicaciones y otras tareas.

Antivirus Residentes

Comparte con los antivirus inmunizadores la característica de tener que estar instalados en la memoria principal de la computadora. La función principal del antivirus residente es la de analizar todas las peticiones de las aplicaciones que ejecutamos desde que las lanzamos, con el fin de detectar si llevan a cabo alguna actividad sospechosa.

El hecho de que estos tipos de antivirus residan en la memoria de la computadora logra una disminución del rendimiento del mismo.

Heurísticos

Por último, este tipo de antivirus ofrece la posibilidad de simular el comportamiento de las diferentes aplicaciones que tenemos instaladas en el sistema, con el fin de comprobar cómo estas se comportan en diferentes escenarios, lo que le permite luego establecer patrones y actuar si se realizan operaciones sospechosas.

Tipos de antivirus según su categoría

Para culminar con este completo informe acerca de los tipos de antivirus y su clasificación, a partir de este punto conoceremos las diferentes categorías de virus de acuerdo a su funcionamiento o lugar de instalación.

Antivirus Pasivo

Son aquellas aplicaciones que no ofrecen protección permanente, debido a que no están siempre funcionando, ya que los tenemos que ejecutar de manera manual.

Antivirus Activo

Son todas aquellas aplicaciones que si bien se encuentran siempre en ejecución en nuestro sistema, no realizan una tarea de protección constante, aunque sí se encuentran realizando alguna acción relacionada con la seguridad.

Antivirus online

Existe una gran variedad de servicios de antivirus online, es decir aquellos antivirus que residen en la Nube. Este tipo de antivirus no requiere que lo tengamos instalado en la computadora, ya que realiza todos los análisis pertinentes a la búsqueda de virus directamente desde Internet.

Los antivirus online no pueden funcionar como una protección constante de nuestro equipo, pero son muy útiles para tener una forma de limpiar cualquier tipo de virus de la computadora cuando todo lo demás falla.

Antivirus offline

Son los clásicos programas antivirus que es necesario instalar en la computadora que se desea proteger.

REGULATORIO

Dada la naturaleza y cuantía del objeto a contratar, y de conformidad con lo dispuesto en Literal b del numeral 2 del artículo 2 de la Ley 1150 de 2007, se concluye que la modalidad bajo la cual el DANE debe adelantar el proceso de Selección para la presente contratación es la "Selección Abreviada de Menor Cuantía".

Teniendo en cuenta los componentes del objeto del proceso que se pretende adelantar, y el presupuesto estimado para ejecutar el objeto, a este proceso de Selección Abreviada de Menor Cuantía y al contrato que de él se derive, le son aplicables los principios y normas de la Constitución Política, la Ley 80 de 1993, la Ley 1150 de 2007, Ley 1474 de 2011, Decreto 019 de 2012, Decreto 1082 de 2015 y demás normas concordantes o complementarias. Para aquellos aspectos no regulados en las normas anteriormente señaladas, se aplicarán las normas comerciales y civiles pertinentes, así como las reglas previstas en el presente proceso.

También tendrán aplicación las normas legales que se dicten sobre la materia durante el desarrollo de esta contratación y que deban empezar a regir durante la vigencia de la misma, con las excepciones que al respecto se determinen y las que se desprendan de las normas generales sobre vigencia de normas.

En aplicación a lo dispuesto en el Decreto 680 de 2021, en relación con el apoyo a la Industria Nacional, en cuanto a la aplicación del puntaje para la promoción de dicha industria, en los procesos de selección de contratistas que se adelanten a través de licitaciones, convocatorias o concursos públicos o mediante cualquier modalidad de contratación, conforme al análisis y necesidad de aplicación, se establece por parte del equipo de Sistema de la Subdirección de Diseño y Análisis Estratégico, en este caso en particular:

En lo que respecta a la seguridad, las normas relacionadas son las siguientes:

Ley 1273 de 2009. Llamada también ley de delitos informáticos contempló como bien jurídico tutelado la protección de la información y los datos.

En dicha norma se encuentran tipificados nueve delitos que van dirigidos a la protección de la información, los datos y el patrimonio económico.

Resolución 1790 de 2017, establece los lineamientos para la implementación de medidas de seguridad de la información en las entidades del Estado.

Decreto 338 de 2022: normativa de ciberseguridad en Colombia. Establece los lineamientos generales para fortalecer la seguridad digital en Colombia, el modelo de atención y gestión de incidentes, y formaliza el Comité Nacional de Seguridad Digital, sus participantes y cómo deben operar.

LEY 1581 DE 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

ANÁLISIS DE OPORTUNIDAD Y CONVENIENCIA SOBRE INCLUIR O NO LAS OBLIGACIONES DEL ARTÍCULO 2.2.1.2.4.2.16. DEL DECRETO 1082 DE 2015

El DANE, no considera procedente incluir en el presente proceso contractual la referida disposición, teniendo en cuenta el objeto contractual, el alcance de las obligaciones contractuales y las especificaciones técnicas requeridas, según las cuales para la ejecución del contrato que se pretende celebrar, no es posible establecer la obligación de vincular personas en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

especial protección constitucional, ya que por la naturaleza del objeto del contrato, el contratista deberá contratar personal especializado y experiencia específica para su correcta ejecución., como los solicitados el numeral 6.4.2.2. Otros Requisitos Técnicos Habilitantes del estudio previo.

ESTUDIO DE LA OFERTA

QUIEN VENDE

En Colombia existen 8 empresas que se dedican a prestar el servicio, acorde al objeto del presente proceso de contratación, las cuales cuentan con estándares de calidad y respaldo por parte de fabricantes de marcas reconocidas. Algunas de ellas son:

EMPRESA	TAMAÑO
SOFTSECURITY SAS	PEQUEÑA
MULTISOFT S.A.S.	MEDIANA
COLOMBIANA DE SERVICIOS TECNOLOGICOS S.A.S.	PEQUEÑA
PCM S.A.S.	PEQUEÑA
SOFTNET SAS	PEQUEÑA
CCD SAS	MEDIANA
SERVIDATOS B.A LTDA	MICROEMPRESA
HEIMCORE SAS	GRANDE

SOFTSECURITY SAS.

Empresa de consultoría en Ciberseguridad que cuenta con un equipo de especialistas para ayudar a sus clientes a elevar la seguridad y garantizar la integridad, Confidencialidad y Disponibilidad de su información.

Sus especialidades son:

- Infraestructura
- Servidores, Networking
- Cableado Estructurado y Redes Eléctricas

MULTISOFT S.A.S.

Empresa Colombiana con más de 25 años. Diseñan, implementan y mantienen Soluciones de Seguridad de la Información, Cyber-Seguridad e Infraestructura Tecnológica flexibles y adaptadas a las necesidades de sus clientes.

Sus especialidades son:

- IT integrated solutions and professional IT services
- Infrastructure and Information Security
- Productivity and Collaboration
- Cloud Computing

COLOMBIANA DE SERVICIOS TECNOLOGICOS S.A.S.

Colsistec establecimiento dedicado a: comercio al por mayor de computadores, equipo periférico y programas de informática, comercio al por menor de computadores, equipos periféricos, programas de informática y equipos de telecomunicaciones en establecimientos especializados, otras actividades de tecnologías de información y actividades de servicios informáticos, actividades de servicios de sistemas de seguridad. El portafolio de servicios está conformado



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

por servidores, convergencia e hiperconvergencia, almacenamiento, big data y analítica, redes y seguridad, respaldo y recuperación, soluciones en la nube, virtualización: internet de las cosas e inteligencia artificial,

PCM S.A.S.

Empresa con 40 años de experiencia aportando conocimiento experto para construir soluciones de tecnologías de la información, que garantizan la gestión integral de la seguridad y operación de las TICs trabajando a través de procesos certificados internacionalmente y especialización en ISO/IEC 20000. Sufavor allegar portafolio de servicios está conformado por Ciber seguridad, seguridad TI, mesa de servicios, plataforma TI, consultoría TI.

SOFTNET SAS

Consultores, diseñadores y gestores de soluciones que apoyan la continuidad del negocio de sus clientes, en las áreas de seguridad, disponibilidad y uso de las tecnologías de la información, con el apoyo de aliados estratégicos expertos y de alto reconocimiento en el mercado.

Ofrece servicios en los Sectores de seguridad de redes y sistemas informáticos.

Especialidades: seguridad de la información, respaldo e infraestructura.

CCD SAS

CCD - Compañía de Ciberseguridad y Defensa, es una compañía colombiana, conformada por personal experto fundada desde el año 2006, apoyan a las empresas por medio de la protección durante todo el ciclo de las amenazas informáticas y de seguridad en el ahora y en el futuro siendo insumo fundamental de sostenibilidad para el proyecto social de la compañía que busca una Colombia Justa, desarrollada y en paz.

Brindan la prestación de servicios y productos de seguridad informática, gestión proactiva y anticipativa de amenazas, consultoría de seguridad y redes de datos, lo que permite generar valor a los clientes a fin de que sus empresas sean más seguras protegiendo su principal activo, la información.

HEIMCORE SAS

Es una empresa colombiana especializada en ofrecer soluciones y servicios de tecnología de la información (TIC), que incluyen la comercialización, implementación y soporte de plataformas tecnológicas para sus clientes. Su enfoque está en la gestión integral de las TIC, apoyando los objetivos estratégicos de las empresas a través de su experiencia y personal calificado en el área

Una vez revisados los acuerdos marco de precios publicado en <http://www.colombiacompra.gov.co> se evidencia que el objeto a contratar no se encuentra contemplado en ninguno de ellos.

INDICADORES FINANCIEROS

De acuerdo con las directrices, manual e instructivo del Sistema Electrónico de contratación pública SECOP II y con el objeto del proceso contractual requerido por el DANE, la Coordinación Financiera identifico el sector de tecnologías software - hardware, por medio de la información suministrada por la Superintendencia de Sociedades - SIIS, con los cuales posibles oferentes se presentaran al proceso contractual en curso y se realizó mediante muestreo del sector de pequeña , mediana y gran empresa.

También se tuvo en cuenta factores económicos de estudios, reportes y bases de datos realizados por RUES (Registro único empresarial y social) y entidades nacionales como el Banco de la República, Ministerio de Hacienda y Crédito Público y estudios DANE, con respecto al comportamiento y crecimiento económico nacional, para el análisis de indicadores financieros y

de capacidad organizacional requeridos, los cuales reflejen salud y solidez financiera de los proponentes. Estas condiciones muestran la capacidad y aptitud del proponente para cumplir oportuna y cabalmente el objeto del contrato a través de su liquidez, endeudamiento y rendimiento económico de sus activos e inversión, los proponentes deberán reportar en el Registro Único de Proponentes RUP la información contable del último año fiscal anteriores, es decir 2024 en firme y vigente.

Los indicadores financieros se deben incluir para todas las modalidades de selección, menos en la mínima cuantía. Estos indicadores son elaborados por el Área Financiera con base en el estudio de mercado elaborado por el área requirente.

Para la verificación financiera del presente proceso la entidad ha determinado 4 indicadores financieros y 2 indicadores de capacidad organizacional en las siguientes condiciones:

INDICADOR	FÓRMULA	MARGEN SOLICITADO
LIQUIDEZ	Activo corriente dividido por el pasivo corriente	Mayor o igual a 1.50 por lote o lotes que se presenten
NIVEL DE ENDEUDAMIENTO	Pasivo total dividido por el activo total	Menor o igual a 70.0% por lote o lotes que se presenten
RAZÓN DE COBERTURA DE INTERESES	Utilidad operacional dividida por los gastos de intereses	Mayor o igual a 2.00 por lote o lotes que se presenten
CAPITAL DE TRABAJO	Activo Corriente Menos pasivo corriente	Mayor o igual al 80.0% del presupuesto asignado.

El **capital de trabajo** es un indicador financiero que refleja la capacidad de una empresa para atender sus obligaciones de corto plazo y mantener la continuidad operativa durante la ejecución de un contrato. Se calcula como la diferencia entre los activos corrientes y los pasivos corrientes (Capital de trabajo = Activo corriente – Pasivo corriente).

En el marco del proceso contractual, es preciso indicar que, existe dentro del proceso el soporte técnico por un año, conforme a las características y condiciones técnicas definidas, situación que, el Área Financiera, establece un indicador que garantice que el proveedor tenga la solvencia y liquidez suficientes, para garantizar el cumplimiento del objeto contractual.

Por tanto, el indicador de capital de trabajo se incluye como un **requisito habilitante de capacidad financiera**, con el fin de garantizar la **idoneidad económica del proponente** y la **protección de los recursos públicos** invertidos, proporcional a la naturaleza del presente proceso contractual.

Para este indicador, se tomó una muestra de los posibles oferentes, analizando información financiera con corte a 31 de diciembre de 2024, y se tomó la información de SIIS filtrando por actividad económica Estado de resultados y estado de situación financiera, obteniendo el promedio del sector también, con



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

respecto al indicador de capacidad financiera capital de trabajo, con base en la información financiera se encontró lo siguiente:

EMPRESA	INDICE CAPITAL DE TRABAJO
COLSOF	\$ 56.968.244.000
COMWARE S.A.	\$ 32.956.177.800
CARVAJAL TECNOLOGIA Y SERVICIOS	\$ 7.763.159.000
NECSYS SAS	\$ 558.184.351
PROCIBERNETICA	\$ 5.805.966.000
GOLD SYS LTDA.	\$ 2.196.248.000
SOFTSECURITY S.A.S	\$ 4.419.435.972
MULTISOFTWARE TRANSACCIONAL COLOMBIANA DE SERVICIOS	\$ 4.442.268.795
P C MICROS S.A.S	\$ 683.143.000
SOFTNET S.A.S.	\$ 1.445.095.087
CCD COMPAÑIA DE CIBERSEGURIDAD Y DEFENSA	\$ 13.423.930.718
RED COMPUTO	\$ 1.370.257.904
HEIMCORE S.A.S	\$ 26.495.779.807
CONTROLES EMPRESARIALES	\$ 72.510.519.295
PROMEDIO MUESTRA DEL SECTOR	\$ 15.427.685.449
MEDIA GEOMETRICA	\$ 4.956.612.878,15

Además de lo anterior, se tomó una muestra de los estados financieros de 15 posibles proponentes, en donde, solamente un proveedor no cumple con indicador, el cual estaría muy por debajo del 80% inicial.



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

	<table border="1"><tr><td>RP= <u>Utilidad Operacional</u> Patrimonio</td><td>Mayor o igual a 6.0% Registrado en el RUP como 0.06</td></tr><tr><td>RA = <u>Utilidad Operacional</u> Activo Total</td><td>Mayor o igual a 5.0% Registrado en el RUP como 0.05</td></tr></table>	RP= <u>Utilidad Operacional</u> Patrimonio	Mayor o igual a 6.0% Registrado en el RUP como 0.06	RA = <u>Utilidad Operacional</u> Activo Total	Mayor o igual a 5.0% Registrado en el RUP como 0.05
RP= <u>Utilidad Operacional</u> Patrimonio	Mayor o igual a 6.0% Registrado en el RUP como 0.06				
RA = <u>Utilidad Operacional</u> Activo Total	Mayor o igual a 5.0% Registrado en el RUP como 0.05				
DINÁMICA DE PRODUCCIÓN, DISTRIBUCIÓN Y ENTREGA DE BIENES Y/O SERVICIOS	<p>En el mercado colombiano se encuentran varias empresas dedicadas a la distribución, prestación de servicio y soporte de soluciones de antivirus.</p> <p>La dinámica de prestación de los servicios del presente objeto se lleva a cabo a través de las empresas especializadas. Algunas de las empresas que brindan este servicio son: Conectics, Softsecurity, PC Micros, Olimpiait, Pcm Ti, Multisoft, Ona Systems, Servidatos y Softnet SAS.</p> <p>La distribución de las licencias Software Antivirus, es a través de distribuidores autorizados en diferentes categorías. Además, se facilita la prestación del servicio, dado que las transacciones se hacen con empresas locales con normas y leyes que rigen el sector, para solicitar garantías y soporte especializado.</p>				

ESTUDIO DE LA DEMANDA

Adquisición de Bienes y Servicios histórico del DANE y (o) FONDANE

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA (DANE)	
PROCESO O CONTRATO	SASI-012-2024- CONTRATO CO1.PCCNTR.7156627
MODALIDAD DE SELECCIÓN DEL CONTRATISTA.	Selección abreviada subasta inversa
OBJETO DEL CONTRATO	Contratar el upgrade de la solución de antivirus Trellix Endpoint Security Suite (TRXE1), así como efectuar la renovación de las licencias de la Suite Cloud Workload Security - Essentials - (CWS-E) existentes en la entidad, con soporte técnico por 1 año, de acuerdo con las características y condiciones técnicas definidas.
CANTIDAD DEL BIEN O SERVICIO	1 contrato



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

VALOR DE LOS CONTRATOS Y FORMA DE PAGO.	<p>Valor del contrato: \$544.147.080</p> <p>Un (1) único pago correspondiente a la entrega del código de autorización de las licencias: 3.800 licencias de la solución de Trellix Endpoint Security Suite (TRXE1) y 80 licencias Cloud Workload Security Essentials (CWS-E) con 1 año de actualización y soporte, así como la entrega del primer informe establecido en la obligación específica 13, previa presentación de la factura o cuenta de cobro y certificación de cumplimiento a satisfacción generada por el supervisor del contrato.</p> <p>Es de mencionar que para el pago se debe tener en cuenta que el ítem Trellix Endpoint Security Suite (TRXE1) no incluye IVA y el ítem Cloud Workload Security Essentials CWS-E, si incluye IVA.</p>																				
NÚMERO DE CONTRATOS SUSCRITOS PARA EL EFECTO Y VIGENCIAS DE LOS MISMOS	<p>Uno (1), hasta el 30 de diciembre 2024</p>																				
VIGENCIA DE LOS CONTRATOS	<p>El plazo de ejecución será contado a partir de la puesta en ejecución en la plataforma SECOP II y hasta el 30 de diciembre de 2024, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato.</p> <p>El plazo de vigencia de las licencias upgrade de la solución de antivirus Trellix Endpoint Security Suite (TRXE1), así como efectuar la renovación de las licencias de la Suite Cloud Workload Security - Essentials - (CWS-E) será desde el 21/12/2024 hasta el 20/12/2025.</p>																				
PRESUPUESTO Y SI HA HABIDO LUGAR A VIGENCIAS FUTURAS	<p>\$544.147.080 No reporta ninguna vigencia futura</p>																				
COMPORTAMIENTO DE LOS CONTRATISTAS, IMPOSICIÓN DE SANCIONES	<p>Revisando el SECOP y consultando el Registro Mercantil en la plataforma del RUES no se evidencia imposiciones y sanciones a ninguno de los contratistas.</p>																				
GARANTÍAS EXIGIDAS EN LOS PROCESOS DE CONTRATACIÓN Y SINIESTROS	<table border="1"><thead><tr><th>AMPARO</th><th>PORCENTAJE</th><th>BASE</th><th>VIGENCIA</th></tr></thead><tbody><tr><td>Cumplimiento</td><td>15%</td><td>Valor del contrato</td><td>Vigente por el plazo de ejecución del contrato, y seis (6) meses más, en todo caso vigente hasta su liquidación</td></tr><tr><td>Pago de salarios, prestaciones sociales legales e indemnizaciones laborales</td><td>5%</td><td>Valor del Contrato</td><td>Vigente por el plazo de ejecución del contrato y tres (3) años más,</td></tr><tr><td>Calidad del Servicio</td><td>10%</td><td>Valor del contrato</td><td>Vigente por el plazo de ejecución del contrato y dieciocho (18) meses más.</td></tr><tr><td>Calidad y correcto funcionamiento de los bienes</td><td>10%</td><td>Valor del contrato</td><td>Vigente por el plazo de ejecución del contrato y dieciocho (18) meses más.</td></tr></tbody></table>	AMPARO	PORCENTAJE	BASE	VIGENCIA	Cumplimiento	15%	Valor del contrato	Vigente por el plazo de ejecución del contrato, y seis (6) meses más, en todo caso vigente hasta su liquidación	Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5%	Valor del Contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más,	Calidad del Servicio	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y dieciocho (18) meses más.	Calidad y correcto funcionamiento de los bienes	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y dieciocho (18) meses más.
AMPARO	PORCENTAJE	BASE	VIGENCIA																		
Cumplimiento	15%	Valor del contrato	Vigente por el plazo de ejecución del contrato, y seis (6) meses más, en todo caso vigente hasta su liquidación																		
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5%	Valor del Contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más,																		
Calidad del Servicio	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y dieciocho (18) meses más.																		
Calidad y correcto funcionamiento de los bienes	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y dieciocho (18) meses más.																		
EMPRESAS QUE PRESENTARON OFERTA	<p>PCM COLOMBIA SOFTSECURITY S.A.S</p>																				
LINK SECOP	<p>https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.7089480</p>																				



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

PROCESO O CONTRATO	SAMC-003-2023 - CONTRATO CO1.PCCNTR.5633187												
MODALIDAD DE SELECCIÓN DEL CONTRATISTA.	Selección Abreviada de Menor Cuantía												
OBJETO DEL CONTRATO	Contratar la renovación anual del licenciamiento y soporte técnico de la solución de antivirus Trellix MVISION Protect Plus EDR for Endpoint existente en la entidad y adquisición del licenciamiento de la Suite Cloud Workload Security - Essentials - (CWS-E) con soporte técnico por 1 año, de acuerdo con las características y condiciones técnicas definidas.												
CANTIDAD DEL BIEN O SERVICIO	1 contrato												
VALOR DE LOS CONTRATOS Y FORMA DE PAGO.	Valor del contrato: \$387.786.304 Un (1) único pago correspondiente a la entrega del código de autorización de las licencias: 3.600 licencias de la solución de antivirus Trellix MVISION Protect Plus EDR for Endpoint y 152 licencias Cloud Workload Security Essentials CWS-E con 1 año de actualización y soporte, así como entrega del primer informe establecido en la obligación específica 13, previa presentación de la factura o cuenta de cobro y certificación de cumplimiento a satisfacción generada por el supervisor del contrato. Es de mencionar que para el pago se debe tener en cuenta que el ítem Cloud Workload Security Essentials CWS-E, incluye IVA.												
NÚMERO DE CONTRATOS SUSCRITOS PARA EL EFECTO Y VIGENCIAS DE LOS MISMOS	Uno (1), hasta el 29 de diciembre 2023												
VIGENCIA DE LOS CONTRATOS	El plazo de ejecución será contado a partir de la puesta en ejecución en la plataforma SECOP II y hasta el 29 de diciembre de 2023, previo cumplimiento de los requisitos de perfeccionamiento, legalización y ejecución del contrato. La vigencia del soporte técnico de las licencias será por un (1) año, contado a partir del 21/12/2023 y hasta el 20/12/2024.												
PRESUPUESTO Y SI HA HABIDO LUGAR A VIGENCIAS FUTURAS	\$488.006.808 No reporta ninguna vigencia futura												
COMPORTAMIENTO DE LOS CONTRATISTAS, IMPOSICIÓN DE SANCIONES	Revisando el SECOP y consultando el Registro Mercantil en la plataforma del RUES no se evidencia imposiciones y sanciones a ninguno de los contratistas.												
GARANTÍAS EXIGIDAS EN LOS PROCESOS DE CONTRATACIÓN Y SINIESTROS	<table border="1"><thead><tr><th>AMPARO</th><th>PORCENTAJE</th><th>BASE</th><th>VIGENCIA</th></tr></thead><tbody><tr><td>Cumplimiento</td><td>15%</td><td>Valor del contrato</td><td>Vigente por el plazo de ejecución del contrato, y dieciséis (16) meses más</td></tr><tr><td>Pago de salarios, prestaciones sociales legales e indemnizaciones laborales</td><td>5%</td><td>Valor del Contrato</td><td>Vigente por el plazo de ejecución del contrato y tres (3) años más,</td></tr></tbody></table>	AMPARO	PORCENTAJE	BASE	VIGENCIA	Cumplimiento	15%	Valor del contrato	Vigente por el plazo de ejecución del contrato, y dieciséis (16) meses más	Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5%	Valor del Contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más,
AMPARO	PORCENTAJE	BASE	VIGENCIA										
Cumplimiento	15%	Valor del contrato	Vigente por el plazo de ejecución del contrato, y dieciséis (16) meses más										
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5%	Valor del Contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más,										



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

	Calidad del Servicio	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y dieciséis (16) meses más.
EMPRESAS QUE PRESENTARON OFERTA	PC MICROS SAS CCD- Compañía de Ciberseguridad y Defensa			
LINK SECOP	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.5206948			

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA (DANE)	
PROCESO O CONTRATO	SAMC-005-2022 - CONTRATO CO1.PCCNTR.4319683
MODALIDAD DE SELECCIÓN DEL CONTRATISTA.	Selección Abreviada de Menor Cuantía
OBJETO DEL CONTRATO	Contratar la renovación anual del licenciamiento y soporte técnico de la solución de antivirus McAfee con que cuenta la entidad, de acuerdo con las características y condiciones técnicas señaladas.
CANTIDAD DEL BIEN O SERVICIO	1 contrato
VALOR DE LOS CONTRATOS Y FORMA DE PAGO.	Valor del contrato: CUATROCIENTOS CUARENTA Y SEIS MILLONES SETECIENTOS SESENTA MIL PESOS (\$446.760.000,00) M/CTE., exento de IVA Un (1) único pago correspondiente a la entrega del código de autorización de renovación de las 3.600 licencias de la suite de McAfee MVISION PROTECT PLUS con EDR por 1 año de actualización y soporte, previa presentación de la factura o cuenta de cobro y certificación de cumplimiento a satisfacción generada por el supervisor del contrato.
NÚMERO DE CONTRATOS SUSCRITOS PARA EL EFECTO Y VIGENCIAS DE LOS MISMOS	Uno (1), hasta el 31 de diciembre 2022
VIGENCIA DE LOS CONTRATOS	El contratista ejecutará el objeto del presente contrato a partir de su puesta en ejecución en la plataforma SECOP II, previo cumplimiento de los requisitos de perfeccionamiento, así como los de ejecución y hasta por cinco (5) días hábiles sin superar el 31 de diciembre de 2022
PRESUPUESTO Y SI HA HABIDO LUGAR A VIGENCIAS FUTURAS	\$ 448.560.000 No reporta ninguna vigencia futura
COMPORTAMIENTO DE LOS CONTRATISTAS, IMPOSICIÓN DE SANCIONES	Revisando el SECOP y consultando el Registro Mercantil en la plataforma del RUES no se evidencia imposiciones y sanciones a ninguno de los contratistas



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

	AMPARO	PORCENTAJE	BASE	VIGENCIA
GARANTÍAS EXIGIDAS EN LOS PROCESOS DE CONTRATACIÓN Y SINIESTROS	↑ Cumplimiento	15%	↑ Valor del contrato	Vigente por el plazo de ejecución del contrato, y dieciséis (16) meses más, contado a partir del perfeccionamiento del contrato.
	Pago de salarios, prestaciones sociales, legales e indemnizaciones laborales	5%	Valor Total del Contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más, contados a partir del perfeccionamiento del contrato.
	Calidad del Servicio	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y dieciséis (16) meses más, contado a partir del perfeccionamiento del contrato.
EMPRESAS QUE PRESENTARON OFERTA	PC MICROS SAS SOFTSECURITY SAS			
LINK SECOP	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.3594320&isFromPublicArea=True&isModal=true&asPopupView=true			

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA (DANE)

PROCESO O CONTRATO	SAMC-002-2021
MODALIDAD DE SELECCIÓN DEL CONTRATISTA.	Selección Abreviada de Menor Cuantía
OBJETO DEL CONTRATO	Contratar la migración del licenciamiento y soporte técnico de la solución de antivirus McAfee con que cuenta la entidad y adquisición de nuevas licencias, de acuerdo con las características y condiciones técnicas señaladas.
CANTIDAD DEL BIEN O SERVICIO	1 contrato
VALOR DE LOS CONTRATOS Y FORMA DE PAGO.	Valor del contrato: 283.000.000 incluido IVA Un (1) único pago correspondiente a la entrega del código de autorización de las 3600 licencias de la suite de McAfee MVISION PROTECT PLUS con EDR por 1 año de actualización y soporte, así como la migración del licenciamiento de la Suite McAfee CTP®, previa presentación de la factura o cuenta de cobro y certificación de cumplimiento a satisfacción generada por el encargado de ejercer el control y vigilancia del contrato.
NÚMERO DE CONTRATOS SUSCRITOS PARA EL EFECTO Y VIGENCIAS DE LOS MISMOS	Uno (1), hasta el 31 de diciembre 2021
VIGENCIA DE LOS CONTRATOS	El contratista ejecutará el objeto del presente contrato a partir de su puesta en ejecución en la plataforma SECOP II, previo cumplimiento de los requisitos de perfeccionamiento y hasta el 31 de diciembre de 2021. Sin embargo, el plazo para la migración de la Suite McAfee Complete Endpoint Treath Protection CTP®, a la Suite McAfee MVISION PROTECT PLUS con EDR será de hasta cinco (5) días hábiles contados a partir del inicio de ejecución del contrato y con una vigencia de soporte técnico de la solución por un (1) año.



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

PRESUPUESTO Y SI HA HABIDO LUGAR A VIGENCIAS FUTURAS	\$ 284.160.000 incluido IVA No reporta ninguna vigencia futura																
COMPORTAMIENTO DE LOS CONTRATISTAS, IMPOSICIÓN DE SANCIONES	Revisando el SECOP y consultando el Registro Mercantil en la plataforma del RUES no se evidencia imposiciones y sanciones a ninguno de los contratistas.																
GARANTÍAS EXIGIDAS EN LOS PROCESOS DE CONTRATACIÓN Y SINIESTROS	<table border="1"><thead><tr><th>AMPARO</th><th>PORCENTAJE</th><th>BASE</th><th>VIGENCIA</th></tr></thead><tbody><tr><td>Cumplimiento</td><td>15%</td><td>Valor del contrato</td><td>Vigente por el plazo de ejecución del contrato y seis (6) meses más, contados a partir del perfeccionamiento del contrato.</td></tr><tr><td>Pago de salarios, prestaciones sociales legales e indemnizaciones laborales</td><td>5%</td><td>Valor Total del Contrato</td><td>Vigente por el plazo de ejecución del contrato y tres (3) años más, contados a partir del perfeccionamiento del contrato.</td></tr><tr><td>Calidad del Servicio</td><td>10%</td><td>Valor del contrato</td><td>Vigente por el plazo de ejecución del contrato y un (1) año más, contados a partir del perfeccionamiento del contrato.</td></tr></tbody></table>	AMPARO	PORCENTAJE	BASE	VIGENCIA	Cumplimiento	15%	Valor del contrato	Vigente por el plazo de ejecución del contrato y seis (6) meses más, contados a partir del perfeccionamiento del contrato.	Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5%	Valor Total del Contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más, contados a partir del perfeccionamiento del contrato.	Calidad del Servicio	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y un (1) año más, contados a partir del perfeccionamiento del contrato.
AMPARO	PORCENTAJE	BASE	VIGENCIA														
Cumplimiento	15%	Valor del contrato	Vigente por el plazo de ejecución del contrato y seis (6) meses más, contados a partir del perfeccionamiento del contrato.														
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5%	Valor Total del Contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más, contados a partir del perfeccionamiento del contrato.														
Calidad del Servicio	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y un (1) año más, contados a partir del perfeccionamiento del contrato.														
EMPRESAS QUE PRESENTARON OFERTA	PC MICROS SAS SOFTSECURITY SAS																
LINK SECOP	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.2428225&isFromPublicArea=True&isModal=true&asPopupView=true																

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA (DANE)

PROCESO O CONTRATO	SAMC-007-2020
MODALIDAD DE SELECCIÓN DEL CONTRATISTA.	Selección Abreviada de Menor Cuantía
OBJETO DEL CONTRATO	Contratar la renovación de las licencias de la solución antivirus McAfee existente en la entidad y brindar el servicio de soporte técnico especializado de acuerdo con las especificaciones técnicas señaladas.
CANTIDAD DEL BIEN O SERVICIO	1 contrato
VALOR DE LOS CONTRATOS Y FORMA DE PAGO.	Valor del contrato: \$230.526.800 incluido IVA Forma de Pago <ul style="list-style-type: none">Un pago correspondiente a la renovación de las 3.200 licencias de la solución de antivirus McAfee existente en la entidad, previa presentación de la factura y/o cuenta de cobro y



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

	<p>certificación de cumplimiento a satisfacción generada por el encargado de ejercer el control y vigilancia del contrato.</p> <ul style="list-style-type: none">Un pago final proporcional a los servicios efectivamente prestados, correspondientes al valor de los servicios de soporte técnico especializado, previa presentación de la factura y/o cuenta de cobro y certificación de cumplimiento a satisfacción generada por el encargado de ejercer el control.																
NÚMERO DE CONTRATOS SUSCRITOS PARA EL EFECTO Y VIGENCIAS DE LOS MISMOS	Uno (1), hasta el 31 de diciembre 2020																
VIGENCIA DE LOS CONTRATOS	El plazo de ejecución será contado a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato y hasta el treinta y uno (31) de diciembre de 2020. Sin embargo, el plazo para la renovación de la Suite McAfee CTP® será de hasta diez (10) días hábiles contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato y con una vigencia de un (1) año.																
PRESUPUESTO Y SI HA HABIDO LUGAR A VIGENCIAS FUTURAS	\$ 233.978.725 incluido IVA No reporta ninguna vigencia futura																
COMPORTAMIENTO DE LOS CONTRATISTAS, IMPOSICIÓN DE SANCIONES	Revisando el SECOP y consultando el Registro Mercantil en la plataforma del RUES no se evidencia imposiciones y sanciones a ninguno de los contratistas.																
GARANTÍAS EXIGIDAS EN LOS PROCESOS DE CONTRATACIÓN Y SINIESTROS	<table border="1"><thead><tr><th>AMPARO</th><th>PORCENTAJE</th><th>BASE</th><th>VIGENCIA</th></tr></thead><tbody><tr><td>Cumplimiento</td><td>15%</td><td>Valor del contrato</td><td>Vigente por el plazo de ejecución del contrato y seis (6) meses más, contados a partir del perfeccionamiento del contrato.</td></tr><tr><td>Pago de salarios, prestaciones sociales legales e indemnizaciones laborales</td><td>5%</td><td>Valor Total del Contrato</td><td>Vigente por el plazo de ejecución del contrato y tres (3) años más, contado a partir del perfeccionamiento del contrato.</td></tr><tr><td>Calidad del Servicio</td><td>10%</td><td>Valor del contrato</td><td>Vigente por el plazo de ejecución del contrato y un (1) año más, contados a partir del perfeccionamiento del contrato.</td></tr></tbody></table>	AMPARO	PORCENTAJE	BASE	VIGENCIA	Cumplimiento	15%	Valor del contrato	Vigente por el plazo de ejecución del contrato y seis (6) meses más, contados a partir del perfeccionamiento del contrato.	Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5%	Valor Total del Contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más, contado a partir del perfeccionamiento del contrato.	Calidad del Servicio	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y un (1) año más, contados a partir del perfeccionamiento del contrato.
AMPARO	PORCENTAJE	BASE	VIGENCIA														
Cumplimiento	15%	Valor del contrato	Vigente por el plazo de ejecución del contrato y seis (6) meses más, contados a partir del perfeccionamiento del contrato.														
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5%	Valor Total del Contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más, contado a partir del perfeccionamiento del contrato.														
Calidad del Servicio	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y un (1) año más, contados a partir del perfeccionamiento del contrato.														
EMPRESAS QUE PRESENTARON OFERTA	PC MICROS SAS SOFTSECURITY SAS																
LINK SECOP	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.1595103&isFromPublicArea=True&isModal=true&asPopupView=true																

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA (DANE)

PROCESO O CONTRATO	SAMC-008-2019
MODALIDAD DE SELECCIÓN DEL CONTRATISTA.	Selección Abreviada de Menor Cuantía



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

OBJETO DEL CONTRATO	Contratar la renovación de las licencias de la solución antivirus McAfee existente en la entidad y brindar el servicio de soporte técnico especializado de acuerdo con las especificaciones técnicas señaladas.																		
CANTIDAD DEL BIEN O SERVICIO	1 contrato																		
VALOR DE LOS CONTRATOS Y FORMA DE PAGO.	Valor del contrato: \$188.948.200 incluido IVA Forma de Pago <ul style="list-style-type: none">Un pago correspondiente a la renovación de las licencias de la solución de antivirus McAfee existente en la entidad, previa presentación de la factura y/o cuenta de cobro y certificación de cumplimiento a satisfacción generada por el encargado de ejercer el control y vigilancia del contrato.Pagos fijos mensuales y si llegare el caso se hará un pago final proporcional a los servicios efectivamente prestados, correspondientes al valor de los servicios de soporte técnico especializado, previa presentación de la factura y/o cuenta de cobro y certificación de cumplimiento a satisfacción generada por el encargado de ejercer el control.																		
NÚMERO DE CONTRATOS SUSCRITOS PARA EL EFECTO Y VIGENCIAS DE LOS MISMOS	Uno (1), hasta el 31 de diciembre 2019																		
VIGENCIA DE LOS CONTRATOS	El plazo de ejecución será contado a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato y hasta por tres (3) meses sin que sobrepase el treinta y uno (31) de diciembre de 2019. Sin embargo, el plazo para la renovación de la Suite McAfee CTP® será de hasta diez (10) días hábiles contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato y con una vigencia de un (1) año.																		
PRESUPUESTO Y SI HA HABIDO LUGAR A VIGENCIAS FUTURAS	\$189.375.600 incluido IVA No reporta ninguna vigencia futura																		
COMPORTAMIENTO DE LOS CONTRATISTAS, IMPOSICIÓN DE SANCIONES	Revisando el SECOP y consultando el Registro Mercantil en la plataforma del RUES no se evidencia imposiciones y sanciones a ninguno de los contratistas.																		
GARANTÍAS EXIGIDAS EN LOS PROCESOS DE CONTRATACIÓN Y SINIESTROS	<table border="1"><thead><tr><th>AMPARO</th><th>PORCENTAJE</th><th>BASE</th><th>VIGENCIA</th></tr></thead><tbody><tr><td>Cumplimiento</td><td>15%</td><td>Valor del contrato</td><td>Vigente por el plazo de ejecución del contrato y seis (6) meses más, contados a partir del perfeccionamiento del contrato.</td></tr><tr><td>Pago de salarios, prestaciones sociales legales e indemnizaciones laborales</td><td>5%</td><td>Valor Total del Contrato</td><td>Vigente por el plazo de ejecución del contrato y tres (3) años más, contado a partir del perfeccionamiento del contrato.</td></tr><tr><td>Calidad del Servicio</td><td>10%</td><td>Valor del contrato</td><td>Vigente por el plazo de ejecución del contrato y un (1) año más, contados a partir del perfeccionamiento del contrato.</td></tr></tbody></table>	AMPARO	PORCENTAJE	BASE	VIGENCIA	Cumplimiento	15%	Valor del contrato	Vigente por el plazo de ejecución del contrato y seis (6) meses más, contados a partir del perfeccionamiento del contrato.	Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5%	Valor Total del Contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más, contado a partir del perfeccionamiento del contrato.	Calidad del Servicio	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y un (1) año más, contados a partir del perfeccionamiento del contrato.		
AMPARO	PORCENTAJE	BASE	VIGENCIA																
Cumplimiento	15%	Valor del contrato	Vigente por el plazo de ejecución del contrato y seis (6) meses más, contados a partir del perfeccionamiento del contrato.																
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5%	Valor Total del Contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más, contado a partir del perfeccionamiento del contrato.																
Calidad del Servicio	10%	Valor del contrato	Vigente por el plazo de ejecución del contrato y un (1) año más, contados a partir del perfeccionamiento del contrato.																
EMPRESAS QUE PRESENTARON OFERTA	PC MICROS SAS																		
LINK SECOP	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.955924&isFromPublicArea=True&isModal=true&asPopupView=true																		



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

Adquisición de Bienes y (o) Servicios de Otras Entidades Estatales y las empresas del sector privado

De la búsqueda realizada se identificaron los procesos que se relacionan en la siguiente tabla:

Entidad y/o Empresa contratista y Link SECOP	Objeto	Número, fecha del contrato	Valor Unitario (IVA - Si aplica)
SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.8413649	Adquirir una solución de protección Antivirus de nueva generación para los equipos de cómputo de la Secretaría General de la Alcaldía Mayor de Bogotá D.C.	SGA-SASI-012-2025 CO1.REQ.8524616	\$291.625.100
PERSONERÍA DE BOGOTÁ https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.8472537	RENOVACIÓN DE LAS LICENCIAS ANTIVIRUS PARA LA PERSONERÍA DE BOGOTÁ D.C.	PB-SASI-2025-0006	\$316.262.796
SUPERINTENDENCIA DE ECONOMIA SOLIDARIA https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.6840305&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATAR LA RENOVIACION Y ACTUALIZACION DE LA SOLUCION DE ANTIVIRUS PARA LA SUPERINTENDENCIA DE LA ECONOMÍA SOLIDARIA	SASI 06-2024	\$210.742.032
UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.4926381	Renovación y adquisición del licenciamiento de antivirus Trellix EndPoint, con destino a la Unidad Administrativa Especial de la Justicia Penal Militar y Policial.	UAEJMP - SASI-013-2023 CO1.PCCNTR.5437842 19/10/2023	\$178.111.100
AEROCIVIL https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.4512785&isFromPublicArea=True&isModal=true&asPopupView=true	SOPORTAR, MANTENER Y ADQUIRIR LICENCIAS PARA EL SISTEMA DE SEGURIDAD ANTIVIRUS TRELLIX	23000663 H3 DE 2023 / CO1.NTC.4490892	\$282.516.400
DEPARTAMENTO NACIONAL DE PLANEACION https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.3147515&isFromPublicArea=True&isModal=true&asPopupView=true	Renovación y adquisición del licenciamiento del antivirus McAfee Trellix incluido el mantenimiento y soporte, de conformidad con las condiciones técnicas exigidas por el Departamento Nacional de Planeación (DNP) en la FICHA TÉCNICA Y CONDICIONES EXIGIDAS	DNP-SI-002-2022 CO1.NTC.3080563 16/09/2022	\$485.234.500
SUPERINTENDENCIA DE LA ECONOMIA SOLIDARIA https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=	CONTRATAR LA RENOVIACIÓN DE LAS LICENCIAS DE LA SOLUCIÓN ANTIVIRUS McAfee EXISTENTE EN LA SUPERINTENDENCIA DE LA ECONOMÍA SOLIDARIA. ADQUIRIR 30 LICENCIAS DE McAfee MVISION PLUS Y BRINDAR EL SERVICIO DE SOPORTE TÉCNICO	SASI 01-2022 CO1.PCCNTR.3765915 01/07/2022	\$63.743.570



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

CO1.NTC.2964662&isFromPublicArea=True&isModal=true&asPopupView=true	ESPECIALIZADO DE ACUERDO CON LAS ESPECIFICACIONES TÉCNICAS DEFINIDAS		
SUPERINTENDENCIA DE LA ECONOMIA SOLIDARIA https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.2384006&isFromPublicArea=True&isModal=true&asPopupView=true	CONTRATAR LA RENOVACIÓN DE LAS LICENCIAS DE LA SOLUCIÓN ANTIVIRUS McAfee EXISTENTE EN LA SUPERINTENDENCIA DE LA ECONOMÍA SOLIDARIA Y BRINDAR EL SERVICIO DE SOPORTE TÉCNICO ESPECIALIZADO DE ACUERDO CON LAS ESPECIFICACIONES TÉCNICAS DEFINIDAS	SAMC-05-2021 CO1.NTC.2373494	56.405.758
UNIDAD ADMINISTRATIVA ESPECIAL DE AERONÁUTICA CIVIL AEROCIVIL https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.2896713&isFromPublicArea=True&isModal=true&asPopupView=true	SOPORTAR Y MANTENER LA SEGURIDAD PERIMETRAL (FIREWALL FORCEPOINT, IPS MCAFEE Y WEBGATE PROXY MCAFEE).	22001032 H3 DE 2022 30/09/2022	91.011.200
DEPARTAMENTO ADMINISTRATIVO PARA LA PROSPERIDAD SOCIAL https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.2454576&isFromPublicArea=True&isModal=true&asPopupView=true	Renovar el licenciamiento, actualización, optimización, soporte y mantenimiento de los productos que hacen parte de la suite McAfee de PROSPERIDAD SOCIAL.	SASI 07 DE 2021 CONTRATO 352 DE 2021 30/12/2021	166.320.000
DEPARTAMENTO DE CUNDINAMARCA- SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.2409720&isFromPublicArea=True&isModal=true&asPopupView=true	ACTUALIZACIÓN DE LA LICENCIA MCAFEE MVISION STANDARD CON SOPORTE GOLD DE FÁBRICA POR (1) AÑO PARA 1500 NODOS.	CO1.PCCNTR.3079956 02/12/2021	71.221.500
UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.2359212&isFromPublicArea=True&isModal=true&asPopupView=true	Renovación del licenciamiento de antivirus McAfee EndPoint, con destino a la Unidad Administrativa Especial de la Justicia Penal Militar y Policial.	045-2021 UAEJPMP CO1.PCCNTR.3071425 01/01/2022	101.003.000

ANÁLISIS VALOR ESTIMADO DE PRECIOS



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

Para hacer el análisis del valor estimado se solicitaron cotizaciones a proveedores de este tipo de soluciones. Se recibieron 4 cotizaciones por parte de HEIMCORE SAS, SOFSECURITY, MULTISOFTWARE TRANSACCIONAL SAS y PCM SAS.

Las cotizaciones allegadas corresponden a las mostradas en el siguiente cuadro:

Descripción del bien o servicio	Cantidad	HEIMCORE SAS			SOFSECURITY			MULTISOFTWARE TRANSACCIONAL SAS			PCM SAS			Valor Unitario Promedio	Valor Unitario Promedio (redondeado) Incluido IVA (si aplica)	Valor Unitario Promedio (redondeado) Incluido IVA (si aplica)	Valor total promedio por ítem (para cantidad requerida) incluido IVA (si aplica)
		3/9/2025			3/9/2025			3/9/2025			3/9/2025						
		VALOR UNITARIO	IVA	Valor unitario incluido IVA	VALOR UNITARIO	IVA	Valor unitario incluido IVA (si aplica)	VALOR UNITARIO	IVA	Valor unitario incluido IVA (si aplica)	VALOR UNITARIO	IVA	Valor unitario incluido IVA (si aplica)				
Renovación de licencias Trellix Endpoint Security Suite (TRXE1) existentes en la entidad, con soporte técnico por 1 año.	3.800	\$ 94.628.00	NA	\$ 94.628.00	\$ 140.000	NA	\$ 140.000.00	\$ 141.500.00	NA	\$ 141.500.00	\$ 138.100	NA	\$ 138.100.00	\$ 139.866.67	\$ 139.866.67	\$ 139.867.00	\$ 531.494.600.00
Adquisición de licencias Trellix Endpoint Security Suite (TRXE1).	100	\$ 582.704.00	NA	\$ 582.704.00	\$ 185.000	NA	\$ 185.000.00	\$ 186.000.00	NA	\$ 186.000.00	\$ 195.000	NA	\$ 195.000.00	\$ 192.000.00	\$ 192.000.00	\$ 192.000.00	\$ 16.200.000.00
Renovación del licenciamiento existente de la Suite Cloud Workload Security - Essentials - (CWS-E) con soporte técnico por 1 año.	80	\$ 313.764.00	NA	\$ 313.764.00	\$ 310.000	\$ 68.900.00	\$ 388.900.00	\$ 312.000.00	\$ 59.280.00	\$ 371.280.00	\$ 280.000	\$ 53.200.00	\$ 333.200.00	\$ 300.666.67	\$ 357.793.33	\$ 357.794.00	\$ 28.623.520.00
Adquisición de licencias Cloud Workload Security Essentials - (CWS-E).	120	\$ 1.339.720.00	NA	\$ 1.339.720.00	\$ 360.000	\$ 68.400.00	\$ 428.400.00	\$ 365.000.00	\$ 69.350.00	\$ 434.350.00	\$ 290.000	\$ 55.100.00	\$ 345.100.00	\$ 338.333.33	\$ 402.616.67	\$ 402.617.00	\$ 48.314.040.00
Total																	\$ 624.632.160.00

Para el análisis del valor estimado de precios, se utilizó como referente la media aritmética. Se tomaron los **valores unitarios promedio (redondeados)** incluido IVA (si aplica) y se determinó como valor promedio total la suma de **SEISCIENTOS VEINTICUATRO MILLONES SEISCIENTOS TREINTA Y DOS MIL CIENTO SESENTA PESOS M/CTE (\$624,632,160.00)** de los cuales \$547.694.600,00 están exentos de IVA y \$76.937.560,00 incluyen IVA. Incluye costos directos e indirectos, tasas, contribuciones y demás costos tributarios inherentes al proceso de contratación.

VALOR ESTIMADO DE LA CONTRATACIÓN – VALOR DEL PRESUPUESTO OFICIAL ESTIMADO

El valor estimado de la contratación corresponde a la suma **SEISCIENTOS VEINTICUATRO MILLONES SEISCIENTOS TREINTA Y DOS MIL CIENTO SESENTA PESOS M/CTE (\$624,632,160.00)**, de los cuales \$547.694.600,00 están exentos de IVA y \$76.937.560,00 incluyen IVA. Incluye costos directos e indirectos, tasas, contribuciones y demás costos tributarios inherentes al proceso de contratación.

ÍTEM	DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO INCLUIDO IVA (si aplica)	VALOR TOTAL ESTIMADO
1	Renovación de licencias Trellix Endpoint Security Suite (TRXE1) existentes en la entidad, con soporte técnico por 1 año.	Licencia (3.800)	\$ 139,867.00 (Exento de IVA)	\$ 531,494,600.00 (Exento de IVA)



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

2	Adquisición de licencias Trellix Endpoint Security Suite (TRXE1).	Licencia (100)	\$ 162,000.00 (Exento de IVA)	\$ 16,200,000.00 (Exento de IVA)
3	Renovación del licenciamiento existente de la Suite Cloud Workload Security - Essentials - (CWS-E) con soporte tecnico por 1 año.	Licencia (80)	\$ 357,794.00 (IVA incluido)	\$ 28,623,520.00 (IVA incluido)
4	Adquisición de licencias Cloud Workload Security Essentials – (CWS-E).	Licencia (120)	\$ 402,617.00 (IVA incluido)	\$ 48,314,040.00 (IVA incluido)
VALOR TOTAL ESTIMADO				\$ 624,632,160.00

Nota: El numeral 24 del artículo 476 del Estatuto Tributario - Decreto 624 de 1989 - adicionado por el artículo 187 de la ley 1819 de 2016 - señala que, el suministro de páginas web, servidores (hosting) y computación en la nube (cloud computing) están excluidos del impuesto sobre las ventas.

ANEXO 1

Anexo 1: Informe de cada proceso de contratación	
INFORME DIARIO DEL PROCESO DE COTIZACIÓN – ELABORACIÓN ESTUDIO DE MERCADO	
Proceso N°	
Objeto	Contratar la renovación de la solución de antivirus Trellix Endpoint Security Suite (TRXE1), Suite Cloud Workload Security - Essentials - (CWS-E) existentes en la entidad, y adquisición del licenciamiento adicional con soporte técnico por 1 año, de acuerdo con las características y condiciones técnicas definidas.
Fecha de radicación estudios previos	21/10/2025
Fecha entrega de estudios previos por mail	21/10/2025
DANE y/o FONDANE	DANE
Observaciones de los históricos	Se consultaron los procesos históricos de la entidad en el SECOP II
Fecha en que se realizaron las solicitudes de cotización	27/08/2025
N° de proveedores que se invitaron a cotizar	4
Plazo para cotización	03/09/2025
Observaciones	Para calcular el promedio de las ofertas recibidas no se tuvo en cuenta la cotización del proveedor HEIMCORE SAS, ya que la mayoría de sus valores se encuentran atípicos y el cálculo de la desviación estándar aumenta al incluirla pasando de 14.494.289,45 a 15.790.076,34.
Conclusiones	Se recibieron en total tres (4) cotizaciones y el precio promedio arrojado es de \$624,632,160.00



ANÁLISIS DEL SECTOR – PROCESOS DE CONTRATACIÓN

CÓDIGO: GCO-040-PDT-007-f-001

VERSIÓN: 9

Cotizaron las siguientes empresas	<ol style="list-style-type: none">1. HEIMCORE SAS2. PCM SAS3. SOFSECURITY4. LTISOFTWARE TRANSACCIONAL SAS.
Por un valor \$	<ol style="list-style-type: none">1. \$603.724.320,002. \$608.348.000,003. \$629.420.000,004. \$636.124.400,00
Fecha de realización estudio de mercado	10/08/2025

Luis Martin Barrera Pino
Jefe Oficina de Sistemas

Leonard Páez Ramírez
Coordinador Área Financiera DANE

Proyectó: Jenny Paola Pabón B. – Profesional Contratista - Oficina de Sistemas
Nelson Mauricio Parada Botia- Asesor OSIS

Revisó: Diana Giraldo – Profesional Especializado - Oficina de Sistema
Claudia Liliana Olivares – Abogada Contratista OSIS