Agencia de Renovación del Territorio

ANALISIS DEL SECTOR

OBJETO DE LA CONTRATACIÓN

Adquirir licenciamiento, extensión de garantías de la plataforma FORTINET y realizar análisis de vulnerabilidades de los activos tecnológicos que permita el aseguramiento de toda la infraestructura tecnológica de la Agencia de Renovación del Territorio.

OBJETIVO DEL ANÁLISIS

El presente Análisis tiene como objetivo realizar un estudio de la oferta y demanda del sector del bien y/o servicio requerido, permitiendo entre otros aspectos; conocer sobre su comportamiento en el mercado, el mercado de oferentes, el estudio de la demanda, las condiciones y limitaciones del bien y/o servicio, los precios promedio en el mercado y el valor estimado del proceso de selección, tomando como referencia el estudio efectuado de los precios suministrados por parte del sector.

Para lograr el fin antes planteado, se hace necesario revisar las condiciones particulares de otros procesos de contratación similares, calidad, condiciones, plazos de entrega con otros clientes del proveedor, consolidar información suficiente de precios, solicitar información a los proveedores, verificar la idoneidad de estos y plasmar tal información en los documentos del proceso.

Lo anterior, con el propósito de que la decisión de compra/adquisición sea adecuada y garantice la satisfacción de la necesidad de la entidad, cumpliendo con los principios de eficiencia, eficacia, economía y transparencia, buscando promover la pluralidad de oferentes y libre competencia.

Junio 2026

1. ASPECTOS GENERALES

La Oficina de Tecnologías de la Información – OTI, de la Agencia de Renovación del Territorio, en cumplimiento de sus objetivos y la realización de sus actividades encomendadas, requiere asegurar, mantener y optimizar la infraestructura tecnológica, para soportar las operaciones digitales y apoyar a la Agencia en el cumplimiento de su misión y sus objetivos estratégicos a través del uso de tecnologías de la información TI, además de diseñar e implementar estrategias que faciliten la comunicación entre los sistemas de información, las herramientas informáticas, las tecnologías emergentes, el uso de redes e internet y las personas que interactúan con cada uno de los activos, bajo los lineamientos de la Política de Seguridad de la Información (PSI).

Ahora bien, en aras de asegurar el cumplimiento administrar los sistemas información, equipos, redes y herramientas tecnológicas y brindar el soporte técnico para su funcionamiento adecuado, la cual consiste en gestionar la infraestructura tecnológica dentro de la Agencia y la de dirigir la ejecución de programas y soluciones, para este caso, se requiere una solución integral de hardware y software licenciado que garanticen los niveles de seguridad desde y hacia el servicio de Internet, toda vez que el mismo es fundamental para la operación de la entidad, ya que sobre él se soportan los sistemas de información, la página web, los servicios de navegación entre otros, que generan que el Equipo de Infraestructura y Soporte Tecnológico, deba velar por la protección de todos los servicios expuestos en Internet, los cuales deben estar protegidos para minimizar el riesgo de un ciberataque.

Con estos equipos, la ART se protege de actividades maliciosas que pueden ocasionar indisponibilidad en los servicios tecnológicos como lo puede ser los Rasomware, Phishing, Spam y Denegación de servicios. Estas actividades maliciosas deben ser controladas por Appliance (equipos) de propósito específico como los son Firewall, Web Application Firewall, Sandbox etc.

Adicionalmente, la seguridad de los datos actualmente es un componente importante en todas las organizaciones, como lo promueve la norma ISO 27000, como introducción a los Sistemas de Gestión de Seguridad de la Información (SGSI). Por tal razón, la ausencia de una medida de seguridad que permita monitorear y auditar la actividad en las bases de datos, es un riesgo de exponer la información, el cual puede prevenirse con el uso de herramientas que contribuyan a salvaguardar los datos, ya que, el Programa de Gobierno Digital, plantea la seguridad de la información como uno de los ejes transversales, gestionado por el modelo Sistema de Administración de Seguridad de la Información de Gobierno en Digital - SASIGEL, en el marco de la Ley 1341 de 2009, con el fin de dar cumplimiento a sus principios por parte de las Entidades del Estado, para garantizar la confidencialidad, integridad, y disponibilidad de sus activos de información; solo al personal autorizado se le dará acceso a la información y sus métodos de procesamiento y exactitud, la cual deberá estar disponible en todo momento únicamente para ellos.

En este punto, es importante señalar que la Agencia cuenta actualmente con equipos FORTINET®, los cuales fueron adquiridos desde el año 2018, estos equipos tecnológicos soportan el servicio de seguridad perimetral. Así las cosas, la Agencia anualmente ha realizado la ampliación, actualización, implementación y renovación de garantía y soporte de seguridad perimetral.

Por consiguiente, es importante precisar que, la Agencia actualmente cuenta con equipos FortiGate NGFW que son los firewalls de red, los cuales ofrecen un rendimiento de seguridad potenciado por IA e inteligencia de amenazas única, junto con visibilidad completa, seguridad y convergencia de redes. De igual forma, los equipos con los que cuenta la Agencia, cuya marca es FORTINET®, se encuentra ubicada en el cuadrante mágico de Gartner, como una de las soluciones líderes en el segmento de firewalls de red, tal y como se evidencia a continuación:

Fuente: https://www.fortinet.com/lat/resources/analyst-reports/gartner-network-firewalls

Teniendo en cuenta lo anterior, y que algunos de los dispositivos del servicio de ciberseguridad aún se encuentran vigentes en el mercado, se hace necesario adquirir la garantía y el soporte de fábrica hasta, al menos, el **31 de agosto de 2027,** con el fin de garantizar el óptimo funcionamiento y la estabilidad de la infraestructura tecnológica de la Agencia en materia de seguridad, así como la ejecución de análisis de vulnerabilidades que permitan su detección y remediación.

Para tal efecto, se implementará la práctica de co-término (CO-TERM) definida por FORTINET©[1], mediante la cual se alinearán las fechas de vencimiento de soporte y garantía de todos los dispositivos a una misma fecha. Esta práctica es avalada por el fabricante y permite una gestión unificada, eficiente y controlada del ciclo de vida de los servicios de ciberseguridad.

En ese orden de ideas y con el fin de desarrollar estos objetivos alineados de igual forma al Sistema de Gestión de Seguridad de la Información (Gobierno en Digital), que incluye la política general de seguridad de la información cuyo objetivo es brindar a las entidades del Orden Nacional y Territorial, un insumo base o plantilla, para la elaboración de su propia Política General de Seguridad y Privacidad de la Información, se requiere adquirir el soporte y garantía de los equipos de seguridad con los que cuenta actualmente la Agencia.

1.1. FACTOR ECONÓMICO:

1.1.1. INFRAESTRUCTURA TECNOLÓGICA.

[1] https://docs.fortinet.com/document/fortitokencloud/latest/admin-guide/382967/stackable-co-termed-licenses

Para el desarrollo del objeto a contratar, es fundamental contar con empresas vinculadas al sector económico terciario, también conocido como sector de servicios. Este sector agrupa actividades que no implican la producción ni la transformación directa de bienes materiales, pero que son esenciales para el funcionamiento económico moderno.

Dentro de este sector se encuentran subsectores con dinámicas y características muy diversas, como la biotecnología, la energía, los fondos de capital privado, el desarrollo de software y los servicios TI, la tercerización de procesos de negocio (BPO), la infraestructura hotelera y turística, los bienes y servicios relacionados con el sector petrolero y los centros de servicios compartidos, entre otros.

Las proyecciones económicas oficiales para Colombia en **2026** anticipan un **crecimiento moderado del Producto Interno Bruto (PIB) de entre 2.5% y 2.8%**, junto con un **repunte de la inflación (IPC) que cerraría el año entre 6.2% y 6.7%**, debido a presiones por el salario mínimo, indexación de arriendos y factores climáticos, lo que mantiene una estabilidad con TRM en ascenso moderado (alrededor de y bajo déficit fiscal.

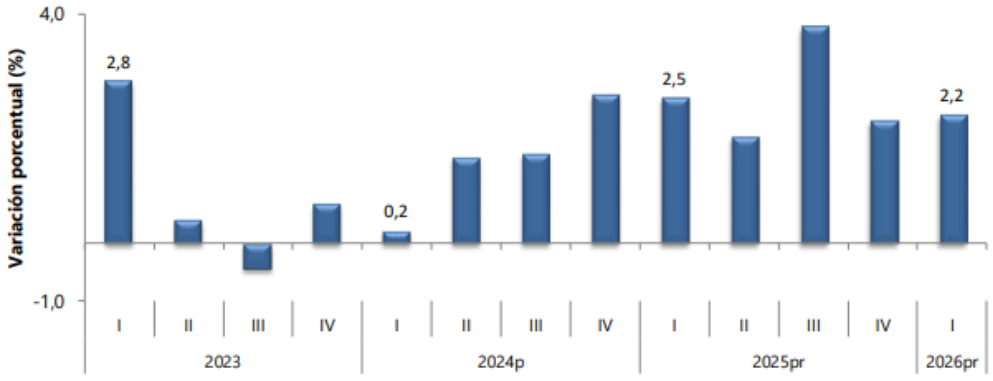
El PIB de Colombia creció 2,7% en el primer trimestre de 2026 (datos DANE). Proyecciones para 2026 mantienen estabilidad, con TRM en ascenso moderado alrededor de los 3.700 COP/USD) y bajo déficit fiscal.

El sector software y ciberseguridad crece por encima del doble del PIB mundial, reflejando su importancia estratégica en Colombia pese a inflación moderada.

El PIB es la suma del valor monetario de la producción de bienes y servicios al interior de un país, una tasa de crecimiento elevada bajo circunstancias normales refleja una situación económica favorable.

En este entorno se procede a analizar el comportamiento del PIB en la actualidad dado que este indicador permite visualizar el decrecimiento o crecimiento del mismo y por tanto el impacto que podría generarse con las empresas que comercializan los productos y servicios objeto del presente proceso de contratación.

Gráfico 1. Producto Interno Bruto
Tasa de crecimiento en volumen[1]
2023-I / 2026pr-I



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

En el primer trimestre de 2026pr, el Producto Interno Bruto en su serie original, crece 2,2% respecto al mismo periodo de 2025pr (ver tabla 1). Las actividades económicas que más contribuyen a la

dinámica del valor agregado son:

- Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales crece 5,7% (contribuye 0,9 puntos porcentuales a la variación anual).
- Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida crece 2,9% (contribuye 0,6 puntos porcentuales a la variación anual).

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

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

- Industrias manufactureras crece 2,3%.
- Actividades financieras y de seguros crece 2,2%.

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

Tasas de crecimiento en volumen[1]
Primer trimestre 2026pr

Actividad económica	Tasas de crecimiento (%)	
	Serie original	Serie ajustada por efecto estacional y calendario
	Anual	Trimestral
	2026pr-I / 2025pr-I	2026pr-I / 2025pr-IV
Agricultura, ganadería, caza, silvicultura y pesca	-1,4	-0,5
Explotación de minas y canteras	-0,1	0,8
Industrias manufactureras	2,9	2,3
Suministro de electricidad, gas, vapor y aire acondicionado[2]	2,6	0,3
Construcción	-5,4	-4,6
Comercio al por mayor y al por menor[3]	2,9	0,2
Información y comunicaciones	1,3	1,1
Actividades financieras y de seguros	2,8	2,2
Actividades inmobiliarias	2,0	0,5
Actividades profesionales, científicas y técnicas[4]	2,2	0,5
Administración pública, defensa, educación y salud[5]	5,7	1,3
Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios[6]	3,2	1,4
Valor agregado bruto	**2,2**	**0,6**
Impuestos menos subvenciones sobre los productos	2,9	0,9
Producto Interno Bruto	**2,2**	**0,6**

Fuente: DANE, PIB_T

En el primer trimestre de 2026, el valor agregado de información y comunicaciones crece 1,3% en su serie original, respecto al mismo periodo de 2025. Para la serie ajustada por efecto estacional y calendario, el valor agregado crece en 1,1%, respecto al trimestre inmediatamente anterior.

Tasas de crecimiento en volumen[1]
Primer trimestre 2026[pr]

Actividad económica	Tasas de crecimiento (%)	
	Serie original	Serie ajustada por efecto estacional y calendario
	Anual	Trimestral
	2026[pr]-I / 2025[pr]-I	2026[pr]-I / 2025[pr]-IV
Información y comunicaciones	**1,3**	**1,1**

Fuente: DANE, PIB_T
[pr]preliminar
[1] Series encadenadas de volumen con año de referencia 2015.

En el mes de mayo de 2026, el IPC registró una variación de 0,47% en comparación con abril de 2026, cinco divisiones se ubicaron por encima del promedio nacional (0,47%): Alojamiento, agua, electricidad, gas y otros combustibles (0,86%), Recreación y cultura (0,77%), Transporte (0,61%), Muebles, artículos para el hogar y para la conservación ordinaria del hogar (0,53%) y por último, Salud (0,52%). Por debajo se ubicaron: Prendas de vestir y calzado (0,42%), Restaurantes y hoteles (0,38%), Bebidas alcohólicas y tabaco (0,27%), Información y comunicación (0,25%), Bienes y servicios diversos (0,22%), Educación (0,00%) y por último, Alimentos y bebidas no alcohólicas (-0,02%).

Cuadro 1. IPC Variación y contribución mensual
Según divisiones de gasto
Mayo 2025 - 2026

		2025		2026	
Divisiones de Gasto	Peso (%)	Variación (%)	Contribución Puntos Porcentuales	Variación (%)	Contribución Puntos Porcentuales
Alojamiento, agua, electricidad, gas y otros combustibles	33,12	0,48	0,15	0,86	0,26
Recreación y cultura	3,79	-0,52	-0,02	0,77	0,02
Transporte	12,93	-0,08	-0,01	0,61	0,08
Muebles, artículos para el hogar y para la conservación ordinaria del hogar	4,19	0,18	0,01	0,53	0,02
Salud	1,71	0,39	0,01	0,52	0,01
TOTAL	100,00	0,32	0,32	0,47	0,47
Prendas de vestir y calzado	3,98	0,39	0,01	0,42	0,01
Restaurantes y hoteles	9,43	0,36	0,04	0,38	0,04
Bebidas alcohólicas y tabaco	1,70	0,39	0,01	0,27	0,00
Información y comunicación	4,33	-0,15	0,00	0,25	0,01
Bienes y servicios diversos	5,36	0,28	0,01	0,22	0,01
Educación	4,41	0,00	0,00	0,00	0,00
Alimentos y bebidas no alcohólicas	15,05	0,60	0,11	-0,02	0,00

Fuente: DANE, IPC
Nota: La diferencia en la suma de las variables obedece al sistema de aproximación en el nivel de dígitos trabajados en el índice.

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

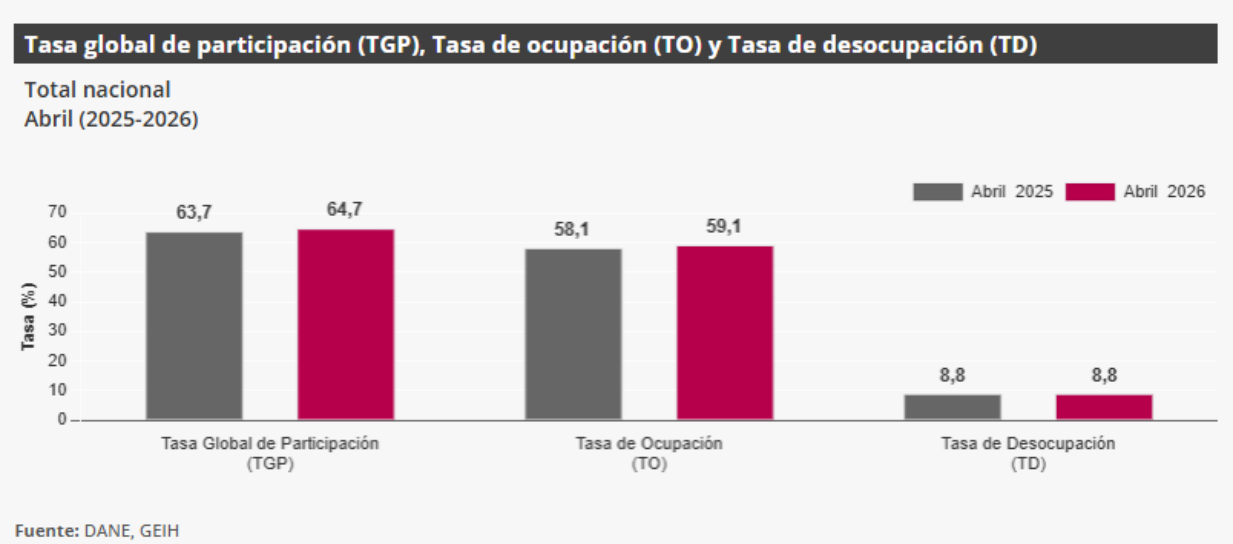
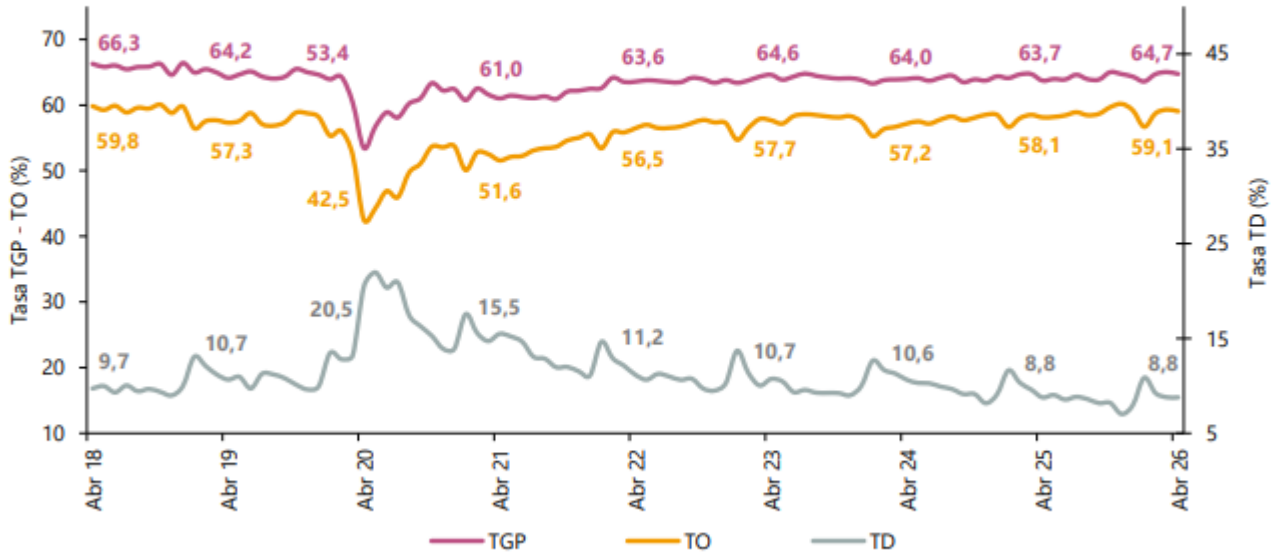


Gráfico 1. Tasa global de participación (TGP), Tasa de ocupación (TO) y Tasa de desocupación (TD)
Total nacional
Abril (2018 - 2026)



Fuente: DANE, Gran Encuesta Integrada de Hogares (GEIH).

Este contexto indica que existe una oferta suficiente de talento humano especializado en el mercado, lo cual favorece la participación de proponentes con capacidades técnicas adecuadas para la ejecución del contrato.

Así mismo, reduce el riesgo de sobrecostos asociados a escasez de personal calificado y contribuye a garantizar la viabilidad operativa del proceso en condiciones de competencia y eficiencia.

Salario Mínimo Legal Vigente (SMMLV)

Para el año 2026, mediante el Decreto 0159 del 19 de febrero de 2026, el Gobierno Nacional fijó de manera transitoria el salario mínimo mensual legal en $1.750.905, lo que representa un incremento aproximado del 23 % respecto al año anterior. Así mismo, el auxilio de transporte fue establecido en $249.095, para un ingreso total de referencia cercano a $2.000.000 mensuales.

Este incremento significativo tiene incidencia directa en los costos laborales de la economía, particularmente en actividades operativas, logísticas y de soporte. No obstante, en el contexto del presente proceso contractual, el impacto es indirecto, dado que se trata de servicios altamente especializados que requieren personal técnico y profesional certificado, cuyos costos se encuentran más asociados a condiciones de mercado del sector TIC que al salario mínimo.

En consecuencia, si bien el ajuste del SMMLV puede generar presiones marginales en algunos componentes de la estructura de costos de los proveedores, se considera que estos han sido internalizados en las propuestas económicas, por lo cual no se prevén afectaciones sustanciales en la ejecución del contrato.

Entidades que integran el sector:
Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

El Ministerio TIC es la entidad encargada de formular y coordinar las políticas del Estado en materia de tecnologías de la información, comunicaciones, seguridad digital y transformación digital. Dentro de su rol institucional, establece lineamientos estratégicos, técnicos y normativos para fortalecer la seguridad informática en entidades públicas, fomentar la interoperabilidad y promover entornos digitales confiables.

Entre los documentos más relevantes que enmarcan el presente proceso contractual, se destacan:

Circular Externa MinTIC 003 de 2022 – Lineamientos de seguridad digital para entidades públicas.

Manual de Seguridad Digital – Estándares mínimos de ciberseguridad en la administración pública.

Política de Gobierno Digital (CONPES 3975 de 2019) – Requiere plataformas robustas de seguridad para la operación digital del Estado.

Estas disposiciones exigen que las entidades públicas cuenten con soluciones tecnológicas actualizadas, protegidas frente a riesgos cibernéticos, y alineadas con las mejores prácticas internacionales.

Consejo Internacional de Seguridad de la Información (ISF/ISO)

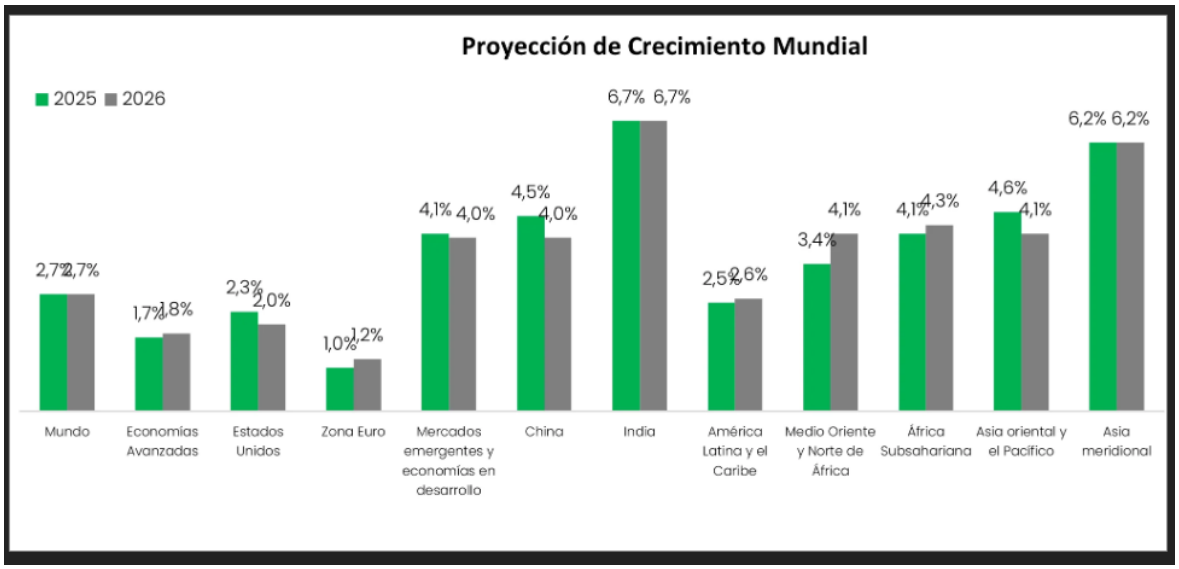
A nivel internacional, los estándares ISO 27001 (seguridad de la información) y 20000 (gestión de servicios TI) son referentes clave que definen las mejores prácticas para la gestión de infraestructuras críticas. Estos estándares son ampliamente adoptados por fabricantes como **FORTINET** y forman parte de los criterios técnicos en los procesos de adquisición de soluciones de ciberseguridad en Colombia.

Su adopción garantiza interoperabilidad, trazabilidad de eventos, continuidad del servicio, protección contra vulnerabilidades y mecanismos de respuesta ante incidentes.

Crecimiento del Sector Terciario

Datos DANE muestran dinamismo en comercio y servicios en trimestres recientes (3,9% en Bogotá Q1 2025), con aporte clave al PIB total pese a inflación moderada al 4,2%.

Este crecimiento favorece la renovación de licencias Fortinet, ya que el 70% del mercado de ciberseguridad se concentra en servicios terciarios como banca y gobierno.



El sector terciario (servicios) es el motor principal de la economía colombiana y soporta la demanda de soluciones de ciberseguridad como Fortinet, con proyecciones estables para 2026 pese a retos fiscales.

El licenciamiento de Fortinet, especialmente en su modalidad de modelo de renovación de licencias con soporte y garantía extendida (FortiCare y FortiGuard), es clave para mantener la continuidad operativa en entornos de seguridad perimetral, como firewalls FortiGate, Access Points y switches en Colombia. Esta renovación asegura servicios activos de inteligencia de amenazas, actualizaciones y soporte técnico (5x8 o 24x7), evitando riesgos como exposición a vulnerabilidades sin parches o pérdida de funcionalidades críticas en 2026.

Proyecciones 2026
Se espera un crecimiento moderado del 3,2%, liderado por servicios digitales y financieros, alineado al PIB nacional estimado en 2,6-3,1% pese a retos fiscales.

Sector Específico	Crecimiento Estimado 2026	Factores Clave
Comercio y Transporte	3,5-4,0%	Remesas y consumo interno.
Servicios Financieros/TIC	4,0%+	Digitalización y ciberseguridad.
Entretenimiento/Profesionales	2,5-6,6%	Recuperación post-pandemia.

Esta tendencia soporta inversiones en licenciamiento Fortinet, ya que el sector terciario concentra el 70% de la demanda de ciberseguridad en Colombia. Para gráficos visuales oficiales, consulta el sitio DANE o DNP

directamente.

Lo anterior evidencia que los servicios de TI y de tercerización que ofrecen las empresas integradoras de servicios tecnológicos, se encuentran en el mercado nacional, impactando la economía del país y que harán parte integral de este proceso de contratación y del análisis del sector frente a la oferta y la demanda. Además de aportar al cumplimiento de la misionalidad y los objetivos estratégicos, permitiendo el acceso a la información y la automatización de los procesos, asimismo de optimizar la infraestructura (el hardware, el software y la redes) de cada una de las sedes regionales de la ART.

Según los reportes más recientes del **DANE** (con corte a febrero de 2026), la economía colombiana ha mostrado una resiliencia notable, jalonada principalmente por el sector servicios.

- **Crecimiento Consolidado 2025:** El PIB cerró el año con un crecimiento promedio de **2.8%** (según datos preliminares del ISE a noviembre y proyecciones de cierre).
- **Proyección 2026:** Se espera que el PIB mantenga una senda de expansión similar, situándose entre el **2.8% y 2.9%**.
- **Sector de Información y Comunicaciones:** Este rubro ha sido uno de los motores de crecimiento, registrando expansiones trimestrales de hasta el **2.3%**, superando el promedio nacional. Esto indica que la inversión en tecnología no es solo un gasto, sino el eje de la productividad del país.

Si se revisan los servicios TI de este contrato, damos cuenta como la infraestructura de TI mejorada, juega un papel importante. Los Equipos como Servidores físicos, Switches y Access Point, no solo le aportan a través de Hardware, si no que tienen una finalidad sobre las comunicaciones y la seguridad informática de la Agencia, esto dado que las crecientes filtraciones de datos, las preocupaciones sobre los costos relacionados con la personalización de productos y la migración de datos son algunas de las razones que representan una amenaza para las entidades públicas y privadas, es necesario que todo se apalanque dentro de los Sistemas de Seguridad de la Agencia para que las sedes regionales puedan ser monitoreadas y puedan utilizar los demás servicios TI que tiene la entidad.

Por último, los servicios de TI para las redes que hacen parte de la conectividad y que utilizan dispositivos como los Switch y los Access Point no solo hacen parte de las telecomunicaciones en las sedes sino de la seguridad informática de la infraestructura tecnológica de la ART, estas comunicaciones y dispositivos de seguridad informática son ofrecidos actualmente por el fabricante FORTINET® el cual tiene una amplia gama de soluciones de seguridad, que incluyen firewalls de próxima generación (NGFW), soluciones de seguridad para la nube, seguridad de redes inalámbricas, seguridad de endpoints, sistemas de prevención de intrusiones (IPS), sistemas de detección y respuesta de amenazas (EDR), dispositivos Networking, entre otros. Esta variedad de productos permite a las organizaciones construir una defensa integral contra amenazas de seguridad.

En resumen, el fabricante FORTINET® que es la marca de la infraestructura de comunicaciones, red y seguridad con que cuenta la agencia, es una opción para la seguridad informática debido a su amplia gama de soluciones, enfoque en la integración y sincronización de productos, alto rendimiento y escalabilidad, enfoque en la innovación y compromiso con la educación en seguridad cibernética, marca que actualmente es utilizada por gran cantidad de entidades del estado.

Por esto, FORTINET® es de las marcas mejores ranqueadas en diferentes benchmarking en seguridad perimetral, tal como lo es el cuadrante mágico de Gartner como se indicó anteriormente, ya que dicho fabricante es referenciado como lideres en el sector, por lo tanto, se cuenta con confianza de que se tienen elementos de buena reputación en la industria de la seguridad informática. [2]

[2] https://www.isc.cl/que-es-el-cuadrante-magico-de-gartner-transformacion-digital/

Es importante mencionar que estas inversiones en seguridad que realiza la agencia mitigan las materializaciones de ataques cibernéticos, ya que cada vez hay más ataques a las entidades públicas y estas deben estar protegidas con equipos que sirvan como controles de seguridad informática, por esta razón es necesario tener una plataforma completa en seguridad para mejorar los análisis de vulnerabilidades, la correlación de eventos y el monitoreo de amenazas del Nivel Central y de Nivel Regional.

Estas inversiones en ciberseguridad se enmarcan dentro de una creciente demanda global. Según el Worldwide Security Spending Guide de IDC, para 2025 se proyecta un crecimiento del 12,2 % en el gasto mundial en seguridad informática, impulsado por amenazas cada vez más sofisticadas y la adopción de inteligencia artificial.

Se estima que este año el mercado global de ciberseguridad superará los $377 000 millones, con software de seguridad como principal categoría (crecimiento del 14,4 %) y servicios gestionados en segundo lugar.

El mercado de ciberseguridad en 2026 se caracteriza por una **industrialización del cibercrimen**. Según proyecciones de Fortinet, el cibercrimen se posiciona como la tercera economía mundial.

- **Evitación de multas por retroactividad:** Fortinet aplica cobros retroactivos si la licencia expira. Renovar *antes* del vencimiento evita el pago de "meses perdidos" y posibles penalizaciones que pueden incrementar el costo hasta en un **20-30%**.
- **Retorno de Inversión (ROI):** Estudios recientes indican que las soluciones integradas de Fortinet pueden ofrecer un ROI de hasta **1093%**, principalmente al reducir el tiempo de respuesta a incidentes en un 99%, lo que ahorra en promedio **$1.9 millones de dólares anuales** en costos de remediación por brechas de seguridad.
- **Tasa de Cambio y Presupuesto:** Dado que los precios suelen estar anclados al dólar (USD), la planeación temprana permite mitigar la volatilidad cambiaria y aprovechar descuentos por renovaciones multi-anuales (3 a 5 años), que suelen ser más eficientes que las anuales.

Finalmente se constata que la agencia de renovación del Territorio se ha certificado en ISO27000:2022 como marco de trabajo para seguridad de la información, por lo tanto, se deben de cumplir todos los requerimientos que exige la norma para tener la información y los datos lo más asegurado posible.

Contexto Técnico:

La Organización de las Naciones Unidad advierte que no existe un concepto uniforme, pero que se puede definir a la ciberdelincuencia como un acto que infringe la ley, que se comete a través de las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, páginas web y tecnología o para facilitar un delito.

Adicionalmente, en la 58ª Reunión del Grupo de Expertos para el Control del Lavado de Activos (GELAVEX), celebrada los días 17 y 18 de junio de 2025, se presentaron diagnósticos regionales avanzados sobre el combate al lavado de activos vinculado a delitos cibernéticos. El encuentro profundizó en la coordinación entre Unidades de Inteligencia Financiera y organismos investigadores, con un enfoque especial en el uso de inteligencia artificial y criptoactivos como nuevos vectores de riesgo. Se adoptó un plan de trabajo robusto para 2025–2027, que refuerza la cooperación internacional y los mecanismos de decomiso, alineados con la agenda hemisférica de seguridad financiera. se clasifican los delitos cibernéticos de la siguiente manera:

1- Delitos contra la confidencialidad, la integridad y la accesibilidad (Triada CIA) de los datos y sistemas informáticos:
   Acceso ilícito a sistemas informáticos.
   Interceptación ilícita de datos informáticos.
   Interferencia en el funcionamiento de un sistema informático.

Abuso de dispositivos que faciliten la comisión de delitos.

2- Delitos informáticos:
   Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
   Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
3- Delitos relacionados con el contenido:
   Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.
4- Delitos relacionados con infracciones de la propiedad intelectual y derechos afines (copia y distribución de programas informáticos, o la piratería informática). 3

Los ciberdelincuentes usan diferentes estrategias para vulnerar los sistemas, las más conocidas son:

Spear phising: Gracias a los correos electrónicos de phishing los delincuentes acaban consiguiendo datos de acceso y contraseñas. No obstante, hoy en día, las probabilidades de que los usuarios caigan en el engaño de los mensajes falsos son bastante reducida. Ahora hay una nueva variante de este tipo de engaño, el spear phishing, mucho más concreta y, por lo tanto, peligrosa.

El principio del phishing es relativamente sencillo: los estafadores crean correos electrónicos, páginas web e incluso mensajes cortos de carácter falso que parecen auténticos y que solicitan información de inicio de sesión de los usuarios. Es así como los estafadores se hacen con los datos de acceso para tiendas online, redes sociales o espacios de almacenamiento en la nube. En el peor de los casos, se hacen incluso con información bancaria o datos de la tarjeta de crédito. Los estafadores saben que hay muchos usuarios que no se toman en serio la seguridad de las contraseñas y que usan una misma contraseña para diferentes servicios. De esta forma, con una página web de phishing sencilla se pueden obtener datos sensibles, información que tiene un alto valor económico en el mercado negro digital.

Además, con esta técnica, los delincuentes pueden copiar virus y otro tipo de software malicioso en los ordenadores de las víctimas para hacerse con el control del dispositivo. Por norma general, la víctima ni se entera y cree que simplemente ha abierto un correo electrónico inofensivo o visitado una página web segura.[4]

Spoofing: (falsificación, modificación de los datos) es el acto de suplantación en el que una fuente desconocida de comunicación está disfrazada de otra, conocida y fiable para el receptor. Los hackers usan spoofing para conseguir el acceso a los datos sensibles de la víctima o para usar sus recursos computacionales para llevar a cabo ciber ataques.[5]

Watering Hole: Los ataques 'Watering hole' o ataques de abrevadero, llamados así por la similitud de un depredador acechando a la presa en un abrevadero, son una de las técnicas más sofisticadas empleadas por los ciberatacantes. Su complejidad es directamente proporcional a su alta tasa de éxito y eficiencia, siendo uno de los ataques más difíciles de detectar y detener que acechan actualmente a las compañías.

¿En qué consiste?

Este tipo de ataques están enfocados a compañías, con altos niveles de seguridad, en las que los usuarios visitan asiduamente sitios web de confianza relacionados con el contenido de la organización. Estos sitios web, han sido previamente estudiados e infectados por los atacantes, quienes suelen realizar primero un perfil de las potenciales víctimas llevando a cabo un estudio de sus costumbres. Una vez el empleado de la compañía

[3] https://www.oas.org/es/sms/ddot/gelavex/53/docs/6-Diagn%C3%B3stico%20regional%20lavado%20y%20delitos%20cibern%C3%A9ticos.pdf

[4] https://www.ionos.es/digitalguide/correo-electronico/seguridad-correo-electronico/spear-phishing/
[5] https://softwarelab.org/es/que-es-spoofing/

objetivo visite el sitio web infectado, como suele hacer a menudo, infectará su equipo con programa maligno que permitirá a los atacantes tomar el control del equipo del empleado y poder así espiar y robar información de la compañía.

Suplantación de identidad: Como definición de suplantación de identidad podríamos decir que:
"La suplantación de identidad consiste en hacerse pasar por otra persona para obtener un beneficio. Está tipificado como delito en el Código Penal."

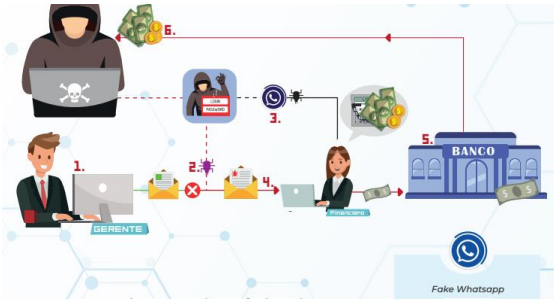
Los fines por los que se realiza la suplantación de identidad pueden ser:

- Cometer otro delito.
- Contratar servicios de telefonía.
- Obtener una hipoteca o un crédito.
- Realizar compras tanto en tiendas físicas como a través de tiendas online, etc.

Debido a la facilidad con la que puede crearse un perfil en una red social (con un correo electrónico simplemente), los casos de suplantación de identidad se han multiplicado. Una persona puede usar fotografías de otra persona sin su consentimiento expreso y crear un perfil en Twitter, Facebook o cualquier otra red, incluso utilizando también su nombre. Y utilizará esta cuenta para insultar o acosar a terceras personas y hasta para conseguir datos personales y bancarios de otros usuarios con los cuales continuar cometiendo otras ilegalidades.[6]
Con estas estrategias los ciberdelincuentes pueden ejecutar una serie de ataques a las empresas o entidades, entre los cuales se encuentran:[7]

-Ataques BEC: Cerca del 90% de los ciberataques que sufren las empresas en Colombia se deben a ingeniería social.

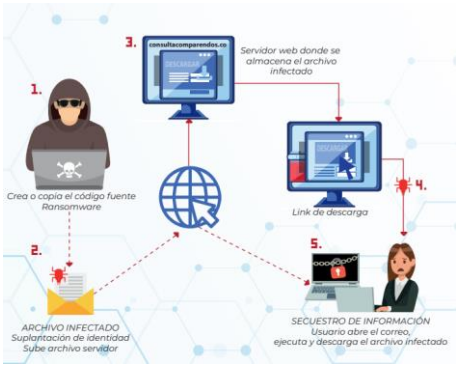
A través de distintas técnicas los cibercriminales obtienen información confidencial de empresas, directivos y empleados, para luego suplantar identidades, falsificar correos electrónicos y conseguir en la mayoría de los casos desviar dinero hacia cuentas bancarias bajo su control o generar despachos de insumos y mercancías engañando a clientes y proveedores.



Tomado de: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

-Rasomware: Aunque no se trata de una modalidad reciente, este tipo de ataque que deriva su nombre de la combinación de las palabras Ransom ó rescate en inglés y Ware alusivo a Software (Ransomware: Software de Rescate), ha tenido un auge en los últimos años en Colombia muy vinculado al creciente uso de las Criptomonedas como medio para monetizar las ganancias del Cibercrimen a nivel mundial.

[6] https://ayudaleyprotecciondatos.es/2018/09/10/suplantacion-identidad/
[7] https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf



Tomado de: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

-Ataque de DDOS: Los Ataques de Denegación de Servicio son utilizados para inhabilitar un servicio ofrecido por un servidor, haciendo colapsar el sistema aprovechando sus vulnerabilidades.

Tomado de: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

-Malware: Los cibercriminales utilizan el malware con múltiples finalidades, tales como extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo. Puede protegerse contra el malware mediante el uso de software antimalware.

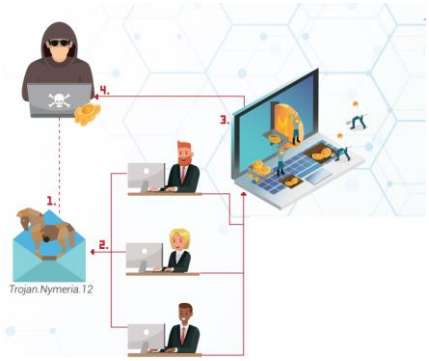
Tomado de: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

-SIM Swapping: Este tipo de estafa explota una de las mayores vulnerabilidades de las tarjetas SIM: el hecho de que funcionan en cualquier plataforma. Lo hace gracias a loque se conoce como “ingeniería social”, la

técnica de los cibercriminales para llevar a cabo el SIM Swaping, el cual consiste en confundir a los vendedores de empresas de celulares y lograr que transfieran los números a tarjetas controladas por ellos.

Tomado de: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

-Cryptojacking: El uso de un hardware del visitante de una página web sin su permiso, para minar criptomonedas es un problema para usuarios y compañías que se financian con la publicidad (el 90% de Internet). Y más ahora que el Bitcoin está batiendo récords.



Tomado de: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

Por lo anterior, la entidad debe mantener los controles actuales que eviten la materialización de este tipo de incidentes de seguridad, adicionalmente, se debe realizar un análisis de vulnerabilidades ya que este es un mecanismo de mejora continua en la gestión de la seguridad[8], una vez se tenga el resultado de esta actividad se aplicarán las recomendaciones para corregir los puntos débiles de los sistemas de la entidad,

Por otro lado, al analizar el CONPES 3995 del 2020[9] donde se formula una política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, por lo tanto, es necesario maximizar los esfuerzos para asegurar la información que se manejan en los diferentes entes estatales.

Las diferentes entidades o empresas colombianas manejan diferentes controles de seguridad como lo son mecanismos más seguros son conexiones cifradas como las VPN(s), firewall de última generación y soluciones de antivirus, la Agencia tiene configurada una plataforma de seguridad, en la cual se maneja el antivirus y el

[8] https://revistaseguridad360.com/destacados/analisis-de-vulnerabilidades/
[9] https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

firewall de marca FORTINET®, que por su compatibilidad y estabilidad de la solución permite mitigar incidentes de seguridad, por ello es requerido contar la renovación de la licencia de estos equipos de frecuencia anual tal como lo maneja dicho fabricante de la industria de la seguridad en su modelo de soporte y de servicios.

Los elementos actuales que tiene la ART en la infraestructura de seguridad son los descritos en la ficha técnica del proceso.

Técnicamente, una licencia de Fortinet activa no es opcional si se desea mantener la integridad de la red.

- **Ciclo de Vida (EOL/EOS):** Es crítico verificar si tus equipos (como los modelos FortiGate-90E o 52E) están en su fase de *End of Support* (EOS) en 2026. Si el hardware ha llegado al EOS, Fortinet **no permitirá abrir tickets de soporte ni recibirá actualizaciones de firmware**, dejando el equipo vulnerable a *zero-days*.
- **Inteligencia de Amenazas (FortiGuard):** En 2026, los ataques son impulsados por IA autónoma. Sin la renovación, el equipo pierde el acceso a las firmas de Antivirus, AntiSpam e IPS en tiempo real, convirtiéndose en un router básico sin capacidad de defensa proactiva.
- **Soporte FortiCare:** El soporte 24x7 asegura el reemplazo físico del hardware (RMA) en caso de falla. Sin garantía activa, una falla de hardware implica la compra de un equipo nuevo a precio de lista y días de inactividad total.

La ART debe estar preparada para proteger la información y los datos que maneja y así poder cumplir en la normatividad vigente en la protección de datos personales, también debe asegurar el resguardo confiable de esta, una de las estrategias para poder cumplir con este aseguramiento, es la ejecución de un análisis de vulnerabilidades a los diferentes activos de la información que se encuentran con acceso público, pero *¿qué es el análisis de vulnerabilidades?,* primero se debe definir qué es una vulnerabilidad, según la ISO 27001:2022 las vulnerabilidades son defectos o debilidades de un activo, cuyas amenazas pueden desencadenar o explotar la misma materializando una agresión sobre dicho activo. En otras palabras, se puede expresar como una falla en un sistema que genera un riesgo de seguridad para la organización o para el mismo sistema; con esta estrategia es posible identificar posibles riesgos y con esta se pueden ejecutar planes de mejora para mitigar la materialización de estos, estas pruebas de penetración son ampliamente ejecutadas por expertos en seguridad informática y se considera como de las mejores prácticas para cumplir con el deber legal que tiene la entidad para proteger la información por lo menos en sus cinco pilares que son: confidencialidad, disponibilidad, integridad, autenticidad y legalidad[10]

Contexto Regulatorio:

El ente regulador de las tecnologías de la información, de la seguridad informática, modelo de seguridad y privacidad de la información[11] y similares está en el ministerio de las tecnologías de la información (MinTic), el proceso de seguridad está enmarcado en las diferentes políticas, lineamientos, normas entre otros expedidos por este ente de control en TI.

Este proceso también se enmarca en el CONPES 3854 que aún está vigente y aplica a toda la política pública en cuanto a seguridad digital[12], anexamos un resumen de otros elementos regulatorios sobre este respecto:
Guías:

- Manual Política de Gobierno Digital.

[10] https://www.flane.com.pa/blog/5-pilares-de-la-seguridad-en-la-informacion/#:~:text=Hay%205%20pilares%20de%20la,%2C%20disponibilidad%2C%20autenticidad%20y%20legalidad.
[11] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/
[12] https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018.
- Conpes 3854: Política Nacional de Seguridad Digital
- Conpes 3995: Política Nacional de Confianza y Seguridad Digital
- Política General de Seguridad de la Información de la ART.
- Manual de Políticas de Seguridad de la Información de la ART.

Normas Técnicas:

- NTC ISO/IEC 27001:2022 Sistemas de Gestión de la Seguridad de la Información.
- GTC-ISO/IEC 27002-2013 Código de Prácticas para los Controles de Seguridad de la Información.
- ISO / IEC 27004: 2016: Monitoreo, Medición, Análisis y Evaluación.
- ISO 31000:2009: Herramienta para Evaluar la Gestión de Riesgos.
- ISO 31000 Gestión de Riesgos.
- ISO 27005 Recomendaciones y Directrices Generales para la Gestión de Riesgo.

Leyes:

- Ley 1712 de 2014: Acceso a la Información Pública.
- Ley 594 de 2000: Ley General de Archivos.
- Ley 1581 de 2012: Protección de Datos Personales.
- Ley Estatutaria 1266 de 2008: Ley de Habeas Data.
- Ley 1712-2014: Ley de Transparencia y Acceso a la Información Pública.

Decretos:

- Decreto 1008 del 14 de junio de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.
- Decreto 338 del 8 de marzo de 2022 “Por el cual se adiciona el Titulo 21 a la Parte 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital y se dictan otras disposiciones”.

Resolución:

- Resolución 500 del 2021 del MINTIC: “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- Resolución 000709 del 2021 de la ART:” Por la cual se adoptan los lineamientos y estándares para la estrategia de seguridad digital, se acoge el Modelo de Seguridad y Privacidad de la Información - MSPI y se crea el Equipo Técnico de Seguridad Digital y de la Información de la Agencia”.

Que en atención a la resolución 00500 de 2021*, “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”*, La entidad debe adoptar el Modelo de Seguridad y Privacidad de la información que imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

Y, por último, con la normativa relacionada anteriormente, la entidad a través de la Resolución 0709 del 2021 estableció los lineamientos para adoptar el MSPI y así dar cumplimiento a lo estipulado por el MinTic,

apoyándose con la implementación del Sistema de Gestión de Seguridad de la Información - SGSI basado en la norma ISO 27001:2022

2. DESCRIPCIÓN DE LA NECESIDAD:

La Agencia de Renovación del Territorio, para el cumplimiento óptimo de su misión y la realización de las funciones encomendadas, desarrolla sus objetivos misionales bajo un enfoque de gestión que garantiza las funciones propias que se derivan de lo que determina la ley y las políticas del Gobierno Nacional para la intervención de las zonas rurales de conflicto priorizadas; esto a través de su planta de personal y colaboradores que laboran o prestan sus servicios en la sede central en la ciudad de Bogotá y en los Grupos Internos de Trabajo Regionales, los cuales desarrollan actividades administrativas y misionales de acuerdo con la labor encomendada.

En cumplimiento de sus objetivos misionales y funcionales, la ART debe disponer de recursos y herramientas tecnológicas que permitan apoyar la implementación y difusión de sus políticas, logrando un óptimo funcionamiento de los procesos de apoyo, garantizando disponibilidad, confiabilidad e integridad de la información, y minimizando el procesamiento manual de datos.

Que, en el marco de lo anterior, y en atención a la necesidad de la Agencia de asegurar los datos obtenidos y la información que resulta en la intervención de las entidades nacionales y territoriales en las zonas rurales afectadas por el conflicto y priorizadas por el Gobierno Nacional se avanzará en el desarrollo en las disposiciones contenidas en el artículo 143 de la Ley 2294 de 2023 en su numeral 7 que consiste en "*Promover un entorno digital seguro para generar confianza en el uso y apropiación de las TIC.*"

Teniendo en cuenta que la Agencia de Renovación del Territorio, tiene presencia a nivel nacional y se encuentra organizada con una sede central en la ciudad de Bogotá y subregiones con sedes en las ciudades de Popayán, Medellín, Cúcuta, Florencia, Villavicencio, Sincelejo, Tumaco, Mocoa, Montería, Ibagué, Barrancabermeja, Apartado, Buenaventura, Santa Marta, Choco, Arauca y que en sus actividades propias de funcionamiento y de misionalidad es necesario el acceso a sistemas de información, bases de datos, aplicaciones, uso de archivos compartidos y accesos a datos de activos o elementos que están dispuestos en la plataforma tecnológica de la Entidad en la sede central y en servicios contratados en nube, por lo tanto se requiere que todo este flujo de información y de datos esté asegurada para cumplir con los confidencialidad, integridad y disponibilidad de la información.

La implementación del Sistema de Gestión de la Seguridad de la Información - SGSI constituyó una actividad de cumplimiento para meta sectorial y fue establecida en el plan estratégico sectorial – PES del Departamento Administrativo de la Presidencia de la República – DAPRE, donde la Agencia se encuentra certificada en la norma ISO 27001-2013 con fecha 28 de abril de 2023 y con renovación en el año 2025 a la versión ISO 27001-2022, por lo anterior la oficina de tecnologías de la información – OTI, debe fortalecer, mantener y optimizar la infraestructura tecnológica, para soportar las operaciones digitales, en cumplimiento de la misión de la Agencia y de sus objetivos estratégicos, a través del uso de tecnologías de la información. También debe diseñar e implementar estrategias que faciliten la comunicación entre los sistemas de información, las herramientas informáticas, las tecnologías emergentes, el uso de redes e internet y las personas que interactúan con cada uno de los activos tecnológicos, entendidos estos como los recursos que utiliza un sistema de gestión de seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que ha propuesto la alta dirección, lo anterior, bajo los lineamientos de la política de seguridad de la Información logrando el fortalecimiento de la cultura digital, es importante destacar que la OTI gestiona las redes WAN, LAN y WIFI, así como los servidores informáticos y equipos de cómputo PC(s) para los colaboradores de la ART; teniendo en cuenta que, el uso de diferentes equipos por parte de los usuarios visitantes que se conectan a la red y que algunos no cuentan con las debidas protecciones de seguridad y antivirus; con el mal uso de estas herramientas incrementa el riesgo de la materialización de diferentes amenazas cibernéticas los cuales deben ser atendidos y mitigados con alguna estrategia de protección en ciberseguridad.

Mientras que por un lado hoy se tiene a disposición cientos de servicios de interconexión entre clientes internos y externos de diferentes entidades públicas y privadas, también se está teniendo mayor exposición de la información personal y corporativa hacia sistemas o personas no autorizadas que utilizan diversos métodos para atacar los sistemas de las entidades, siendo cada vez más complejo, más difícil prevenirlos y sobre todo más dañinos, esto ha llevado a las entidades a ser enfáticas con la ciberseguridad, tanto en los aspectos preventivos como correctivos con el fin de mitigar, prevenir y reaccionar oportunamente ante un ataque de esta índole.

Así las cosas, la ART cuenta actualmente con una infraestructura tecnológica de ciberseguridad basada en soluciones del fabricante FORTINET©, las cuales se encuentran implementadas y operando dentro de la arquitectura de seguridad informática de Agencia.

En consecuencia, desde el año 2018, se ha venido renovando el licenciamiento de la plataforma de ciberseguridad y el soporte brindado por el fabricante Fortinet y su garantía, con una última renovación realizada en la vigencia 2025, mediante contrato SG 0169 2025 por el término de diez (10) meses, esto es hasta el 31 de agosto de 2026. Por lo tanto, para el presente proceso contractual se requiere de la renovación de licenciamiento, soporte, mantenimiento, actualización y garantía tecnológica de los equipos existentes, con el fin de garantizar la continuidad operativa, la interoperabilidad entre los componentes de seguridad y la protección de los activos de información de la Agencia evitando la materialización de amenazas que puedan ocasionar impactos negativos sobre la infraestructura tecnológica.

Dentro de las buenas prácticas en ciberseguridad, se debe considerar realizar el acondicionamiento en materia de seguridad de la información a través del desarrollo de las siguientes actividades que componen la contratación para satisfacer son:

- **Renovación y soporte de las garantías de la plataforma FORTINET® de la Agencia de Renovación del Territorio:** Indispensable para contar con el soporte técnico de fabrica con las herramientas ya adquiridas por la ART.

- **Servicio de análisis y gestión de vulnerabilidades para activos de la Agencia de Renovación del Territorio:** Esto como buena práctica para detectar posibles debilidades en los activos de la información con mejoras de los servicios de seguridad cibernética con este análisis y servicios.

- **Renovación y soporte de las garantías de la plataforma FORTINET® de la Agencia de Renovación del Territorio**

Una vez explicada la fase anterior, se debe continuar con la segunda fase, la cual corresponde a la renovación de las licencias actuales, así como al acceso al soporte técnico especializado, la extensión de garantías y la prestación de servicios de mantenimiento para la plataforma de seguridad FORTINET®, que es la solución actualmente implementada en la Agencia de Renovación del Territorio (ART).

Esta plataforma está compuesta por diversos dispositivos de seguridad, tales como:

- Firewall de perímetro
- SandBox[13]
- Analizador de logs
- Correlacionador de eventos

[13] https://es.wikipedia.org/wiki/Entorno_de_pruebas_(inform%C3%A1tica)

La renovación de estos componentes permitirá actuar tanto preventiva como correctivamente frente a posibles eventos relacionados con la seguridad informática y la operación de la infraestructura tecnológica. Entre las actividades contempladas se incluyen la aplicación de parches de seguridad, la configuración de nuevas políticas y la actualización de las ya existentes, lo cual permitirá mitigar riesgos tales como:

- Riesgos operativos derivados de fallas en los componentes de la solución FORTINET®.
- Baja capacidad de procesamiento ante demandas crecientes.
- Tiempos de respuesta inadecuados frente a incidentes de seguridad.
- Obsolescencia en las configuraciones de los dispositivos y herramientas que integran la solución de seguridad y conectividad.

La renovación del contrato de soporte para la infraestructura tecnológica de seguridad FORTINET© que posee la Agencia de Renovación del Territorio es esencial por varias razones:

Garantía de Componentes y Partes: Este contrato asegura la cobertura de garantías en elementos y partes de los equipos activos de red, lo que es fundamental para mantener la integridad y el funcionamiento continuo de la infraestructura de seguridad.

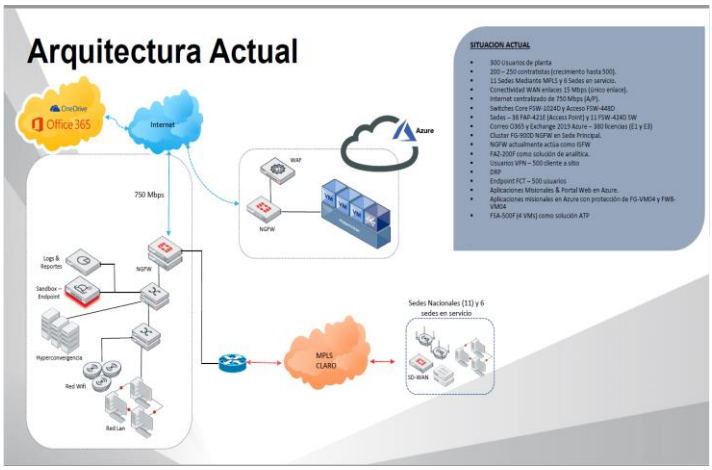
Soporte Especializado del Fabricante: Al contar con el respaldo directo del fabricante, se garantiza acceso a soporte técnico especializado. Esto es crucial para resolver cualquier eventualidad que pueda surgir, ya sea en términos de fallas de hardware, problemas de software, o cualquier otra incidencia técnica.

Asesoría y Apoyo Continuo: La renovación del contrato permite obtener asesoría y apoyo constante en configuraciones, ajustes y requerimientos necesarios. Esto incluye la parametrización y personalización de los equipos según las necesidades específicas de la entidad.

Actualizaciones y Mejoras Continuas: El soporte del fabricante incluye actualizaciones y mejoras del software, lo que garantiza que la infraestructura de seguridad se mantenga al día con las últimas innovaciones y parches de seguridad. Esto es vital para proteger la red contra nuevas amenazas y vulnerabilidades.

Funcionamiento Óptimo y Eficiencia Operativa: Con este contrato, se asegura un funcionamiento óptimo de la infraestructura tecnológica tanto en eventos físicos como en la configuración y parametrización. Esto permite una respuesta y atención oportuna a cualquier necesidad que pueda surgir, asegurando la continuidad operativa de la entidad.

En resumen, la renovación del contrato de soporte con FORTINET© no solo proporciona garantías y soporte técnico, sino que también asegura que la Agencia de renovación del territorio esté preparada para enfrentar cualquier desafío tecnológico con eficiencia y seguridad, manteniendo siempre la operatividad y protección de su infraestructura de red, a continuación, se detallan los elementos a renovar su licenciamiento:



Fuente: Elaboración propia, imagen resumida topología de seguridad de la OTI - ART.

Los elementos actuales con que cuenta la ART en su infraestructura de seguridad informática son los descritos en la ficha técnica del proceso.

- **Servicio de análisis y gestión de vulnerabilidades para activos de la Agencia de Renovación del Territorio.**

Realizar un análisis de vulnerabilidades y de debilidades, considerado una actividad clave para asegurar que la infraestructura tecnológica de la agencia se mantenga protegida y actualizada frente a la creciente y constante evolución de amenazas cibernéticas.

En el marco de sus funciones en materia de seguridad digital, la Oficina de Tecnologías de la Información (OTI) cuenta con un inventario de activos de información, el cual se encuentra articulado con el mapa de procesos del Sistema Integrado de Gestión de la ART. Este inventario permite verificar el nivel de protección de dichos activos, identificar los controles definidos, evaluar su efectividad y determinar si es necesario ajustarlos o implementar nuevos controles para reforzar la seguridad.

Por lo anterior, se requiere adelantar un análisis de vulnerabilidades conforme al anexo técnico adjunto a este proceso. El objetivo es obtener un informe técnico que evidencie el nivel de aseguramiento de los activos frente a amenazas existentes, permitiendo la toma de decisiones fundamentadas en materia de ciberseguridad.

Según la norma ISO/IEC 27001:2022, una vulnerabilidad es una debilidad o defecto en un activo que puede ser explotado por una amenaza, generando un riesgo de seguridad para la organización. En la misma línea, el Decreto 338 de 2022 define la vulnerabilidad de seguridad digital como una "*debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y redes de la organización*".

El análisis de vulnerabilidades es un servicio técnico mediante el cual se comprueban, a través de herramientas especializadas de hardware y software, las fortalezas y debilidades de la infraestructura tecnológica frente a las amenazas conocidas al momento del análisis. Esta evaluación debe cubrir tanto elementos externos (Internet, servicios SaaS, computación en la nube, dispositivos BYOD, usuarios no autorizados, sniffer(s), robots, entre otros), como internos (usuarios, aplicaciones, redes, estaciones de trabajo, dispositivos móviles, sistemas operativos, etc.).

En el caso de la ART, el análisis busca identificar vulnerabilidades relacionadas con versiones de software desactualizadas, malas prácticas de desarrollo, o configuraciones de seguridad débiles, con el fin de aplicar remediaciones y correcciones oportunas. El contratista deberá realizar al menos una actividad de prueba inicial

y una posterior de verificación, utilizando herramientas de escaneo y pruebas de penetración (pentesting), con el fin de entregar un informe detallado sobre el estado de seguridad de los activos de información definidos.

Este informe debe permitir evaluar la efectividad de los controles existentes, la protección de la red, la organización de la arquitectura, la capacidad de respuesta ante eventos de seguridad, así como el comportamiento del factor humano. Las recomendaciones derivadas del análisis permitirán reforzar los controles actuales, gestionar nuevos controles, actualizar políticas de seguridad, revisar sistemas de redundancia, implementar planes de recuperación ante desastres (DRP), garantizar la continuidad operativa y fortalecer la gestión de incidentes de seguridad.

Cabe resaltar que este servicio no solo busca detectar fallas, sino también aportar a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), mediante el monitoreo y revisión periódica de los activos de información, con el fin de prevenir la materialización de eventos de seguridad. Este servicio ha permitido mitigar vulnerabilidades identificadas, lo cual se debe mantener a lo largo del tiempo conforme al ciclo PHVA (Planear, Hacer, Verificar, Actuar) de mejora continua.

Finalmente, una vez ejecutado el análisis, la OTI implementará las estrategias necesarias para evitar que las vulnerabilidades detectadas evolucionen hacia amenazas que comprometan la seguridad digital. No obstante, se debe tener en cuenta que los riesgos persisten y evolucionan constantemente debido a nuevas técnicas de ataque y al surgimiento de vulnerabilidades no conocidas (ataques de día cero) o ya identificadas, pero no corregidas (ataques de día “N”).

Adicionalmente, se deben realizar pruebas de ingeniería Social: introducción, objetivo, alcance, metodología:

1. Preparación del escenario.
2. Diseño de los correos
3. Simulación de la trampa.
4. Resultado de la prueba
5. Consideraciones éticas,
6. Conclusiones, generando un informe definitivo con el análisis y recomendaciones de la ejecución de las pruebas de ingeniería social.

De esta manera se estaría cumpliendo con el aseguramiento de la información con los activos y/o elementos de la Agencia a nivel de seguridad informática.

3. OBJETO:

Adquirir licenciamiento, extensión de garantías de la plataforma FORTINET y realizar análisis de vulnerabilidades de los activos tecnológicos que permita el aseguramiento de toda la infraestructura tecnológica de la Agencia de Renovación del Territorio.

3.1. ALCANCE DEL OBJETO

Para el correcto aseguramiento de la infraestructura tecnológica de la ART, la ejecución del contrato contiene el siguiente alcance:

1. Servicio de renovación de licenciamiento, soporte mantenimiento y afinamiento, y transferencia del conocimiento de la plataforma FORTINET® de para 75 dispositivos.
2. Servicio de análisis de vulnerabilidades para 100 dispositivos y 20 URL(s) de activos de la ART.

Nota 1: Para el desarrollo del alcance del objeto el contratista deberá cumplir con lo descrito en el presente estudio, anexo técnico y demás documentos que hacen parte integral del contrato.

Nota 2: El detalle del alcance, especificaciones técnicas, actividades y entregables de los servicios anteriormente descritos se encuentra definido en el Anexo Técnico.

3.2. ESPECIFICACIONES TÉCNICAS:

Para la presente contratación, la Agencia de Renovación del Territorio define como requisitos técnicos de obligatorio cumplimiento, las especificaciones y condiciones técnicas que se describen en el Anexo Técnico que corresponde a los bienes y/o servicios a contratar y la cual el futuro contratista se compromete a cumplir con la suscripción del ‘‘Anexo de Aceptación Ficha Técnica”, documentos que hacen parte integral del proceso y del contrato que se llegaré a suscribir.

4. FOMENTO A LA EJECUCIÓN DE CONTRATOS ESTATALES POR PARTE DE POBLACIÓN EN POBREZA EXTREMA, DESPLAZADOS POR LA VIOLENCIA, PERSONAS EN PROCESO DE REINTEGRACIÓN O REINCORPORACIÓN Y SUJETOS DE ESPECIAL PROTECCIÓN CONSTITUCIONAL.

De conformidad con lo dispuesto en el Decreto 1860 de 2021, se dispone lo siguiente:

ARTÍCULO 2.2.1.2.4.2.16. Fomento a la ejecución de contratos estatales por parte de población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional. En los Procesos de Contratación, las Entidades Estatales indistintamente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos fomentarán en los pliegos de condiciones o documento equivalente que los contratistas destinen al cumplimiento del objeto contractual la provisión de bienes o servicios por parte de población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional, garantizando las condiciones de calidad y sin perjuicio de los Acuerdos Comerciales vigentes.

La participación de los sujetos anteriormente mencionados en la ejecución del contrato se fomentará previo análisis de su oportunidad y conveniencia en los Documentos del Proceso, teniendo en cuenta el objeto contractual y el alcance de las obligaciones.

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

Previo análisis de oportunidad y conveniencia, la Entidad Estatal incorporará esta obligación en la minuta del contrato del pliego de condiciones o documento equivalente, precisando las sanciones pecuniarias producto del incumplimiento injustificado de esta a través de las causales de multa que estime pertinentes.

El supervisor o el interventor, según el caso, realizará el seguimiento y verificará que las personas vinculadas al inicio y durante la ejecución del contrato pertenezcan a los grupos poblacionales enunciados anteriormente.

(…)”

No obstante lo anterior, la Agencia de Renovación del Territorio considera no procedente incluir en el presente proceso contractual la referida disposición, teniendo en cuenta que en atención al objeto contractual, el alcance de las obligaciones contractuales, así como las actividades y especificaciones técnicas requeridas para llevar a cabo su cumplimiento, el contratista por la complejidad de la necesidad a satisfacer, deberá contar con personal especializado y que cuente con experiencia específica para su correcta ejecución, ya que las actividades a desarrollar, esto es, la instalación, configuración y puesta en funcionamiento de soluciones integrales de firewall de nueva generación mediante equipos de seguridad perimetral, requieren de un conocimiento altamente calificado otorgado por el fabricante de dichas soluciones, el cual, de someterse a la estipulación normativa aquí referida, podría generar que el contratista no cuenta con la totalidad del equipo de trabajo acá solicitado para el inicio de la ejecución del contrato y en consecuencia se pueda poner en riesgo el cumplimiento adecuado del mismo, lo cual impactaría enormemente la operación de la entidad, conforme a la necesidad planteada en este documento.

5. ESTUDIO DE LA DEMANDA

Para desarrollar el análisis de la demanda de acuerdo con nuestra necesidad, se consultó en el SECOP II procesos de entidades que involucran objetos similares a la renovación de garantías, soporte y afinamiento de la plataforma Fortinet, teniendo en cuenta nuestra necesidad de servicio. El estudio se realizó con la consulta a contrataciones celebradas en los últimos años de entidades públicas incluida la ART:

Contrato	Objeto	Valor	Contratista	Proceso de Selección	Fecha de suscripción	Plazo
SG 0041 18	Adquisición, instalación, configuración, implementación y puesta en marcha de los dispositivos de seguridad perimetral firewall, para asegurar la infraestructura tecnológica y Access Point para la Agencia de Renovación del Territorio.	586.569.867	STS S.A.	Subasta Inversa	02/08/2018	2 meses
SG 0086 18	Adquisición de un sistema de seguridad EndPoint, para protección de la red de 500 usuarios compatible con la plataforma firewall Fortinet de la Agencia de Renovación del Territorio.	170.464.600	STS S.A.	Subasta Inversa	03/12/2018	1 mes
SG 0071 19	Renovar 500 licencias del software de seguridad EndPoint que se integre a la plataforma Sandbox Fortinet con que cuenta la Agencia de Renovación del Territorio.	37.097.060	STS S.A.	Subasta Inversa	17/12/2019	1 mes
SG 0054 20	Adquirir equipos switch tipo 2 de red con soporte de fábrica, mantenimiento físico y lógico para la Agencia de Renovación del Territorio	123.400.000	STS S.A.	Subasta Inversa	11/08/2020	3 meses
SGF 0053 2021	Renovación de garantías, soporte y afinamiento de la plataforma Fortinet de la Agencia de Renovación del Territorio.	300.135.100	STS S.A.	Subasta Inversa	11/08/2021	2 meses
SGF 0046 2022	Prestar los servicios de ciberseguridad mediante el desarrollo de las actividades para la implementación del SGSI realizando el análisis de vulnerabilidades, la integración de un correlacionador de eventos; así como la renovación de garantías y soporte de la plataforma de seguridad que permitan la protección de datos y de la infraestructura tecnológica de la Agencia de Renovación del Territorio.	766.099.065	STS S.A.	Subasta Inversa	26/05/2022	7 meses

Contrato	Objeto	Valor	Contratista	Proceso de Selección	Fecha de suscripción	Plazo
SG 0176 2023	Prestar los servicios de ciberseguridad para el cumplimiento de las actividades del SGSI realizando el análisis y monitoreo de las vulnerabilidades de los activos tecnológicos, renovación y soporte de las garantías de la plataforma TI que permita la protección de los datos y aseguramiento de la infraestructura tecnológica de la Agencia de Renovación del Territorio.	695.500.000	DATASEC S.A.	Subasta Inversa	05/10/2023	2 meses
SG 0136 2024	Prestar los servicios de ciberseguridad, realizando el análisis y monitoreo de las vulnerabilidades de los activos tecnológicos; adquisición, renovación del licenciamiento y soporte de la plataforma de seguridad, que permita la protección de los datos y aseguramiento de la infraestructura tecnológica de la Agencia de Renovación del Territorio.	1.077.000.000	DATASEC S.A.	Subasta Inversa	26/09/2024	3 meses
SG 0169 2025	Adquirir y renovar licenciamiento, hardware y extensión de garantías de la plataforma FORTINET y realizar análisis de vulnerabilidades de los activos tecnológicos que permita el aseguramiento de toda la infraestructura tecnológica de la Agencia de Renovación del Territorio.	1.099.498.68	DATASEC S.A.	Subasta Inversa	26/11/2025	2 meses

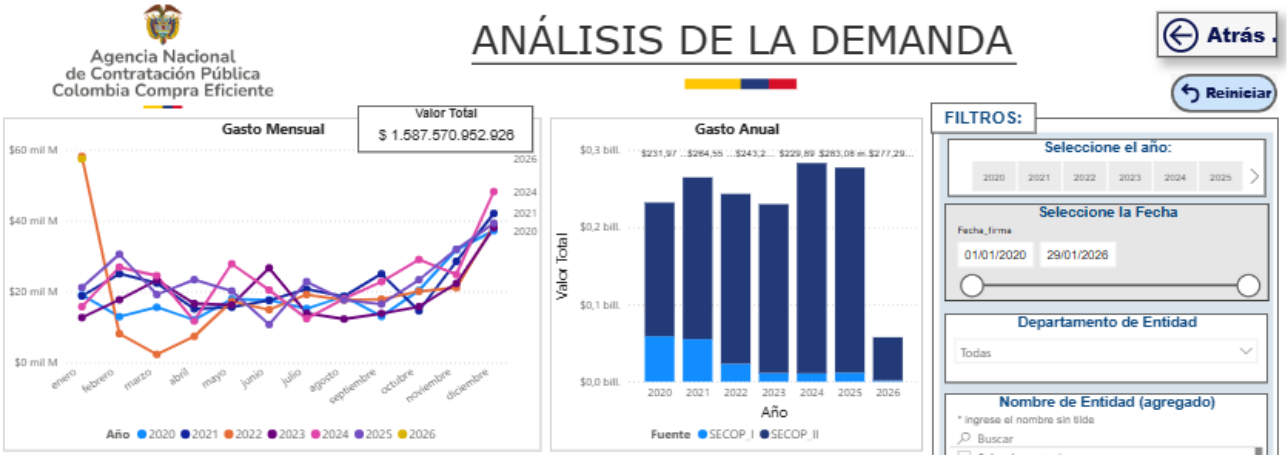
Para la ejecución de los contratos se realizaron por modalidad de subasta inversa, no se requirieron permisos ni autorizaciones para la prestación del servicio, con respecto al presupuesto con el que se ha ejecutado estos contratos ha sido con recursos de Inversión, las condiciones de pago fueron máximo 3 pagos, el proveedor cumplió con el tiempo y lugar de entrega de acuerdo con lo estipulado en las Fichas Técnicas de cada contrato, así como con las garantías que se establecieron en los contratos.

Adicionalmente para el análisis de la demanda, se tuvieron en cuenta procesos similares o relacionados con el proceso requerido por la entidad y que han sido realizados por diferentes entidades públicas y que se encuentran en el SECOP II, con el fin de revisar el valor del proceso, el tiempo de ejecución, garantías, forma de pago, especificaciones técnicas; entre otros aspectos así:

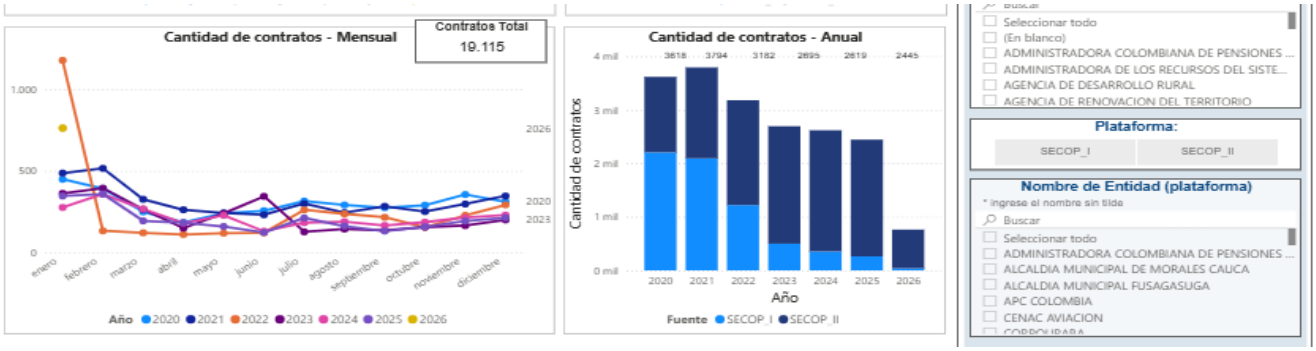
Entidad Estatal	Referencia	Modalidad	Descripción	Contratista	Valor	Vigencia Garantía técnica
Contraloría general de la república	CGR-SI- 004-2023	SASI	Actualización del licenciamiento, con servicios de soporte, mantenimiento y actualización de la plataforma de Seguridad Fortinet, para la contraloría general de la república	WEXLER S.A.S	$3.656.167.017	36 meses
Superintendencia de servicios públicos domiciliarios	SSPD SA-013 DE 2023	SASI	Adquirir la renovación del licenciamiento, soporte y garantía Fortinet y componentes de seguridad con retoma, lo anterior alineado al proyecto de inversión fortalecimiento de la gobernanza de las tecnologías de la información en el cumplimiento de la misionalidad de la superservicios a nivel nacional	UNIÓN TEMPORAL CIBERSEGURID AD SSPD DATASEC STS 2023	$1.385.83 0.601,1	12 meses
Minciencias	SASI-006-2024	SASI	Renovar el licenciamiento, soporte, garantía y mantenimiento sobre la solución de seguridad perimetral Fortinet (ngfw) y el servicio fortisandbox cloud del ministerio de ciencia, tecnología e innovación - minciencias	GAMMA INGENIEROS SAS	$810.190.190	24 meses
Area metropolitana del valle de	SIE 001 DE 2025	SASI	adquisición y renovación del licenciamiento Fortinet para la protección informática del área metropolitana del valle de aburra	UT AMVA SIE 001 DE 2025	$997.539.995	12 meses

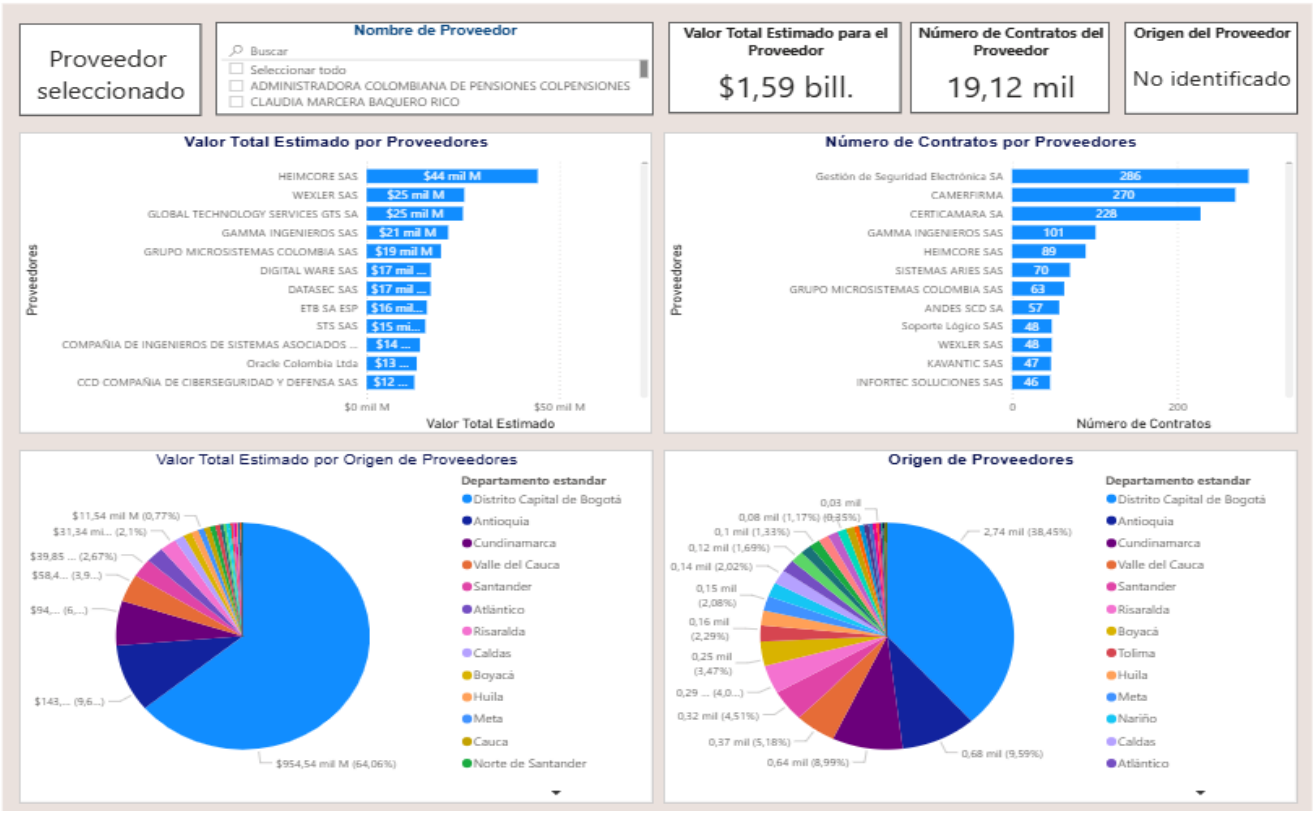
Entidad Estatal	Referencia	Modalidad	Descripción	Contratista	Valor	Vigencia Garantía técnica
aburra						
Superintendencia Nacional De Salud	SNS-SASI-6-2025	SASI	Adquirir y renovar la plataforma de seguridad perimetral Fortinet, incluyendo licenciamiento, soporte y una solución avanzada Anti-DDoS, para fortalecer la protección y continuidad de los servicios de la Superintendencia Nacional de Salud.	WEXLER S.A.S	$5.657.578.360	15 dias
Superintendencia Financiera De Colombia	PSA-009-2025	SASI	Renovar el licenciamiento de los componentes FORTINET que hacen parte del modelo de seguridad de la información de la Superintendencia, incluido servicio de soporte Elite Pro Advanced por parte del fabricante.	DATASEC S.A.S.	$4.009.796.000	15 dias
Instituto geográfico agustín codazzi	SASI-016-2025	SASI	Contratar la renovación del soporte, mantenimiento, garantía y licenciamiento de los dispositivos de seguridad perimetral Fortinet, así como la adquisición de componentes adicionales para robustecer los controles de seguridad de la Entidad.	UT HC-WX SEGURIDAD 2025	$3.491.227.657	15 dias
Secretaría Distrital de Integración Social	SDIS-SASI-015-2025	SASI	Adquisición fortianalyzer y fortiadc, renovación licenciamiento, garantía y esquema de soporte para la plataforma de seguridad fortinet de la secretaría distrital de integración social	Heimcore SAS	$ 1.924.714.175	2 años
Hospital Militar Central	SI-019-2025-HOMIL	SASI	Adquisición de la suscripción de controles de seguridad en la nube y la actualización del licenciamiento y soporte de la solución de fortinet del hospital militar central	Compañia de ingenieros de sistemas asociados coinsa sas	$1.323.145.000	2 meses

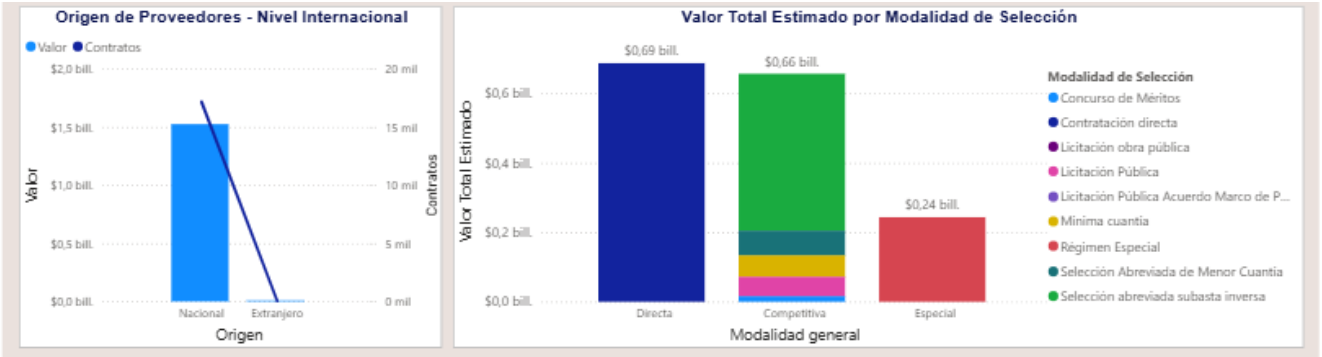
De acuerdo con la información consolidada por Colombia Compra Eficiente – CCE a través de la Herramienta de Visualización para el Análisis de la Demanda y de la Oferta (actualizada en febrero 2026), y considerando los códigos UNSPSC asignados al proceso, y con presupuesto hasta por $2.000.000.000, para presentar la siguiente información relativa a los contratos realizados por entidades del Estado, presupuestos y empresas participativas y las diferentes modalidades de contratación. Estas visualizaciones permiten analizar dinámicas de contratación por plataforma (SECOP I, SECOP II, TVEC), modalidad competitiva, directa o especial, y por origen de proveedor.[14]



[14] https://www.colombiacompra.gov.co/analisis-de-datos-de-compra-publica/visualizaciones-compra-publica/herramienta-de-visualizacion-para-el-analisis-de-la-demanda-y-de-la-oferta


Cantidad de contratos - Mensual
Contratos Total
19.115
Año 2020 2021 2022 2023 2024 2025 2026
Cantidad de contratos - Anual
Cantidad de contratos
Año
Fuente SECOP_I SECOP_II
Seleccionar todo
(En blanco)
ADMINISTRADORA COLOMBIANA DE PENSIONES ...
ADMINISTRADORA DE LOS RECURSOS DEL SISTE...
AGENCIA DE DESARROLLO RURAL
AGENCIA DE RENOVACION DEL TERRITORIO
Plataforma:
SECOP_I
SECOP_II
Nombre de Entidad (plataforma)
* ingrese el nombre sin tilde
Buscar
Seleccionar todo
ADMINISTRADORA COLOMBIANA DE PENSIONES ...
ALCALDIA MUNICIPAL DE MORALES CAUCA
ALCALDIA MUNICIPAL FUSAGASUGA
APC COLOMBIA
CENAC AVIACION


Proveedor seleccionado
Nombre de Proveedor
Buscar
Seleccionar todo
ADMINISTRADORA COLOMBIANA DE PENSIONES COLPENSIONES
CLAUDIA MARCERA BAQUERO RICO
Valor Total Estimado para el Proveedor
$1,59 bill.
Número de Contratos del Proveedor
19,12 mil
Origen del Proveedor
No identificado
Valor Total Estimado por Proveedores
HEIMCORE SAS $44 mil M
WEXLER SAS $25 mil M
GLOBAL TECHNOLOGY SERVICES GTS SA $25 mil M
GAMMA INGENIEROS SAS $21 mil M
GRUPO MICROSISTEMAS COLOMBIA SAS $19 mil M
DIGITAL WARE SAS $17 mil ...
DATASEC SAS $17 mil ...
ETB SA ESP $16 mil...
STS SAS $15 mi...
COMPAÑIA DE INGENIEROS DE SISTEMAS ASOCIADOS ... $14 ...
Oracle Colombia Ltda $13 ...
CCD COMPAÑIA DE CIBERSEGURIDAD Y DEFENSA SAS $12 ...
Proveedores
$0 mil M
$50 mil M
Valor Total Estimado
Número de Contratos por Proveedores
Gestión de Seguridad Electrónica SA 286
CAMERFIRMA 270
CERTICAMARA SA 228
GAMMA INGENIEROS SAS 101
HEIMCORE SAS 89
SISTEMAS ARIES SAS 70
GRUPO MICROSISTEMAS COLOMBIA SAS 63
ANDES SCD SA 57
Soporte Lógico SAS 48
WEXLER SAS 48
KAVANTIC SAS 47
INFORTEC SOLUCIONES SAS 46
Proveedores
0
200
Número de Contratos
Valor Total Estimado por Origen de Proveedores
Departamento estandar
Distrito Capital de Bogotá
Antioquia
Cundinamarca
Valle del Cauca
Santander
Atlántico
Risaralda
Boyacá
Huila
Meta
Cauca
Norte de Santander
$954,54 mil M (64,06%)
Origen de Proveedores
Departamento estandar
Distrito Capital de Bogotá
Antioquia
Cundinamarca
Valle del Cauca
Santander
Risaralda
Boyacá
Tolima
Huila
Meta
Nariño
Caldas
Atlántico
2,74 mil (38,45%)
0,68 mil (9,59%)


Origen de Proveedores - Nivel Internacional
Valor
Contratos
Nacional
Extranjero
Origen
Valor Total Estimado por Modalidad de Selección
$0,69 bill.
$0,66 bill.
$0,24 bill.
Valor Total Estimado
Directa
Competitiva
Especial
Modalidad general
Modalidad de Selección
Concurso de Méritos
Contratación directa
Licitación obra pública
Licitación Pública
Licitación Pública Acuerdo Marco de P...
Mínima cuantía
Régimen Especial
Selección Abreviada de Menor Cuantía
Selección abreviada subasta inversa

Comportamiento contratación por bienes y servicios de UNSPSC

Año	2025		2026			Total		
Clasificador de Bienes y Servicios - Familia	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	P
8111 - Servicios informáticos	$204.444.644.861	12,88%	746	$56.768.233.131	3,58%	15986	$1.222.401.902.438	
4323 - Software	$44.527.404.519	2,80%	15	$739.225.914	0,05%	2653	$248.037.640.389	
4322 - Equipos o plataformas y accesorios de redes multimedia o de voz y datos	$28.318.725.598	1,78%	1	$3.742.973	0,00%	476	$117.131.410.099	
Total	$277.290.774.976	17,47%	762	$57.511.202.018	3,62%	19115	$1.587.570.952.926	

5.1. CONCLUSIONES

Teniendo en cuenta el análisis realizado de la demanda, se determina lo siguiente:

a. Las entidades públicas han contratado este servicio con características similares y calidades que se presentan en la ficha técnicas de la Agencia de Renovación del Territorio.
b. La modalidad empleada en la mayoría de los procesos es la de subasta inversa por las características técnicas uniformes.
c. La tipología contractual expresada por las entidades es la de prestación de servicios y licenciamiento.
d. La necesidad reiterativa en los diversos procesos revisados es la de aumentar la seguridad de los sistemas de información, así como centralizar y proteger la información generada por los funcionarios en el ejercicio de sus actividades.
e. El presupuesto oficial en cada entidad para los procesos varía según la capacidad y la tecnología utilizada, dependiendo de los servicios adquiridos en el marco de la implementación del SGSI.
f. Los riesgos asociados a estos contratos son normalmente fallas de funcionamiento por errores en la instalación y configuración de los servicios.
h. De acuerdo con el análisis de demanda de los procesos revisados en encontró que en promedio se entregaron de 2 a 3 cotizaciones.

6. ESTUDIO DE LA OFERTA

El sector de las tecnologías de la Información y las Comunicaciones - TIC está conformado por empresas en pleno crecimiento, con ventas en ascenso en un ámbito donde la seguridad de la información, las redes y conectividad, el desarrollo de software y las ventajas de contar con diversos servicios y productos tecnológicos, han permitido que estas y entidades colombianas apropien cada día más estrategias basadas en las TIC, fomentando de esta forma la transformación digital del país a través de la adquisición y/o renovación de tecnología y servicios que a su vez impulsan el crecimiento de las ventas de las compañías proveedoras y estos a su vez generan confianza a sus clientes.

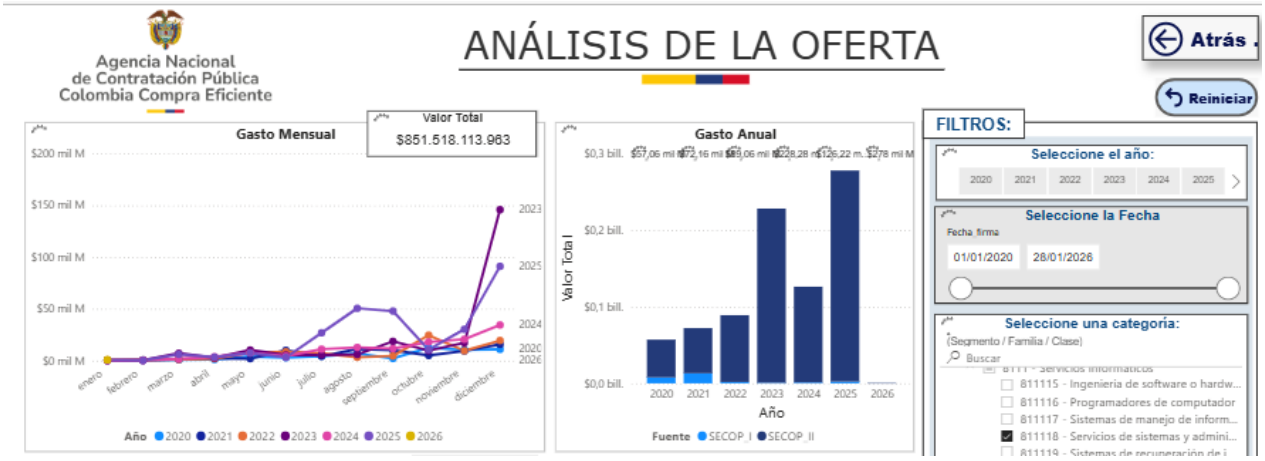
De acuerdo con la consulta realizada en el SECOP II, con los proveedores que han trabajado con el sector gobierno, suministrando los servicios requeridos para el presente proceso, se encuentran varias empresas constituidas en Colombia para prestar sus servicios o vender sus productos, quienes realizan la prestación de servicios en seguridad y ciberseguridad además de implementar y dar soporte a los equipos descritos en la ficha técnica adjunta a este proceso y de las cuales se relacionan entre otras las siguientes:

- ✓ Colsof S.A
- ✓ Italtel
- ✓ Soluciones Integrales
- ✓ Global Technology Services GTS.
- ✓ Openlink Sistemas de Redes de Datos SAS
- ✓ Digiware
- ✓ Redcomputo

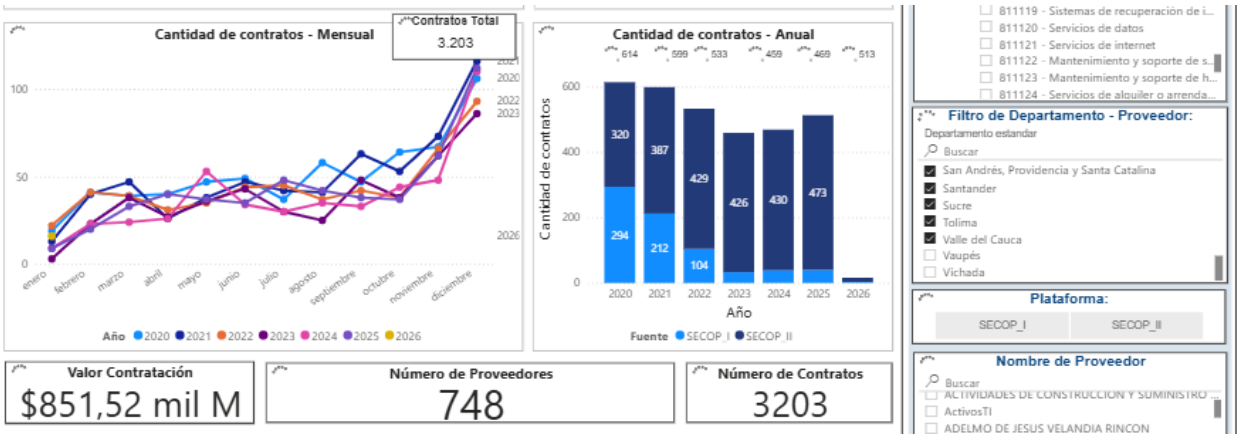
- ✓ Etek International.
- ✓ Sonda de Colombia.
- ✓ Soluciones Tecnología y Servicios STS
- ✓ 2secure SAS
- ✓ U.T. Softpcm
- ✓ CCD Compañia de Ciberseguridad y Defensa SAS
- ✓ Adsum Soluciones Tecnológicas SAS
- ✓ Ecomil SAS
- ✓ Gamma Ingenieros S.A.S.
- ✓ Wexler S.A.S
- ✓ Coinsa SAS
- ✓ Password Consulting Services SAS
- ✓ Softsecurity S.A.S
- ✓ E-Dea Networks SAS
- ✓ Ona Systems S.A.S.

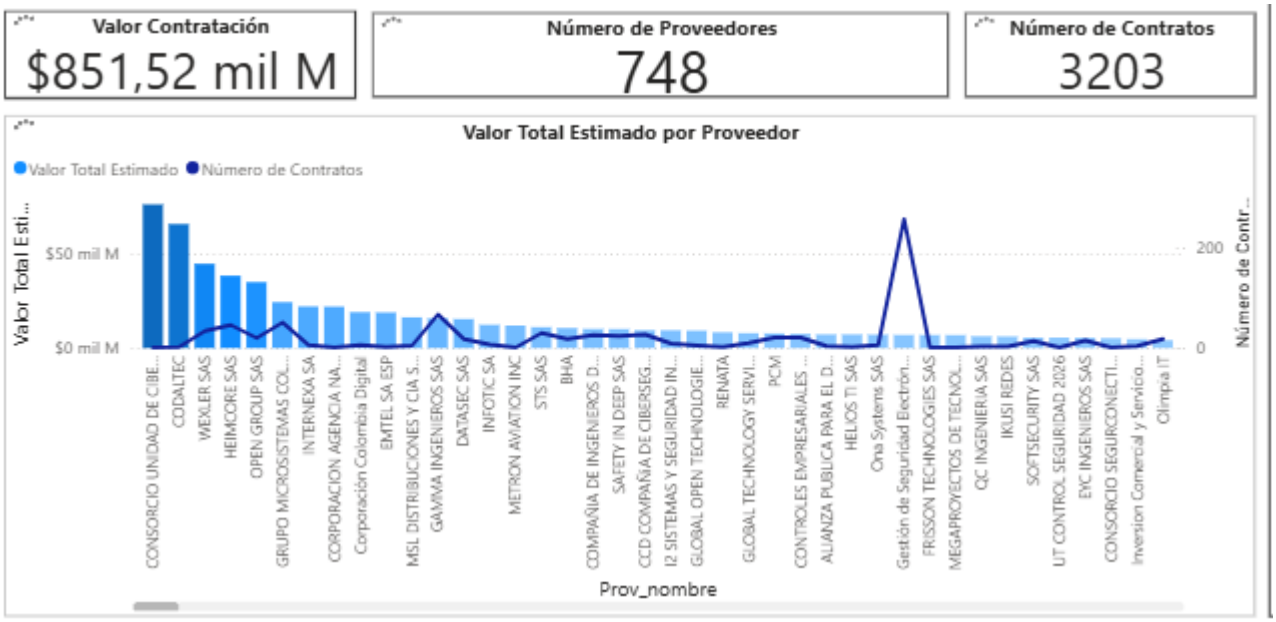
Estas empresas se dividen en diferentes grupos, algunas están conformadas por firmas multinacionales, usualmente grandes empresas, otras se dedican en gran medida a brindar servicios de comercialización de productos que se desarrollan en las casas matrices y en otros casos a la provisión de servicios informáticos mediante outsourcing. Igualmente, existen empresas nacionales de tamaño mediano, que se dedican en gran medida a la provisión de servicios informáticos.

En atención a la información proporcionada por Colombia Compra Eficiente a través del Modelo de Abastecimiento Estratégico en la Herramienta de visualización para el análisis de la oferta, de acuerdo con el y considerando los códigos UNSPSC asignados al proceso, y con presupuesto hasta por $2.000.000.000, para presentar la siguiente información relativa a los contratos realizados por entidades del Estado, presupuestos y empresas participativas y las diferentes modalidades de contratación. Estas visualizaciones permiten analizar dinámicas de contratación por plataforma (SECOP I, SECOP II, TVEC), modalidad competitiva, directa o especial, y por origen de proveedor.[15]



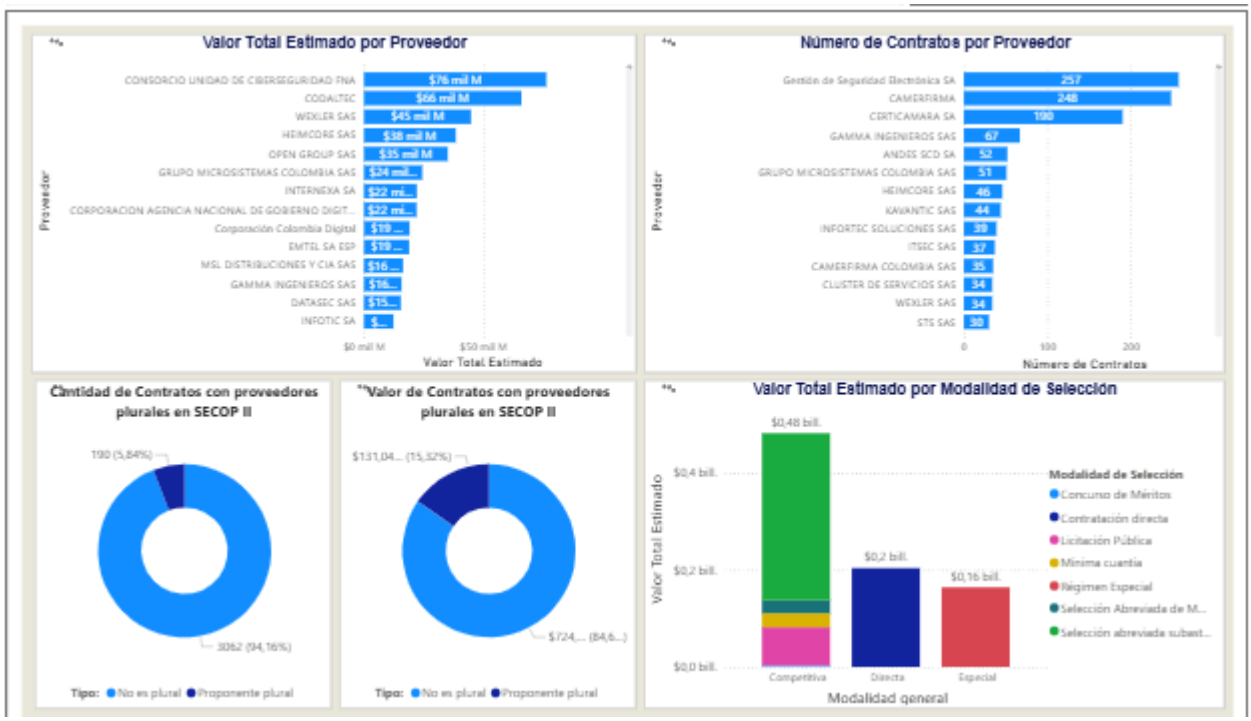
[15] https://www.colombiacompra.gov.co/analisis-de-datos-de-compra-publica/visualizaciones-compra-publica/herramienta-de-visualizacion-para-el-analisis-de-la-demanda-y-de-la-oferta





Comportamiento contratación por bienes y servicios de UNSPSC

Año	2024		2025			2026		
Clasificador de Bienes y Servicios - Familia	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	Participaci
4322 - Equipos o plataformas y accesorios de redes multimedia o de voz y datos	4.161.579.540	6,36%	96	$156.379.798.494	18,36%	1	$3.742.973	0,00%
4323 - Software	2.053.651.465	8,46%	417	$121.620.722.815	14,28%	15	$739.225.914	0,09%
Total	**8.215.231.005**	**14,82%**	**513**	**$278.000.521.309**	**32,65%**	**16**	**$742.983.887**	**0,09%**



MiPymes

La Agencia Nacional de Contratación Pública –Colombia Compra Eficiente ha realizado un estudio sobre el comportamiento de las compras púbicas, en particular, la Ley 2069 de 2020 establece lineamientos para el fomento de la participación de empresas micro, pequeñas y medianas (mipymes) en el sistema de compras públicas y contratación estatal.

El sector de las Mipyme representa el grupo de empresas que jalonan la economía, generan empleo y movilidad social, además, estos negocios representan 99,5% del total del tejido empresarial, emplean a cerca de 65% de los habitantes del país y aportan 40% al Producto Interno Bruto.

Durante el primer semestre de 2025 se registraron 173.907 empresas, cifra que representa un aumento de 1,9% con respecto al mismo período de 2024, donde nacieron 170.741 empresas. Del total de empresas registradas en 2025, el 74% corresponden a personas naturales y el 26% a sociedades. La creación personas naturales aumentó para el primer semestre de 2025 con respecto al primer semestre de 2024. Las personas naturales pasaron de 125.849 a 129.048, lo que representa una variación de 2,5%. Entre 2024 y el primer semestre de 2025, el número de sociedades se mantuvo estable, con una variación mínima de 0,1%.

El sector de comercio presentó la mayor contribución en la creación de empresas para el primer semestre de 2025, con un aumento del 3,3% en el número de empresas. Por el contrario, el sector de construcción fue el que menos contribuyó en la creación de empresas con una disminución del 8,2% en el número de empresas creadas.

Es importante destacar que, las Mipyme tienen un efecto positivo en el desarrollo de la economía nacional por su aporte en la generación de empleo, la capacidad de adaptación y su penetración en diferentes sectores de la industria. Por ello, estás empresas tienen una relación directa con el comportamiento de la economía, en la que influyen variables como la inflación, el crecimiento económico, el costo de la financiación y el desempleo.

En caso de desempate, se tendrá en cuenta la clasificación de MIPYME acreditada en el Registro Único de Proponentes (RUP).

Emprendimiento y Empresas de Mujeres

Teniendo en cuenta que este proceso será llevado a cabo a través de la modalidad de Selección Abreviada por Subasta Inversa y que este incentivo aplica únicamente para las modalidades de licitación pública, selección abreviada de menor cuantía y concurso de méritos; no se incluye para el presente proceso.

Población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional.

El Decreto 1860 de 2021, indica en el Artículo 2.2.1.2.4.2.16. *Fomento a la ejecución de contratos estatales por parte de población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional. En los Procesos de Contratación, las Entidades Estatales indistintamente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos fomentarán en los pliegos de condiciones o documento equivalente que los contratistas destinen al cumplimiento del objeto contractual la provisión de bienes o servicios por parte de población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional, garantizando las condiciones de calidad y sin perjuicio de los Acuerdos Comerciales vigentes.*

Para este proceso, la Agencia considera que no procede incluir para este proceso la referida disposición, teniendo en cuenta que en atención al objeto contractual, el alcance de las obligaciones contractuales, así como las actividades y especificaciones técnicas requeridas para llevar a cabo su cumplimiento, el contratista por la complejidad de la necesidad a satisfacer, deberá contar con personal especializado el cual debe contar con experiencia específica para su correcta ejecución, ya que las actividades a desarrollar, esto es, "*Adquirir licenciamiento, extensión de garantías de la plataforma FORTINET y realizar análisis de vulnerabilidades de los activos tecnológicos que permita el aseguramiento de toda la infraestructura tecnológica de la Agencia de Renovación del Territorio.*", requieren de un conocimiento altamente calificado otorgado por el fabricante de dichas soluciones.

6.1. CONCLUSIONES

Una vez revisadas las tendencias del mercado de las diferentes empresas que cumplen con los requerimientos técnicos para realizar el análisis de vulnerabilidades y la renovación de las licencias los equipos de seguridad de la Infraestructura de la entidad con extensión de soporte y garantía para el aseguramiento de la infraestructura cumpliendo con las mejores prácticas, la normatividad vigente y de estándares internacionales como la norma ISO 27001:2022 entre otras, se evidencia a través del SECOP y con las cotizaciones recibidas que la oferta vs. la demanda de los oferentes que han realizado este tipo de contratos varía dependiendo del avance de implementación del modelo de seguridad y privacidad de la información adoptado por las entidades en las que se ha realizado.

Igualmente, se evidencia que los costos difieren respecto a ese nivel de implementación y la cantidad de activos de información que estén sujetos a las pruebas de vulnerabilidad y la renovación del contrato de fábrica y extensión de garantías de la plataforma de ciberseguridad son valores muy similares por lo tanto se calcula con una media aritmética, sin embargo es importante destacar que son varias las entidades públicas que han buscado la implementación del SGSI con actividades de similares características con el fin de optimizar recursos financieros y humanos que aplican para las diferentes actividades de cada proceso.

Teniendo en cuenta que la Agencia requiere renovar la licencia de la plataforma de seguridad FORTINET® con la que cuenta actualmente y ejecución de un análisis de vulnerabilidades con remediación, se pudo evidenciar en los procesos analizados de la plataforma SECOP lo siguiente:

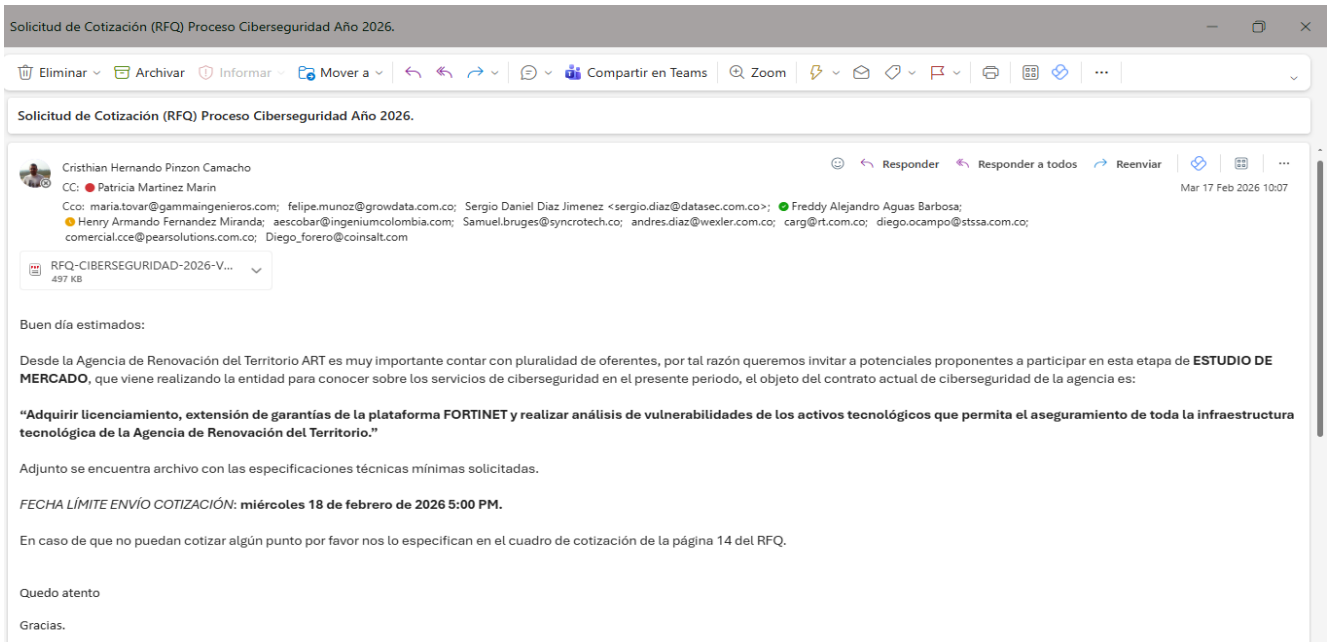
- Que los procesos requieren que los proveedores sean representantes autorizados del fabricante, teniendo en cuenta que hay un programa de canales para las empresas legalmente constituidas en Colombia para distribuir o representar sus servicios.
- Que a su vez los canales pueden estar divididos en sectores o especialidades de acuerdo con los productos a los cuales dan soporte del fabricante, algunos solo se dedican a comercializar, por tanto, es requisito que las empresas sean proveedores con experiencia en la prestación de servicios para el producto que requiere la entidad.
- Que contemplan todos los aspectos relacionados en la ficha técnica respecto a la seguridad y la ciberseguridad

7. ESTUDIO DE COSTOS

Con el objeto de realizar el estudio de los posibles oferentes, la entidad procedió a revisar tanto la plataforma SECOP como las diferentes fuentes y bases de datos en internet, con el fin de identificar los posibles proveedores, empresas o personas naturales en la ciudad de Bogotá.

En este proceso, la metodología para la estructuración del estudio de mercado fue la siguiente:

Para realizar el estudio de costos, la Oficina de Tecnologías de la Información, solicitó cotizaciones a empresas de las más representativas del sector.



Solicitud de Cotización (RFQ) Proceso Ciberseguridad Año 2026.

Eliminar | Archivar | Informar | Mover a | Compartir en Teams | Zoom

Solicitud de Cotización (RFQ) Proceso Ciberseguridad Año 2026.

Cristhian Hernando Pinzon Camacho

Responder | Responder a todos | Reenviar

CC: Patricia Martinez Marin

Mar 17 Feb 2026 10:07

Cco: maria.tovar@gammaingenieros.com; felipe.munoz@growdata.com.co; Sergio Daniel Diaz Jimenez <sergio.diaz@datasec.com.co>; Freddy Alejandro Aguas Barbosa; Henry Armando Fernandez Miranda; aescobar@ingeniumcolombia.com; Samuel.bruges@syncrotech.co; andres.diaz@wexler.com.co; carg@rt.com.co; diego.ocampo@stssa.com.co; comercial.cce@pearsolutions.com.co; Diego_forero@coinsalt.com

RFQ-CIBERSEGURIDAD-2026-V... 497 KB

Buen día estimados:

Desde la Agencia de Renovación del Territorio ART es muy importante contar con pluralidad de oferentes, por tal razón queremos invitar a potenciales proponentes a participar en esta etapa de **ESTUDIO DE MERCADO**, que viene realizando la entidad para conocer sobre los servicios de ciberseguridad en el presente periodo, el objeto del contrato actual de ciberseguridad de la agencia es:

"Adquirir licenciamiento, extensión de garantías de la plataforma FORTINET y realizar análisis de vulnerabilidades de los activos tecnológicos que permita el aseguramiento de toda la infraestructura tecnológica de la Agencia de Renovación del Territorio."

Adjunto se encuentra archivo con las especificaciones técnicas mínimas solicitadas.

FECHA LÍMITE ENVÍO COTIZACIÓN: **miércoles 18 de febrero de 2026 5:00 PM.**

En caso de que no puedan cotizar algún punto por favor nos lo especifican en el cuadro de cotización de la página 14 del RFQ.

Quedo atento

Gracias.

A los siguientes correos:

Gamma Ingenieros S.A.S. - - Maria Paula Tovar Diaz +57 3154599250
maria.tovar@gammaingenieros.com

GrowData - Felipe Muñoz +57 317 2214433
felipe.munoz@growdata.com.co
Datasec S.A.S. Sergio Díaz +57 3213184645
sergio.diaz@datasec.com.co
INGENIUM COLOMBIA S.A.S. - Adriana Escobar Castañeda +57 320 2909525
aescobar@ingeniumcolombia.com
Syncrotech - Samuel Bruges +57 301 3908098
Samuel.bruges@syncrotech.co
Wexler SAS - Andrés Díaz +57 321 4563826
andres.diaz@wexler.com.co
Real Time Consulting - Camilo Rodriguez Gonzalez +57 300 4114512
carg@rt.com.co
STS SAS - Diego Ocampo +57 318 7654914
diego.ocampo@stssa.com.co
Pear Solutions S.A. - Victoria Castiblanco +57 300 8824079
comercial.cce@pearsolutions.com.co
Coinsa S.A.S. - Diego Forero +57 3107955077
Diego_forero@coinsalt.com

De las cuales se pudo obtener respuesta de cuatro (4) de ellas, así:

ÍTEM	Empresa 1	Empresa 2	Empresa 3	Empresa 4	MEDIANA	MEDIA ARITMETICA
SERVICIO DE RENOVACIÓN DE LICENCIAMIENTO, GARANTIA, SOPORTE, MANTENIMIENTO, AFINAMIENTO Y TRANSFERENCIA DEL CONOCIMIENTO DE LA PLATAFORMA FORTINET®	$ 1.039.034.849	$ 1.040.934.938	$ 1.040.470.910	$ 1.041.034.839	$ 1.040.702.924	$ 1.040.368.884
SERVICIO DE ANÁLISIS DE VULNERABILIDADES Y DE DEBILIDADES PARA 100 DISPOSITIVOS Y 20 URL(S) DE ACTIVOS DE ART.	$ 68.603.613	$ 75.633.922	$ 80.394.839	$ 71.034.930	$ 73.334.426	$ 73.916.826
SUBTOTAL	$ 1.107.638.462	$ 1.116.568.860	$ 1.120.865.749	$ 1.112.069.769	$ 1.114.037.350	$ 1.114.285.710
IVA 19%	$ 210.451.308	$ 212.148.083	$ 212.964.492	$ 211.293.256	$ 211.667.097	$ 211.714.285
TOTAL	$ 1.318.089.770	$ 1.328.716.943	$ 1.333.830.241	$ 1.323.363.025	$ 1.325.704.447	$ 1.325.999.995

Según lo anterior, se observa que se tomaron cuatro (4) cotizaciones, para lo cual se utilizó el método aritmético mediana, ya que estaba por debajo de la media aritmética, obteniendo un presupuesto por valor de **MIL TRESCIENTOS VEINTICINCO MILLONES SETECIENTOS CUATRO MIL CUATROCIENTOS CUARENTA Y SIETE PESOS MCTE ($1.325.704.447)**. incluido IVA, demás impuestos, tasas, contribuciones, costos directos e indirectos que conlleve la celebración y ejecución total del contrato que resulte del presente proceso de selección, para prestar los servicios de ciberseguridad mediante el desarrollo de las actividades para la implementación del SGSI realizando el análisis de vulnerabilidades, la integración de un correlacionador de eventos y la renovación, soporte y afinamiento y adquisición de la plataforma de seguridad, que permitan la protección de datos e infraestructura sobre la plataforma de la Agencia de Renovación del Territorio.

CONCLUSIÓN DEL ANÁLISIS DEL SECTOR[16]

Realizado el análisis del sector, se pudo determinar que la relación de la oferta Vs. la demanda del presente proceso depende del nivel de implementación del Modelo de Seguridad y Privacidad de la Información que tenga la Agencia respecto del inventario de sus activos de información y los controles de seguridad de la plataforma tecnológica.

[16] Examen detallado de una cosa para conocer sus características o cualidades, o su estado, y extraer conclusiones, que se realiza separando o considerando por separado las partes que la constituyen

Se pudo observar que de la madurez del Modelo de Seguridad y Privacidad de la Información de cada entidad depende el tipo de análisis, configuración y la renovación de la plataforma de seguridad, ya que si es débil pues se necesitará otro tipo de actividades que complementen los procesos, ahora bien, con respecto a si el nivel de madurez es más robusto, se deben medir la efectividad de los controles de seguridad y sus calidades técnicas, lo que permitirá evidenciar que tan vulnerable es o no cada activo a ser sometido del análisis respectivo y la actualización de los ya existentes.

Respecto de la modalidad de contratación se evidencia que la misma depende de los servicios adquiridos por cada entidad en el marco de la implementación del SGSI los cuales varían entre menor cuantía y subasta inversa, razón por la cual se revisaron los diferentes objetos de contratación de estas entidades públicas, especificaciones técnicas, obligaciones, forma de pago, plazos, garantías y se determinó que lo requerido por la ART, corresponde a bienes y/o servicios con características técnicas uniformes en materia de ciberseguridad; por tanto, se opta por la modalidad de selección abreviada por subasta inversa.

De acuerdo con el análisis realizado de servicios prestados por las empresas de seguridad informática y ciberseguridad y revisando las condiciones particulares de éstas en los procesos de contratación ejecutados con objetos similares, se logra verificar que los procesos cumplan con los principios de eficiencia, economía y transparencia, así como también se ajusten a los precios promedio del mercado para poder fijar el presupuesto estimado del presente proceso de selección. Lo cual conlleva a determinar cómo presupuesto oficial estimado, hasta la suma de **MIL TRESCIENTOS VEINTICINCO MILLONES SETECIENTOS CUATRO MIL CUATROCIENTOS CUARENTA Y SIETE PESOS MCTE ($1.325.704.447)**. **,** incluido IVA, demás impuestos, tasas, contribuciones, costos directos e indirectos que conlleve la celebración y ejecución total del contrato que resulte del presente proceso de selección.

Por último, las actividades a realizar en el presente proceso darán cumplimiento a lo establecido en la Resolución 000709 del 2021, a las metas fijadas por la ART en el Plan Estratégico Sectorial - PES y a la implementación de la Política de Gobierno Digital.

Se expide el presente en Bogotá a los diecisiete (17) días del mes de junio de 2026

Freddy Alejandro Aguas Barbosa
Jefe de Oficina de Tecnologías de la información
Agencia de Renovación del Territorio

Elaboró: Cristhian Hernando Pinzón – Henry Armando Fernández
Revisó: Claudia Patricia Martinez Marin
Aprobó: Freddy Alejandro Aguas

Contacto área solicitante	Nombre: Cristhian Pinzon Teléfono:6014221030- Extensión: 1999