ESTUDIO DEL SECTOR SOPORTE DE LA LICITACIÓN PÚBLICA PARA SELECCIONAR A LOS PROVEEDORES DE UN ACUERDO MARCO DE PRECIOS/SISTEMA DINÁMICO DE ADQUISICIÓN DE CIBERSEGURIDAD

Lista de Gráficas

Lista de Tablas

1. INTRODUCCIÓN

Las Entidades Estatales, para el cumplimiento de sus fines constitucionales y legales, requieren la adquisición permanente de bienes y servicios especializados que soporten su operación misional, administrativa y tecnológica. Estas adquisiciones deben responder a los principios de eficiencia, economía, transparencia, pluralidad de oferentes y selección objetiva, conforme al régimen de contratación estatal.

En este contexto, la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, en ejercicio de sus funciones legales, diseña y administra instrumentos de agregación de demanda, como los Acuerdos Marco de Precios, orientados a optimizar el uso de los recursos públicos, reducir cargas administrativas, fortalecer la planeación de las compras estatales y generar condiciones de competencia efectiva en el mercado.

El presente Estudio del Sector tiene como finalidad soportar la estructuración de un proceso de selección, mediante la modalidad de licitación pública, orientado a la vinculación de proveedores al Acuerdo Marco de Precios de Bienes y Servicios de Ciberseguridad. Este instrumento permitirá a las Entidades Estatales acceder de manera ágil, estandarizada y competitiva a soluciones y servicios especializados, bajo condiciones técnicas, jurídicas y económicas previamente definidas.

La necesidad de estructurar un Acuerdo Marco de Precios en materia de ciberseguridad se sustenta en la acelerada transformación digital del Estado colombiano, caracterizada por la creciente adopción de servicios digitales, infraestructuras interconectadas, soluciones en la nube, automatización de procesos y prestación digital de servicios a la ciudadanía. Este proceso, si bien genera importantes beneficios en términos de eficiencia, cobertura y calidad del servicio público, incrementa de manera significativa la exposición de las Entidades Estatales a riesgos cibernéticos cada vez más frecuentes, complejos y sofisticados.

En este escenario, la ciberseguridad deja de ser un asunto meramente tecnológico para consolidarse como un factor estratégico de continuidad institucional, protección de la información pública, salvaguarda de infraestructuras críticas y mantenimiento de la confianza ciudadana en el Estado. Los incidentes cibernéticos pueden afectar de manera directa la prestación de servicios esenciales, la integridad de los procesos administrativos y la estabilidad

operativa de las Entidades Estatales, generando impactos económicos, jurídicos y reputacionales.

Este enfoque se encuentra alineado con la Estrategia Nacional de Seguridad Digital de Colombia 2025–2027, la cual reconoce la seguridad digital como un pilar fundamental para el desarrollo socioeconómico, la estabilidad institucional y el bienestar de la sociedad. Dicha estrategia prioriza la consolidación de la gobernanza de la seguridad digital, el fortalecimiento de la ciberresiliencia nacional, el desarrollo de capacidades técnicas y humanas, y la articulación entre el sector público, el sector privado, la academia y la sociedad civil.

En coherencia con lo anterior, la contratación pública se configura como un instrumento clave para materializar los objetivos de la política nacional de seguridad digital, al facilitar el acceso de las Entidades Estatales a proveedores especializados, tecnologías actualizadas y servicios de alto valor agregado, bajo esquemas contractuales que promuevan la competencia, la innovación y la mejora continua.

Adicionalmente, el diseño del presente Acuerdo Marco de Precios se articula con lo dispuesto en el artículo 102 de la Ley 2294 de 2023, mediante el cual se incorporó al ordenamiento jurídico colombiano el Sistema Dinámico de Adquisición (SDA), como un mecanismo que permite la habilitación continua de proveedores y la adaptación del instrumento a la evolución del mercado y de las necesidades institucionales. Así mismo, se observa lo establecido en la Resolución 358 de 2025 de Colombia Compra Eficiente, que reglamenta la implementación de este tipo de instrumentos.

En este sentido, el Acuerdo Marco de Precios de Bienes y Servicios de Ciberseguridad se concibe como un mecanismo de agregación de demanda de carácter dinámico, que combina estandarización, flexibilidad y competencia efectiva, permitiendo responder oportunamente a un entorno de amenazas digitales en constante evolución, sin sacrificar los principios que rigen la contratación estatal.

El mercado de bienes y servicios de ciberseguridad se caracteriza por ciclos tecnológicos cortos, innovación constante y evolución acelerada de amenazas digitales. En este contexto, un modelo contractual cerrado podría generar obsolescencia técnica o limitar la participación de nuevos actores especializados. La incorporación de atributos dinámicos al Acuerdo Marco permite mantener abierta la competencia durante su vigencia, habilitar proveedores que acrediten

capacidades técnicas actualizadas y adaptar el instrumento a la evolución del mercado y de los riesgos digitales que enfrenta el Estado.

La estructuración del presente instrumento no implica la estandarización rígida de soluciones tecnológicas, sino la estandarización de condiciones de competencia, habilitación y reglas de operación, preservando la flexibilidad necesaria para que las Entidades Compradoras definan en cada Orden de Compra los alcances técnicos específicos, niveles de servicio y requerimientos particulares conforme a sus necesidades institucionales.

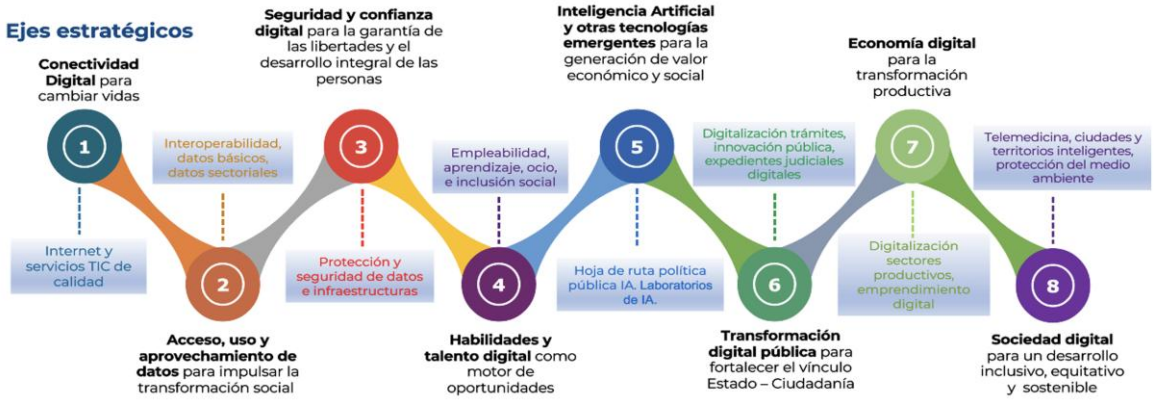
Finalmente, el presente Estudio del Sector analiza las condiciones técnicas, económicas y operativas del mercado de bienes y servicios de ciberseguridad, identifica la oferta disponible, caracteriza la demanda pública y sustenta la definición de los requisitos, criterios y condiciones del proceso de selección. Todo ello con el propósito de que el Acuerdo Marco de Precios se constituya en una herramienta estratégica para fortalecer la postura de seguridad digital del Estado colombiano, garantizar la continuidad de los servicios públicos y contribuir de manera efectiva a la implementación de la política nacional de seguridad digital.

2. DEFINICIONES

Para los fines de este proceso de contratación a menos que expresamente se estipule de otra manera, los términos deben entenderse de acuerdo con la definición contenida en el artículo 2.2.1.1.1.3.1 del Decreto 1082 de 2015 y el Anexo 1 - Definiciones. Los términos no definidos deben comprenderse de conformidad con su significado natural y obvio.

De igual forma, el artículo 29 del Código Civil establece: "Las palabras técnicas de toda ciencia o arte se tomarán en el sentido que les den los que profesan la misma ciencia o arte; a menos que aparezca claramente que se han formado en sentido diverso.", lo que conlleva a que se definan palabras que corresponden a modismos, es decir, una expresión que se usa dentro del ámbito informal, cuyo significado no puede ser deducido a partir de las palabras que lo componen, sino que, es necesario conocer cuál es su significado, aunque a veces se puede deducir.

3. ASPECTOS GENERALES DEL SECTOR



En el proceso para analizar la dinámica del mercado de adquisición de bienes y servicios de Ciberseguridad, han sido identificadas las tendencias de la oferta y de la demanda; todo esto con el fin de ofrecer a las Entidades Estatales la posibilidad de adquirir diferentes tipos de bienes y servicios que estén alineados con los lineamientos de la *"Estrategia Nacional Digital de Colombia 2023-2026"*[1], la cual busca desencadenar el potencial de la transformación digital mediante el desarrollo de ejes estratégicos para superar los desafíos que enfrenta Colombia nivel económico, social y ambiental, a través de un impulso decidido al uso y apropiación de los datos y las tecnologías digitales por parte de las personas y los hogares, las entidades públicas y el sector productivo, abordando los retos, riesgos y daños potenciales que trae consigo la aceleración de la digitalización.

Gráfica 1 - Ejes estratégicos de la END 2023-2026

Fuente: DNP

Así mismo, fueron desarrolladas mesas de trabajo y se generaron solicitudes de información que contaron con la participación de Entidades Estatales y Proveedores de Ciberseguridad, donde se pudo determinar que los bienes y servicios relacionados con este sector, son fundamentales para optimizar recursos y promover la eficiencia operativa en el Estado. Estos servicios permiten escalabilidad, reducción de costos administrativos y energéticos, y mayor rapidez en la implementación de infraestructuras digitales.

El National Institute of Standards and Technology -NIST- define la ciberseguridad como la prevención de daños, protección y restauración de

[1] 2024-02-05_Estrategia_Nacional_Digital_word.pdf

sistemas y datos para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio. Esta definición se basa en la protección de sistemas informáticos y electrónicos contra daños y en la capacidad de restaurarlos después de un incidente, asegurando que los datos y aplicaciones sean seguros y accesibles cuando se necesiten.

- **Prevención y Protección:** Implica la implementación de medidas para evitar que personas no autorizadas accedan o dañen los sistemas.
- **Restauración:** Se refiere a la capacidad de recuperar los sistemas y datos después de que hayan sido comprometidos o dañados.
- **Disponibilidad:** Asegura que los sistemas y datos estén accesibles y funcionales cuando se requieran.
- **Integridad:** Garantiza que la información no sea modificada ni destruida de forma no autorizada.
- **Confidencialidad:** Protege la información para que solo los usuarios autorizados puedan acceder a ella.
- **Autenticación:** Verifica la identidad de los usuarios para asegurar que son quienes dicen ser.
- **No Repudio:** Asegura que no se pueda negar la participación en una acción o la autoría de una comunicación.

Desde una perspectiva de mercado y contratación pública, los bienes y servicios de ciberseguridad pueden clasificarse en segmentos funcionales, de acuerdo con el tipo de activo protegido, el alcance del control de seguridad y el rol que cumplen dentro de la gestión integral del riesgo digital. Esta clasificación permite estructurar de manera ordenada la oferta del mercado y facilita la definición de requisitos técnicos y condiciones de contratación acordes con cada tipo de servicio.

De manera general, los principales segmentos funcionales de la ciberseguridad son los siguientes:

1. Seguridad de Infraestructura y Redes
   Comprende los servicios y soluciones orientados a la protección del perímetro tecnológico, la conectividad y el tráfico de red. Incluye, entre otros, firewalls de nueva generación (NGFW), sistemas de prevención y detección de intrusiones (IPS/IDS), firewalls de aplicaciones web (WAF), mitigación de ataques de denegación de servicio distribuido (DDoS), redes definidas por software seguras (SD-WAN), microsegmentación y control de acceso a la red (NAC).

2. Seguridad de Endpoints y Dispositivos
   Abarca la protección de estaciones de trabajo, servidores, dispositivos móviles y entornos de Internet de las Cosas (IoT) y tecnología operacional (OT), mediante soluciones de protección de endpoints (EPP), detección y respuesta en endpoints (EDR), detección y respuesta extendida (XDR), gestión de dispositivos móviles (MDM) y control de dispositivos y periféricos.

3. Gestión de Identidades y Accesos (IAM / PAM)
   Orientada a garantizar el acceso seguro a sistemas, aplicaciones y datos críticos. Incluye mecanismos de autenticación multifactor (MFA), inicio de sesión único (SSO), federación de identidades, gestión de accesos privilegiados (PAM) y gobierno y administración de identidades (IGA).

4. Protección de Datos y Continuidad del Negocio
   Enfocada en la protección, integridad, disponibilidad y recuperación de la información. Comprende soluciones de prevención de fuga de información (DLP), cifrado de datos, respaldo y recuperación (backup), planes de recuperación ante desastres (DRP) y programas de continuidad del negocio (BCP).

5. Seguridad en la Nube y de Aplicaciones
   Dirigida a la protección de entornos híbridos y multinube, así como de aplicaciones y servicios digitales. Incluye herramientas y servicios de gestión de la postura de seguridad en la nube (CSPM), protección de cargas de trabajo en la nube (CWPP), plataformas integradas de seguridad en la nube (CNAPP), brokers de seguridad de acceso a la nube (CASB), arquitecturas SASE y Zero Trust, y prácticas de seguridad en el ciclo de desarrollo de aplicaciones (DevSecOps).

6. Monitoreo, Orquestación y Automatización de la Seguridad
   Comprende la centralización, correlación y análisis de eventos de seguridad, mediante plataformas de gestión de eventos e información de seguridad (SIEM), orquestación, automatización y respuesta (SOAR), inteligencia de amenazas (Threat Intelligence), simulación de ataques y validación de controles (BAS), y análisis avanzado de registros (logs).

7. Servicios Gestionados y Operaciones de Seguridad
   Incluye la prestación continua de servicios especializados, tales como Centros de Operaciones de Seguridad (SOC) como servicio, detección y respuesta gestionada (MDR), búsqueda proactiva de amenazas (Threat

Hunting), respuesta a incidentes y análisis forense digital (DFIR), Centros de Operaciones de Red (NOC/CNOC) y gestión continua de vulnerabilidades.

8. Consultoría, Gobierno y Gestión de la Ciberseguridad
   Abarca servicios de asesoría especializada, auditorías técnicas y evaluaciones de seguridad, tales como pruebas de penetración, ejercicios de Red Team, implementación y maduración de marcos de referencia como ISO/IEC 27001, NIST, COBIT y el Modelo de Seguridad y Privacidad de la Información (MSPI), así como programas de capacitación y fortalecimiento de capacidades institucionales.

9. Confianza y Seguridad Digital
   Orientada a la protección criptográfica y a los servicios de confianza digital, incluyendo infraestructuras de clave pública (PKI), certificados digitales, firma electrónica y digital, módulos de seguridad de hardware (HSM) y servicios de sellado de tiempo.

10. Ciberseguridad Avanzada y Tendencias Emergentes
    Comprende servicios y soluciones asociados a tecnologías y riesgos emergentes, tales como seguridad en inteligencia artificial, blockchain y Web3, resiliencia cibernética, protección de entornos industriales y de control (OT/ICS), y mecanismos de transferencia de riesgo como los ciberseguros.

Tabla 1– Clasificación de servicios de Ciberseguridad en segmentos

Segmento	Categoría principal	Descripción	Ejemplos comerciales / Marcas representativas
1. Seguridad de Infraestructura y Red	Firewalls, Control Perimetral, Seguridad Web y Mitigación DDoS	Protege la red y el perímetro institucional frente a ataques, intrusiones y accesos no autorizados mediante control de tráfico, filtrado, segmentación y monitoreo continuo.	**Fortinet**, **Palo Alto Networks**, **Cisco**, **Check Point**, **F5**, **Radware**, **Juniper**, **Huawei**, **Appgate**
2. Seguridad de Endpoints y Dispositivos	Protección de estaciones,	Garantiza la seguridad de dispositivos finales, detectando y respondiendo a amenazas con agentes	**Microsoft Defender**, **CrowdStrike Falcon**, **SentinelOne**, **Sophos**, **Trend Micro**, **Trellix**,

	servidores, móviles e IoT	inteligentes y gestión centralizada.	**VMware Carbon Black**, **Kaspersky**
3. Gestión de Identidades y Accesos (IAM/PAM)	Autenticación, accesos privilegiados y gobierno de identidades	Controla el acceso de usuarios y privilegios sobre sistemas críticos mediante autenticación multifactor, SSO, y administración de credenciales.	**Okta**, **CyberArk**, **Microsoft Entra ID**, **Ping Identity**, **One Identity**, **ForgeRock**, **BeyondTrust**
4. Protección de Datos y Continuidad	DLP, Cifrado, Backup, DRP y BCP	Asegura la confidencialidad, integridad y disponibilidad de la información mediante prevención de fugas, cifrado y planes de recuperación ante incidentes.	**Veeam**, **Veritas**, **Commvault**, **Acronis**, **Dell EMC**, **Forcepoint**, **Symantec (Broadcom)**, **Varonis**
5. Seguridad en la Nube y Aplicaciones	CSPM, CASB, CWPP, CNAPP, DevSecOps, CDN	Protege entornos multi-nube e híbridos, asegurando la configuración, despliegue y operación segura de aplicaciones y servicios en la nube.	**Zscaler**, **Netskope**, **Palo Alto Prisma Cloud**, **Check Point CloudGuard**, **Akamai**, **Cloudflare**, **Wiz**, **Orca Security**
6. Monitoreo, Orquestación y Automatización	SIEM, SOAR, Threat Intelligence, BAS	Centraliza el análisis y correlación de eventos de seguridad, automatiza respuestas e integra inteligencia de amenazas.	**Fortinet, Paloalto, Splunk**, **IBM QRadar**, **Microsoft Sentinel**, **Elastic**, **Exabeam**, **Rapid7**, **LogRhythm**, **ThreatConnect**
7. Servicios Gestionados y Operaciones de Seguridad	SOC/NOC, MDR, DFIR, Gestión de vulnerabilidades	Servicios especializados de operación, monitoreo 24/7, detección, respuesta y contención de incidentes en tiempo real.	**IBM Security Services**, **Mandiant (Google)**, **Telefónica Tech**, **Secureworks**, **Claro**, **EY**, **Deloitte**, **KPMG**, **Tenable**, **Qualys, Mandiant**
8. Consultoría y Gobierno en Ciberseguridad	Implementación de marcos, auditorías y formación	Servicios profesionales para implementar SGSI/MSPI, realizar auditorías, pentesting, Red Teaming y capacitar al personal.	**PwC**, **KPMG**, **EY**, **Deloitte**, **BDO**, **ISACA Partners**, **NCC Group**, **Trustwave**

Fuente: Colombia Compra Eficiente

Aunque existen tipos distintos de Ciberseguridad, en la práctica, las soluciones suelen combinarlos para adaptarse a las necesidades y complejidades específicas de cada proyecto.

En respuesta al dinamismo y constante actualización de este mercado, Colombia Compra Eficiente, en colaboración con el MinTIC, diseñará y pondrá en marcha un nuevo Mecanismo de Agregación de Demanda para la adquisición de bienes y servicios de Ciberseguridad. Este mecanismo tiene como objetivo facilitar el acceso al mercado de compras públicas de MiPymes y actores de la economía popular, en consonancia con el Plan Nacional de Desarrollo 2022-2026 "Colombia Potencia Mundial de la Vida" y la Estrategia Nacional de Seguridad Digital de Colombia 2025-2027.

En efecto, la Agencia considera pertinente abrir el proceso de contratación de ciberseguridad bajo un esquema dinámico, con el propósito de fortalecer los principios de eficiencia, transparencia, concurrencia e innovación en el marco de la contratación pública. La implementación de atributos asociados a un **Sistema Dinámico de Adquisición (SDA)** responde a la necesidad de adaptar los mecanismos contractuales a las particularidades del mercado tecnológico, caracterizado por su constante evolución y alta especialización.

Las principales ventajas que ofrece este modelo pueden resumirse en:

- **Optimización presupuestal**, al permitir la comparación continua de ofertas durante la vigencia del mecanismo, lo que impulsa mejores condiciones económicas para la prestación de los servicios.
- **Mayor concurrencia**, ya que los atributos dinámicos facilitan una convocatoria abierta y permanente al mercado, incentivando la participación de un mayor número de proveedores y generando un efecto positivo en la oferta disponible.
- **Transparencia en la adjudicación**, al estar regida por reglas objetivas, públicas y uniformes, lo que fortalece la confianza en el proceso contractual.
- **Igualdad de trato**, al establecer condiciones equitativas de participación y evaluación basadas en criterios técnicos y proporcionales, garantizando la selección de la mejor propuesta en términos de calidad-precio.

En este contexto, la incorporación de atributos dinámicos representa una oportunidad de modernización y transformación del modelo de agregación de demanda, ya que permite a la Agencia —y a las entidades compradoras vinculadas— contar con un procedimiento flexible y normalizado que facilita la

gestión contractual, promueva la innovación y amplíe el acceso al mercado de soluciones de ciberseguridad. En conjunto, estos elementos permiten desarrollar procesos contractuales más transparentes, eficientes y orientados al logro de resultados, en armonía con los fines esenciales del sistema de compras públicas.

3.1. Entorno económico

3.1.1. Contexto nacional

La gestión de incidentes de seguridad digital y ciberseguridad se ha consolidado como una actividad crítica para las áreas de tecnología y seguridad de la información, tanto en el sector público como en el privado, debido al incremento sostenido en el volumen, frecuencia y sofisticación de los ataques dirigidos contra las infraestructuras tecnológicas.

En el contexto colombiano, los indicadores recientes evidencian un **alto nivel de exposición a amenazas cibernéticas**. Durante el año 2024, se registraron decenas de miles de millones de intentos de ciberataques dirigidos a infraestructuras tecnológicas del país. Así mismo, reportes especializados de inteligencia de amenazas señalan que, durante el primer semestre de 2025, Colombia se ubicó entre los países más atacados de la región, concentrando miles de millones de intentos de ataque, lo que refleja un escenario de riesgo persistente y creciente.

Los sectores más impactados por este tipo de incidentes han sido el **sector financiero**, el **sector salud** y el **sector energético**, los cuales operan infraestructuras críticas y prestan servicios esenciales para la población. Este panorama evidencia vulnerabilidades relevantes en sistemas estratégicos y resalta la necesidad de fortalecer las capacidades de prevención, detección, respuesta y recuperación frente a incidentes cibernéticos.

Entre las principales tipologías de ataque identificadas se encuentran el **phishing**, el **ransomware**, el **malware**, la **suplantación de identidad** y los **ataques de denegación de servicio distribuido (DDoS)**, los cuales afectan la disponibilidad de los servicios, la integridad de la información y la confianza de los usuarios en los entornos digitales.

De manera paralela, el mercado nacional de servicios de ciberseguridad ha mostrado un crecimiento sostenido, impulsado por la creciente demanda de soluciones especializadas por parte de entidades públicas y privadas. Empresas

del sector de telecomunicaciones y tecnología han incorporado la ciberseguridad como una línea estratégica de negocio, reflejando la madurez progresiva del mercado y la disponibilidad de oferta especializada a nivel nacional.

Desde el ámbito de la política pública, el **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)** ha promovido estrategias orientadas a la consolidación de un entorno digital **seguro, confiable y resiliente**, con énfasis en la protección de los derechos fundamentales, la dignidad humana y el desarrollo integral de las personas. En este sentido, la **Estrategia Nacional de Seguridad Digital** constituye el principal marco de referencia para fortalecer las capacidades institucionales del país en materia de gestión del riesgo digital.

Dicha estrategia se orienta a garantizar que la ciudadanía, las Entidades Estatales y los sectores productivos cuenten con mejores capacidades técnicas, organizacionales y humanas para enfrentar los riesgos y amenazas del entorno digital, promoviendo una gestión preventiva, coordinada y resiliente de la seguridad digital a nivel nacional.

Aunado a lo anterior, los números apuntan a una creciente materialización de incidentes de ciberseguridad.

Incidentes relevantes de ciberseguridad en entidades públicas (2024–2025)

Durante los años 2024 y 2025 se presentaron diversos **incidentes de ciberseguridad que afectaron a Entidades Estatales en Colombia**, los cuales fueron reportados a través de comunicados oficiales, pronunciamientos institucionales o reportes de equipos de respuesta a incidentes. Estos eventos evidencian la materialización de los riesgos asociados a la operación de infraestructuras tecnológicas públicas y refuerzan la necesidad de fortalecer las capacidades institucionales en materia de ciberseguridad.

Año	Tipo de entidad afectada	Tipo de incidente	Impacto principal	Fuente de referencia
2024	Entidad del sector salud	Ransomware	Interrupción temporal de sistemas de información y afectación a la disponibilidad de servicios administrativos	Comunicados institucionales / reportes sectoriales

Año	Tipo de entidad afectada	Tipo de incidente	Impacto principal	Fuente de referencia
2024	Alcaldía municipal	Ataque de denegación de servicio (DDoS)	Indisponibilidad de portales web y trámites en línea	Reportes CSIRT / medios oficiales
2024	Entidad del sector justicia	Compromiso de credenciales (phishing)	Accesos no autorizados y medidas de contención preventiva	Pronunciamientos institucionales
2025	Entidad del sector social	Malware / acceso no autorizado	Afectación parcial de sistemas internos y activación de planes de respuesta a incidentes	Reportes técnicos sectoriales
2025	Entidad territorial	Ataque a infraestructura tecnológica	Interrupción temporal de servicios digitales y recuperación desde respaldos	Comunicaciones oficiales

Fuente: Reportes oficiales (CSIRT/MinTIC)

Nota: Los casos presentados corresponden a incidentes reportados públicamente o a eventos conocidos a través de los mecanismos de gestión de incidentes del sector público, y se incluyen con fines ilustrativos y analíticos, sin perjuicio de las acciones de investigación o contención adelantadas por las entidades competentes.

Tipologías de incidentes recurrentes en el sector público

El análisis de los incidentes reportados durante 2024 y 2025 permite identificar las siguientes **tipologías recurrentes de ciberataques** en Entidades Estatales:

- Ataques de **ransomware** dirigidos a servidores y sistemas críticos.
- Campañas de **phishing** orientadas al compromiso de credenciales de funcionarios públicos.
- **Ataques de denegación de servicio distribuido (DDoS)** contra portales institucionales.
- Infecciones por **malware** en estaciones de trabajo y servidores.
- Accesos no autorizados derivados de configuraciones inseguras o vulnerabilidades conocidas.

Estos eventos han generado impactos en la **disponibilidad de los servicios digitales**, la **integridad de la información**, y en algunos casos han requerido la activación de **planes de contingencia, recuperación y continuidad del negocio**, lo cual refuerza la necesidad de contar con proveedores especializados y capacidades técnicas adecuadas.

3.1.2. PIB desde el enfoque de la producción

De acuerdo con el boletín técnico del Producto Interno Bruto publicado por el Departamento Administrativo Nacional de Estadística - DANE, en el segundo trimestre de 2025pr, el Producto Interno Bruto en su serie original, crece 2,1% respecto al mismo periodo de 2024pr. Las actividades económicas que más contribuyen a la dinámica del valor agregado son:

- Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida crece 5,6% (contribuye 1,1 puntos porcentuales a la variación anual).
- Agricultura, ganadería, caza, silvicultura y pesca crece 3,8% (contribuye 0,4 puntos porcentuales a la variación anual).

- Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales crece 1,8% (contribuye 0,3 puntos porcentuales a la variación anual).

Tabla 2- Tasa de Crecimiento a precios corrientes segundo trimestre 2025, actividad económica.

Actividad económica	Tasas de crecimiento (%)		
	Serie original		Serie ajustada por efecto estacional y calendario
	Anual	Año corrido	Trimestral
	2025[pr]-II / 2024[pr]-II	2025[pr]/ 2024[pr]	2025[pr]-II / 2025[pr]-I
Agricultura, ganadería, caza, silvicultura y pesca	3,8	5,3	1,5
Explotación de minas y canteras	-10,2	-7,6	-5,1
Industrias manufactureras	0,9	1,1	1,0
Suministro de electricidad, gas, vapor y aire acondicionado[2]	0,9	-0,3	1,0
Construcción	-3,5	-3,3	-0,1
Comercio al por mayor y al por menor[3]	5,6	4,8	0,03
Información y comunicaciones	3,0	1,8	2,3
Actividades financieras y de seguros	2,8	3,0	0,8
Actividades inmobiliarias	2,0	2,0	0,6
Actividades profesionales, científicas y técnicas[4]	1,5	1,3	0,7
Administración pública, defensa, educación y salud[5]	1,8	2,7	-0,04
Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios[6]	7,5	11,4	-2,4
Valor agregado bruto	**2,1**	**2,4**	**0,3**
Impuestos menos subvenciones sobre los productos	2,4	2,3	0,3
Producto Interno Bruto	**2,1**	**2,4**	**0,5**

Fuente: DANE

Como se evidencia en la tabla anterior, el valor agregado de información y comunicaciones en la cual está incluida la industria de Ciberseguridad, creció un 3,0% en su serie original comparada con la vigencia. Para efectos de la serie ajustada por efecto estacional y calendario, el valor agregado crece en 2,3%, respecto al trimestre inmediatamente anterior.

Se proyecta que para el 2025, la inversión en ciberseguridad en Colombia crecerá a una tasa anual cercana a 11%[2].

3.1.3. PIB desde el enfoque del gasto

[2] https://www.larepublica.co/empresas/la-inversion-en-ciberseguridad-aumentara-11-este-ano-ante-crecimiento-en-ataques-4215835

De acuerdo con el boletín técnico del Producto Interno Bruto publicado por el Departamento Administrativo Nacional de Estadística – DANE[3] En el segundo trimestre de 2025pr, el Producto Interno Bruto en su serie original crece 2,1% respecto al mismo periodo de 2024pr.

Esta dinámica se explica por los siguientes comportamientos del componente del gasto:

- Gasto en consumo final crece 3,8%.
- Formación bruta de capital crece 6,4%.
- Exportaciones decrecen 1,6%.
- Importaciones crecen 9,7%.

Gráfica 2 - Tasa de Crecimiento a precios corrientes cuarto trimestre 2025, componente del gasto.

Componentes del gasto	Tasas de crecimiento (%)		
	Serie original		Serie ajustada por efecto estacional y calendario
	Anual	Año corrido	Trimestral
	2025pr-II / 2024pr-II	2025pr/ 2024pr	2025pr-II / 2025pr-I
Gasto de consumo final[2]	3,8	3,8	0,7
Formación bruta de capital[3]	6,4	7,3	2,7
Exportaciones	-1,6	0,7	-0,3
Importaciones	9,7	10,7	2,6
Producto Interno Bruto	**2,1**	**2,4**	**0,5**

Fuente: DANE

3 DANE, Boletín técnico Bogotá D.C. 15 de agosto de 2025, https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-nacionales-trimestrales/pib-informacion-tecnica

Así mismo, la Dirección de Síntesis y Cuentas Nacionales del DANE, define el gasto de consumo final como "Los bienes y servicios utilizados por los hogares individuales o por la comunidad, para satisfacer sus necesidades, deseos individuales o colectivos."

En el segundo trimestre de 2025pr el gasto de consumo final crece 3,8% en su serie original, respecto al mismo periodo de 2024pr. Los componentes del gasto que explican este comportamiento son:

• Gasto de consumo final individual de los hogares crece 3,7%.

• Gasto de consumo final del gobierno general crece 3,9%.

Respecto al trimestre inmediatamente anterior, el gasto de consumo final crece en 0,7% en su serie ajustada por efecto estacional y calendario. Cuando se observa el comportamiento de sus componentes:

• Gasto de consumo final individual de los hogares crece 0,1%.

• Gasto de consumo final del gobierno general crece 2,6%.

3.1.4. Generación de Empleos

El sector de las Tecnologías de la Información genera numerosos empleos a través de diversas áreas como lo son:

1. **Desarrollo de software y programación:** Un software de programación es el conjunto de utilidades y herramientas utilizadas para el desarrollo, programación o creación de programas o aplicaciones informáticas por parte de los programadores. Dichas utilidades y herramientas pueden hacer uso de diversos lenguajes de programación y metodologías de desarrollo a través de, como mínimo, un editor de texto y un compilador.[4]

2. Soporte técnico y servicios de tecnología: Con el aumento de la adopción de tecnología, se ha incrementado la demanda de profesionales que brinden soporte técnico y servicios de tecnología a empresas y usuarios.[5]

[4] Velneo, recuperado dehttps://velneo.com/blog/software-de-programacion/
[5]Cámara Colombiana de Informática y Telecomunicaciones, TicTac, Otros Estudios, https://www.ccit.org.co/otros-estudios/

3. **Ciberseguridad:** Con la creciente dependencia de la tecnología y la digitalización de la información, las amenazas cibernéticas se han vuelto más sofisticadas y frecuentes. Las organizaciones necesitan profesionales en ciberseguridad para proteger sus sistemas y datos contra estos ataques.

Actualmente, existe una falta de entre 515.000 y 701.000 profesionales en la región, lo que pone en riesgo la seguridad de las organizaciones. [6]

4. **Analítica de datos:** La capacidad de recopilar y analizar grandes cantidades de datos han generado la necesidad de profesionales en análisis de datos, que puedan interpretar la información y tomar decisiones basadas en ella.[7]

3.1.5. Principales cifras

De acuerdo con el boletín del Producto Interno Bruto del segundo trimestre de 2025, publicado por el DANE, el sector de Información y comunicaciones en el segundo trimestre de 2025, su valor agregado creció un 3,0% en su serie original, respecto al mismo periodo de 2024. No obstante, para la serie ajustada por efecto estacional y calendario, el valor agregado crece en 2,3%, respecto al trimestre inmediatamente anterior tal como se observa en la tabla.

Tabla 3 Tasa de crecimiento - Información y Comunicaciones

Actividad económica	Tasas de crecimiento (%)		
	Serie original		Serie ajustada por efecto estacional y calendario
	Anual	Año corrido	Trimestral
	2025^{pr}-II / 2024^{pr}-II	2025^{pr}/ 2024^{pr}	2025^{pr}-II / 2025^{pr}-I
Información y comunicaciones	3,0	1,8	2,3

Fuente: DANE

[6] Infobae, Ciberseguridad y empleo, la nueva oportunidad para transformar vidas en Colombia https://www.infobae.com/tecno/2025/02/20/ciberseguridad-y-empleo-la-nueva-oportunidad-para-transformar-vidas-en-colombia/

[7] Cámara Colombiana de Informática y Telecomunicaciones, TicTac, Otros Estudios, https://www.ccit.org.co/otros-estudios/

Según cifras de Claro Colombia presentadas en su Summit, las grandes empresas destinan presupuestos en ciberseguridad que pueden superar los $15.000 millones, mientras que datos de ERC Colombia indican que, en el caso de las pymes, las inversiones oscilan entre $800 millones y $4.000 millones.[8]

Se proyecta que la inversión en ciberseguridad en Colombia tendrá un crecimiento en el cual, las pymes lideran este aumento con una tasa aproximada del 16,9%. El mercado podría alcanzar los US$1.880 millones para 2030, al impulsar por la digitalización, la migración a la nube y la presión regulatoria. Las soluciones más demandadas por las empresas incluyen firewalls, antivirus, herramientas de inteligencia artificial, auditorías y servicios SOC gestionados.[9]

En la actualidad, las empresas destinan entre el 7% y el 15% de su presupuesto de TI a seguridad digital, lo que representa entre el 0,3% y el 0,6% de sus ingresos anuales.

> *"La ciberseguridad ya no es un gasto técnico, sino una inversión estratégica que puede determinar la continuidad de un negocio. No actuar implica un riesgo mucho más costoso que cualquier presupuesto asignado", explica Óscar Díaz, Chief Commercial Officer de ERC Colombia.*

3.2. Entorno internacional

- **Tendencias internacionales en contratación pública de ciberseguridad**

A nivel internacional, se evidencia una tendencia creciente hacia la adopción de modelos de contratación pública flexibles y dinámicos para la adquisición de servicios tecnológicos especializados, particularmente en materia de ciberseguridad. La rápida evolución de amenazas digitales, la innovación constante en soluciones tecnológicas y la necesidad de actualización permanente de capacidades institucionales han llevado a diversos Estados a implementar mecanismos que permitan mantener abierta la competencia durante la vigencia contractual y facilitar la incorporación continua de nuevos proveedores.

[8]Portafolio, ¿Cuánto invierten realmente las empresas en ciberseguridad en Colombia? https://www.portafolio.co/tecnologia/cuanto-invierten-realmente-las-empresas-en-ciberseguridad-en-colombia-638893

[9]La Republica, La inversión en ciberseguridad aumentará 11% este año, ante crecimiento en ataques, https://www.larepublica.co/empresas/la-inversion-en-ciberseguridad-aumentara-11-este-ano-ante-crecimiento-en-ataques-4215835

En la Unión Europea, los **Sistemas Dinámicos de Adquisición (Dynamic Purchasing Systems – DPS)** han sido utilizados como herramienta para la contratación de servicios tecnológicos y de seguridad digital, permitiendo la habilitación progresiva de proveedores que cumplan requisitos previamente definidos, bajo esquemas de competencia reiterada. De manera similar, el Reino Unido, a través del Crown Commercial Service, y los Estados Unidos, mediante esquemas como los Federal Supply Schedules administrados por la General Services Administration (GSA), han desarrollado marcos de proveedores preaprobados para servicios de ciberseguridad, priorizando la flexibilidad, la actualización tecnológica y la eficiencia en la adquisición.

Estas experiencias comparadas demuestran que la contratación pública en materia de ciberseguridad requiere instrumentos que equilibren estandarización y adaptabilidad, permitiendo a las entidades públicas responder de manera ágil a riesgos emergentes, sin sacrificar los principios de transparencia, competencia y selección objetiva.

- **Protección de infraestructura crítica y resiliencia cibernética**

En el ámbito internacional, la protección de infraestructuras críticas digitales y la resiliencia cibernética se han consolidado como prioridades estratégicas de política pública, especialmente frente al incremento de ataques dirigidos a sectores como energía, salud, justicia, finanzas y administración pública. En este contexto, los Estados han fortalecido sus marcos normativos y contractuales para garantizar la continuidad de servicios esenciales y mitigar los impactos económicos, sociales y reputacionales derivados de incidentes de alto impacto.

La experiencia comparada evidencia que la formulación de políticas de seguridad digital debe ir acompañada de instrumentos contractuales ágiles que permitan su implementación efectiva. En consecuencia, la adopción de mecanismos de agregación de demanda con atributos dinámicos se alinea con las mejores prácticas internacionales, al facilitar la actualización continua de capacidades técnicas y la ampliación progresiva de la oferta habilitada.

Panorama Internacional

- **China**

El pasado lunes 8 de septiembre de 2025, los legisladores chinos comenzaron a revisar un proyecto de enmienda a la Ley de Ciberseguridad con el objetivo de

fortalecer las responsabilidades legales. La enmienda propone una mejor articulación con leyes relevantes, incluidas la Ley de Seguridad de Datos, la Ley de Protección de Información Personal y la Ley de Sanciones Administrativas, a fin de garantizar un marco legal más coherente. También plantea establecer responsabilidades legales diferenciadas para diversas infracciones, abarcando áreas como la seguridad de operación de red y la seguridad de la información.[10]

- **México**

El gobierno celebra la protección del dominio gob.mx y la instauración de alertas tempranas. Asimismo, se habla de una Política General de Ciberseguridad que aún está en proceso, el problema es que los ciberataques no esperan a que los borradores se conviertan en políticas definitivas. El ransomware, el robo de datos y las intrusiones a infraestructura crítica avanzan en semanas, no en años.

Mientras México redacta documentos, los atacantes afinan nuevas técnicas, desarrollan malware más sofisticado y prueban vulnerabilidades en los sistemas gubernamentales y empresariales.[11]

- **Europa y Norteamérica**

Europa y Norteamérica han sido víctimas de números ciberataques los cuales son atribuidos a la banda de Ransomware Interlock, quien mantiene una campaña muy activa para atacar a organizaciones e infraestructuras críticas. Así lo ha advertido la Agencia de Seguridad de Infraestructuras de Ciberseguridad de EE. UU (CISA).12

Desde el FBI sostienen que estos actores escogen sus víctimas basándose en la oportunidad y aseguran que su actividad tiene motivaciones económicas.

3.3. Marco regulatorio

[10]El País, China estudia enmienda a ley de ciberseguridad para fortalecer responsabilidades legaleshttps://www.elpais.cr/2025/09/08/china-estudia-enmienda-a-ley-de-ciberseguridad-para-fortalecer-responsabilidades-legales/

[11] Infobae, La velocidad y contundencia de los ciberataques vs los avances en ciberseguridad del primer informe de Sheinbaum https://www.infobae.com/mexico/2025/09/06/la-velocidad-y-contundencia-de-los-ciberataques-vs-los-avances-en-ciberseguridad-del-primer-informe-de-sheinbaum/

[12]Escudodigital, CISA advierte sobre un incremento de los ataques del grupo de ransomware Interlock https://www.escudodigital.com/ciberseguridad/cisa-advierte-sobre-un-incremento-de-los-ataques-del-grupo-de-ransomware-interlock.html

El marco regulatorio aplicable, normas técnicas, especificaciones, regulaciones del sector, gravámenes, entre otros, que se relacionan a continuación son algunos de los temas aplicables al proceso de selección que se pretende adelantar y la posterior ejecución del Acuerdo Marco, aclarando que las leyes y normativa son de obligatorio cumplimiento, indistintamente que se encuentren relacionadas o no en este documento; y el desconocimiento de las mismas no exime a las partes de su responsabilidad:

Tabla 4– Marco regulatorio aplicable

Ítem	Número	Nombre/Tema	Tipo/Sector
1	Decreto 624 de 1989	Por el cual se expide el Estatuto Tributario de los impuestos administrados por la Dirección General de Impuesto Nacionales.	Tributario
2	Ley 80 de 1993	Estatuto General de Contratación de la Administración Pública	Contratación estatal
3	Ley 1150 de 2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.	Contratación estatal
4	Ley 1273 de 2009 modificada por la Ley 1978 de 2019	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.	Ciberseguridad / Penal
5	Ley 1341 de 2009 modificada por Ley 1978 de 2019 Marco general del sector TIC	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC, se crea la Agencia Nacional de	Ciberseguridad / TIC

		Espectro y se dictan otras disposiciones	
6	CONPES 3701 de 2011 No está derogado, pero quedó superado por: CONPES 3854 de 2016 CONPES 3995 de 2020 No es un error mantenerlo, pero podemos aclarar que fue reemplazado en política pública posterior.	Lineamientos de política para ciberseguridad y ciberdefensa	Ciberseguridad / Política Pública
7	Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	Protección de Datos
	Ley 1712 de 2014	Ley de Transparencia y Acceso a la Información Pública	Transparencia
	Decreto 1074 de 2015	Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Compila la reglamentación en materia de protección de datos personales	Protección de Datos
8	Decreto 1377 de 2013 Fue compilado dentro del Decreto 1074 de 2015. No está formalmente derogado, pero	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.	Protección de Datos

	lo correcto hoy es citar: Decreto 1074 de 2015 (protección de datos)		
9	Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.	Transparencia / Acceso a la Información
10	Decreto 1082 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del sector Administrativo de Planeación Nacional	Contratación estatal
	Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Incluye disposiciones relacionadas con la Política de Gobierno Digital, seguridad y privacidad de la información en entidades públicas.	TIC / Gobierno Digital
11	CONPES 3854 de 2016	Política Nacional de Seguridad Digital	Ciberseguridad / Política Pública
12	Ley 1978 de 2019	Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones	Ciberseguridad / TIC
13	CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital	Ciberseguridad / Política Pública
14	Ley 2294 de 2023	Por el cual se expide el Plan Nacional de Desarrollo 2022 – 2026 "Colombia potencia mundial de la vida".	Social

Notas: El Acuerdo Marco será regido por las Leyes, Decretos, Resoluciones, Directivas, Especificaciones, Normas Técnicas, etc., vigentes para cada orden de compra, según la jerarquía normativa.

Las Leyes, Decretos y Resoluciones que sean de obligatorio cumplimiento y que por algún motivo no se encuentren listadas en esta tabla, no implica que no sean aplicables, ya que son de obligatorio cumplimiento según las disposiciones de cada una de estas y la materia que regulen.

Fuente: Investigación normativa realizada por Colombia Compra Eficiente

3.4. Normas técnicas o certificaciones internacionales

El sector de la ciberseguridad se rige por marcos normativos, estándares técnicos y buenas prácticas de alcance internacional y nacional, los cuales constituyen referentes ampliamente reconocidos para la gestión del riesgo digital, la protección de la información, la continuidad de la operación y la respuesta a incidentes cibernéticos. En el marco del presente Estudio del Sector, se identifican los siguientes instrumentos como relevantes para la contratación pública de servicios de ciberseguridad.

Convenio de Budapest sobre la Ciberdelincuencia

Colombia es Estado Parte del Convenio sobre la Ciberdelincuencia de Budapest, principal instrumento internacional para la cooperación en la prevención, investigación y sanción de delitos informáticos. Este tratado promueve la adopción de medidas orientadas a la gestión de incidentes, la preservación de evidencia digital y la cooperación transnacional.

En el contexto de la contratación estatal, el Convenio de Budapest se constituye en un referente normativo, en tanto orienta a las Entidades Estatales a promover prácticas de interoperabilidad y cooperación internacional, sin que ello implique la exigencia directa de certificaciones asociadas a dicho tratado.

Recomendaciones de la Organización para la Cooperación y el Desarrollo Económicos (OCDE)

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha emitido lineamientos y recomendaciones en materia de seguridad digital y

gestión del riesgo tecnológico, que Colombia, en su calidad de país miembro, ha incorporado progresivamente en sus políticas públicas.

Estas recomendaciones promueven principios como la gestión integral del riesgo digital, la seguridad por diseño, la responsabilidad compartida y la integración de la ciberseguridad en los esquemas de gobernanza institucional. Su consideración en los procesos de contratación pública permite estructurar instrumentos alineados con buenas prácticas internacionales, fomentando la innovación y la competencia, sin imponer requisitos desproporcionados.

Lineamientos y marcos nacionales en materia de ciberseguridad

En el ámbito nacional, se destacan como referentes técnicos y normativos los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en particular el Modelo de Seguridad y Privacidad de la Información (MSPI), en sus versiones y actualizaciones más recientes.

Así mismo, se consideran las guías, lineamientos técnicos y publicaciones emitidas por las autoridades competentes en materia de ciberseguridad en Colombia durante los últimos dos (2) años, orientadas al fortalecimiento de las capacidades de prevención, detección, respuesta y recuperación frente a incidentes cibernéticos, y al desarrollo de una cultura de seguridad digital en el sector público.

Estos instrumentos constituyen un marco nacional de referencia para evaluar la madurez organizacional y técnica de los proveedores de servicios de ciberseguridad.

Estándares y marcos técnicos internacionales

Entre los principales estándares y marcos técnicos de carácter internacional que resultan pertinentes para el objeto del Acuerdo Marco de Precios se encuentran:

- ISO/IEC 27001, norma internacional para la implementación de Sistemas de Gestión de la Seguridad de la Información (SGSI), orientada a la protección de la confidencialidad, integridad y disponibilidad de la información.
- ISO/IEC 27032, que proporciona directrices específicas para la gestión de la ciberseguridad, con un enfoque integral que abarca la gestión de riesgos, la gestión de incidentes y la continuidad del negocio.

- Marco de Ciberseguridad del NIST (National Institute of Standards and Technology), ampliamente reconocido a nivel internacional, que establece un enfoque estructurado para la identificación, protección, detección, respuesta y recuperación frente a riesgos cibernéticos.

Estos estándares se consideran marcos de referencia técnicos, cuya observancia puede acreditarse mediante evidencias de implementación, evaluaciones internas, auditorías de tercera parte o mecanismos equivalentes, sin que sea necesario exigir certificaciones formales como requisito habilitante.

Estándares complementarios aplicables:

- ISO/IEC 27017, que establece directrices para la implementación de controles de seguridad específicos en servicios de computación en la nube, tanto para proveedores como para clientes de servicios cloud.

- ISO/IEC 27018, orientada a la protección de datos personales identificables (PII) en entornos de nube pública, proporcionando lineamientos para el tratamiento seguro de información personal bajo esquemas de servicios cloud.

- ISO 22301, norma internacional para la implementación de Sistemas de Gestión de Continuidad del Negocio, relevante en la prestación de servicios críticos de ciberseguridad que requieren altos niveles de disponibilidad y resiliencia operacional.

Esquemas de aseguramiento independiente

En el mercado de servicios de ciberseguridad se han consolidado esquemas de aseguramiento independiente, tales como los informes SOC 2, los cuales permiten evaluar la efectividad de los controles relacionados con seguridad, disponibilidad, confidencialidad, integridad del procesamiento y privacidad.

Estos informes constituyen un mecanismo objetivo de verificación de la madurez de los proveedores, pudiéndose aceptar informes equivalentes emitidos por terceros independientes que acrediten el cumplimiento de principios similares.

Certificaciones de competencias profesionales

Adicionalmente, el sector reconoce diversas certificaciones profesionales que validan la formación, conocimientos y experiencia del talento humano en ciberseguridad, entre las cuales se destacan:

- CISSP (Certified Information Systems Security Professional)
- CISM (Certified Information Security Manager)
- CEH (Certified Ethical Hacker)
- CCSP (Certified Cloud Security Professional)

Estas certificaciones pueden considerarse como indicadores de capacidad técnica y especialización, sin que su exigencia individual o conjunta resulte obligatoria para la participación en los procesos de contratación.

Consideraciones sobre certificaciones de calidad

Si bien existen normas de gestión de calidad de carácter general, como la ISO 9001:2015, estas no acreditan de manera directa la implementación de controles técnicos de ciberseguridad. En consecuencia, no resulta procedente exigir este tipo de certificaciones como requisito habilitante, en tanto podrían constituir barreras injustificadas a la libre concurrencia y no guardan relación directa con el objeto contractual.

3.5. Compras públicas sostenibles

Una compra es sostenible cuando satisface la necesidad y contribuye a la protección del ambiente, la reducción en el consumo de recursos, o la inclusión y la justicia social durante el desarrollo de un proceso de compra pública.

Las Compras Públicas Sostenibles generan valor por dinero, pues las entidades estatales que las desarrollan: (i) satisfacen la necesidad (eficacia); (ii) reducen los costos asociados al ciclo de vida del bien o servicio (economía); (iii) disminuyen el uso de recursos (eficiencia); (iii) incluyen a empresas o poblaciones con dificultades para participar en el sistema de compra pública, y (iv) promueven la innovación en el sector privado.

CPS con el ambiente

Como parte de la labor de planeación, se realiza el análisis de los criterios de sostenibilidad aplicables al Acuerdo Marco de Precios, para este caso Colombia Compra Eficiente revisó la Guía conceptual y metodológica de compras públicas

sostenibles y las fichas técnicas publicadas por el Ministerio de Ambiente y Desarrollo Sostenible, la cual define los bienes y servicios sostenibles como:

> *"Un bien o servicio es sostenible cuando utiliza de manera racional y eficiente los recursos naturales, humanos y económicos a lo largo de su ciclo de vida, generando así beneficios para el medio ambiente, la sociedad y la economía."*[13]

Considerando que los bienes que harán parte del AMP de Ciberseguridad, cuentan con una regulación o norma técnica colombiana, es necesario contemplar las variables para la selección y la priorización definidas en la Guía de Compras Públicas Sostenibles desarrolladas por el Ministerio de Medio Ambiente y Desarrollo Sostenible, en donde indica la cual enuncia en su numeral 6 *"software de servicios de TI***", esta se encuentra orientada a elementos periféricos (Hardware)**, así las cosas, y teniendo en cuenta que los bienes a adquirir mediante el presente Acuerdo Marco de Precios están enfocados también a la adquisición de Hardware, se brindará aplicabilidad a los criterios de sostenibilidad relevantes.

4. ANÁLISIS DE LA OFERTA

El siguiente análisis, desde el punto de vista técnico y económico, busca definir y estimar las condiciones de la oferta en el mercado de Ciberseguridad para estructurar un Mecanismo de Agregación de Demanda en todo el territorio nacional. Para ello, Colombia Compra Eficiente realizó un análisis basado en: (I) Mesas de trabajo con fabricantes, proveedores, gremios, entidades estatales (II) Documentos sectoriales y (III) la información de TVEC, SECOP y EMIS.

4.1. Cadena de suministro

Los servicios de Ciberseguridad son proporcionados por los Fabricantes, quienes disponen de amplios catálogos publicados en sus sitios web, en los cuales se pueden identificar diferentes ítems asociados a software y hardware. Dichos catálogos se actualizan constantemente, incorporando nuevos bienes y servicios o mejorando las características de los existentes, lo que garantiza una oferta amplia, diversa y actualizada para los compradores.

[13] Min Ambiente, GUÍA CONCEPTUAL Y METODOLÓGICA DE COMPRAS PÚBLICAS SOSTENIBLES, https://quimicos.minambiente.gov.co/wp-content/uploads/2021/06/guia_compras_publicas_sostenibles.pdf

Los Fabricantes tienen intermediarios que se encargan de comercializar los bienes y servicios, estos son denominados canales o partners los cuales se encargan de realizar el acompañamiento y la administración de los servicios adquiridos por los compradores, debido a la complejidad técnica para adquirir estos. Estos partners deben estar certificados por cada Fabricante para que puedan ofrecer sus bienes y servicios como representantes de la marca y ofrecen servicios adicionales tales como profesionales especializados en arquitectura, migración, almacenamiento de datos, seguridad, entre otros.

Por otra parte, los integradores adaptan soluciones a las necesidades del cliente, hacen integraciones con la infraestructura existente, gestionan proyectos de seguridad, auditorías, implementaciones, entre otros.

4.2. Identificación de proveedores

Los proveedores del Acuerdo Marco de Precios serán aquellas empresas registradas como Proveedores de servicios de Ciberseguridad, y cuya Clasificación Industrial Internacional Uniforme (CIIU) corresponda a alguna de las siguientes categorías:

(i) 6202 Actividades de consultoría informática y actividades de administración de instalaciones informáticas.

(ii) 6209 Otras actividades de tecnologías de información y actividades de servicios informáticos.

Esta clasificación se ha integrado en las Bases de Datos de EMIS, una herramienta financiera y de análisis de negocios para mercados emergentes; se ha cruzado esta información con la Base de Datos del Ministerio de Tecnologías de la Información y las Comunicaciones de los PRST (Proveedor de Redes y Servicios de Telecomunicaciones en Colombia), con el objetivo de realizar un análisis financiero y estadístico de las empresas capacitadas para ofrecer

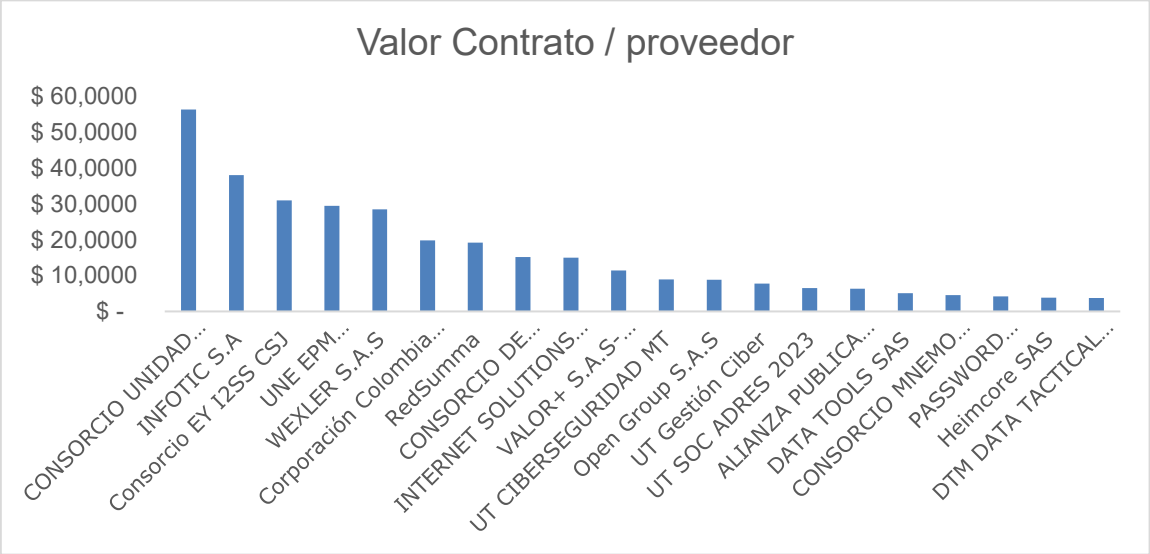
servicios de ciberseguridad. Este proceso ha involucrado un total de 127 empresas analizadas, proporcionando así una visión integral del panorama de proveedores en el mercado de servicios de ciberseguridad en el país.

Tabla 5– Top 20 proveedores servicios Ciberseguridad (valores en miles de millones)

Nom Raz Social Contratista	Valor Contrato
CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA	$ 56,4226
INFOTIC S.A.	$ 38,1145
CONSORCIO EY I2SS CSJ	$ 31,0028
UNE EPM TELECOMUNICACIONES S.A.	$ 29,5347
WEXLER S.A.S	$ 28,5330
CORPORACIÓN COLOMBIA DIGITAL	$ 19,8436
REDSUMMA	$ 19,1789
CONSORCIO DE CIBERSEGURIDAD ORGANIZACION ELECTORAL	$ 15,1997
INTERNET SOLUTIONS S.A.S.	$ 15,0446
VALOR+ S.A.S-PROVEEDOR	$ 11,4000
UT CIBERSEGURIDAD MT	$ 8,9232
OPEN GROUP S.A.S.	$ 8,8471
UT GESTIÓN CIBER	$ 7,7719
UT SOC ADRES 2023	$ 6,5431
ALIANZA PUBLICA PARA EL DESARROLLO INTEGRAL AL DESARROLLO - PROVEEDOR	$ 6,3591
DATA TOOLS SAS	$ 5,0649
CONSORCIO MNEMO SOC-MHCP	$ 4,5298
PASSWORD CONSULTING SERVICES SAS	$ 4,1595
HEIMCORE SAS	$ 3,8312
DTM DATA TACTICAL MANAGEMENT	$ 3,7773

Fuente: Datos Abiertos

Gráfica 3 - Top 20 proveedores servicios Ciberseguridad (valores en miles de millones)



Fuente: Datos Abiertos

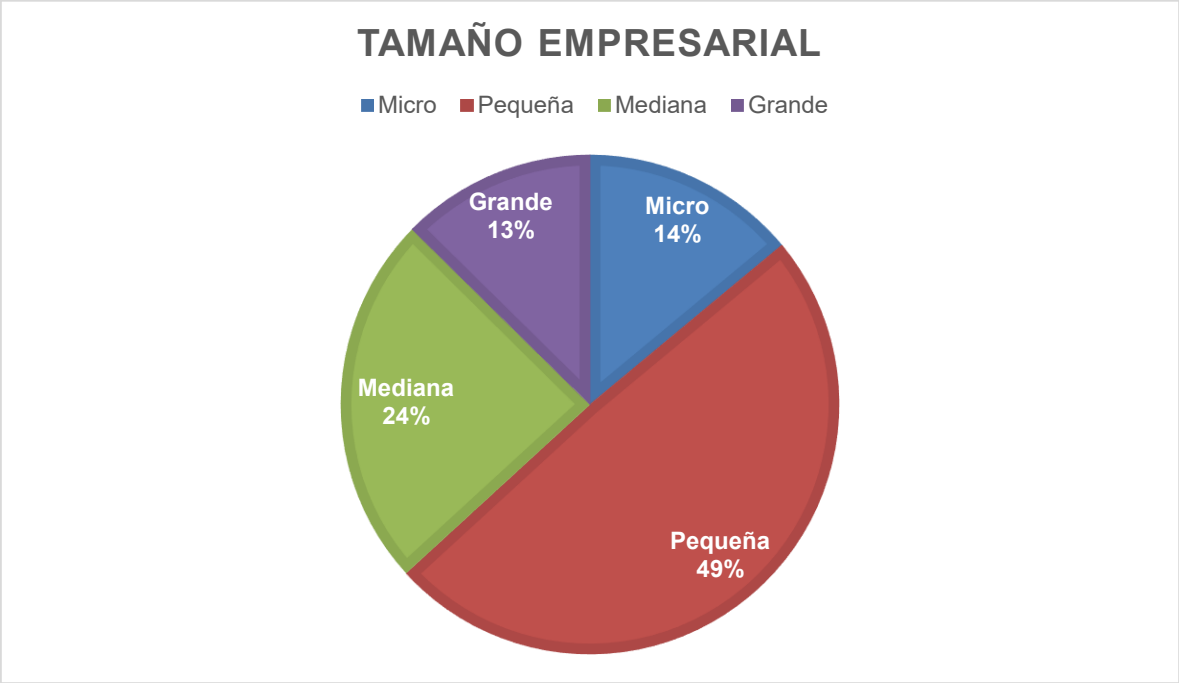
Por otra parte, el Decreto 957 del 5 de junio de 2019 "Por el cual se adiciona el capítulo 13 al Título 1, de la Parte 2 del Libro 2, del Decreto 1074 de 2015, Decreto Único del Sector Comercio, Industria y Turismo, y se reglamenta el artículo 2° de la Ley 590 de 2000, modificado por el artículo 43 de la Ley 1450 de 2011.", que entró en vigencia en junio de 2019, establece los tamaños de las empresas de la siguiente manera:

Tabla 6– Rangos para definición del Tamaño Empresarial.

SECTOR	MICRO	PEQUEÑA	MEDIANA
Manufacturero	Inferior o igual a 23.563 UVT.	Superior a 23.563 UVT e inferior o igual a 204.995 UVT.	Superior a 204.995 UVT e inferior o igual a 1'736.565 UVT.
Servicios	Inferior o igual a 32.988 UVT.	Superior a 32.988 UVT e inferior o igual a 131.951 UVT.	Superior a 131.951 UVT e inferior o igual a 483.034 UVT.
Comercio	Inferior o igual a 44.769 UVT.	Superior a 44.769 e inferior o igual a 431.196 UVT.	Superior a 431.196 UVT e inferior o igual a 2'160.692 UVT.

Por otro lado, se deberá tener en cuenta la regulación que en materia de determinación de UVT expedida por la autoridad competente, y en ese sentido establecer una distribución de tamaños empresariales de acuerdo con la siguiente gráfica:

Gráfica 4 – Distribución del tamaño empresarial de acuerdo con la muestra representativa tomada.



Respecto al tamaño empresarial, Colombia Compra Eficiente evidenció que, del total de la muestra, se obtuvo como resultado que el 87% corresponden a MiPymes y el 13% a grandes empresas. Con base en el análisis anterior, Colombia Compra Eficiente considera relevante incluir criterios que permitan la participación de las Microempresas.

4.3. Economía Popular

A partir de la identificación de proveedores, Colombia Compra Eficiente evidenció la necesidad de incluir al presente Mecanismo de Agregación de Demanda elementos que promuevan la participación de la Economía Popular, teniendo como objetivo desarrollar e impulsar políticas públicas y herramientas orientadas a la organización y articulación de los partícipes del Sistema de Compra Pública, con el fin de lograr una mayor eficiencia, transparencia y optimización de los recursos del Estado.

Ahora bien, el Plan Nacional de Desarrollo (PND) 2022-2026 "Colombia Potencia Mundial de la Vida", aprobado mediante la Ley 2294 del 19 de mayo de 2023, contempla como pilares: la Paz total, la Lucha contra el hambre, la Transición Energética, la Transparencia y la Economía Popular y Comunitaria, a través de los cuales establece unos mandatos y líneas estratégicas en relación con la contratación y compras públicas en el país, que incluye, entre otros:

- Sostenibilidad y crecimiento de las unidades económicas y formas de asociatividad de la Economía Popular y su participación en el sistema de compras y contratación pública.

- Promoción de la participación de organizaciones de pequeños productores, pescadores artesanales y de mujeres rurales en las compras públicas locales de alimentos.

- Reindustrialización para la sostenibilidad, el desarrollo económico y social, que incorpora una política de compras públicas para la reindustrialización, mecanismos para que las empresas públicas y mixtas realicen inversiones estratégicas.

- Desarrollo de una estrategia para impulsar las compras públicas de innovación.

  Para atender los mandatos descritos, se requiere de un cambio técnico y cultural que permita ampliar el acceso al Sistema de Compras y Contratación Pública, para que las compras del Estado sean estratégicas y atiendan a las necesidades planteadas. En este contexto, se ha identificado que la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente - debe reorientar sus objetivos, procesos y acciones, para lo cual se ha planteado atender, entre otros, los siguientes aspectos:

  - Ampliar e incluir la participación de actores interesados en los procesos de compra y contratación pública que no han sido incluidos hasta la fecha, como es el caso de los actores pertenecientes a la Economía Popular. Para lograrlo, la Agencia debe realizar una serie de diseños orientados a la ampliación de su oferta y alcance en materia de transferencia de conocimiento; la transformación de sus procedimientos, instrumentos y herramientas; la adaptación de su normatividad, en clave de estos nuevos actores que se integran a la contratación pública. Todo lo

anterior, en el marco de una democratización del Sistema de Compras y Contratación Pública, con un enfoque territorial.

- Fortalecimiento de las plataformas y el Sistema de Compras y Contratación Pública mediante la interoperabilidad de los sistemas de información y plataformas del Estado y de los particulares, garantizando la gobernanza de información y permitiendo el uso de las Tecnologías de la Información y las Comunicaciones (TIC) para que la economía popular, y los demás actores del Sistema de Compras y Contratación Pública puedan proveer directamente al Estado, usando herramientas como la Tienda Virtual del Estado Colombiano a través de Instrumentos de Agregación de Demanda Dinámicos (AMP/SDA) para compras a actores de la Economía Popular.

- El diseño y organización de Sistemas Dinámicos de Adquisición como atributos de Mecanismos de Agregación de Demanda enfocados en la inclusión de los actores de la Economía Popular, de acuerdo con las directrices establecidas en el Plan Nacional de Desarrollo (PND), entre otras iniciativas.

Debe resaltarse que de conformidad con lo establecido en el artículo 102 de la Ley 2294 de 2023 (PND 2022-2026), la ANCP-CCE debe diseñar y organizar los Sistemas Dinámicos de Adquisición, los cuales técnicamente son un conjunto de condiciones que permiten la operación flexible y dinámica de los Mecanismos de Agregación de Demanda. Además, durante su vigencia cada mecanismo permitirá el ingreso de nuevos proveedores, es decir, Colombia Compra Eficiente dará apertura de ventanas de ingreso, en determinados periodos de tiempo, para la habilitación de nuevos proveedores.

Entre los mencionados mecanismos, Colombia Compra Eficiente estructurará Mecanismos de Agregación de Demanda Dinámicos AMP/SDA, como el especificado en el presente documento.

Adicionalmente, el artículo ibidem establece en su inciso tercero que "La Agencia Nacional de Contratación Pública - Colombia Compra Eficiente podrá realizar procesos de contratación cuyos oferentes sean actores de la economía popular. En dichos casos no se requerirá la presentación del RUP para participar en el proceso de selección." Así las cosas, queda claro que la norma faculta a Colombia Compra Eficiente para adelantar la estructuración de Mecanismos de Agregación

de Demanda con características o atributos Dinámicos, cuyos proveedores solamente podrán ser actores de la economía popular.

Lo anterior, con el objetivo de que los interesados que cumplan los requisitos se adhieran a estos mecanismos mediante la habilitación en los términos definidos en los documentos del proceso.

No obstante, la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente aclara que en cumplimiento al principio de contratación estatal "Selección Objetiva" definido en el artículo 5 de la Ley 1150 de 2007, solicitará la acreditación de experiencia a los interesados mediante certificaciones contractuales las cuales deberán cumplir con los requisitos definidos en el presente documento.

Adicionalmente, y de conformidad con el artículo 102 Ley 2294 de 2023 (PND 2022-2026) la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente -, ha diseñado y organizado un Mecanismo de Agregación de Demanda Dinámico para el cual se habilitarán unidades económicas cuyo tamaño se encuentre en la clasificación Microempresa, puesto que, de conformidad con las bases del Plan Nacional de Desarrollo – PND, este tipo de empresas forman parte de los actores de la Economía Popular, definida de la siguiente manera:

"La economía popular se refiere a los oficios y ocupaciones mercantiles (producción, distribución y comercialización de bienes y servicios) y no mercantiles (domésticas o comunitarias) desarrolladas por unidades económicas de baja escala (personales, familiares, micronegocios o microempresas), en cualquier sector económico. Los actores de la EP pueden realizar sus actividades de manera individual, en unidades económicas, u organizados de manera asociativa." Negrita fuera de texto.

En dicho contexto, el presente Mecanismo de Agregación de Demanda Dinámico para compras a actores de la Economía Popular puede constituirse en un instrumento que permitirá a dichos actores superar las barreras de acceso al mercado de la compra pública; teniendo como resultado el fortalecimiento, aumento en la productividad y desarrollo para los actores de la Economía Popular.

4.4. Fomento a emprendimientos y empresas de mujeres y demás sectores poblacionales de especial protección

Colombia cuenta con un marco jurídico de protección a aquellas personas que debido a su particular condición física, psicológica o social merecen una acción positiva estatal para efectos de lograr una igualdad real y efectiva. Dentro de esta categoría denominada "sujetos de especial protección constitucional", se encuentran, entre otros, las víctimas del conflicto armado interno, las mujeres cabeza de familia, los adultos mayores, las personas en condición de discapacidad, así como la población de las comunidades indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitanas.

Así, en la contratación pública se contemplan medidas afirmativas, cuyo objetivo es incentivar la participación de estos sujetos de especial protección constitucional y de otras personas discriminadas históricamente del sistema de compras públicas y del mundo laboral en general, como las mujeres.

Adicionalmente, en los últimos años se han adoptado estímulos tendientes a fortalecer las micro, pequeñas y medianas empresas como un generador de empleo en el país y como motor de crecimiento y reactivación económica, principalmente después de la pandemia generada por el Covid-19.

En efecto, en el Informe de Dinámica de Creación de empresas del año 2021 de Confecámaras, se concluyó que las nuevas unidades productivas están conformadas principalmente por microempresas en un porcentaje de 99,5 %, seguido por las pequeñas empresas que representan el 0,4 % y el restante se encuentra en las medianas y grandes empresas cuyo valor es el cero coma cero tres por ciento 0,03 %.

Por su parte, en el Informe de Dinámica de Creación de Empresas del año 2022, se evidenció que "las nuevas unidades productivas están conformadas por microempresas (99,69%), seguido por las pequeñas empresas (0,30%) y el restante se encuentra en las medianas y grandes empresas (0,01%)".

Así mismo, en este mismo informe para el año 2023, se concluyó que, durante ese año, se crearon 78.428 empresas como sociedades, de las cuales 77.505 eran microempresas, 883 pequeñas, 34 medianas y 6 grandes. Por otro lado, se crearon 227.569 empresas constituidas como personas naturales, de las cuales 227.377 eran microempresas, 167 pequeñas, 20 medianas y 5 grandes.

A pesar de lo anterior, en estudio realizado por la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente-, desde la Subdirección de Estudios de Mercado de Abastecimiento Estratégico, se demostró, a partir de la revisión de las empresas u organizaciones registradas en la plataforma del

SECOP, que el 85% de los proveedores registrados son grandes empresas y un 15% corresponde a micro, pequeñas y medianas empresas.

Los datos presentados demuestran que pese a la importancia que tienen las micro y pequeñas empresas para la economía del país, el acceso a la contratación pública es aún muy limitado.

Por lo expuesto, resulta indispensable incorporar criterios diferenciales (requisitos habilitantes diferenciales y puntajes adicionales) en este proceso de selección, para fortalecer el acceso de las mujeres, los sujetos de especial protección constitucional y las MiPymes al sistema de compras públicas, lo cual también garantizará mayor nivel de concurrencia de oferentes y, con ello, economía y eficiencia administrativa. Lo anterior, en cumplimiento de los artículos 31, 32, 33 y 34 de la Ley 2060 de 2020, reglamentados por el Decreto 1860 de 2021.

4.4.1. Emprendimientos y empresas de mujeres

Según las mesas de trabajo realizadas por Colombia Compra Eficiente, no se puede determinar un porcentaje de participación de emprendimientos y empresas de mujeres en el sector, pero sí se puede afirmar que existen empresas de mujeres en el sector. Por tal razón, se establecerá dentro de los factores ponderables del proceso de contratación, el otorgamiento de un puntaje adicional de hasta el cero punto veinticinco por ciento (0.25%) del valor total de los puntos establecidos.

En relación con los requisitos habilitantes, considerando el histórico de los criterios diferenciales aplicados en los mecanismos de agregación de demanda desde el Decreto 1860 de 2021, se establecerá como criterio diferencial el valor de la garantía de seriedad de la oferta en favor de los proponentes que acrediten tener emprendimientos y empresas de mujeres, en los términos del artículo 2.2.1.2.4.2.14. del Decreto 1082 de 2015.

4.4.2. Fomento a la ejecución de contratos estatales por parte de la población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional.

El Gobierno Nacional expidió el Decreto 1860 de 24 de diciembre de 2021, el cual adicionó el artículo 2.2.1.2.4.2.16 a la Subsección 2 de la Sección 4 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, Único

Reglamentario del Sector Administrativo de Planeación Nacional. Esto para desarrollar el inciso cuarto del artículo 34 de la Ley 2069 de 2020, el cual dispone que "[…] en los pliegos de condiciones dispondrán, de mecanismos que fomenten en la ejecución de los contratos estatales la provisión de bienes y servicios por población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y, sujetos de especial protección constitucional en las condiciones que señale el reglamento; siempre que se garanticen las condiciones de calidad y cumplimiento del objeto contractual".

La aplicación del artículo 2.2.1.2.4.2.16 del Decreto 1082 de 2015, que se traduce en la inclusión de obligaciones a cargo del contratista cuyo incumplimiento podría acarrearle sanciones pecuniarias, no es automática en todos los procesos de selección iniciados a partir de la vigencia del Decreto 1860 de 2021. Esto ya que el incentivo, además de garantizar las condiciones de calidad y el cumplimiento adecuado del objeto contractual sin perjuicio de los acuerdos comerciales suscritos por el Estado colombiano, también está supeditado al análisis previo de oportunidad y conveniencia en los documentos del Proceso.

Así las cosas, conforme a lo explicado en la memoria de la reglamentación, es necesario considerar que la regla de fomento:

"[…] además de estar condicionada por un desarrollo normativo posterior, está limitada en el sentido que los mecanismos que se implementen para incentivar la provisión de bienes y servicios por población en pobreza extrema, desplazados por la violencia, personas en procesos de reintegración y reincorporación, o sujetos de especial protección constitucional, no afecten las condiciones de calidad y cumplimiento del objeto contractual. En ese sentido, cuando la norma se refiere al desarrollo reglamentario posterior, lo que hace es confiar al decreto la definición de reglas que permitan que los mecanismos que introduzcan las entidades en sus pliegos de condiciones y documentos equivalentes no atenten contra el debido cumplimiento del objeto contractual. Por tanto, la inclusión de los mecanismos de fomento mencionados en inciso 4 del artículo 34 de la Ley 2069 en los pliegos de condiciones, e incluso en las obligaciones del contrato, es un asunto que compete a las entidades contratantes, dentro del marco que determine el reglamento"

Así las cosas, corresponde a la Agencia en el marco del proceso de estructuración valorar criterios políticos, técnicos o de mera oportunidad o conveniencia (económica, social, organizativa), y determinar la ventaja de la incorporación de reglas y obligaciones sin que se vea afectado el desarrollo del objeto contractual.

Para el presente proceso se determinó no incluir en cabeza de los proveedores adjudicatarios obligaciones específicas de provisión de servicios o bienes por parte de la población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional. Se fundamenta esta decisión en que, se requiere el cumplimiento de condiciones técnicas mínimas por tratarse de los servicios de ciberseguridad que son ejecutados por perfiles expertos certificados y no se identificó la contratación de esta población en los documentos enviados por las diferentes empresas que hacen parte del sector.

4.4.3. Mipymes

Como se señaló en el acápite 4.2 del presente documento, a partir de la información extraída de la plataforma EMIS (Emerging Markets Group Company) y del análisis del mercado nacional de ciberseguridad, Colombia Compra Eficiente identificó que la mayoría de las empresas cuya actividad principal corresponde a servicios de ciberseguridad se clasifican como Micro, Pequeñas y Medianas Empresas (MiPymes), evidenciándose una participación significativamente mayor de este tipo de empresas frente a las grandes compañías del sector.

Estos resultados confirman la predominancia de las MiPymes en el sector de ciberseguridad, así como su relevancia en la prestación de servicios especializados, innovación tecnológica y atención de nichos específicos del mercado.

En atención a lo dispuesto en la Ley 2069 de 2020 y en el Decreto 1082 de 2015, en particular lo establecido en el artículo 2.2.1.2.4.2.18, y con fundamento en el análisis de las condiciones económicas del sector, Colombia Compra Eficiente establecerá condiciones habilitantes diferenciales orientadas a promover y facilitar la participación efectiva de las MiPymes en el presente Proceso de Selección, sin afectar los principios de selección objetiva, eficiencia y transparencia.

Adicionalmente, considerando la experiencia acumulada en la aplicación de criterios diferenciales en los Mecanismos de Agregación de Demanda, conforme a lo dispuesto en el Decreto 1860 de 2021, se definirá como criterio diferencial específico para las MiPymes la reducción del valor de la garantía de seriedad de la oferta, como medida concreta de fomento a su participación en el Sistema de Compras Públicas.

4.4 Características de los productos que ofrece el mercado

Respecto a la tipología de productos que ofrece el mercado se cuenta con los siguientes, por solo mencionar algunos a modo de ejemplo:

Tipo / Segmento	Familia de productos	Descripción funcional	Ejemplos comerciales / marcas
1. Seguridad de Infraestructura y Red	**Firewalls de nueva generación (NGFW)**	Filtrado de tráfico, inspección profunda de paquetes, control de aplicaciones, VPN y segmentación de red.	*Fortinet FortiGate, Palo Alto PA-Series, Cisco Firepower, Check Point Quantum, Huawei USG*
	IPS/IDS – Sistemas de prevención/ detección de intrusiones	Detectan y bloquean ataques de red, exploits y comportamientos anómalos.	*Snort, Suricata, Trend Micro TippingPoint, Cisco Secure IPS*
	WAF / Web Application Firewall	Protección específica de aplicaciones web ante ataques OWASP (SQLi, XSS, etc.).	*F5 Advanced WAF, Imperva, Akamai Kona Site Defender, Cloudflare WAF*
	Anti-DDoS / Mitigación Distribuida	Defensa contra ataques de denegación de servicio.	*Radware DefensePro, Arbor Networks, Cloudflare Magic Transit*
	Proxy / Secure Web Gateway / SD-WAN seguro	Control de navegación, filtrado de contenidos y conexión segura entre sedes.	*Zscaler, Forcepoint SWG, Palo Alto Prisma SD-WAN, Cisco Meraki SD-WAN*
2. Seguridad de Endpoints y Dispositivos	**EPP / EDR / XDR**	Protección, detección y respuesta ante amenazas en estaciones de trabajo, servidores y dispositivos móviles.	*CrowdStrike Falcon, Microsoft Defender, SentinelOne, Trellix, Sophos Intercept X, Trend Micro Apex One*
	MDM / MAM / Gestión de dispositivos móviles	Control de acceso, apps y datos corporativos en smartphones, tablets o IoT.	*Microsoft Intune, VMware Workspace ONE, IBM MaaS360, MobileIron*
	Control de periféricos y	Previene copias o fugas de información mediante medios externos.	*Symantec Endpoint Encryption, BitLocker, Sophos Device Control*

	cifrado de disco		
3. Gestión de Identidades y Accesos (IAM/PAM)	**MFA / SSO / Federación de identidades**	Controla el acceso seguro con múltiples factores y sesiones unificadas.	*Okta, Microsoft Entra ID, Ping Identity, ForgeRock, Duo Security*
	PAM / Accesos privilegiados / IGA	Controla y audita accesos de administradores y cuentas críticas.	*CyberArk, BeyondTrust, One Identity Safeguard, Delinea*
4. Protección de Datos y Continuidad	**DLP / Prevención de fuga de datos**	Monitorea y bloquea exfiltración de información sensible.	*Forcepoint DLP, Symantec DLP, Digital Guardian, Trellix DLP*
	Backup / DRP / BCP / Cifrado	Recuperación ante incidentes y continuidad del negocio.	*Veeam, Commvault, Veritas NetBackup, Acronis Cyber Protect, Dell EMC Avamar*
5. Seguridad en la Nube y Aplicaciones	**CSPM / CWPP / CNAPP / CASB / SASE / ZTNA**	Aseguran configuraciones, cargas de trabajo y accesos en entornos cloud e híbridos.	*Zscaler, Netskope, Palo Alto Prisma Cloud, Wiz, Orca Security, Check Point CloudGuard*
	DevSecOps / Seguridad en ciclo de desarrollo	Integración de seguridad en CI/CD y análisis de código.	*SonarQube, Checkmarx, Veracode, GitLab Secure*
	CDN / Protección web / API Security	Mejora el rendimiento y seguridad de aplicaciones distribuidas.	*Akamai, Cloudflare, Imperva, Fastly*
6. Monitoreo, Orquestación y Automatización	**SIEM / SOAR / Threat Intelligence / BAS**	Plataformas de análisis de logs, correlación de eventos, simulación de ataques y automatización de respuesta.	*Splunk, IBM QRadar, Microsoft Sentinel, Exabeam, Rapid7 InsightIDR, Mandiant Advantage, ThreatConnect*
7. Servicios Gestionados y Operaciones de Seguridad	**SOC-as-a-Service / MDR / DFIR / Threat Hunting / CNOC**	Servicios gestionados de detección, monitoreo, análisis forense y respuesta ante incidentes.	*Mandiant (Google Cloud), IBM Security, Secureworks, Telefónica Tech, Claro, Deloitte, EY, KPMG*

8. Consultoría y Gobierno en Ciberseguridad	**Auditorías, Pentesting, Red Teaming, ISO 27001, NIST, MSPI**	Evaluaciones técnicas y normativas, implementación de SGSI/MSPI, concienciación y formación.	*PwC, KPMG, EY, Deloitte, BDO, NCC Group, ISACA Partners*

4.5 Estructura de costos

La estructura de costos de los **servicios de ciberseguridad** se caracteriza por su **alta dependencia del componente humano especializado**, el uso intensivo de **tecnologías avanzadas** y la necesidad de mantener **capacidades operativas permanentes**, lo cual introduce variabilidad en los costos según el tipo de servicio, el nivel de madurez requerido y el alcance de la prestación.
A partir del análisis del mercado y de la información recopilada en el Estudio del Sector, se identifican como principales componentes de la estructura de costos los siguientes:

1. **Talento humano especializado:** Incluye profesionales con perfiles técnicos y estratégicos en ciberseguridad, tales como analistas SOC, ingenieros de seguridad, arquitectos de seguridad, especialistas en respuesta a incidentes, gestores de riesgos y auditores. Este componente representa uno de los mayores costos del sector, debido a la escasez de talento, la alta rotación y la necesidad de formación continua.

2. **Licenciamiento y uso de herramientas tecnológicas:** Comprende los costos asociados a plataformas de monitoreo, detección y respuesta (SIEM, SOAR, EDR, XDR), herramientas de gestión de vulnerabilidades, soluciones de identidad y acceso, y demás tecnologías necesarias para la prestación de los servicios de ciberseguridad, ya sea bajo esquemas de licenciamiento propio, suscripción o uso como servicio.

3. **Infraestructura tecnológica y operativa:** Incluye los costos de infraestructura física o en la nube requeridos para la operación de centros de seguridad, almacenamiento y procesamiento de información, así como la disponibilidad de ambientes seguros, redundantes y con altos niveles de disponibilidad.

4. **Gestión de continuidad y resiliencia operacional:** Considera los costos asociados a planes de continuidad del negocio,

recuperación ante desastres, pruebas periódicas, redundancia de personal y plataformas, y demás medidas orientadas a garantizar la prestación ininterrumpida de los servicios.

5. **Cumplimiento normativo y marcos de referencia:** Incluye los costos derivados de la implementación y mantenimiento de marcos de gestión y buenas prácticas en seguridad de la información y ciberseguridad, tales como el **Modelo de Seguridad y Privacidad de la Información (MSPI)**, estándares internacionales o sus equivalentes, así como auditorías internas o de terceros que permitan verificar su cumplimiento.

6. **Soporte, actualización y mejora continua:** Comprende los costos relacionados con la actualización permanente de herramientas, metodologías y capacidades técnicas, la atención de incidentes, el soporte especializado y la adaptación a nuevas amenazas y riesgos emergentes.

La combinación y peso relativo de estos componentes varía según el **segmento del servicio de ciberseguridad**, el nivel de criticidad del servicio, los acuerdos de niveles de servicio (SLA) y las condiciones particulares de cada Entidad Compradora. En consecuencia, no es posible establecer una estructura de costos uniforme ni precios de referencia generales aplicables a todos los servicios.

Este análisis de la estructura de costos respalda la decisión de **no fijar precios de referencia en el Acuerdo Marco de Precios**, permitiendo que las condiciones económicas se definan de manera competitiva en la etapa de operación, de acuerdo con las necesidades específicas de las Entidades Compradoras y las ofertas presentadas por los Proveedores habilitados.

Tabla 7– Variables que componen la estructura de costos de los servicios de ciberseguridad

Variable	Incidencia en el costo
Talento humano	Alta
Licenciamiento	Alta
Infraestructura	Media
SLA	Alta
Continuidad	Media
Cumplimiento	Media
Soporte y mejora	Media

Variable	Incidencia en el costo
Administración	Baja
Margen y riesgo	Variable

4.6 Análisis financiero del sector (Indicadores financieros y organizacionales)

A partir de una muestra representativa tomada de los posibles proveedores que se encuentran asociados a la labor de prestación del servicio de Nube Pública en Colombia, empleando como herramienta la base de datos con los resultados de EMIS, se obtuvo la información financiera de los proveedores que su actividad principal corresponde a los códigos CIIU:

- 6202: Actividades de consultoría informática y actividades de administración de instalaciones informáticas.
- 6209: Otras actividades de tecnologías de información y actividades de servicios informáticos.

En ese sentido, se obtuvo:

Tabla 8– Indicadores financieros y de organización muestra representativa

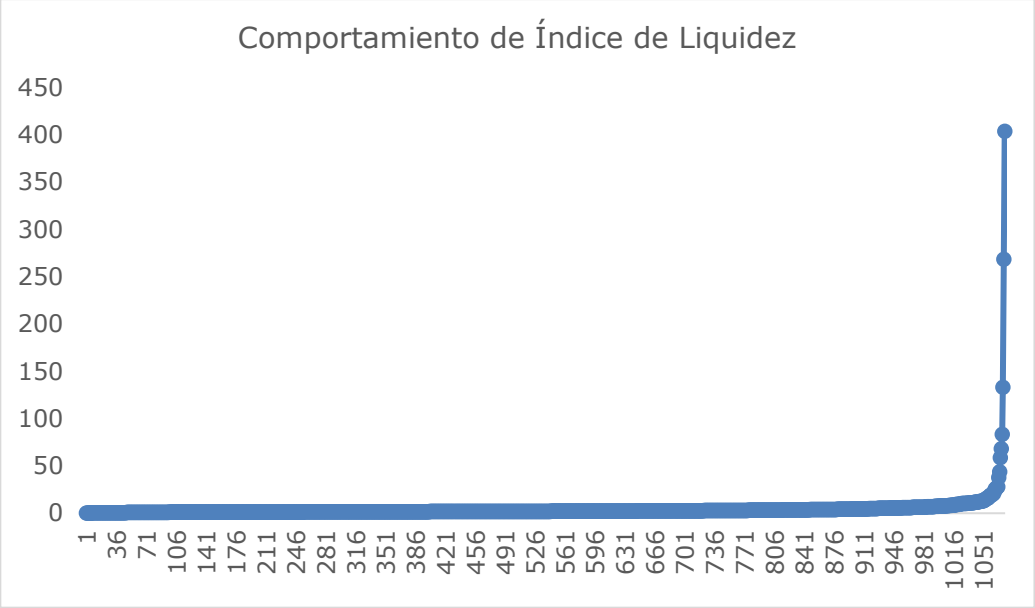
	Índice de Liquidez	Endeudamiento	Razón de cobertura de intereses	Rentabilidad Patrimonio	Rentabilidad Activo
Mínimo	0,09	0,00	0,83	-58,65	-34,69
Promedio	3,93	0,58	0,83	0,19	0,04
Mediana	1,96	0,51	0,83	0,17	0,07
Máximo	403,49	11,85	0,83	44,66	1,19

Posteriormente, la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente- realizó un análisis a través del concepto de percentiles para estadísticamente establecer los indicadores financieros, considerando cada uno en función de dos criterios principales, el percentil 15 y el percentil 85.

De dicho análisis se obtuvo:

4.6.1 Índice de liquidez

Gráfica 5 – Comportamiento del Índice de liquidez de la muestra representativa.



Analizado por percentiles:

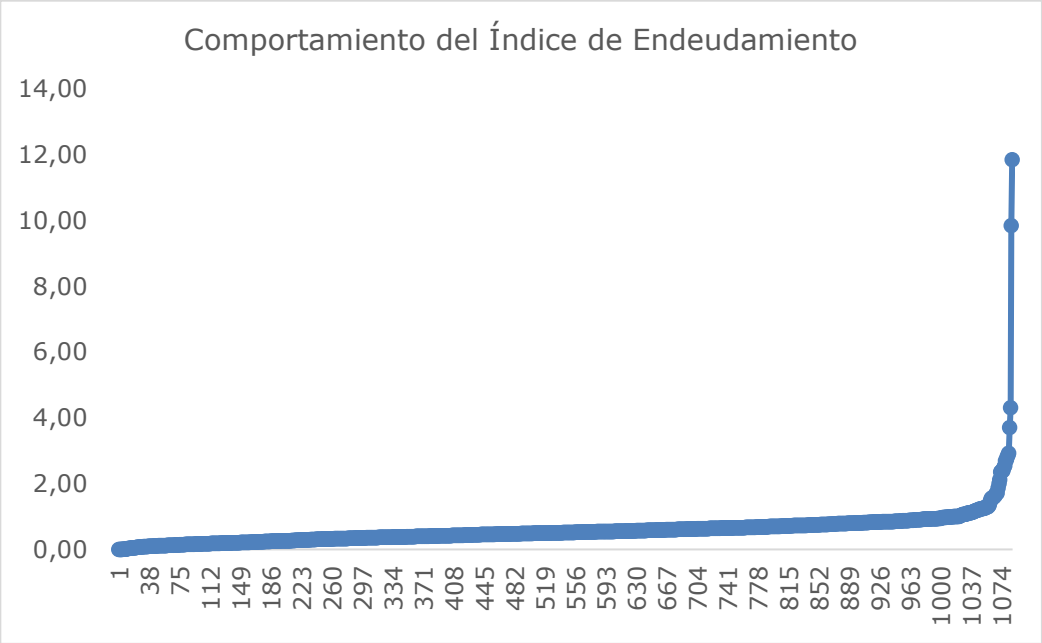
Tabla 9– Análisis a través de percentiles del Índice de liquidez.

Percentil	Valor
0,1	1,01
0,15	1,13
0,2	1,24
0,3	1,46
0,4	1,71
0,5	1,96
0,6	2,33
0,7	2,87
0,8	3,85
0,9	6,06
1	403,49

En ese sentido se consideró el percentil 15 para fijar el índice de liquidez, teniendo en cuenta que el 85 % de la muestra cumpliría con dicho valor.

4.6.2 Nivel de endeudamiento

Gráfica 6 – Comportamiento del Nivel de Endeudamiento.



Analizado por percentiles:

Tabla 10– Análisis a través de percentiles del nivel de endeudamiento.

Percentil	Valor
0,1	0,18
0,2	0,28
0,3	0,37
0,4	0,44
0,5	0,51
0,6	0,59
0,7	0,66
0,8	0,77
0,85	0,84
0,9	0,91
1	11,85

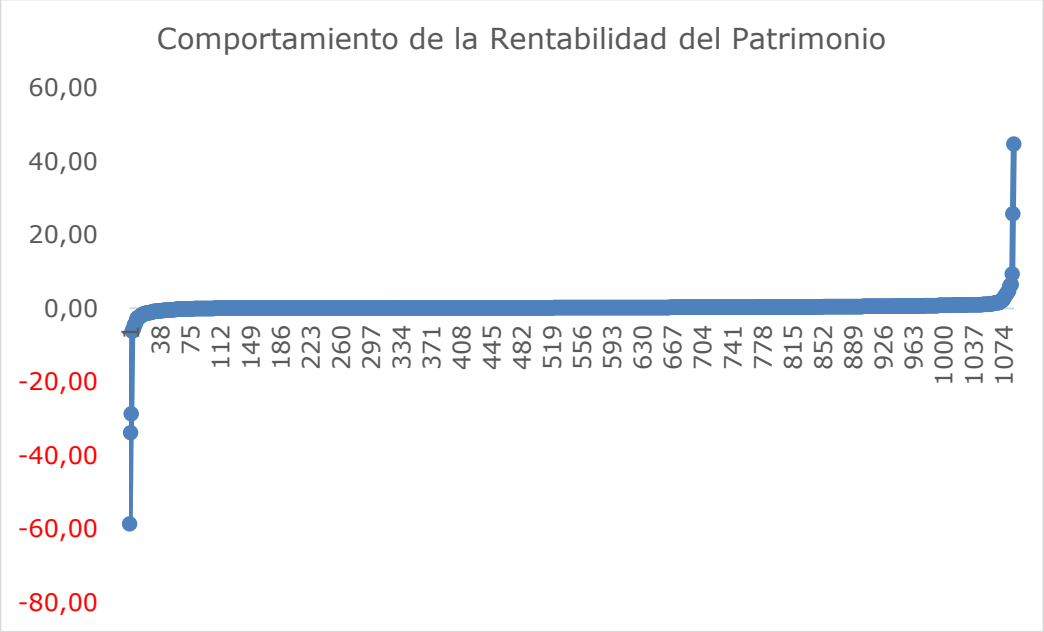
En ese sentido se consideró el percentil 85 para fijar el nivel de endeudamiento, teniendo en cuenta que el 85 % de la muestra cumpliría con dicho valor.

4.6.3 Razón de cobertura de intereses

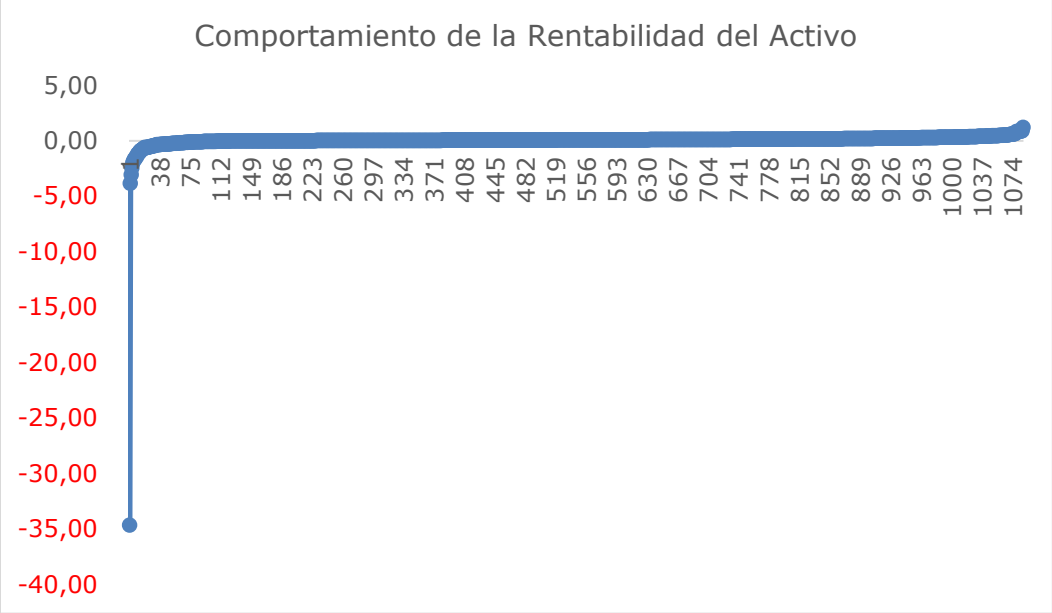
Considerando que este indicador se encuentra en función de la utilidad operación y los gastos de intereses, se tuvo el mismo como indeterminado por las siguientes dos situaciones: 1) no todas las empresas reportaron los gastos de intereses o 2) no reportaron la información acerca de su utilidad operación y en algunos casos no hubo reporte de ninguno de dichos valores. Por tal motivo, la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente- no pudo establecer cifras para analizar; no obstante, en función de la definición de este indicador y las variables que lo conforman, fue fijado como valor mínimo de 1,00.

4.6.4 Rentabilidad del patrimonio y del activo

Gráfica 7 – Comportamiento de la rentabilidad del patrimonio.



Gráfica 8 – Comportamiento de la rentabilidad del activo



Analizando por percentiles:

Tabla 11– Análisis a través de percentiles de la rentabilidad del patrimonio.

Percentil	Valor
0,1	0,00
0,2	0,03
0,3	0,08
0,4	0,12
0,5	0,17
0,6	0,24
0,7	0,32
0,8	0,46
0,9	0,68
1	44,66

Tabla 12– Análisis a través de percentiles de la rentabilidad del activo.

Percentil	Valor
0,1	-0,05
0,2	0,01
0,3	0,03
0,4	0,05
0,5	0,07
0,6	0,10
0,7	0,13
0,8	0,18

0,9	0,29
1	1,19

En ese sentido se consideró el percentil 20 para fijar los indicadores de rentabilidad del patrimonio y rentabilidad del activo, teniendo en cuenta que el 80% de la muestra cumpliría con dicho valor.

4.6.5 Consolidado de indicadores

El consolidado de indicadores financieros producto del estudio sectorial realizado es:

Tabla 13– Consolidado de Indicadores financieros y organizacionales**.**

	Valor
Liquidez	Mayor o igual a 1,13
Endeudamiento	Menor o igual al 84%
Razón de cobertura de intereses	Mayor o igual a 1,00
Rentabilidad patrimonio	Mayor o igual a 0,03
Rentabilidad activa	Mayor o igual a 0,01

5 ANÁLISIS DE LA DEMANDA

Colombia Compra Eficiente busca a través del análisis de la demanda de las Entidades Estatales, determinar las necesidades de estas para la adquisición de los bienes y servicios de ciberseguridad, a través del análisis de sus procesos de contratación, así como de otras variables vinculadas a dicho análisis.

Para completar esta información, Colombia Compra Eficiente sostuvo reuniones con el Gremio, Grupos de interés, entre otros y realizó mesas de trabajo con fabricantes, distribuidores, integradores y con entidades estatales interesadas en contratar estos servicios, de acuerdo con data obtenida en SECOP I y II.

5.4 Análisis de la contratación de las Entidades Estatales

Todas las Entidades Estatales cuyo régimen jurídico en materia contractual se sujete a las disposiciones contenidas en el Estatuto General de Contratación de la Administración Pública están obligadas a adquirir bienes y servicios de condición técnica uniforme y común utilización a través del Acuerdo Marco, sin distingo de que el trámite precontractual sea adelantado a través de las

plataformas del SECOP I o II. Lo anterior de conformidad con lo consagrado en la Ley 1955 de 2019.

Con el fin de conocer la forma en que las Entidades Estatales contratan los servicios de ciberseguridad, la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente- revisó la información de contratación disponible en las diferentes plataformas de SECOP I y II en series históricas.

Para seleccionar la muestra del SECOP, Colombia Compra Eficiente realizó un filtro de los procesos y contratos suscritos por las Entidades Estatales para los bienes y servicios relacionados con ciberseguridad, durante las vigencias 2023, 2024 y 2025, con las siguientes palabras claves:

Centro de seguridad, Security Operations Center, Centro de Operaciones de Red, ciberataques, Continuidad de la operación, NOC, seguridad en la nube, forense, informática forense, antispyware, antivirus, ciberseguridad, firewall, seguridad de la información y WAF.

La información encontrada por Colombia Compra Eficiente se resume de la siguiente manera a partir del portal de Datos Abiertos (https://www.datos.gov.co/browse?q=secop&sortBy=relevance):

Tabla 14– Número de procesos de Ciberseguridad en plataformas Secop

No.	SECOP	Procesos
1	I	30
2	II	209

Fuente: Datos abiertos

Gráfica 9 –Procesos por plataforma -Años 2023-2025

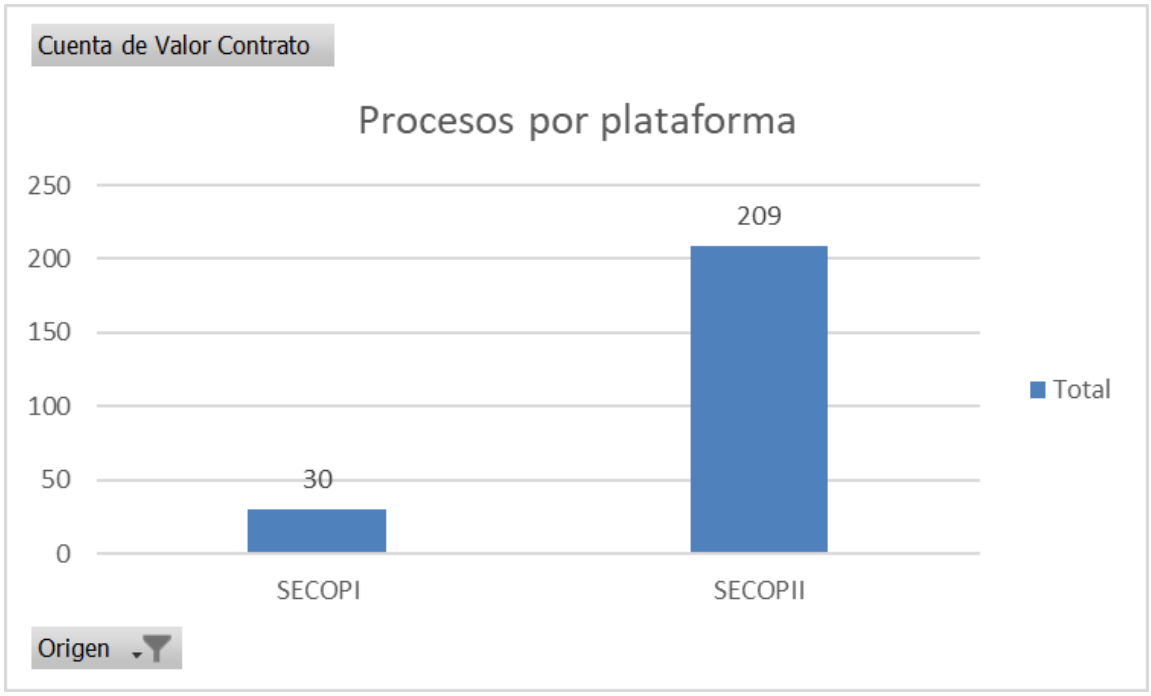


Tabla 15– Valor de los contratos en SECOP para Ciberseguridad.

No.	SECOP	Valor de los contratos
1	I	$ 4.584.944.878
2	II	$375.893.157.551

Fuente: Datos abiertos

Gráfica 10 - Valor contratos por plataforma -Años 2023-2025

Podemos identificar que el gran volumen de contratación se tranzó a través de SECOP II, con un 87.45% con respecto al valor total, cumpliendo así la obligatoriedad de uso de los Acuerdos Marco, como también aprovechando los beneficios de uso de esto mecanismos de agregación de demanda.

De igual forma, observamos la tendencia de contrataciones por año:

Gráfica 11 – Tendencia de valor de las contrataciones por vigencias 2023 - 2025

Fuente: Datos abiertos

Se aprecia una variación relevante en el valor de la contratación; sin embargo, hay un incremento importante en el número de procesos de contratación, del 2023 al 2024, reflejando el interés de las entidades estatales por proteger sus sistemas informáticos y lo más valioso: la información.

Adicional, se analiza el comportamiento de la contratación a nivel regional, observando la distribución de los procesos de contratación en los diferentes municipios del país, evidenciando una alta participación de Bogotá; le siguen Bucaramanga, Manizales, Cali, Barranquilla y Medellín; en el resto de los municipios menor participación.

Se muestra a continuación el top 10:

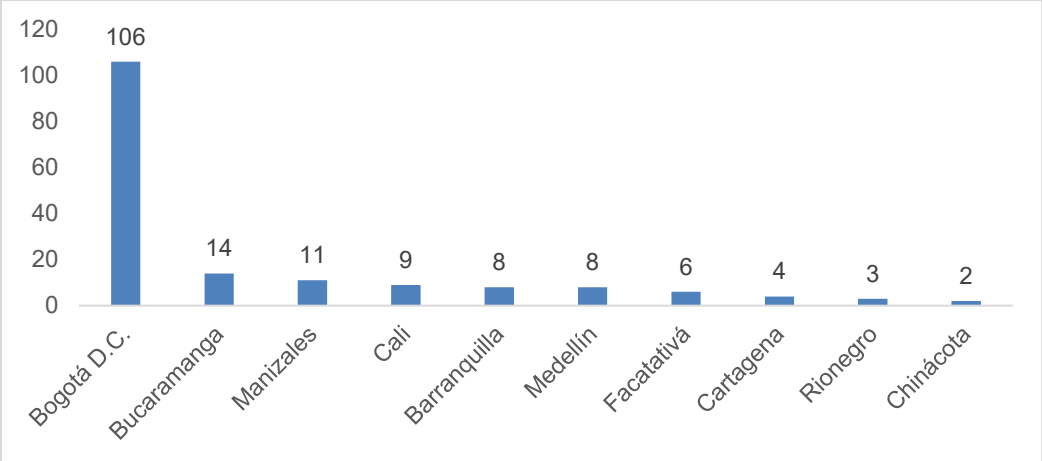
Tabla 16– Top 10 -Ubicación geográfica de los procesos

Municipio	No. procesos
Bogotá D.C.	106
Bucaramanga	14
Manizales	11
Cali	9
Barranquilla	8
Medellín	8
Facatativá	6
Cartagena	4
Rionegro	3
Chinácota	2

Fuente: Datos abiertos

Podemos observar que no hay participación de todos los municipios del país, lo que conlleva a pensar en estrategias de educación para la prevención de riesgos digitales y protección de la información.

Gráfica 12 – Ubicación geográfica de los procesos



5.4.1 Identificación de las principales Entidades Estatales

Colombia Compra Eficiente identificó las Entidades Estatales con un mayor gasto en servicios de ciberseguridad, según la información del SECOP I y II.

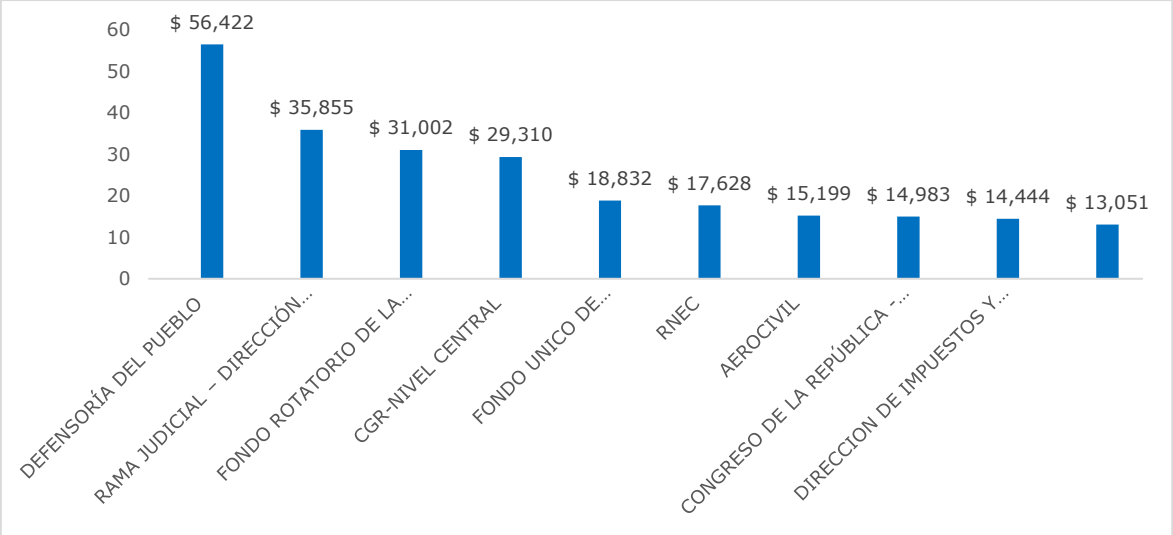
En la siguiente tabla mostramos el top 10 de las entidades que realizaron mayor gasto en servicios de seguridad de la información, de acuerdo con muestra de 239 procesos de contratación, entre los años 2023 al 2025.

Tabla 17– Top 10 -Entidades con mayor contratación (valores en miles de millones)

NOMBRE ENTIDAD	Valor Contrato
FONDO NACIONAL DEL AHORRO S.A.	$ 56,422
DEFENSORÍA DEL PUEBLO	$ 35,855
RAMA JUDICIAL – DIRECCIÓN EJECUTIVA DE ADMINISTRACIÓN JUDICIAL	$ 31,002
FONDO ROTATORIO DE LA REGISTRADURIA	$ 29,310
CGR-NIVEL CENTRAL	$ 18,832
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	$ 17,628
RNEC	$ 15,199
AEROCIVIL	$ 14,983
CONGRESO DE LA REPÚBLICA - HONORABLE SENADO DE LA REPÚBLICA	$ 14,444
DIRECCION DE IMPUESTOS Y ADUANAS NACIONALES*	$ 13,051
	$ 246,731

Fuente: Datos abiertos

Gráfica 13 – Top 10 -Entidades con mayor contratación (valores en miles de millones)



Así mismo, es importante mencionar que el objeto contractual se enfocó en la adquisición, contratación, diagnóstico e implementación de una solución de seguridad, contratación del servicio especializado de un Centro de Operaciones de Seguridad SOC (Security Operations Center) y de Control de Red NOC (Network Operations Center) para el monitoreo de las redes y los servicios tecnológicos, suscripción soluciones SaaS de seguridad en la nube, adquisición solución de protección perimetral integral (dispositivos y servicios), consultorías especializadas para atender y resolver situaciones generales relacionadas con ciberseguridad y seguridad de la información, diagnóstico estado de madurez, elaboración PETI (Planeación Estratégica TI) y consolidación de estrategias de procesos de seguridad continuidad del negocio, entre las más relevantes y significativas. La grafica no me coincide con la tabla 18 …

6 IDENTIFICACIÓN DE LOS PRINCIPALES PROVEEDORES

A partir del análisis de la información disponible en las plataformas SECOP I y SECOP II, se identificaron ciento veintisiete (127) proveedores que han resultado adjudicatarios en procesos de contratación pública relacionados con la prestación de servicios de ciberseguridad durante el periodo analizado. Esta muestra permite contar con una visión representativa del panorama de proveedores que operan en el mercado nacional de servicios de ciberseguridad.

Del análisis de los datos abiertos de contratación, se destacan los siguientes proveedores como los principales adjudicatarios de servicios de ciberseguridad

en el periodo 2023–2025, medidos por el valor agregado de los contratos celebrados:

Tabla 18– Top 20 proveedores servicios de ciberseguridad 2023_2025 (valores en miles de millones)

Razón Social Contratista	Valor Contrato
CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA	$ 56,422
INFOTIC S.A.	$ 38,114
CONSORCIO EY I2SS CSJ	$ 31,002
UNE EPM TELECOMUNICACIONES S.A.	$ 29,534
WEXLER S.A.S	$ 28,533
CORPORACIÓN COLOMBIA DIGITAL	$ 19,843
REDSUMMA	$ 19,178
CONSORCIO DE CIBERSEGURIDAD ORGANIZACION ELECTORAL	$ 15,199
INTERNET SOLUTIONS S.A.S.	$ 15,044
VALOR+ S.A.S-PROVEEDOR	$ 11,400
UT CIBERSEGURIDAD MT	$ 8,923
OPEN GROUP S.A.S.	$ 8,847
UT GESTIÓN CIBER	$ 7,771
UT SOC ADRES 2023	$ 6,543
ALIANZA PUBLICA PARA EL DESARROLLO INTEGRAL ALDESARROLLO - PROVEEDOR	$ 6,359
DATA TOOLS SAS	$ 5,064
CONSORCIO MNEMO SOC-MHCP	$ 4,529
PASSWORD CONSULTING SERVICES SAS	$ 4,159
HEIMCORE SAS	$ 3,831
DTM DATA TACTICAL MANAGEMENT	$ 3,777

Fuente: Datos abiertos

El análisis de la información complementaria disponible en la plataforma EMIS evidencia que los principales proveedores del sector concentran su domicilio y operación en ciudades como Bogotá D.C., Medellín, Cali, Barranquilla y Envigado, sin que ello limite su capacidad de prestación de servicios a nivel nacional, dada la naturaleza tecnológica y remota de la mayoría de los servicios de ciberseguridad.

Teniendo en cuenta la cobertura y alcance operativo de los proveedores identificados, así como las necesidades de las Entidades Estatales a nivel territorial, el Acuerdo Marco de Precios de Bienes y Servicios de Ciberseguridad tendrá cobertura en todo el territorio nacional, garantizando que las entidades públicas puedan acceder a las soluciones y servicios en cualquiera de las siguientes regiones administrativas.

7 MODALIDAD DE CONTRATACIÓN

Tabla 19– Modalidades de contratación de procesos de ciberseguridad 2023_2025 (valores en miles de millones)

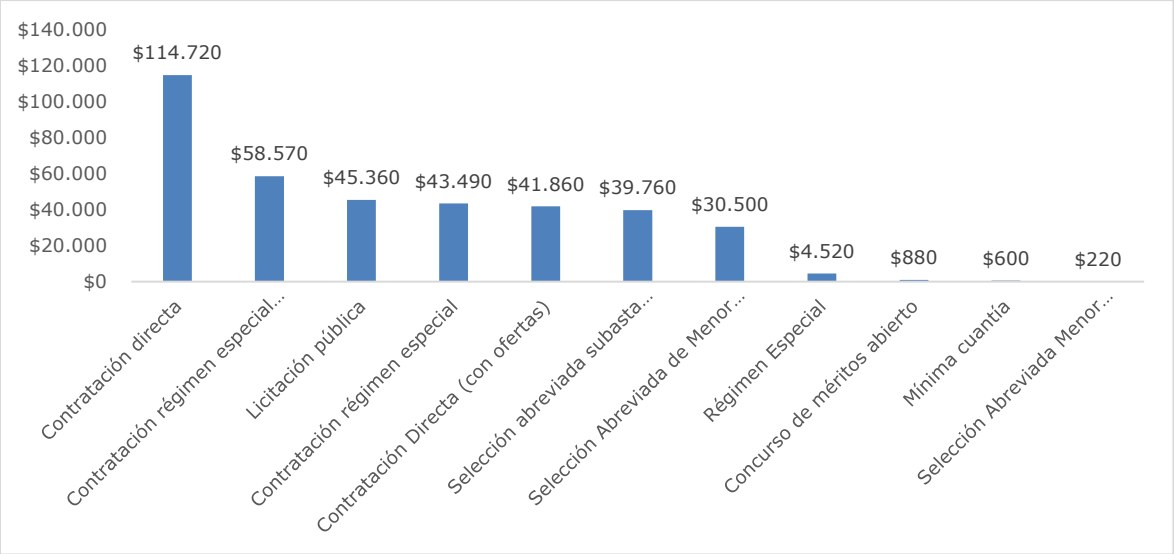
Modalidad de contratación	Valor Contrato
Contratación directa	$ 114,720
Contratación régimen especial (con ofertas)	$ 58,570
Licitación pública	$ 45,360
Contratación régimen especial	$ 43,490
Contratación Directa (con ofertas)	$ 41,860
Selección abreviada subasta inversa	$ 39,760
Selección Abreviada de Menor Cuantía	$ 30,500
Régimen Especial	$ 4,520
Concurso de méritos abierto	$ 880
Mínima cuantía	$ 600
Selección Abreviada Menor Cuantía Sin Manifestación Interés	$ 220
Total general	**$ 380,480**

Fuente: Datos abiertos

La siguiente gráfica presenta la distribución del valor de los contratos de bienes y servicios de Ciberseguridad, categorizados según la modalidad de selección del proveedor y obtenidos de las plataformas SECOP I y SECOP II, para el período comprendido entre 2023 y 2025. En su mayoría, estos contratos fueron adjudicados mediante la modalidad de selección de contratación directa, seguida por Contratación régimen especial (con ofertas), licitación pública, contratación régimen especial, contratación directa (con ofertas), Selección abreviada subasta inversa y posteriormente Selección abreviada menor cuantía.

Observamos que el régimen especial tiene una gran participación en los procesos realizados en el periodo de tiempo indicado; sin embargo, las entidades que contratan por medio de este régimen podrían hacer parte del acuerdo Marco, si los servicios que solicitan se encuentran dentro de los catálogos dispuestos en el presente proceso de contratación.

Gráfica 14 – Modalidades de contratación de procesos de ciberseguridad 2023_2025 (valores en miles de millones)



Fuente: Cálculos realizados por Colombia Compra Eficiente.

8 VIGENCIA DE LOS CONTRATOS

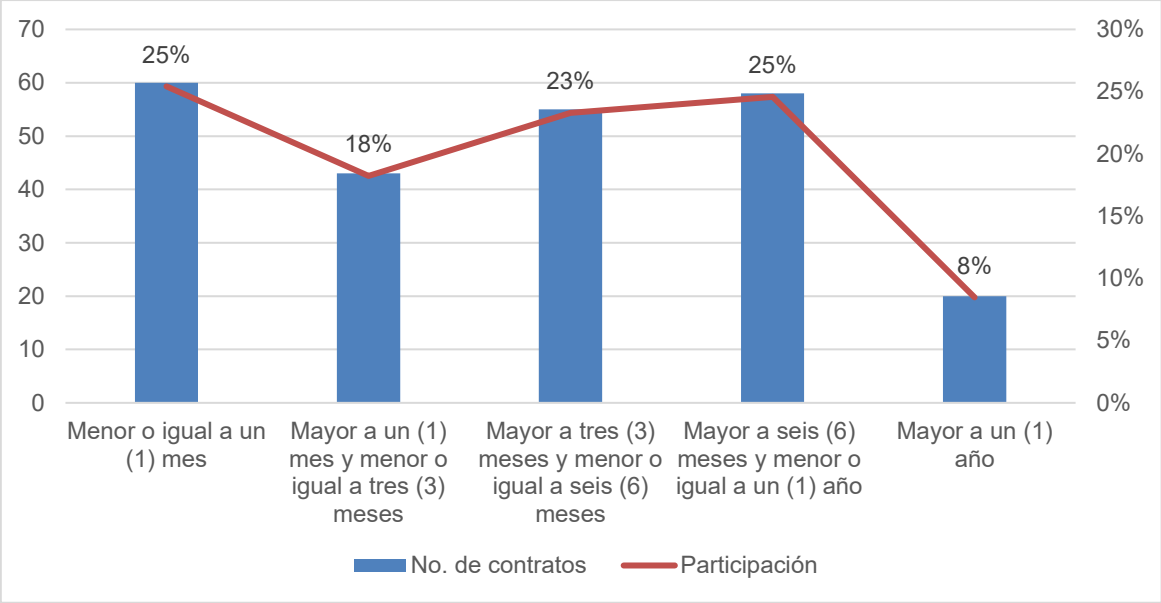
Colombia Compra Eficiente realizó el análisis de la vigencia de los contratos en el lapso comprendido entre 2023-2025, identificando un alto porcentaje en los contratos con vigencia menor o igual a un (1) año (92%), para la adquisición de bienes y servicios de ciberseguridad; esto, probablemente, por el presupuesto asignado a las entidades estatales para la inversión en TI.

Tabla 20– Vigencia de los contratos de ciberseguridad

Vigencia	No. de contratos	Participación
Menor o igual a un (1) mes	60	25%
Mayor a un (1) mes y menor o igual a tres (3) meses	43	18%
Mayor a tres (3) meses y menor o igual a seis (6) meses	55	23%
Mayor a seis (6) meses y menor o igual a un (1) año	58	25%
Mayor a un (1) año	20	8%

Fuente: Datos abiertos

Gráfica 15 – Vigencia los contratos



9 FACTURACIÓN Y PAGO

La facturación y el pago de los servicios de ciberseguridad que se contraten en el marco del Acuerdo Marco de Precios de Bienes y Servicios de Ciberseguridad se realizarán exclusivamente en la fase de operación, a través de las Órdenes de Compra que emitan las Entidades Compradoras, de conformidad con las condiciones establecidas en el Acuerdo Marco, el pliego de condiciones, el Anexo Técnico y la respectiva Orden de Compra.

Colombia Compra Eficiente no realiza pagos ni asume obligaciones presupuestales derivadas del Acuerdo Marco, toda vez que este instrumento no implica la ejecución directa de recursos públicos por parte de dicha entidad. Las obligaciones de pago recaerán únicamente en las Entidades Compradoras que celebren Órdenes de Compra con los Proveedores habilitados.

La facturación deberá realizarse conforme a los hitos de ejecución, entregables o periodos de prestación del servicio definidos en cada Orden de Compra, de acuerdo con la naturaleza del servicio contratado y las condiciones específicas acordadas entre la Entidad Compradora y el Proveedor.

Los pagos se efectuarán con cargo al presupuesto de la Entidad Compradora, previa verificación del cumplimiento de las obligaciones contractuales, la

aceptación a satisfacción de los servicios prestados y el cumplimiento de los requisitos legales, fiscales y administrativos aplicables, incluyendo los establecidos en materia tributaria y de facturación electrónica.

Las condiciones específicas de pago, tales como la periodicidad, los plazos, la modalidad de pago y los documentos soporte requeridos, serán definidas por cada Entidad Compradora en la respectiva Orden de Compra, dentro del marco de las reglas establecidas en el Acuerdo Marco y la normativa vigente.

La facturación y el pago se realizarán en pesos colombianos (COP). En ningún caso se reconocerán ajustes automáticos de precios ni indexaciones, salvo que así se haya previsto expresamente en la Orden de Compra, de conformidad con la normativa aplicable.

Este esquema de facturación y pago es consistente con la vigencia del Acuerdo Marco, la cual es de dos (2) años, prorrogable de acuerdo con las condiciones establecidas en los documentos del proceso, y permite a las Entidades Compradoras definir las condiciones económicas de los servicios de ciberseguridad de acuerdo con sus necesidades particulares, garantizando eficiencia, transparencia y adecuada ejecución de los recursos públicos.

10 CARACTERÍSTICAS DE LOS SERVICIOS DE CIBERSEGURIDAD CONTRATADOS POR LAS ENTIDADES ESTATALES

Los servicios de ciberseguridad que contraten las Entidades Estatales en el marco del Acuerdo Marco de Precios de Bienes y Servicios de Ciberseguridad se caracterizan por su naturaleza especializada, su alto componente técnico y su enfoque en la gestión integral del riesgo digital, orientados a proteger la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de la operación institucional.

En términos generales, los servicios de ciberseguridad presentan las siguientes características:

1. **Especialización técnica y alta complejidad**
   Los servicios requieren conocimientos avanzados, experiencia comprobada y capacidades técnicas especializadas, que varían según el segmento del servicio, el nivel de criticidad de los activos protegidos y el contexto operativo de cada Entidad Estatal.

2. **Prestación continua o bajo demanda**
   Dependiendo del tipo de servicio, estos pueden prestarse de manera continua (por ejemplo, monitoreo y operación de seguridad) o bajo demanda (por ejemplo, respuesta a incidentes, pruebas de seguridad o asesorías especializadas), lo cual incide directamente en la forma de contratación y en la estructura de costos.

3. **Adaptabilidad a las necesidades institucionales**
   Los servicios deben ajustarse a las particularidades de cada Entidad Estatal, considerando su tamaño, sector, nivel de madurez en seguridad de la información, arquitectura tecnológica y riesgos específicos, lo que impide la estandarización absoluta de los alcances y precios.

4. **Dependencia de niveles de servicio (SLA)**
   La calidad y efectividad de los servicios se miden a través de acuerdos de niveles de servicio (SLA), tales como tiempos de respuesta, disponibilidad, resolución de incidentes y cumplimiento de entregables, los cuales son definidos en cada Orden de Compra.

5. **Uso intensivo de tecnología y herramientas especializadas**
   La prestación de los servicios implica el uso de herramientas tecnológicas avanzadas, plataformas de monitoreo, análisis y respuesta, así como metodologías y procesos alineados con marcos de referencia reconocidos en la industria.

6. **Gestión de información sensible y confidencial**
   Los servicios involucran el tratamiento de información crítica y sensible, lo cual exige altos estándares de seguridad, confidencialidad y control de accesos, así como el cumplimiento de la normativa aplicable en materia de protección de datos y seguridad de la información.

7. **Enfoque en la mejora continua y evolución del riesgo**
   Dada la naturaleza dinámica de las amenazas cibernéticas, los servicios requieren actualización permanente, mejora continua de capacidades y adaptación a nuevos riesgos, tecnologías y regulaciones.

8. **Responsabilidad compartida**
   La prestación de los servicios de ciberseguridad se desarrolla bajo un esquema de responsabilidad compartida entre la Entidad Estatal y el Proveedor, en el cual ambas partes deben cumplir con las obligaciones y controles definidos para garantizar la efectividad del servicio.

Estas características justifican la utilización de un Acuerdo Marco de Precios como mecanismo de agregación de demanda, permitiendo a las Entidades Estatales acceder de manera ágil y eficiente a servicios de ciberseguridad especializados, bajo condiciones previamente definidas, sin perjuicio de la flexibilidad necesaria para atender las necesidades particulares de cada entidad a través de las Órdenes de Compra.

11 CONCLUSIONES

Del análisis de las condiciones económicas, técnicas y operativas del **sector de ciberseguridad**, se establece la **pertinencia y conveniencia** de adelantar un proceso de selección para la adjudicación del **Acuerdo Marco de Precios de Bienes y Servicios de Ciberseguridad**, como un instrumento de agregación de demanda que permita a las Entidades Estatales realizar sus adquisiciones de manera **eficiente, transparente y competitiva**.

El Acuerdo Marco se configura como un mecanismo idóneo para atender las necesidades recurrentes y especializadas de ciberseguridad del Estado, teniendo en cuenta la diversidad de servicios requeridos, la rápida evolución tecnológica del sector y la necesidad de contar con proveedores calificados que aseguren la continuidad y calidad de los servicios.

De manera general, los principales beneficios asociados a la implementación del Acuerdo Marco de Precios son los siguientes:

- **Disponibilidad de un instrumento de contratación estandarizado** que permita a las Entidades Estatales acceder a servicios especializados de ciberseguridad, tales como consultoría técnica, monitoreo y operación de seguridad, servicios de Centro de Operaciones de Seguridad (SOC) y Centro de Operaciones de Red (NOC), diagnósticos de madurez, definición de estrategias de seguridad y continuidad del negocio, implementación de soluciones de protección y respuesta, entre otros, de acuerdo con sus necesidades particulares.

- **Agilidad y transparencia en la contratación**, al permitir que las Entidades Estatales realicen sus adquisiciones a través de un mecanismo previamente estructurado, reduciendo cargas administrativas y tiempos de contratación, y aprovechando el poder de compra del Estado para generar eficiencias en la operación secundaria.

- **Mejores condiciones de competencia**, al fomentar la participación de proveedores nacionales y extranjeros con capacidades técnicas verificadas, promoviendo la concurrencia, la innovación y la mejora continua en la prestación de los servicios de ciberseguridad.

- **Optimización de la segmentación del mercado**, lo cual permite atender de manera diferenciada los distintos tipos de servicios de ciberseguridad, reconociendo los niveles de especialización, madurez y capacidad de los proveedores, y facilitando una asignación más eficiente de las Órdenes de Compra.

- **Gestión adecuada de los riesgos**, mediante la definición de requisitos técnicos, financieros y de experiencia proporcionales a la realidad del mercado, así como la implementación de esquemas de garantías y mecanismos de supervisión acordes con la criticidad de los servicios.

- **Fortalecimiento del sector tecnológico**, al promover un instrumento de agregación de demanda que incentive la participación de proveedores con presencia local, capacidades operativas consolidadas y buenas prácticas en seguridad de la información y ciberseguridad, sin imponer barreras injustificadas de acceso al mercado.

- **Claridad en los alcances y métricas de los servicios**, mediante la definición de especificaciones técnicas, niveles de servicio y condiciones de ejecución que permiten a las Entidades Estatales evaluar y controlar de manera efectiva la prestación de los servicios contratados.

En consecuencia, el diseño y adopción del **Acuerdo Marco de Precios de Bienes y Servicios de Ciberseguridad** responde de manera adecuada a las condiciones del mercado, a las necesidades del Estado y a los principios que rigen la contratación pública, constituyéndose en una herramienta estratégica para fortalecer la postura de ciberseguridad del sector público colombiano.

YENNY LISETH PÉREZ OLAYA
Subdirectora de Negocios

		Firma/VoBo
Elaboró:	Daniel Orlando Pardo López – Contratista Eric Mauricio Vargas Forero – Contratista	Daniel Pardo.

	Wilson Daniel Elles Maestre - Contratista	
Revisó:	Germán Enrique Olier - Asesor Sergio Andrés Peña Aristizábal – Gestor T1 - 15	
Aprobó:	Yenny Liseth Pérez Olaya Subdirectora de Negocios	
Fecha de elaboración:	Según publicación de este documento en la plataforma del SECOP II.	

12 REFERENCIAS

Asorenting. (aogsto de 2020). Sobre renting. Obtenido de Asorenting: http://www.asorenting.com/rent

DANE. (15 de mayo de 2020). Departamento Administrativo Nacional de Estadística (DANE). Obtenido de Cuentas nacionales trimestrales: https://www.dane.gov.co/files/investigaciones/boletines/pib/bol_PIB_Itrim20_produccion_y_gasto.pdf

Invierta en Colombia. (enero de 2010). Sector Automotor en Colombia. Obtenido de Invierta en Colombia. Procolombia: https://www.inviertaencolombia.com.co/Adjuntos/078_Perfil-Automotriz-esp.pdf

13ANEXO 1 FICHAS TÉCNICAS DE INFORMACIÓN ESTADÍSTICA

Tabla 21 Ficha técnica información SECOP I

Criterios	Descripción
Objetivos	Analizar el comportamiento de las contrataciones de Ciberseguridad en el SECOP I. Obtener la información para calcular el valor estimado del Acuerdo Marco.
Alcance	Los datos del SECOP I corresponden al valor de los contratos de Ciberseguridad por Entidades Estatales en el SECOP I.
Cobertura geográfica	Nacional
Fuente de datos	Datos abiertos
Universo	Todos los contratos del SECOP I
Período de referencia	Series históricas disponibles.
Metodología	Extracción de información del SECOP I correspondiente a los contratos de Ciberseguridad.

Fuente: cálculos realizados por Colombia Compra Eficiente

Tabla 22 - Ficha Técnica información SECOP II

Criterios	Descripción
Objetivos	Analizar el comportamiento de las contrataciones de Ciberseguridad en el SECOP II. Obtener la información para calcular el valor estimado del Acuerdo Marco.

Criterios	Descripción
Alcance	Los datos del SECOP I corresponden al valor de los contratos de Ciberseguridad por Entidades Estatales en el SECOP II.
Cobertura geográfica	Nacional
Fuente de datos	Datos abiertos
Universo	Todos los contratos del SECOP II
Período de referencia	Series históricas disponibles.
Metodología	Extracción de información del SECOP II correspondiente a los contratos de Ciberseguridad.

Fuente: cálculos realizados por Colombia Compra Eficiente