REPÚBLICA DE COLOMBIA

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES GIT COLCERT

ESTUDIOS DE MERCADO Y DEL SECTOR

3020009- Prestar servicios especializados orientados al fortalecimiento de la seguridad digital en Colombia, mediante el desarrollo de competencias prácticas, la automatización de herramientas especializadas y la integración de acciones alineadas con la Estrategia Nacional de Seguridad Digital, con el propósito de reducir brechas sectoriales y apoyar la transparencia electoral

Bogotá D.C., enero de 2026

CONTENIDO

1. INTRODUCCIÓN

Conforme lo indicado en el artículo 2o. de la Constitución Política "*Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo. (…)".*

De igual forma, de acuerdo con lo señalado en el artículo 209 de la Constitución Política: *"La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones"*, se debe tener en cuenta que el principio de economía que proclama la Carta Política, es aplicable al trámite de las actuaciones administrativas, garantizando acciones eficientes que generen la menor cantidad posible de costos administrativos y presupuestales para la adopción de la decisión que se requiere, a la par que se logre la mayor calidad posible en las actuaciones y la protección de los vigilados y los usuarios que activan los procedimientos administrativos.

Atendiendo las disposiciones constitucionales antes indicadas, el artículo 4° de la Ley 1341 de 2009[1] Modificado por el Art. 4 de la Ley 1978 de 2019[2], establece que el Estado intervendrá en el sector de tecnologías de la información y las comunicaciones, para lograr fines como promover el acceso a las Tecnologías de la Información y las Comunicaciones, teniendo como fin último el servicio universal, el desarrollo de contenidos y aplicaciones, la prestación de servicios que usen TIC y la masificación del Gobierno en Línea e incentivar y promover el desarrollo de la industria de tecnologías de la información y las comunicaciones para contribuir al crecimiento económico, la competitividad, la generación de empleo y las exportaciones.

Por su parte, el artículo 17 de la Ley 1341 de 2009, modificado parcialmente por el artículo 13 de la Ley 1978 de 2019 establece como objetivos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), entre otros: "(…) 1. Diseñar, formular, adoptar y promover las políticas, planes, programas y proyectos del sector de Tecnologías de la Información y las Comunicaciones, en correspondencia con la Constitución Política y la ley, con el fin de contribuir al desarrollo económico, social y político de la Nación, y elevar el bienestar de los colombianos. 2. Promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación. 3. Impulsar el desarrollo y fortalecimiento del sector de las Tecnologías de la Información y las Comunicaciones, promover la investigación e innovación buscando su competitividad y avance tecnológico conforme al entorno nacional e internacional (…)".

De igual manera, el artículo 18 de la Ley 1341 de 2009, modificado parcialmente por el artículo 14 de la Ley 1978 de 2019 señala como funciones del MinTIC, además de las que determinan la Constitución Política y la Ley 489 de 1998, la siguiente: *"3. Promover el establecimiento de una cultura de las Tecnologías de la Información y las Comunicaciones en el país, a través de programas y proyectos que favorezcan la apropiación y masificación de las tecnologías, como instrumentos que facilitan el bienestar y el desarrollo personal, social y económico".*

---

[1] LEY 1341 DE 2009 (julio 30), "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 Espectro y se dictan otras disposiciones". DIARIO OFICIAL. AÑO CXLIV. N. 47426. 30, JULIO, 2009. PÁG. 4.

[2] LEY 1978 DE 2019 (julio 25) "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". Año CLV NO. 51.025, Bogotá, D. C., jueves, 25 de julio de 2019. PAG. 1

Ahora bien, de conformidad con lo indicado en el artículo 34 de la Ley 1341 de 2009, modificado por el artículo 21 de la Ley 1978 de 2019, el MinTIC cuenta con un Fondo Único de TIC, creado como una Unidad Administrativa Especial del orden nacional, dotado de personería jurídica y patrimonio propio, adscrita a este, que tiene como objeto: *"(…) financiar los planes, programas y proyectos para facilitar prioritariamente el acceso universal y el servicio universal de todos los habitantes del territorio nacional a las Tecnologías de la Información y las Comunicaciones, garantizar el fortalecimiento de la televisión pública, la promoción de los contenidos multiplataforma de interés público y cultural, y la apropiación social y productiva de las TIC, así como apoyar las actividades del Ministerio de Tecnologías de la Información y las Comunicaciones y la Agencia Nacional del Espectro, y el mejoramiento de su capacidad administrativa, técnica y operativa para el cumplimiento de sus funciones", el cual dentro de sus funciones, según lo dispuesto en el artículo 35 de la Ley 1341 de 2009, modificado por el artículo 22 de la Ley 1978 de 2019, tiene las siguientes: "6. Financiar y establecer planes, programas y proyectos que permitan masificar la apropiación de las Tecnologías de la Información y las Comunicaciones y el fortalecimiento de las habilidades digitales, con prioridad para la población pobre y vulnerable. (…) 8. Apoyar económicamente las actividades del Ministerio de Tecnologías de la Información y las Comunicaciones y de la Agencia Nacional de Espectro, en el mejoramiento de su capacidad administrativa, técnica y operativa para el cumplimiento de sus funciones"*, por lo que a través de dicho Fondo se financian los planes, programas y proyectos asociados a la apropiación de las TIC.

Según lo anterior, y en virtud de las metas planteadas para el cuatrienio en el Plan Estratégico Institucional MinTIC 2023-2026, se han adelantado actividades orientadas a enmarcar sus esfuerzos en cada línea estratégica de democratización digital, articulándolas con las iniciativas propuestas, los procesos y los servicios de la Entidad, para apoyar el cumplimiento a las directivas nacionales y, a su vez, encaminar a la Entidad en la postulación de proyectos aterrizados a las necesidades del Ministerio.

Ahora bien, el Decreto 338 del 8 de marzo de 2022, reglamentó parcialmente los artículos 64 de la Ley 1437 de 2011, 147 de la Ley 1955 de 2019 y 230 de la Ley 1450 de 2011, modificado por el artículo 148 de la Ley 1955 de 2019, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital.

En el mencionado Decreto, el Artículo 2.2.21.1.1.4. estableció que las autoridades deberán adoptar medidas técnicas, humanas y administrativas para garantizar la gobernanza de la seguridad digital, la gestión de riesgos de seguridad digital, la identificación y reporte de infraestructuras críticas cibernéticas y servicios esenciales, y la gestión y respuesta a incidentes de seguridad digital.

En este marco, el Decreto 767 del 16 de mayo de 2022 "*Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones", en el capítulo 1°, sección 1°, señala en el artículo 2.2.9.1.1.1 el objeto de la Política de Gobierno Digital, así: "El presente capítulo establece los lineamientos generales de la Po lítica de Gobierno Digital, entendida como el uso y aprovechamiento de las tecnologías de la información y las comunicaciones con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y en general, los habitantes del territorio nacional y la competitividad del país promoviendo la generación del valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio"*; así busca apoyar los procesos de transformación digital en las entidades públicas del país y lograr:

Por otro lado, se tiene la acción 2.10 (CONPES 3995 de 2020) *"Elaborar un reporte anual para el Coordinador Nacional de Seguridad Digital, sobre los logros y avances de ejecución (desde las perspectivas cualitativa y cuantitativa) de los*

planes de fortalecimiento de las capacidades para cada una de las instancias y entidades responsables de la ciberseguridad y ciberdefensa de la Nación. Dicho reporte debe tener como objetivo fomentar la prevención en seguridad digital, la promoción de toma de decisiones y la mejora continua de la gestión y respuesta a incidentes cibernéticos a nivel nacional", por lo que en cada vigencia deberá cumplirse con dicho reporte.

Mediante la Política Nacional de Seguridad Digital, contenida en el CONPES 3854 de 2016, se generaron mecanismos estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital a nivel nacional e internacional y se creó la figura de Coordinador Nacional de Seguridad Digital- COLCERT a través del Ministerio de Tecnologías de la Información y las Comunicaciones, la cual se encuentra actualmente en cabeza de la Consejería Presidencial para la Transformación Digital y Gestión y Cumplimiento de la Presidencia de la República.

El artículo 230 de la Ley 1450 de 2011, modificado por el artículo 148 de la Ley 1955 de 2019, señala que "Todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través del Ministerio de Tecnologías de la información y las Comunicaciones para la implementación de la política de Gobierno Digital". Dentro de las acciones prioritarias se encuentra el cumplimiento de los lineamientos y estándares para el incremento de la confianza y la seguridad digital.

El CONPES 3995 de 2020, Política Nacional de Confianza y Seguridad digital, señala el objetivo de establecer medidas para desarrollar la confianza digital a través de la mejora en la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

El Ministerio de Tecnologías de la información y las Comunicaciones estableció, a través de la Resolución 500 de 2021, los lineamientos y estándares para la estrategia de seguridad digital, y la adopción del Modelo de Seguridad y Privacidad de la Información - MSPI, como habilitador de la política de Gobierno Digital, el cual conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Mediante el Decreto 338 de 2022 se adicionó el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones. Con la expedición de este Decreto se: (i) actualizó el marco para la Gobernanza nacional de la seguridad digital, (ii) se fortaleció los equipos nacionales de respuesta a incidentes de seguridad digital y (iii) se definieron instrumentos para la identificación de infraestructuras críticas del sector público.
En el artículo 2.2.21.1.5.2 del Decreto 338 de 2022, se establece que el Ministerio de Tecnologías de la Información y las Comunicaciones coordinará el Equipo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT), cuya finalidad es asesorar, apoyar y coordinar a las múltiples partes interesadas para la adecuada gestión de los riesgos e incidentes digitales. Así mismo, el COLCERT es el punto único de contacto y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los incidentes de seguridad digital y a gestionar de forma activa las amenazas de seguridad digital, incluyendo la coordinación a nivel nacional e internacional de las distintas capacidades de respuesta a incidentes o Centros de Operaciones de Seguridad Digital existentes. Dentro de las actividades que debe cumplir COLCERT se encuentran:

- El desarrollo y divulgación de procedimientos, protocolos, guías y recomendaciones para la gestión de riesgos e incidentes de Seguridad Digital.

- La Generación de acciones efectivas para la recuperación y puesta en operación de las entidades u organizaciones que así lo soliciten, una vez se presenta y un incidente, tales como:

  - Direccionamiento para el plan de acción frente a la recuperación de la operación del incidente.
  - Coordinar: (i) apoyos con industria, (ii) capacidades de otras instancias del Estado (iii) Capacidades con homólogos locales, regionales y globales.
  - Iniciar las gestiones pertinentes con las autoridades (DIJIN, FGN y SIC, etc.), haciendo seguimiento al cumplimiento del marco jurídico frente a la notificación del caso ante las autoridades.
  - La ejecución de acciones para promover el desarrollo de capacidades locales y sectoriales, mediante la implementación del modelo de Gobernanza de Seguridad Digital (determinación de roles y responsabilidades a nivel, nacional, regional, local e individual, frente a la gestión de los riesgos e incidentes de seguridad digital).
  - La definición de la metodología para la identificación de las infraestructuras críticas cibernéticas y servicios esenciales, así como levantar el inventario de infraestructuras críticas públicas cibernéticas nacionales y de servicios esenciales en el ciberespacio.

Adicionalmente, la implementación de esta política propició la expedición del Decreto 338 de 2022, que:

- Renovó el marco para la gobernanza nacional de seguridad digital.
- Reforzó los equipos nacionales de respuesta ante incidentes de seguridad digital.
- Estableció mecanismos para la identificación de infraestructuras críticas del sector público.

Este decreto respondió a la necesidad de fortalecer la resiliencia institucional y ofrecer mecanismos claros de coordinación entre las entidades estatales responsables de la prevención, gestión y respuesta ante amenazas y ataques cibernéticos. Asimismo, impulsó la integración de mejores prácticas internacionales en el diseño de estrategias y protocolos de actuación.
La normativa vigente también define los roles y responsabilidades de los diversos entes encargados de la ciberseguridad en el país, así como sus mecanismos de coordinación. Asimismo, oficializa el Comité Nacional de Seguridad Digital, cuyo propósito es consolidar un esquema de múltiples partes interesadas y brindar confianza a la ciudadanía, estableciendo su composición y funcionamiento. Igualmente, fortalece y promueve las estructuras de los equipos y grupos de respuesta a emergencias cibernéticas, tales como ColCERT, Csirt Gobierno y Csirt Defensa, entre otros.

Estos instrumentos de gobernanza permiten establecer sinergias efectivas entre los sectores público y privado, promoviendo la cooperación internacional y optimizando los recursos disponibles para la protección de los activos digitales críticos. Por medio de espacios de diálogo y capacitación, Colombia avanza hacia la consolidación de una cultura nacional de ciberseguridad, capaz de anticipar y mitigar riesgos en un entorno globalizado y cambiante.

Es importante resaltar y precisar que en las funciones y competencias del MINTIC tiene la de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones, materializando de acuerdo con lo preceptuado en el artículo N°4 de la Ley 1341 de 2019, como se menciona a continuación:

(…)

9. Garantizar la interconexión y la interoperabilidad de las redes de telecomunicaciones, así como el acceso a los elementos de las redes e instalaciones esenciales de telecomunicaciones necesarios para promover la provisión y comercialización de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones.

10. Imponer a los proveedores de redes y servicios de telecomunicaciones obligaciones de provisión de los servicios y uso de su infraestructura, por razones de defensa nacional, atención y prevención de situaciones de emergencia y seguridad pública.

11. Promover la seguridad informática y de redes para desarrollar las Tecnologías de la Información y las Comunicaciones.

(…)

Por esta razón, el Gobierno Colombiano, en El Plan Nacional de Desarrollo (PND) 2022–2026 reconoce la educación digital como pilar fundamental para la equidad y el desarrollo territorial. Mediante la END, se busca garantizar acceso universal a herramientas y competencias digitales, facilitando el desarrollo personal y profesional de la población.

El PND incorpora disposiciones específicas para fortalecer la educación digital:

- Artículo 142: Impulsa la conectividad digital para mejorar calidad de vida y productividad, prioritariamente en zonas vulnerables.
- Artículo 143: Desarrolla programas de alfabetización digital con enfoque étnico, de género y diferencial, promoviendo el uso de tecnologías digitales en la educación.

Así, el fortalecimiento de capacidades en seguridad digital trasciende la habilitación de roles técnicos, abarcando funciones estratégicas, educativas, regulatorias y de liderazgo. El abordaje integral propuesto por estas políticas garantiza que la formación en ciberseguridad esté alineada con los retos contemporáneos y futuros, facilitando la inserción laboral y la movilidad social en una economía cada vez más dependiente de la tecnología.

La ciberseguridad se consolida como un pilar estratégico y prioritario tanto para el sector público como para el privado. El incremento sostenido de los servicios digitales, el auge del comercio electrónico y la masificación del uso de tecnologías de la información han ampliado de manera significativa la superficie de exposición de ciudadanos, empresas e instituciones a riesgos cada vez más sofisticados. Esta realidad ha puesto de manifiesto brechas relevantes en las competencias digitales orientadas a la prevención, detección y mitigación de ciberataques, lo que genera vulnerabilidades críticas en el ecosistema digital nacional.

La limitada cultura y conciencia en materia de seguridad digital ha propiciado un aumento de los delitos informáticos, impactando la privacidad de los usuarios y comprometiendo la integridad de la infraestructura tecnológica. Esta situación se traduce en que tanto personas naturales como organizaciones no identifiquen ni implementen controles básicos de protección, incrementando la exposición a incidentes como robo de información, fraudes electrónicos o sabotaje de sistemas críticos. Por ello, la capacitación permanente y especializada de ciudadanos, profesionales y servidores públicos emerge como un imperativo para robustecer la defensa ante amenazas cibernéticas avanzadas.

Frente a este escenario, el Ministerio TIC, a través del ColCERT, asume un rol estratégico en la formulación, despliegue y seguimiento de la Estrategia Nacional de Seguridad Digital. Esta función implica no solo la articulación de esfuerzos interinstitucionales y el fortalecimiento de la gobernanza, sino también la anticipación y respuesta efectiva ante desafíos derivados de la expansión de servicios digitales, la sofisticación de los actores maliciosos y la protección integral de la infraestructura crítica y la privacidad ciudadana.

A través del CONPES 3995 de 2020, Colombia se ha propuesto consolidar un ecosistema donde el talento humano sea el principal recurso para garantizar una sociedad digital segura y confiable, integrando la ciberseguridad en los programas educativos y elevando la calidad de la formación técnica y superior. Este enfoque se complementa con la promoción de certificaciones internacionales, la creación de alianzas estratégicas con universidades y centros de investigación, y la adaptación curricular basada en los requerimientos dinámicos del mercado laboral.

No obstante, la implementación efectiva de estas políticas enfrenta desafíos considerables, como la rápida evolución de las amenazas cibernéticas, la brecha de talento especializado y la necesidad de actualizar permanentemente los enfoques pedagógicos y regulatorios. Por ello, resulta indispensable mantener un monitoreo continuo de los indicadores de desempeño, promover la investigación aplicada y fortalecer la cooperación internacional en torno a la ciberseguridad.

Es así como entre 2022 y 2025 el ColCERT ha implementado un programa de transferencia de conocimiento que ha fortalecido a más de 8.000 funcionarios, contratistas y colaboradores de conformidad a la base datos de la dependencia. La adquisición prevista de recursos y mecanismos permitirá la continuidad y expansión de estos procesos, alineándose con la macrometa institucional de formación en seguridad digital y preparando a los equipos nacionales y territoriales para responder con eficacia ante incidentes de seguridad.

De la misma forma y en cumplimiento de los lineamientos constitucionales, legales y regulatorios en materia de gestión del riesgo, respuesta a incidentes y gobernanza de la seguridad digital, el ColCERT requiere consolidar un portafolio robusto de herramientas tecnológicas, capacidades especializadas y servicios estratégicos que soporten la continuidad, disponibilidad y resiliencia del ecosistema de seguridad digital estatal. Esta necesidad adquiere especial relevancia durante el ciclo electoral 2026, dado el rol del ColCERT como Secretaría Técnica del PMU Cyber Electoral, liderando la articulación nacional para la protección de la infraestructura electoral, en coordinación con la Registraduría Nacional del Estado Civil (RNEC), el Consejo Nacional Electoral (CNE) y demás entidades.

Es importante indicar, que en las elecciones legislativas de 2022, **la infraestructura digital de la Registraduría fue blanco de un ataque cibernético que afectó la disponibilidad de su página web y aplicaciones oficiales**[3]. Este ataque consistió en un temporalmente los canales digitales para consulta de información electoral. Las autoridades confirmaron que, aunque este incidente no afectó el derecho al voto ni el escrutinio oficial, puso de manifiesto la vulnerabilidad de los sistemas electorales frente a amenazas cibernéticas. Desde entonces, la **Registraduría ha implementado un sistema propio de ciberseguridad que incorpora tecnologías avanzadas para proteger la integridad y continuidad de los procesos electorales futuros**.

De acuerdo al informe interno de ColCERT de 24 de octubre de 2025 por medio del cual se realizó un análisis de riesgos sobre las posibles escenarios de amenazas y tendencias que podrían afectar el ecosistema electoral colombiano en 2026, se evidenció que en las elecciones de Consejos de Juventud 2025, si bien no se reportaron ciberataques disruptivos, las amenazas de los años anteriores mantienen a las autoridades en alerta permanente, especialmente ante riesgos de bombardeo digital y, principalmente, la propagación masiva de desinformación que afecta la percepción pública y la confianza en la democracia. Este escenario refleja un ambiente electoral nacional que, aunque cuenta con controles técnicos y alta participación juvenil, permanece vigilante frente a amenazas de ciberinterferencia y campañas de desinformación que podrían escalar en las elecciones mayores de 2026.

[3] https://www.elespectador.com/politica/elecciones-colombia-2022/registraduria-asegura-que-actividad-irregular-tumbo-su-pagina/

Tendencias regionales

En 2025, América Latina continúa enfrentando un panorama electoral marcado por dinámicas políticas complejas, incluyendo polarización, fragmentación de partidos y desconfianza ciudadana, lo que incrementa la vulnerabilidad a ciberinterferencias. Un patrón recurrente en la región es el uso intensivo de redes sociales para campañas que mezclan mensajes legítimos con una fuerte presencia de noticias falsas, desinformación y apelaciones demagógicas. Esta desinformación busca no sólo influir en el voto, sino también erosionar la confianza en las instituciones democráticas y en los procesos electorales mismos.

En paralelo, los Estados Unidos, tras las elecciones presidenciales de 2024, evidenciaron la continuidad de campañas de desinformación dirigidas especialmente a comunidades latinas e inmigrantes, con mensajes falsos que intentan infundir miedo, desincentivar la participación electoral y crear un ambiente de desconfianza sobre la seguridad y legitimidad del voto. Las agencias de seguridad como el FBI y CISA han enfatizado que, hasta la fecha, no existen evidencias de que ataques cibernéticos hayan comprometido la integridad técnica del voto o el recuento, pero sí que actores maliciosos intentan manipular la narrativa pública para socavar la confianza.

País	Año	Táctica observada	Descripción breve del incidente
Colombia	2022	Ataques DDoS y saturación de infraestructura electoral	Durante las elecciones legislativas y consultas interpartidistas, la página web de la Registraduría Nacional sufrió múltiples intentos de denegación de servicio (más de 400.000 conexiones automatizadas). Aunque la Fiscalía no confirmó un "ataque cibernético" como tal, el evento demostró vulnerabilidades en la infraestructura y deficiencias en la comunicación institucional.
Brasil	2022	Desinformación coordinada y campañas de "fake news"	Redes de apoyo político utilizaron plataformas sociales y canales de mensajería para difundir información falsa sobre fraude electoral y manipulación de urnas electrónicas. Las autoridades judiciales investigaron una estructura informal conocida como "gabinete del odio".
Estados Unidos	2024	Narrativas falsas de hackeo y manipulación del voto	En vísperas de las elecciones presidenciales, el FBI, ODNI y CISA emitieron un comunicado conjunto advirtiendo sobre campañas de desinformación y afirmaciones falsas de hackeo a sistemas electorales, destinadas a sembrar desconfianza en los resultados.

México	2021	Filtración de datos y hacktivismo electoral	Se registraron intentos de acceso no autorizado a bases de datos del Instituto Nacional Electoral (INE) y la difusión de supuestos padrones electorales, posteriormente desmentidos. Algunos grupos hacktivistas latinoamericanos reivindicaron las acciones.
Ucrania / EE. UU. / UE	2020–2024	Interferencia digital y operaciones híbridas	Grupos vinculados a intereses geopolíticos (APT28, APT29, KillNet, entre otros) desplegaron operaciones para influir en la opinión pública y comprometer sitios gubernamentales mediante ciberataques y campañas de influencia.

Mapa de actores de amenazas

En el ecosistema de riesgo electoral conviene distinguir varios tipos de actores: colectivos hacktivistas, actores comerciales o mercenarios de desinformación, grupos criminales con motivaciones económicas u oportunistas, y redes políticas domésticas o "milicias digitales". Cada uno actúa con tácticas y objetivos distintos, y todos han estado activos en distintas medidas en Colombia, en América Latina y en Estados Unidos durante los últimos ciclos electorales.

Hacktivistas y grupos ideológicos regionales

Colectivos autodenominados hacktivistas han intervenido en al menos dos niveles: filtraciones y operaciones informáticas (exposición de datos) y operaciones de "naming & shaming" público para apoyar causas específicas. En América Latina se han destacado grupos como Guacamaya por campañas de exfiltración y divulgación de datos en contextos políticos y de protesta, sus operaciones han tenido impacto informativo y político en la región. Grupos como Anonymous y KillNet han intervenido en elecciones, por ejemplo, en México durante 2021 y 2024, donde expusieron supuestas irregularidades electorales mediante fugas de datos y ataques DDoS a sitios gubernamentales, erosionando la confianza pública. En EE. UU., hacktivistas alineados con movimientos extremistas, como QAnon o far-right groups, han amplificado desinformación durante 2020 y 2024, utilizando bots para promover narrativas de fraude electoral, aunque su rol es secundario comparado con actores estatales.

Redes domésticas de influencia y "milicias digitales"

Un patrón muy visible en países como Brasil ha sido la existencia de redes organizadas de difusión de mensajes, a veces con vínculos a actores políticos (denominadas en prensa e investigaciones como "gabinete del odio" o "milicias digitales"), que coordinan creación de contenido, promoción de *hashtags* y ataque a adversarios políticos. Estas redes han sido señaladas por investigaciones periodísticas y por autoridades como actores con capacidad real de amplificación y polarización en momentos electorales. En Colombia también se han registrado operaciones de origen local, incluyendo el uso de bienes de comunicación pagados o de firmas de publicidad digital, para impulsar narrativas sobre candidatos y procesos; algunos informes independientes han documentado la actuación de operadores y campañas vinculadas al entorno político regional.

Grupos cibercriminales con motivaciones económicas y políticas

Operadores APT (Amenazas Persistentes Avanzadas) como Blind Eagle en Colombia usan técnicas sofisticadas de *spearphishing* y *malware* (troyanos de acceso remoto como Quasar RAT) para infiltrarse en entidades gubernamentales y financieras, actividades que podrían vincularse con espionaje y manipulación digital durante períodos electorales. APT15 es otro grupo relevante que ataca ministerios y organismos oficiales en varios países latinoamericanos con tácticas avanzadas de ingeniería social y software espía.

Cibercriminales y actores oportunistas

Grupos orientados al lucro (*ransomware*, extorsión, fraude) pueden convertirse en amenazas secundarias para procesos electorales: ataques a proveedores, a plataformas transaccionales o a infraestructura de soporte (o bien el aprovechamiento de incidentes operativos para extorsionar o filtrar información). Aunque los ataques directos a la cadena de conteo siguen siendo menos frecuentes en la región cuando los procesos son mayoritariamente físicos o manuales, estos actores representan un riesgo para la continuidad operativa y la disponibilidad de servicios asociados (por ejemplo, portales de consulta), así como para la reputación institucional si logran filtrar información.

Bots, cuentas automatizadas y redes de amplificación

A nivel táctico, las operaciones que más se han observado en ciclos recientes son las redes de amplificación (bots y cuentas coordinadas) y la cooptación de micro-influencers para viralizar mensajes. Estas tácticas permiten transformar un rumor o un fallo operativo (por ejemplo, una latencia en el sitio de resultados) en un tema dominante en pocas horas. Empresas de análisis y plataformas han exhibido que estas técnicas han sido recurrentes tanto en Brasil como en procesos regionales y en campañas de influencia dirigidas a audiencias estadounidenses

Vectores de riesgo 2026

A continuación, se destacan los principales escenarios que podrían amenazar la confianza, integridad y disponibilidad de la información electoral en los próximos comicios:

Vector	Descripción	Impacto esperado	Medidas de mitigación recomendadas
Desinformación digital	Difusión masiva de contenidos falsos y manipulados en redes sociales, foros y medios alternativos.	Pérdida de confianza ciudadana, polarización y afectación de la participación electoral.	Fortalecer monitoreo de redes, alianzas con verificadores de datos y comunicación institucional transparente.

Ataques a infraestructuras electorales	Intentos de intrusión, sabotaje o denegación de servicio sobre portales oficiales y sistemas de registro.	Interrupción del servicio, retraso en resultados y daño reputacional a autoridades electorales.	Implementar medidas de ciberresiliencia, pruebas de penetración y redundancia de sistemas críticos.
Filtraciones o manipulación de datos	Captura o alteración de información de votantes, partidos o candidatos.	Manipulación mediática, pérdida de integridad y cuestionamiento de la legitimidad electoral.	Aplicar cifrado, control de acceso y monitoreo continuo de datos sensibles.
Interferencia extranjera	Grupos APT o actores patrocinados por estados con interés geopolítico en el resultado electoral.	Desestabilización política y diplomática, pérdida de confianza internacional.	Coordinación con aliados internacionales y fortalecimiento de inteligencia cibernética.
Deepfakes y contenido sintético	Uso de IA para generar videos, audios o imágenes falsificadas de candidatos o autoridades.	Manipulación de la opinión pública y deterioro de la reputación de figuras públicas.	Campañas de alfabetización mediática y desarrollo de herramientas de detección automática.
Vulnerabilidades en la cadena de suministro	Dependencia de software y proveedores externos comprometidos o inseguros.	Riesgo de inserciones maliciosas, sabotaje o espionaje.	Auditorías de seguridad, gestión de riesgos de terceros y certificación de proveedores.

El aumento significativo de incidentes de seguridad digital en el país, sumado a los riesgos asociados a los procesos electorales recientes, evidencia que la capacidad actual del Estado debe ampliarse y modernizarse. La tendencia ascendente de ataques de denegación de servicio, campañas de desinformación, explotación de vulnerabilidades y la sofisticación de actores maliciosos —tanto locales como internacionales— obliga a adoptar tecnologías robustas, actualizadas y alineadas con mejores prácticas globales. Adicionalmente, la experiencia acumulada en acompañamientos a entidades públicas, así como la creciente demanda de asesorías, monitoreo, validaciones de infraestructura y apoyo en incidentes, exige herramientas de mayor alcance, automatización y precisión analítica.

Por último, se deja constancia que la presente contratación se encuentra incluida en el Plan Anual de Adquisiciones de la Entidad con Código 3020009- Prestar servicios especializados orientados al fortalecimiento de la seguridad digital en Colombia, mediante el desarrollo de competencias prácticas, la automatización de herramientas especializadas y la integración de acciones alineadas con la Estrategia Nacional de Seguridad Digital, con el propósito de reducir brechas sectoriales y apoyar la transparencia electoral, con Código BPIN: 2022011000093 a cuyo cargo se ha solicitado el certificado de disponibilidad presupuestal expedido por el Coordinador del Grupo de Presupuesto de la Entidad, previa elaboración de los estudios y documentos previos.

ASPECTOS GENERALES DEL MERCADO

En cumplimiento de los dispuesto en el Decreto 1082 de 2015 artículo 2.2.1.1.1.6.1., "Deber de análisis de las Entidades Estatales. La entidad debe hacer, durante la etapa de planeación, el análisis necesario para conocer el sector relativo al objeto del proceso de contratación desde la perspectiva legal, comercial, financiera, organizacional, técnica, y de análisis de riesgo. La entidad estatal debe dejar constancia de este análisis en los documentos del proceso", y en concordancia con la GUÍA DE ELABORACIÓN DE ESTUDIOS DEL SECTOR - GEES (Versión 02 del 24 de junio de 2022) emitida por Colombia Compra Eficiente, el Ministerio TIC realiza el análisis del sector, de la siguiente manera:

1.1 ASPECTO ECONÓMICO

En cumplimiento de los dispuesto en el Decreto 1082 de 2015 artículo 2.2.1.1.1.6.1., "Deber de análisis de las Entidades Estatales. La entidad debe hacer, durante la etapa de planeación, el análisis necesario para conocer el sector relativo al objeto del proceso de contratación desde la perspectiva legal, comercial, financiera, organizacional, técnica, y de análisis de riesgo. La entidad estatal debe dejar constancia de este análisis en los documentos del proceso", y en concordancia con la GUÍA DE ELABORACIÓN DE ESTUDIOS DEL SECTOR - GEES (Versión 02 del 15 de agosto de 2025) emitida por Colombia Compra Eficiente, el Ministerio TIC realiza el análisis del sector, de la siguiente manera:

1. **Conectividad y adopción digital (tamaño del mercado)**

En Colombia dos de cada tres hogares disponen de Internet (65,6 %), es decir que este sería piso de la demanda potencial en ciudadanía, pymes y sector público (DANE, 2025a).

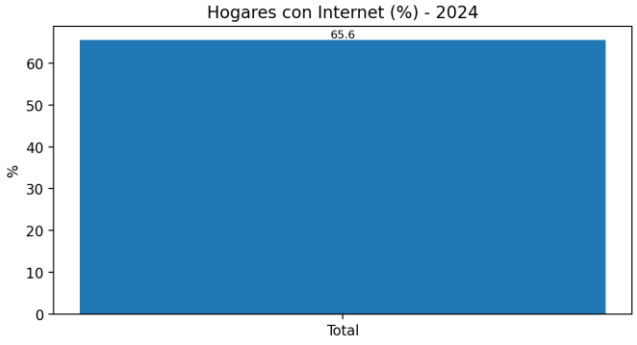


Figura 1. Hogares con Internet (%), 2024. Fuente: DANE – ENTIC Hogares 2024 (DANE, 2025a).

El acceso fijo nacional alcanzó 9,68 millones al término del segundo trimestre de 2025 (MinTIC, 2025b). Con respecto a la conectividad móvil, el país registró una cobertura cercana a 92 accesos por cada 100 habitantes en el primer trimestre de 2025 (MinTIC, 2025c).

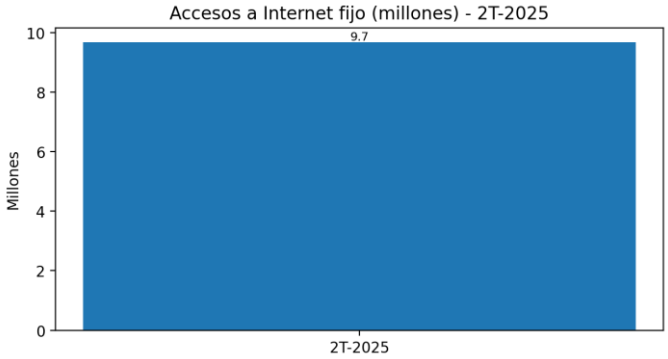


Figura 2. Accesos a Internet fijo (millones) – 2T-2025. Fuente: MinTIC – Boletín Trimestral TIC (MinTIC, 2025b).

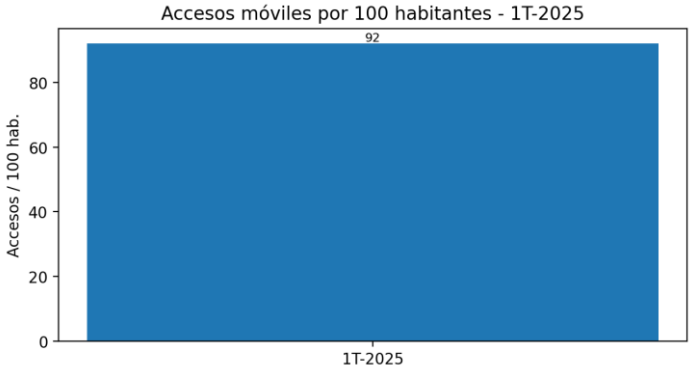


Figura 3. Accesos móviles por 100 habitantes – 1T-2025. Fuente: MinTIC – Boletín Trimestral TIC / ONTIC (MinTIC/ONTIC, 2025a).

2. Brechas territoriales de uso y conectividad

Con respecto al uso de Internet por departamento, se observa que las mayores proporciones se registran en Meta (86,7 %), Bogotá D.C. (85,9 %), Valle (84,7 %) y Cundinamarca (83,5 %); mientras que Vichada (14,5 %) y Vaupés (34,1 %) reportan los menores niveles de uso (DANE, 2024b). Estas brechas sugieren guiar la focalización territorial de estrategias de formación de manera focalizada y progresiva.

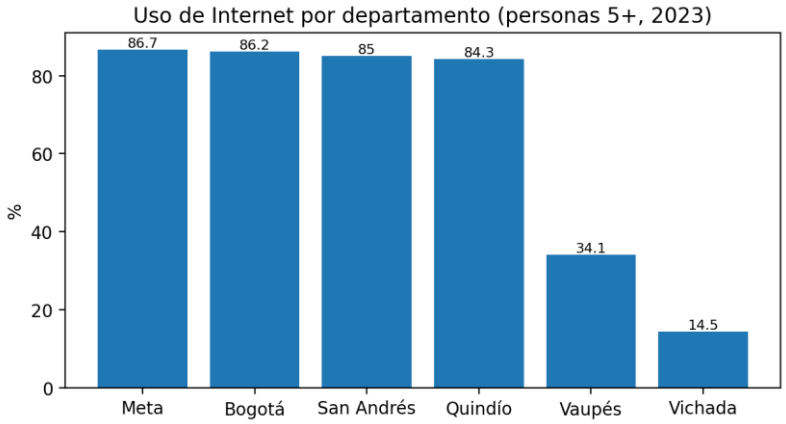


Figura 4. Uso de Internet por departamento (personas 5+, 2023). Fuente: DANE – ECV (DANE, 2024b).

El acceso fijo de internet por 100 habitantes lo lidera Bogotá con 29 accesos por cada 100 habitantes, seguida de Antioquia con 24 y Risaralda con 23 accesos por cada 100 habitantes (MinTIC, 2025c).

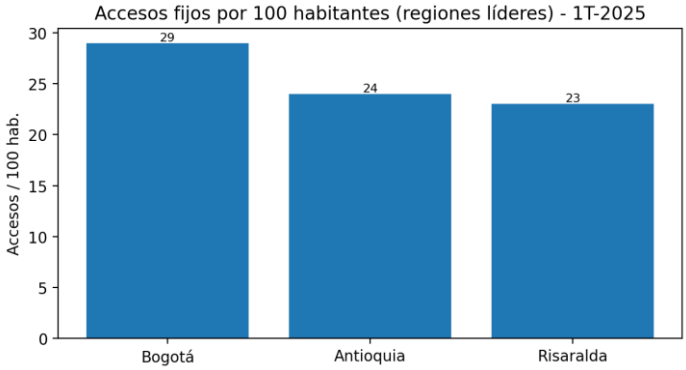


Figura 5. Accesos fijos por 100 hab. (regiones líderes, 1T-2025). Fuente: MinTIC – Boletín Trimestral TIC (MinTIC, 2025c).

3. Exposición al riesgo: cibercrimen y presión de demanda de formación

Según el registro de Cibercrimen, en 2024 se denunciaron 77.866 delitos informáticos, lo que representa un incremento del 23% frente a 2023 (63.249). Las modalidades con mayor volumen continúan asociadas a hurto por medios informáticos y semejantes y acceso abusivo a sistema informático (Policía Nacional, 2024).

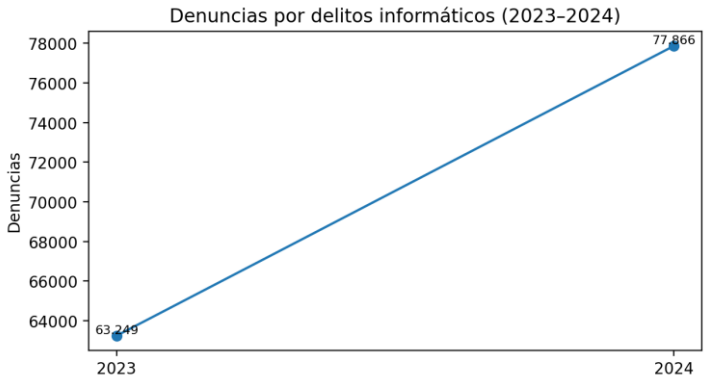


Figura 6. Denuncias por delitos informáticos (2023–2024). Fuente: Policía Nacional – Centro Cibernético Policial, Balance anual 2024 (Policía Nacional, 2024).

4. Mercado de formación: educación básica y media (docentes)

De acuerdo con el censo EDUC 2023 se reportan 494.374 docentes en total; 453.540 con asignación académica, 70,8 % en educación oficial (321.289) y 29,2 % en educación no oficial (132.251) (DANE, 2024).

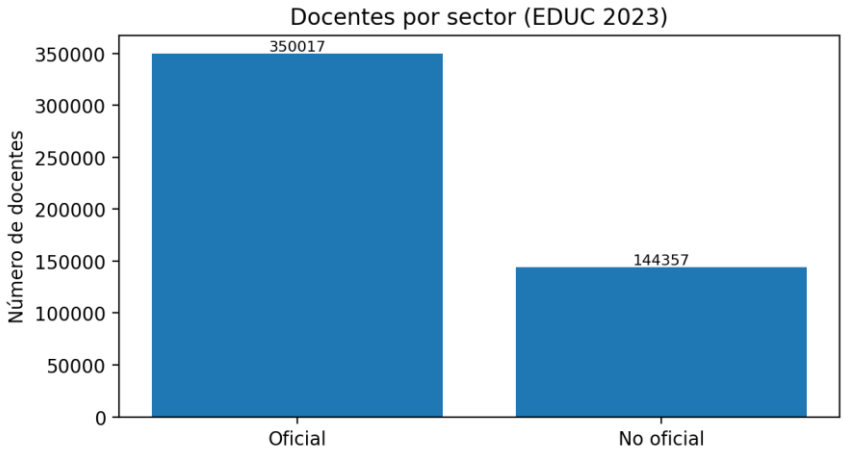


Figura 7. Docentes por sector (oficial y no oficial). Fuente: DANE – EDUC 2023 (DANE, 2024).

El MEN informó que 103.025 docentes participaron en procesos de evaluación y formación (ascensos y reubicaciones salariales) en 2025, con más de 80.000 beneficiados (MEN, 2025a). Estos volúmenes evidencian una plataforma de adopción para currículos de ciberseguridad -por ejemplo, módulos de gestión de identidad, protección de datos personales, convivencia y ciudadanía digital- orientados a la comunidad educativa.

Así mismo, cabe resaltar que las directrices del Plan Territorial de Formación Docente 2024 priorizan competencias docentes para reducir brechas y fortalecer prácticas pedagógicas; esto habilita la inclusión explícita de contenidos de ciberseguridad educativa en los planes territoriales (MEN, 2025b).

5. Mercado de formación: educación superior (SNIES/OLE)

En 2024, la educación superior alcanzó 2.553.560 estudiantes matriculados, lo que representa un incremento del 3,1% respecto a 2023 (SNIES, 2025a).

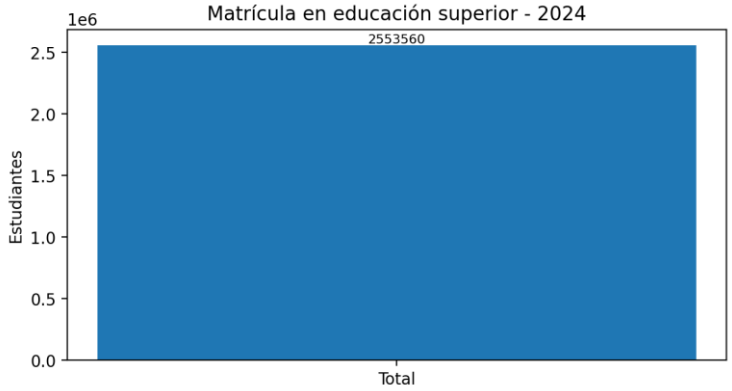


Figura 8. Matrícula en educación superior – 2024. Fuente: MEN – SNIES (SNIES, 2025a).

Los tableros del Observatorio Laboral para la Educación (OLE) permiten monitorear inserción y salarios por áreas de conocimiento, en este sentido se observa que las ingenierías asociadas a TIC suelen exhibir altas tasas de vinculación temprana, lo que refuerza la pertinencia de perfilar programas de ciberseguridad con orientación práctica (MEN/OLE).

6. Mercado empresarial y adopción de capacidades (ENTIC-Empresas)

En 2020, cerca de 17 % de las empresas de industria y comercio contaban con un área TIC interna enfocada en seguridad. El módulo de ENTIC-Empresas evidencia que menos de un tercio tenía políticas formales de administración de riesgos TIC (DANE, 2022b). Esto revela una demanda latente por formación corporativa aplicada en gestión de riesgos, continuidad, respuesta a incidentes, protección de datos y cumplimiento, entre otros.

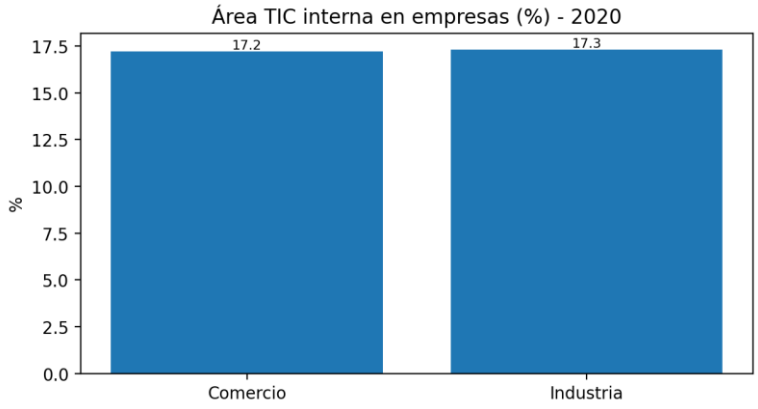


Figura 9. Área TIC interna en empresas (%). Fuente: DANE – ENTIC-Empresas 2020.

7. Hábitos digitales emergentes: IA y cultura de seguridad

El 18,0% de las personas (5+ años) que usaron Internet en 2024 reportó uso de herramientas de IA; en cabeceras municipales fue de 20,4 % y en zonas rurales de 8,1 % (DANE, 2025a). La adopción de IA introduce nuevos vectores de riesgo (fugas de datos, suplantación sintética, entre otros tipos de fraude y engaño), reforzando la necesidad de formación en seguridad digital para docentes, estudiantes, servidores públicos y ciudadanía en general.

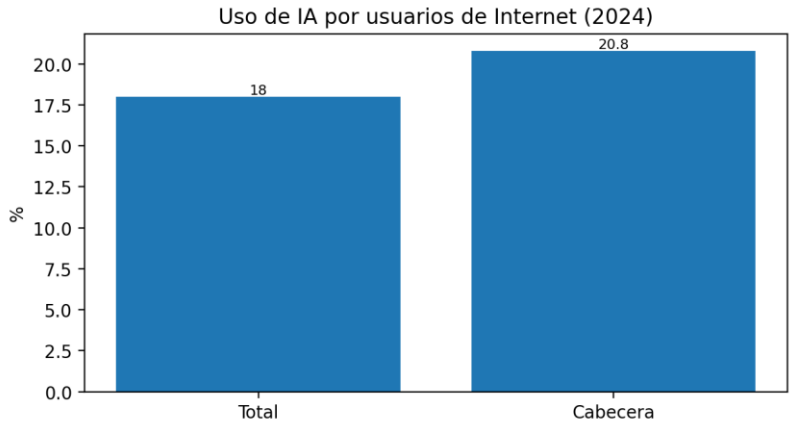


Figura 10. Uso de IA por usuarios de Internet (2024). Fuente: DANE – ENTIC Hogares 2024

8. Seguridad digital

En la actualidad, la ciberseguridad se ha convertido en un eje estratégico para la protección de la infraestructura digital, los datos y la confianza en el entorno tecnológico. Colombia, al igual que otros países de la región, enfrenta un escenario cada vez más complejo debido al incremento de la conectividad, la digitalización de servicios y la expansión del cibercrimen. Las cifras recientes evidencian no solo la magnitud de las amenazas, sino también las vulnerabilidades estructurales que persisten en distintos sectores productivos y en la ciudadanía en general. Bajo este panorama, resulta fundamental analizar los indicadores oficiales más recientes que permiten dimensionar la situación del país frente a los riesgos y desafíos en materia de seguridad digital.

Colombia enfrenta un entorno de ciberamenazas en rápida expansión. En 2025 se registraron alrededor de 36.000 millones de intentos de ciberataques, mientras que la criminalidad informática atendida por la Policía Nacional alcanzó 59.033 denuncias en 2024 (-10% frente a 2023). La conectividad creciente (64% de hogares con Internet en 2024 y más de 9,09 millones de accesos fijos en 2025) amplía la superficie de ataque. Al mismo tiempo, persisten brechas de gestión y talento en seguridad en las empresas (en sectores como industria solo, aproximadamente, 41% cuenta con un área/rol formal de seguridad).

La masificación del acceso a Internet y la digitalización de procesos críticos incrementan la exposición de hogares, empresas y entidades públicas. La siguiente tabla resume indicadores recientes y oficiales.

Indicador	Valor	Fuente
Hogares con acceso a Internet (2024)	64%	MinTIC (ref. DANE), 2025
Accesos fijos a Internet (4T-2025)	9,09 millones	MinTIC-ONTIC, 2025
Accesos móviles a Internet por cada 100 hab. (2T-2025)	93,8	MinTIC-ONTIC, 2025

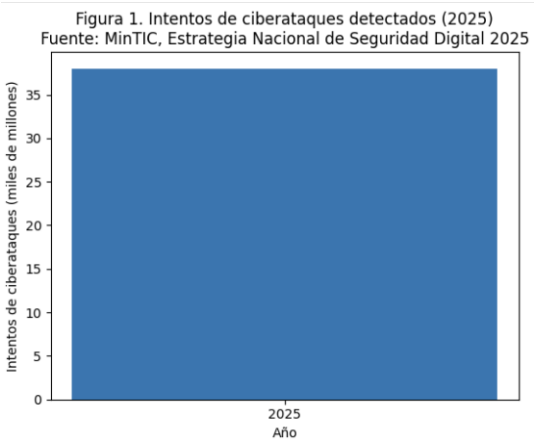


Figura 1. Intentos de ciberataques detectados (2025). Fuente: MinTIC, Estrategia Nacional de Seguridad Digital 2025.

La Figura 1 representa el volumen de intentos de ciberataques detectados durante 2025, de acuerdo con la Estrategia Nacional de Seguridad Digital 2025 del MinTIC. En términos prácticos, el indicador refleja la intensidad y frecuencia con la que actores maliciosos realizan actividades de exploración, intrusión o explotación sobre infraestructuras digitales (públicas y privadas) conectadas a Internet.

El comportamiento evidenciado en la gráfica sugiere un entorno de amenaza persistente y de alta escala, donde los intentos de ataque no corresponden a hechos aislados, sino a campañas automatizadas y recurrentes (por ejemplo, barridos masivos, intentos de fuerza bruta, phishing a gran escala, explotación de vulnerabilidades conocidas). Esto implica que el riesgo no depende únicamente de “si” ocurrirá un intento de intrusión, sino de cuán preparados están los sistemas para detectarlo y contenerlo de forma temprana.

9. Dinámica de la cibercriminalidad

De acuerdo con la Policía Nacional (SIEDCO), en 2024 se reportaron 59.033 denuncias por delitos informáticos en el país, con una reducción del 10% frente a 2023. Las modalidades recurrentes incluyen hurto por medios informáticos, acceso abusivo a sistema informático, violación de datos personales y suplantación de sitios web. En paralelo, el Ministerio de Justicia reporta para 2025 una carga procesal relevante en regiones como la Costa Atlántica y la Costa Pacífica.

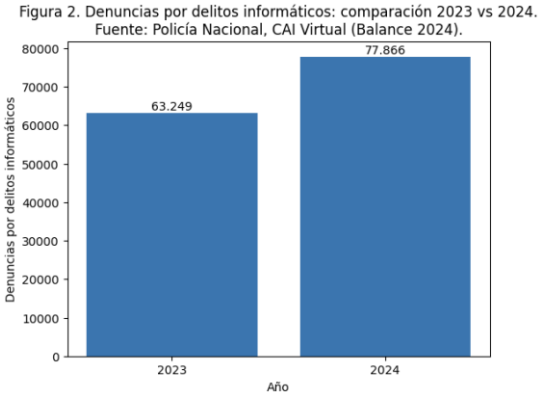


Figura 2. Denuncias por delitos informáticos: comparación 2023 vs 2024. Fuente: Policía Nacional, CAI Virtual (Balance 2024).

La Figura 2 compara el número de denuncias por delitos informáticos registradas en Colombia durante 2023 y 2024, según el Balance 2024 del CAI Virtual de la Policía Nacional. La gráfica permite observar la evolución reciente de la cibercriminalidad denunciada, entendida como los hechos que llegan al sistema formal de atención y reporte.

El comportamiento comparativo evidencia un incremento de denuncias en 2024 frente a 2023, lo que puede interpretarse como una combinación de factores: (i) mayor ocurrencia de delitos asociados al uso de medios digitales (fraude, suplantación, acceso abusivo, hurto por medios informáticos, entre otros), (ii) mayor exposición derivada de la digitalización de trámites, servicios y pagos, y (iii) un posible fortalecimiento de los canales de reporte y la cultura de denuncia ciudadana.

Desde la perspectiva del análisis del sector, este aumento refuerza que la ciberseguridad no es solo un riesgo técnico, sino también un fenómeno con impactos económicos, legales y reputacionales para ciudadanos, empresas y entidades públicas. En consecuencia, se justifica la necesidad de medidas preventivas y de respuesta como monitoreo continuo, detección temprana, gestión de incidentes, campañas de sensibilización y fortalecimiento de capacidades institucionales para reducir la materialización del riesgo y mejorar la atención oportuna de incidentes.

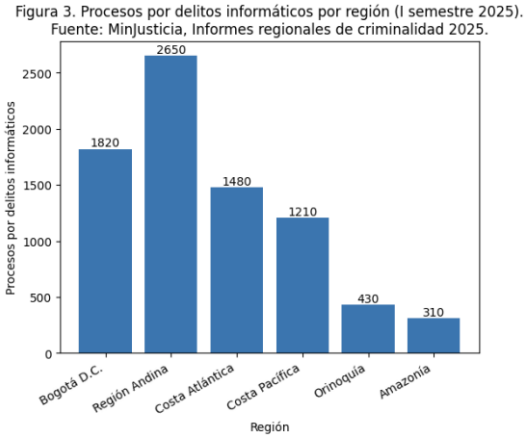


Figura 3. Procesos por delitos informáticos por región (I semestre 2025). Fuente: MinJusticia, Informes regionales de criminalidad 2025.

La Figura 3 muestra la distribución de los procesos por delitos informáticos registrados en Colombia por regióndurante el primer semestre de 2025, con base en los Informes regionales de criminalidad 2025 del Ministerio de Justicia (MinJusticia). La gráfica permite identificar dónde se concentra la carga procesal asociada a cibercriminalidad y, por tanto, en qué territorios la problemática tiene mayor presión sobre la institucionalidad.

En términos generales, la variación entre regiones sugiere que los procesos no se distribuyen de manera homogénea, sino que se concentran en zonas con mayor densidad poblacional, actividad económica y digitalización de servicios. Regiones con altos niveles de conectividad, comercio electrónico y transacciones digitales tienden a presentar mayor volumen de casos, mientras que territorios con menor conectividad o con capacidades institucionales más limitadas pueden presentar menores registros, lo cual no necesariamente implica menor ocurrencia, sino posibles diferencias en denuncia, judicialización y capacidad de investigación.

Desde la perspectiva del análisis del sector, esta información es relevante porque evidencia la necesidad de estrategias diferenciadas por territorio. Las regiones con mayor carga procesal requieren fortalecimiento en prevención, investigación y respuesta, mientras que en regiones con menores registros se vuelve clave robustecer los canales de reporte, la sensibilización y la articulación interinstitucional. En conjunto, la gráfica respalda la importancia de capacidades de monitoreo, detección temprana y atención de incidentes, así como de coordinación entre actores nacionales y regionales para enfrentar la cibercriminalidad con enfoque territorial

10. Vulnerabilidad empresarial y capacidades actuales

La ENTIC Empresas 2020 del DANE revela que, aunque varios sectores cuentan con un área de seguridad de la información, persiste heterogeneidad: mientras telecomunicaciones y educación superior privada superan el 80%, la industria se ubica cerca del 41%. Además, el estudio indaga sobre incidentes de seguridad digital, protocolos implementados y responsables de la administración de riesgos.

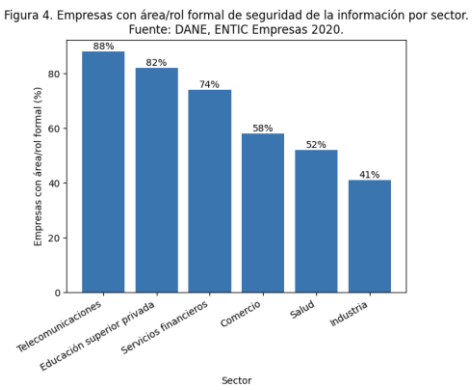


Figura 4. Empresas con área/rol formal de seguridad de la información por sector. Fuente: DANE, ENTIC Empresas 2020.

La Figura 4 muestra el porcentaje de empresas que cuentan con un área o un rol formal de seguridad de la información, desagregado por sector económico, con base en la ENTIC Empresas 2020 del DANE. En términos prácticos, el indicador refleja el grado de formalización de la función de ciberseguridad dentro de las organizaciones (es decir, si existe una responsabilidad definida y no solo acciones aisladas desde TI).

La gráfica evidencia una brecha sectorial: los sectores más intensivos en tecnología y manejo de datos (por ejemplo, telecomunicaciones y educación superior privada) tienden a presentar mayores porcentajes de formalización, mientras que sectores tradicionales o con menor madurez digital (como industria) muestran menores niveles de adopción. Esto suele relacionarse con diferencias en: (i) nivel de digitalización y exposición a riesgos, (ii) exigencias regulatorias y de cumplimiento, (iii) disponibilidad de presupuesto y talento especializado, y (iv) cultura organizacional de gestión del riesgo.

Desde la perspectiva del análisis del sector, el hallazgo es clave porque sugiere que una parte importante del tejido empresarial aún opera con capacidades limitadas para prevenir, detectar y responder a incidentes, especialmente donde no hay un responsable formal. En consecuencia, se refuerza la necesidad de servicios y capacidades como monitoreo continuo, correlación de eventos, detección avanzada y respuesta coordinada (incluidos servicios gestionados), para cerrar brechas de madurez y reducir la probabilidad e impacto de incidentes de seguridad digital.

Estas brechas de madurez y cobertura refuerzan la necesidad de monitoreo continuo, correlación de eventos, detección temprana y respuesta automatizada, especialmente en organizaciones con plantillas limitadas de ciberseguridad.

11. Brecha de talento y operación 24/7

A nivel regional, la OEA y aliados reportan una escasez de entre 515.000 y 701.000 profesionales en ciberseguridad en América Latina y el Caribe. Esta brecha no solo limita la capacidad de las organizaciones para contratar perfiles especializados (analistas SOC, ingenieros de detección, threat hunters, especialistas en respuesta a incidentes), sino que también incrementa la rotación y eleva los costos de operación, afectando la continuidad y madurez de los programas de seguridad.

En la práctica, esta escasez se traduce en dificultades para implementar y sostener centros de monitoreo internos con operación 24/7, especialmente en entidades con equipos reducidos o presupuestos restringidos. Como resultado, se amplían los tiempos de detección y respuesta, se incrementa la exposición frente a incidentes que ocurren fuera del horario laboral y se vuelve más complejo mantener procesos consistentes de correlación de eventos, gestión de alertas, investigación y contención.

En este contexto, cobra relevancia el caso de negocio para servicios de monitoreo gestionado, que permiten asegurar vigilancia continua, acceso a talento especializado y procedimientos estandarizados, reduciendo la dependencia de la disponibilidad interna y mejorando la capacidad de prevención, detección y respuesta. En conclusión, la brecha de talento constituye un factor estructural que justifica la adopción de esquemas de operación 24/7 soportados por servicios especializados, como medida costo-efectiva para fortalecer la postura de seguridad y garantizar continuidad en la gestión del riesgo digital.

1.2 ASPECTO TÉCNICO

El aumento significativo de incidentes de seguridad digital en el país, sumado a los riesgos asociados a los procesos electorales recientes, evidencia que la capacidad actual del Estado debe ampliarse y modernizarse. La tendencia ascendente de ataques de denegación de servicio, campañas de desinformación, explotación de vulnerabilidades y la sofisticación de actores maliciosos —tanto locales como internacionales— obliga a adoptar tecnologías robustas, actualizadas y alineadas con mejores prácticas globales. Adicionalmente, la experiencia acumulada en acompañamientos a entidades públicas, así como la creciente demanda de asesorías, monitoreo, validaciones de infraestructura y apoyo en incidentes, exige herramientas de mayor alcance, automatización y precisión analítica.

El contexto actual evidencia una presión creciente sobre infraestructuras públicas y privadas, marcada por la sofisticación de ataques y la necesidad crítica de talento especializado, soluciones de defensa avanzadas y políticas nacionales sólidas. Como respuesta, el Ministerio TIC define la iniciativa “Ciberseguridad 360”, diseñada para abordar de manera sistemática los desafíos históricos en materia de protección digital. Este programa se fundamenta en una estrategia multidimensional que contempla el fortalecimiento de capacidades técnicas mediante capacitación especializada del talento humano, así como la actualización e integración de infraestructuras tecnológicas avanzadas. Estas acciones estratégicas están dirigidas a optimizar la resiliencia y asegurar la protección eficiente de los activos críticos nacionales frente a amenazas cibernéticas emergentes.

Como componentes fundamentales de la iniciativa se tienen:

1. Un componente técnico que permite cubrir no solamente la infraestructura tecnológica que soporta los servicios propuestos en el marco de la iniciativa garantizando no solo la continuidad del portafolio del ColCERT, sino que amplía su capacidad operativa y estratégica, permitiendo anticipar riesgos, reaccionar con mayor eficiencia y acompañar al país en periodos de alta sensibilidad, como los procesos electorales legislativos y presidenciales.
2. La formación de talento humano especializado es un componente central de esta estrategia. Se busca genera formación práctica y certificable, orientada a fortalecer competencias digitales y consolidar una cultura resiliente y sostenible en ciberseguridad. Esta estrategia responde a la demanda creciente de protección digital y contribuye a la formación de una fuerza laboral capacitada para enfrentar los desafíos emergentes en la materia.

Las acciones de capacitación están diseñadas bajo un enfoque práctico, orientado a la toma de decisiones informadas, la reducción de errores operativos y el fortalecimiento de la resiliencia institucional, aspectos especialmente relevantes para

entidades con funciones críticas durante periodos electorales. La adquisición de herramientas, licenciamientos y capacidades tecnológicas constituye, por tanto, una necesidad estratégica para asegurar la defensa digital del Estado y la confianza en los procesos democráticos.

El portafolio tecnológico propuesto cubre de forma integral las fases de prevención, detección temprana, respuesta, análisis forense y comunicación institucional. Su implementación potencia la capacidad preventiva y reactiva del ColCERT, posicionando a la entidad como referente nacional durante el ciclo electoral 2026 y en la operación continua del ecosistema de seguridad digital del país.

En conclusión, la iniciativa "Ciberseguridad 360" se alinea plenamente con los lineamientos de la Estrategia Nacional de Seguridad Digital, enfocándose en el fortalecimiento de capacidades, la promoción de una cultura de ciberseguridad, la modernización de herramientas y el impulso de la cooperación interinstitucional. Su despliegue permitirá reducir brechas, optimizar la gestión pública y garantizar un entorno digital seguro y confiable para Colombia.

Eta contratación surge con el propósito de reforzar la seguridad digital en el Estado, tomando como base las mejores prácticas tanto nacionales como internacionales y siguiendo los lineamientos de la Estrategia Nacional de Seguridad Digital. El desarrollo del mismo resulta especialmente relevante en el contexto electoral, donde es fundamental salvaguardar la información, mantener la continuidad operativa y generar confianza en la ciudadanía.
De esta forma, el objetivo principal consiste en diseñar e implementar acciones que fortalezcan de manera integral la seguridad digital en de los diferentes sectores, abarcando tanto la modernización de infraestructuras tecnológicas como la capacitación especializada. El alcance del proyecto contempla la identificación de posibles riesgos, la reducción de vulnerabilidades y el desarrollo de capacidades, asegurando así la sostenibilidad y la mejora continua de los servicios digitales institucionales y de los procesos democráticos.
Para el desarrollo de las iniciativas descritas se contemplan dos líneas estratégicas a través de las cuales se desarrollará el proyecto:

Fortalecimiento de la Infraestructura Tecnológica

La protección de infraestructuras críticas será una prioridad, aplicando metodologías avanzadas para gestionar riesgos y aumentar la resiliencia ante nuevas amenazas digitales. Las medidas a implementar abarcan la mejora y actualización de la infraestructura tecnológica con que cuenta el ColCERT teniendo en cuenta:

- **Gestión temprana de vulnerabilidades (Tenable One):** Permite visibilidad integral de activos, configuraciones inseguras y puntos críticos; su renovación fortalece la postura de seguridad del Estado y reduce brechas explotables.
- **Detección y respuesta ante amenazas (Trellix):** Plataforma que identifica comportamientos anómalos, bloquea malware avanzado y contiene ataques; clave para mantener la continuidad operativa y apoyar entidades sin tecnología propia.
- **Protección DNS (Cisco Umbrella):** Actúa como defensa temprana bloqueando conexiones maliciosas, reduciendo phishing y exfiltración de datos; esencial en contextos de alto tráfico como procesos electorales.
- **Mitigación de ataques DDoS (Cloudflare):** Proporciona protección contra denegación de servicio y mejora la estabilidad y rendimiento de servicios críticos durante picos de consultas.
- **Plataforma de comunicaciones (Mailchimp):** Facilita envío masivo y segmentado de alertas, boletines y mensajes institucionales confiables; crucial para contrarrestar desinformación.

- **Laboratorio de simulación y pruebas (VMware ESXi/vCenter):** Permite ejecutar análisis, ejercicios y pruebas sin comprometer producción; su renovación garantiza continuidad y preparación técnica.
- **Capacidad forense digital (MAGNET AXIOM Cyber + Torre Forense):** Habilita adquisición remota de evidencia, análisis profundo y generación de reportes con cadena de custodia; fundamental en incidentes durante procesos electorales.
- **Videowall del Centro de Operaciones:** Es vital para la visualización situacional y coordinación con el PMU Cyber Electoral; requiere soporte y mantenimiento para garantizar operación continua.
- **Servicio MDR con CrowdStrike:** Proporciona monitoreo continuo 24/7, caza de amenazas y contención inmediata; reduce significativamente los tiempos de detección (MTTD) y respuesta (MTTR), fortaleciendo la defensa estatal

Formación Especializada

La formación permanente del personal es esencial para asegurar la protección y eficiencia de las operaciones. Por ello, el proyecto prevé:

- Programas de capacitación y actualización en seguridad digital.
- Desarrollo de habilidades especializadas para prevenir y responder a incidentes
- Impulso al aprendizaje organizativo como medio para fortalecer la democracia.
- Plataforma de formación avanzada basada en **IA y algoritmos propietarios**, para personalizar el aprendizaje y predecir tendencias formativas.
- Solución **parametrizable, escalable y 100% web**, accesible sin instalación desde cualquier navegador.
- Incluye **retos técnicos** en áreas como criptografía, forense, explotación web, pentesting y reversing.
- Ofrece **formatos de competencia**: individual, por equipos, por niveles, tiempo limitado o ranking abierto.
- Posee **gamificación completa**: puntuación automática, rankings, insignias y progresión por niveles.
- Puede integrarse con procesos formativos previos y funcionar como herramienta de **evaluación post-entrenamiento**.
- Genera **métricas detalladas**: análisis por participante, tipo de reto y tiempos de resolución.
- Incluye **administración integral de usuarios**, con autenticación segura y mecanismos de recuperación de credenciales.
- Provee **registro de auditoría exportable**, con datos como ID, IP, fechas, horas y eventos.
- Garantiza compatibilidad con múltiples **dispositivos, sistemas operativos y navegadores**.
- Gestión centralizada de inscripciones mediante **formulario único nacional**, con reportes quincenales y apoyo en certificación.
- Permite **talleres prácticos y laboratorios de simulación (cyber-range)** durante el proyecto.
- Programas de formación de **mínimo 40 horas**, con docentes especializados y al menos una clase sincrónica grabada.
- Enfoque **práctico y aplicado**, evitando contenidos puramente teóricos mediante ejercicios, laboratorios y competencias simuladas.
- Estrategia de formación alineada con los **objetivos del plan sectorial TIC**.

- Actividades clave: talleres, clases sincrónicas, difusión segmentada, integración institucional, monitoreo y retroalimentación continua.
- **Meta de formación:** capacitar a *5.000 usuarios* en competencias básicas y especializadas (Awareness, CTF, ciudadanía, profesionales y funcionarios).
- Toda comunicación cumple lineamientos de **imagen institucional del MinTIC y ColCERT**.
- Mecanismos rigurosos de **seguimiento y mejora continua**, con informes periódicos e indicadores de impacto.

Gracias a esta estructura, se promueve una ejecución global que fortalece la sostenibilidad, genera confianza y contribuye al cumplimiento de los objetivos nacionales en materia de seguridad digital, integrando claramente ambas líneas estratégicas principales.

Objetivos Específicos:

- Implementar prácticas avanzadas para la protección, prevención y respuesta ante incidentes de ciberseguridad, garantizando el cumplimiento de políticas y lineamientos nacionales.
- Optimizar el monitoreo y la administración de sistemas de información, incorporando tecnologías de predicción de demanda que faciliten la toma de decisiones y la resiliencia institucional.
- Fortalecer las competencias técnicas y operativas de entidades frente a los riegos durante los procesos electorales en materia de seguridad digital.
- Desarrollar y consolidar capacidades técnicas avanzadas en las entidades beneficiarias, mediante programas de formación certificados y actividades prácticas que eleven la preparación frente a riesgos y amenazas digitales, especialmente en el contexto de procesos electorales.
- Garantizar la trazabilidad, seguimiento y certificación de los procesos de formación y simulación, mediante la generación de informes estructurados y la retroalimentación continua de los participantes y aliados estratégicos.

ENTREGABLES

El proyecto consolida cinco entregables estratégicos diseñados para fortalecer la seguridad digital del Estado, asegurar la continuidad operativa del ColCERT y soportar los servicios de monitoreo, respuesta, análisis, formación y comunicación. Cada entregable integra actividades de licenciamiento, soporte, despliegue, transferencia de conocimiento y producción de informes, alineadas con los lineamientos del Ministerio TIC.

Licenciamiento, despliegue y operación de soluciones tecnológicas

- Garantizar que todas las herramientas, plataformas y soluciones de ciberseguridad estén **debidamente licenciadas, activas y documentadas** durante un mínimo de 12 meses.
- Asegurar la **entrega oportuna de licencias** antes del vencimiento de las existentes, sin generar interrupciones de operación.
- Incluir tecnologías esenciales como Tenable One, Trellix, Cisco Umbrella, Cloudflare, VMware ESXi/vCenter, MDR, Magnet AXIOM Cyber, Mailchimp, Kiteworks y otras soluciones complementarias.
- Activar la **membresía FIRST** como mecanismo de cooperación internacional en ciberseguridad.

- Desarrollar y entregar un **plan completo de soporte**, mantenimiento, actualizaciones, escalamiento y evidencia documental.
- Ejecutar **transferencia de conocimiento especializada** para cada herramienta, impartida por personal certificado, con materiales, prácticas guiadas y evidencias formativas.

Plataforma de vigilancia y monitoreo continuo (MDR)

- Implementar una plataforma integral de **detección y respuesta 24/7**, capaz de cubrir entre **mínimo 2000 activos de TI**.
- Integrar múltiples fuentes de telemetría: EDR/XDR, DNS seguro, análisis de vulnerabilidades, infraestructura crítica, flujos de red e indicadores de compromiso.
- Desplegar completamente la solución MDR: instalación de agentes, reglas, tableros de monitoreo y afinamiento inicial en máximo 30 días.
- Garantizar soporte 24/7, **gestión de escalamiento**, coordinación con SOC y servicios expertos de cacería de amenazas.
- Documentar cada incidente desde la detección hasta el cierre y asegurar que **toda la información pertenezca al Ministerio TIC**.
- Entregar informes por entidad, incluyendo análisis, resultados, recomendaciones y reportes forenses cuando corresponda.
- Definir y activar **estrategias de contingencia y continuidad operativa**.

Programas de formación y certificación

- Diseñar y ejecutar programas de formación alineados con la **Estrategia Nacional de Seguridad Digital**, con módulos prácticos y certificación verificable.
- Garantizar disponibilidad en una **plataforma web interactiva**, funcional durante toda la vigencia contractual.
- Realizar actividades de difusión y publicidad respetando el manual de identidad del MinTIC.
- Entregar certificados digitales y mantener actualizados los registros de beneficiarios conforme a las políticas de datos personales.
- Incluir entrenamientos especializados para el personal del Centro de Operaciones del ColCERT.
- Alertar al Ministerio sobre **amenazas emergentes** que puedan afectar la continuidad del servicio formativo.

Producción de piezas comunicativas e institucionales

- Diseñar piezas de comunicación alineadas con los lineamientos de imagen y accesibilidad del MinTIC y el ColCERT.
- Apoyar las actividades del proyecto: formación, campañas de ciberseguridad, notificaciones y mensajes institucionales.

- Validar contenido técnico y narrativo en coordinación con el área de comunicaciones.
- Incorporar estas piezas en la plataforma de formación y en las estrategias de comunicación para situaciones de riesgo o eventos críticos.

Informes estratégicos, métricas y evaluación

- Elaborar informes mensuales, trimestrales y de cierre que integren:
    - Métricas de desempeño.
    - Indicadores estratégicos.
    - Análisis de vulnerabilidades e incidentes.
    - Uso del MDR.
    - Avances de formación y resultados del cyber-range.
- Incluir retroalimentación estructurada, análisis de impacto, riesgos y acciones adelantadas con el ColCERT.
- Entregar la totalidad de la información generada y recolectada, asegurando que permanezca bajo propiedad exclusiva del Ministerio TIC.

DESCRIPCIÓN DE LAS LÍNEAS DE DESARROLLO

Línea de servicios para herramientas de Apoyo y Fortalecimiento de la Gestión del ColCERT

El éxito de la operación depende de herramientas tecnológicas actualizadas y ajustadas a las necesidades cambiantes del entorno.

Actualización de licenciamientos

El proyecto contempla la renovación y gestión de licencias de las soluciones identificadas por ColCERT por un periodo no menor a 12 meses, así como la integración de nuevas funcionalidades que optimicen la prestación del servicio y la infraestructura disponible. Se fortalecerá la colaboración a través de la afiliación al FIRST, fomentando el intercambio de información, la participación en ejercicios globales de ciberseguridad y el acceso a alertas y mejores prácticas internacionales. Se prevé un proceso sistemático para la actualización de configuraciones, capacitación del personal en el uso de herramientas y mantenimiento preventivo y correctivo, tales como:

- **Cloudflare DNS**

El servicio de gestión y administración del Sistema de Nombres de Dominio (DNS) para colcert.gov.co reviste una importancia crítica para la correcta publicación y accesibilidad de los servicios del ColCERT en internet. Un DNS gestionado eficientemente garantiza que los usuarios puedan acceder sin problemas a la información, herramientas y recursos que el ColCERT ofrece. Esto implica la configuración precisa de los registros DNS, la monitorización constante para asegurar la resolución adecuada de nombres de dominio y la implementación de medidas de seguridad para proteger contra ataques como el DNS spoofing. En esencia, una administración robusta del DNS es fundamental para la presencia en línea confiable y la operatividad continua de los servicios del ColCERT.

Services:

Services Description	Unit of Measure per Month	Quantity
CDN - Total Data Transfer	TB	2
Foundation DNS - Queries	MM DNS Queries	400
Advanced Certificates Manager - Domains	Zones	35
Foundation DNS - Records	10K DNS Records	100
CDN - Requests	MM Requests	400
Advanced DDoS	TB	Included

Services Description	Unit of Measure per Month	Quantity
Enterprise - Primary - Domains	Zones	5
Enterprise - Secondary - Domains	Zones	35
WAF	TB	Included
Standard Success Offering		Included

- **Sistema Sandbox Trellix Intelligent Sandbox (DoD)**

La actualización del sistema Sandbox DoD a la última versión de Trellix Intelligent Sandbox (Grant Number: 17971347-NAI) representa un avance significativo para la capacidad del ColCERT de ofrecer servicios de análisis automatizado de malware. Esta modernización optimizará la detección y el análisis de amenazas sofisticadas, proporcionando información crucial a entidades públicas, privadas y a la ciudadanía en general. La continuidad de este servicio automatizado es fundamental para la respuesta proactiva ante incidentes de seguridad y para la mejora continua de la postura defensiva del país.

Requisitos: Licenciamiento para una base mínima de 250 usuarios donde cada usuario dispone de una capacidad de 20 envíos mensuales para análisis en Sandbox, garantizando un volumen total de 60,000 procesamientos anuales como requerimiento mínimo.

- **Mailchip (Standard) – Hasta 10.000 Correos electrónicos**

Una plataforma de automatización de marketing digital, enfocada en el envío masivo de correos electrónicos y campañas de email marketing directamente desde los buzones del CSIRT Gobierno y ColCERT, se constituye como un canal estratégico para la difusión de comunicaciones esenciales. Esta herramienta permitirá la distribución eficiente de piezas informativas cruciales, tales como alertas tempranas, advertencias sobre amenazas, informes técnicos detallados y boletines informativos, emanados principalmente de la línea de análisis situacional. Al utilizar los canales de correo electrónico oficiales del CSIRT Gobierno y ColCERT, se asegura una mayor credibilidad y alcance de la información, facilitando que las entidades públicas y privadas en Colombia estén oportunamente informadas sobre el panorama de ciberseguridad y puedan tomar las acciones preventivas necesarias.

- **Tenable ONE (Web y On-premise):** Es una solución integral que escanea y gestiona vulnerabilidades en los activos tecnológicos, Ayuda a medir de forma continua la ciberpostura, identificando debilidades tanto en la nube, web, DA como en servidores locales.

Category	Qty	# Units	Item	Description
New	1	36,200	TONE	Tenable One Tenable Vulnerability Management, Tenable Security Center Plus, Tenable Security Center Director, Tenable Identity Exposure, Tenable Cloud Security Standard and Enterprise, Tenable CIEM, Tenable Web App Scanning, OT Security, Attack Surface Management, Lumin Exposure View and Attack Path Analysis. Number of Tenable Web App Scanning has limits based on the actual asset count purchased. Annual Subscription based on number of Assets.
New	1	4,500	TONE-OT	Tenable One OT Security Companion License for both Tenable One Standard and Tenable One Enterprise

- **Cisco Umbrella DNS Security Advantage**

Solución de seguridad de capa de red que protege la infraestructura mediante el bloqueo preventivo de dominios maliciosos antes de que se establezca una conexión IP. Su arquitectura permite realizar una investigación profunda de consultas DNS para identificar patrones de tráfico sospechosos, proporcionando visibilidad total sobre las solicitudes de internet realizadas por usuarios locales y remotos. Esta herramienta facilita la revisión exhaustiva del tráfico saliente para detectar exfiltración de datos o comunicaciones con centros de comando y control, garantizando una cobertura ininterrumpida por un periodo mínimo de doce meses bajo un modelo de protección nativa en la nube.

- **VMware (ESXi, vCenter, vSphere):**

Software que permite crear y administrar servidores virtuales, optimizando el uso del hardware físico disponible. Su objetivo es dar flexibilidad y estabilidad a la infraestructura del ColCERT, facilitando el despliegue rápido de nuevos servicios.

- **Solución DFIR – Torre Forense:**

Es un conjunto de herramientas especializadas para la respuesta a incidentes y el análisis forense digital directamente en el lugar de los hechos. Permite recolectar evidencias técnicas de ataques de forma segura y profesional para apoyar procesos judiciales o de investigación.

Torre Forense - Características

Procesador:

- Intel Core i9 (14ª Generación) i9-14900KS Procesador Tetracosa-core (24 núcleos) a 3.20 GHz - 36MB de caché L3 - 32MB de caché L2 Velocidad de overclocking de 6.20 GHz - Socket LGA-1700 - Intel UHD Graphics 770 (Sí, gráficos integrados) - 150 W - 32 hilos

Memoria:

- 192GB (4x48GB) DDR5-6000/PC5-48000 DDR5 SDRAM - Memoria de doble rango - CL32 - 1.35 V - No ECC – No registrada - 288 pines – DIMM

Video:

- Tarjeta gráfica NVIDIA GeForce RTX 4070 SUPER - 12 GB GDDR6X - Resolución de 7680 x 4320 - 1.98 GHz de velocidad base - 2.49 GHz de velocidad de impulso - Ancho de bus de 192 bits - PCI Express 4.0 x16 - 3 x DisplayPort – HDMI

Audio:

- Realtek S1220A 7.1 Surround Sound, Códec de audio de alta definición, 5 jacks de audio

Unidad del Sistema/APP:

- 1TB SSD - M.2 2280 Interna - PCI Express NVMe 4.0 x4 - Velocidad máxima de lectura de 7450MB/s - Cifrado AES de 256 bits

Unidad de caché/temporal:

- 2TB SSD - M.2 2280 Interna - PCI Express NVMe 4.0 x4 - Velocidad máxima de lectura de 7450MB/s - Cifrado AES de 256 bits

Unidad PG/DB:

- 4TB SSD - M.2 2280 Interna - PCI Express NVMe 4.0 x4 - Velocidad máxima de lectura de 7450MB/s - Cifrado AES de 256 bits

RAID:

- Controlador SAS 8i - 12Gb/s SAS, RAID soportado - Niveles RAID 0, 1, 5, 6, 10, 50, 60, JBOD - 1 x SFF-8654 – 8 puertos SAS en total

Dispositivos externos de evidencia forense y almacenamiento adicional:

- 1x Caja para discos 5.25" - Interfaz de host Serial ATA/600 interna - Bahías intercambiables en caliente - 5 x bahías para discos de 2.5"/3.5"
- 5x 18TB (RAID-5) HHD - 3.5" Interno - SAS (12Gb/s SAS) - Dispositivo de almacenamiento en arreglo -7200rpm
- 1x Rack miniSAS de 5.25" a 4x 2.5" SATA SAS 12 Gb/s con intercambio en caliente
- 1x SSD QVO de 8TB - 2.5" Interno - SATA (SATA/600)
- 1x SSD EVO de 2TB - 2.5" SATA (SATA/600)
- 2x Bahías abiertas
- 1x Cajón de disco duro SATA (vacío) - Bahía de 5.25” - Rack móvil SATA de 3.5” - Rack - Bahía de disco duro extraíble

HARDWARE FORENSE:

- Óptico: Grabadora triple 16X (DVD/CD/Blu-Ray)
- Logicube WriteProtect-BAY, bloqueador forense de escritura SAS/SATA/USB3/FW. Conexión host USB 3.0

- Ace Exclusive Extendable Cooling Bay con Hub USB 3.X integrado y lector de tarjetas micro forense
- Tarjeta de expansión USB PCIe – Puertos traseros adicionales

Monitor:

- 1x Monitor de 34"

Teclado/raton:

- Combo de teclado y ratón inalámbrico, ratón inalámbrico USB RF - Óptico - 3 botones - Rueda de desplazamiento

Sistema operativo:

- Windows 11 Pro de alta gama (Español)

Capacitación:

- Capacitación certificada de 4 horas por el canal o Fabricante

Soporte:

- Soporte y mantenimiento por 12 meses.

Licenciamiento MAGNET AXIOM CYBER

Solución de respuesta a incidentes y análisis forense digital para adquirir y analizar de forma remota evidencia de computadoras, junto con la nube, IoT y dispositivos móviles.

- MÓVIL: Procesamiento y análisis de extracciones de iOS y Android, con integración directa de GrayKey y soporte para herramientas de terceros como UFED, Oxygen y más.
- COMPUTADORA: Recuperación de evidencia de dispositivos Windows, Mac, Chrome y Linux. para análisis de RAM, historial del navegador, los archivos eliminados entre otros.
- NUBE: Adquirir y analizar información depositada en sitios de Internet, a través de las credenciales y claves de acceso encontradas en dispositivos móviles y que están sincronizados con sitios de servicios web de los usuarios propietarios.
- Transferencia de conocimiento: Transferencia de conocimiento por parte del canal o distribuidor por 4 horas.

Soporte:

Soporte y mantenimiento por 12 meses.
Soporte y mantenimiento sistema de videwall RGBlink - Ref: Q16PRO GEN2-8U

matriz de 3X6 (Pantalla industrial de 55 pulgadas LG Ref 55VSH7J)

Garantizar la operatividad continua del sistema videowall de 3x6 mediante revisiones técnicas periódicas para prevenir fallos y la corrección inmediata de averías en sus paneles o controladores. Incluye el soporte técnico especializado para la calibración de imagen y la actualización de software y firmware de los procesadores de video para asegurar la compatibilidad con nuevas fuentes de señal. El objetivo es mantener una visualización óptima y sin interrupciones para el monitoreo situacional, optimizando la vida útil de los componentes electrónicos del sistema.

Monitoreo Continuo, Detección Avanzada y Respuesta Eficiente ante Incidentes de Seguridad

Para garantizar un esquema de defensa robusto y permanente en las entidades beneficiarias, el proyecto implementará un servicio de monitoreo continuo 24/7 basado en la solución CrowdStrike Falcon® Enterprise. Esta plataforma nativa en la nube unifica en un único agente funciones de antivirus de nueva generación, detección y respuesta extendida, inteligencia de amenazas y cacería gestionada, permitiendo identificar y neutralizar ataques conocidos y desconocidos en tiempo real. Su arquitectura ligera y su capacidad de reconstrucción detallada de incidentes, combinada con análisis contextual e investigación humana especializada, aseguran una respuesta oportuna y una reducción significativa de los tiempos de detección y remediación. Con estas capacidades, el ColCERT podrá centralizar la supervisión de miles de activos territoriales, ejecutando acciones de contención guiada, fortaleciendo la resiliencia institucional y compensando las brechas tecnológicas que actualmente afectan a las entidades públicas, especialmente a aquellas sin infraestructura de seguridad moderna.

Características Tecnicas

- Plataforma nativa en la nube que unifica NGAV, EDR, inteligencia de amenazas y cacería gestionada en un único agente ligero, facilitando despliegues rápidos y operación centralizada.
- Antivirus de nueva generación alimentado por IA y machine learning que bloquea malware conocido, desconocido, ransomware, ataques sin archivos y amenazas de Estado-nación en tiempo real.
- Capacidades avanzadas XDR/EDR con captura de eventos sin procesar, visibilidad histórica y reconstrucción detallada de incidentes mediante CrowdScore™ e Incident Workbench.
- Servicio de cacería gestionada 24/7 (Falcon OverWatch) ejecutado por expertos que investigan actividades sigilosas, priorizan amenazas críticas y reducen falsos positivos.
- Control granular de dispositivos USB con políticas avanzadas para evitar fugas de información y refuerzo adicional mediante un firewall de host administrado centralmente.
- Inteligencia integrada que analiza tácticas, técnicas y procedimientos (TTP) de adversarios, apoyada en Threat Graph para correlación histórica y análisis contextual del entorno.
- Agente multiplataforma de mínimo impacto compatible con Windows, macOS, Linux, ChromeOS, iOS y Android, ofreciendo protección online y offline bajo un modelo de actualización continua.
- Capacidades de respuesta remota que permiten contener, investigar y remediar endpoints comprometidos con acciones guiadas desde la plataforma Falcon.
- Visibilidad unificada del entorno con análisis en tiempo real y datos contextualizados que aceleran la toma de decisiones y reducen significativamente MTTD/MTTR.
- Soporte técnico especializado 24/7 provisto por expertos de CrowdStrike, con recursos educativos avanzados para despliegue, operación y optimización continua de la solución.

Línea de servicios para el proceso de Formación y Generación de Capacidades

La adquisición e implementación de una plataforma tecnológica de formación será el eje articulador de esta línea. Se optará por una solución avanzada, basada en inteligencia artificial y algoritmos propietarios, que favorezca la predicción de tendencias de formación y la personalización del aprendizaje. La plataforma será parametrizable y escalable, adaptable a los requerimientos inmediatos y futuros del MinTIC, y deberá contemplar como mínimo:

- Retos por áreas técnicas que incluyan: criptografía, forense, explotación web, pentesting, reversing, etc.
- Formatos de competencia Individual, por equipos, por niveles, tiempo limitado o ranking abierto.
- Plataforma 100% web Accesible desde navegador sin instalación.
- Gamificación completa Puntuación automática, rankings, badges y progresión por niveles.
- Integración con formación previa Se puede usar como evaluación después de procesos de entrenamiento.
- Métricas y reportes Análisis detallado por participante, tipo de reto, tiempo de resolución.
- Administración integral de usuarios y perfiles, con autenticación segura y mecanismos eficientes de recuperación y modificación de credenciales.
- Registro de auditoría exportable, detallando ID de usuario, dirección IP de origen, fechas y horas de inscripción, eventos y accesos, permitiendo un seguimiento transparente y sistemático.
- Compatibilidad con dispositivos, navegadores y sistemas operativos diversos, garantizando el acceso equitativo para la totalidad de los beneficiarios.
- Gestión integral de solicitudes y seguimiento personalizado de procesos, a través de un único formulario nacional de inscripción, reportes de inscritos cada 15 días y asistencia activa en la certificación de cada participante.
- Provisión de herramientas de simulación durante el desarrollo del proyecto, asegurando la realización de talleres prácticos y laboratorios de simulación (cyber-range).
- Programas de formación con una duración mínima de 40 horas, impartidos por personal docente especializado, entregando certificados a quienes culminen cada nivel y garantizando al menos una clase sincrónica obligatoria, grabada y disponible para consulta posterior.
- Enfoque curricular en la práctica, incorporando ejercicios, laboratorios y competencias en entornos simulados y rastreables, evitando contenidos puramente teóricos.

La estrategia de formación y promoción responderá a los objetivos estratégicos del plan sectorial TIC, alcanzando una amplia difusión y adhesión de los públicos objetivo.

Actividades Claves para la ruta de formación

- Diseño e implementación de talleres prácticos y laboratorios de simulación, con evaluación de competencias en ciberseguridad, alineados al marco de referencia nacional.
- Desarrollo de clases sincrónicas obligatorias, grabadas y disponibles para consulta, que contribuyan a la consolidación de capacidades técnicas especializadas.
- Ejecución de estrategias de difusión segmentada, garantizando el acceso y adhesión de públicos objetivo y favoreciendo la apropiación de la cultura de seguridad digital.
- Integración sistemática de elementos institucionales y visuales en todas las plataformas y materiales, asegurando coherencia y reconocimiento público del proyecto y sus objetivos.
- Establecimiento de mecanismos rigurosos para el monitoreo y seguimiento, con generación de informes basados en indicadores de impacto y canales de comunicación eficaces entre aliados, ColCERT y personas beneficiarias.

- Implementación de procesos de retroalimentación y mejora continua, adaptando las intervenciones a las lecciones aprendidas y a los objetivos específicos del documento de Estrategia Nacional de Seguridad Digital.

Meta de formación:

Formar a 5.000 usuarios en competencias tanto básicas de ciberseguridad como especializadas a través de las siguientes líneas:

- Formación AWARENESS Profesionales
- Competencias CTF Ciudadanía, Profesionales y funcionarios

La iniciativa está dirigida a:

Ciudadanos colombianos mayores de edad interesados en desarrollar competencias digitales en ciberseguridad con formación y experiencia básica en infraestructura tecnológica, riesgo y seguridad digital que quieran ampliar sus conocimientos y servidores públicos de entidades nacionales y territoriales, con funciones relacionadas con infraestructura tecnológica y gestión del riesgo digital.

Para la selección de los beneficiarios se tendrá en cuenta, además de lo anteriormente señalado, la fecha y hora de registro para verificación del cumplimiento de los requisitos para su inscripción a la formación hasta llegar al cupo disponible de este contrato.

Los criterios para seleccionar los beneficiarios son: mayor edad; Técnico, tecnólogo u profesional relacionadas con el sector de las TICs.

En síntesis, este proyecto impactará de manera integral el ecosistema digital colombiano, incrementando el nivel de preparación y habilidades de líderes de seguridad, profesionales TIC y servidores públicos, fortaleciendo la capacidad de las organizaciones para enfrentar los desafíos del panorama de amenazas cibernéticas en el país.

Lo anterior, es debido a la escasez de talento especializado en seguridad digital en Colombia, falta de formación continua y baja sensibilización. La Estrategia Nacional de Seguridad Digital 2025-2027 propone fortalecer la fuerza laboral mediante programas educativos, certificaciones reconocidas, alianzas con instituciones y apoyo a PYMES. Además, promueve la actualización constante en protección de datos y estándares internacionales.

Así mismo, el desarrollo de una fuerza laboral capacitada es clave porque permite responder ante amenazas cibernéticas sofisticadas, fortalece la protección de la información y mejora la estabilidad institucional. Invertir en talento humano especializado facilita la adaptación a nuevas tecnologías, el cumplimiento normativo y posiciona a Colombia como referente regional en seguridad digital.

En consecuencia, se da cumplimiento a la macrometa institucional en lo relacionado a la formación de personas en seguridad digital.

Estrategia de Comunicación e Imagen Institucional

Toda acción de comunicación y difusión cumplirá a cabalidad los lineamientos de imagen institucional del MinTIC y ColCERT. El logotipo oficial se integrará en la plataforma de formación y en todas las piezas publicitarias, garantizando la coherencia visual y la adecuada representación del proyecto ante la ciudadanía. La aprobación y ajuste de materiales se concertarán con las autoridades responsables, asegurando la transparencia y alineación a la política institucional.

1 SEGUIMIENTO, EVALUACIÓN Y MEJORAMIENTO CONTINUO

Se establecerán mecanismos rigurosos para el control de calidad y el monitoreo del avance, mediante la generación de informes periódicos, el seguimiento de indicadores clave y la implementación de canales de comunicación efectivos entre aliados, ColCERT y beneficiarios. Se fomentará la retroalimentación constante para la mejora continua, adaptando los procesos a las lecciones aprendidas y evolucionando conforme a los objetivos estratégicos definidos en el plan sectorial TIC.

PERFILES PROFESIONALES REQUERIDOS – 50% DEDICACIÓN A LA EJECUCIÓN DEL CONTRATO

- Gerente General del Proyecto – Experiencia mínima: 5 años

El Gerente General del Proyecto será el responsable de liderar integralmente la ejecución del contrato, garantizando el cumplimiento de los objetivos, hitos, entregables técnicos y administrativos establecidos por el Ministerio TIC y el ColCERT. Este profesional deberá ser ingeniero de sistemas, telecomunicaciones, electrónico o de carreras afines, con estudios complementarios o certificaciones en gestión de proyectos y conocimientos en ciberseguridad. Su trayectoria deberá demostrar al menos cinco años de experiencia en la dirección, implementación y supervisión de proyectos tecnológicos o de seguridad digital, preferiblemente en el sector público.

Dentro de sus funciones se encuentra asegurar la coordinación continua entre el contratista y el equipo técnico del ColCERT, supervisar la entrega oportuna de licenciamientos, plataformas y servicios asociados al MDR, validar informes técnicos y operativos, y garantizar la correcta ejecución de las actividades previstas en el Anexo Técnico. Será el enlace principal para el seguimiento contractual, la interlocución interinstitucional y la resolución de riesgos o contingencias que puedan afectar el cronograma. Además, deberá velar por la calidad de la documentación entregada, la trazabilidad de los procesos y la estricta adherencia a las políticas de seguridad de la información y tratamiento de datos personales del Ministerio TIC. Con un tiempo de dedicación del 50 %, para el seguimiento de las actividades según las responsabilidades.

- Líder de Despliegue Tecnológico y Operación de Soluciones – Experiencia mínima: 3 años

El Líder de Despliegue Tecnológico será el profesional encargado de coordinar y ejecutar las actividades técnicas relacionadas con la instalación, configuración, afinamiento, operación y soporte de los licenciamientos y herramientas adquiridas o renovadas en el marco del proyecto. Este perfil deberá ser ingeniero de sistemas, telecomunicaciones, electrónico o de áreas relacionadas, con conocimientos demostrables en ciberseguridad y experiencia mínima de tres años en la implementación y operación de plataformas de seguridad digital, gestión de vulnerabilidades, infraestructura virtualizada y servicios de monitoreo. Es indispensable que cuente con experiencia específica en la puesta en marcha y seguimiento de soluciones MDR, EDR/XDR o SOC, incluyendo el despliegue de agentes, integración de fuentes de telemetría, creación de tableros y afinamiento de reglas de detección.

El profesional será responsable de asegurar que todas las soluciones entregadas estén correctamente instaladas y operativas dentro de los plazos definidos, incluyendo la configuración de línea base, la integración con el equipo técnico del ColCERT, el aseguramiento de compatibilidades, la gestión de actualizaciones y la documentación técnica

correspondiente. Asimismo, deberá atender requerimientos de soporte especializado, garantizar la correcta recolección de información para análisis, mantener operativos los dashboards de monitoreo, y acompañar la transferencia de conocimiento al equipo del ColCERT, facilitando sesiones prácticas basadas en estándares del fabricante. Con un tiempo de dedicación del 50 %, para el seguimiento de las actividades según las responsabilidades.

- Líder de Formación, Capacitación y Transferencia de Conocimiento – Experiencia mínima: 3 años

El Líder de Formación y Transferencia de Conocimiento será el responsable del diseño, adecuación, coordinación y ejecución de los programas de capacitación y certificación previstos en el proyecto, incluyendo cursos virtuales, laboratorios prácticos, actividades en cyber-range y sesiones especializadas para el personal del ColCERT y las entidades beneficiarias. Este profesional deberá ser ingeniero de sistemas, telemático, informático o de áreas afines, con conocimientos en seguridad digital, pedagogía aplicada a TI o experiencia comprobada en procesos de formación técnica. Se requiere una experiencia mínima de tres años en el diseño, impartición o gestión de proyectos de capacitación relacionados con ciberseguridad, tecnologías de la información o despliegue de herramientas tecnológicas. Con un tiempo de dedicación del 50 %, para el seguimiento de las actividades según las responsabilidades.

TRANSFERENCIA DE CONOCIMIENTO DE LICENCIAMIENTOS, HERRAMIENTAS Y SOLUCIONES TECNOLÓGICAS

La transferencia de conocimiento constituye un componente esencial para garantizar la apropiación, sostenibilidad y correcta operación de los licenciamientos, soluciones tecnológicas y herramientas adquiridas en el marco del proyecto. Este proceso deberá ser coordinado directamente con la supervisión designada por el Ministerio TIC/ColCERT, asegurando que los contenidos formativos respondan a las necesidades operativas de la entidad y a las capacidades requeridas para la administración técnica de las plataformas durante toda la vigencia contractual.

El contratista deberá garantizar que la transferencia de conocimiento sea impartida por personal certificado por el fabricante de cada herramienta o solución, asegurando el cumplimiento de los estándares oficiales y la calidad formativa. Cada paquete de licenciamiento deberá incluir un mínimo de 16 horas de capacitación especializada, distribuidas en sesiones teóricas y prácticas que aborden la instalación, configuración, operación, afinamiento, monitoreo y mejores prácticas del fabricante. Las capacitaciones deberán incluir la entrega de material técnico en español, documentación actualizada, manuales operativos, guías de referencia rápida y acceso a plataformas de entrenamiento cuando el fabricante así lo permita.

En el desarrollo de la transferencia de conocimiento deberán contemplarse componentes básicos e imprescindibles tales como:

- Arquitectura técnica de la solución y sus principios de funcionamiento.

- Despliegue, configuración inicial y validación de compatibilidad con la infraestructura del Ministerio y las entidades beneficiarias.
- Gestión diaria de la herramienta, interpretación de alertas, buenas prácticas operacionales y lineamientos de administración segura.
- Integración con otros sistemas de monitoreo o gestión de seguridad, cuando aplique.
- Procedimientos para actualización, fortalecimiento, resolución inicial de incidencias y uso adecuado del soporte del fabricante.
- Lineamientos de seguridad, privacidad, tratamiento de información y manejo de registros técnicos derivados del uso de la solución.

La transferencia deberá incluir espacios de demostración funcional, simulación de escenarios de uso real y resolución de dudas técnicas, permitiendo que los equipos técnicos del ColCERT cuenten con capacidades adecuadas para operar las herramientas de manera independiente.

SOPORTE TÉCNICO, MANTENIMIENTO Y ACTUALIZACIÓN DE LICENCIAMIENTOS

El servicio de soporte técnico constituye un componente transversal que garantiza la continuidad operativa, estabilidad funcional y aprovechamiento pleno de las soluciones tecnológicas desplegadas durante los doce (12) meses de vigencia del contrato. El contratista será responsable de proporcionar soporte técnico especializado de primer, segundo y tercer nivel, articulado con el fabricante de cada solución y sujeto a los acuerdos de niveles de servicio establecidos en el Anexo Técnico.

El soporte incluirá actividades de mantenimiento preventivo y correctivo, atención de incidentes, gestión de actualizaciones, aplicación de parches, acompañamiento en ajustes de configuración, análisis de fallas y validación de funcionamiento posterior a cada intervención. Cada licenciamiento entregado deberá acompañarse del servicio de soporte oficial del fabricante, garantizando acceso directo a documentación especializada, bases de conocimiento, actualizaciones, matrices de compatibilidad y gestión de casos técnicos que requieran intervención experta.

El contratista deberá establecer un plan de escalamiento formal, que contemple los tiempos máximos de respuesta y resolución, los flujos de comunicación entre niveles técnicos y los responsables de cada instancia. Este plan incluirá la interacción directa con el fabricante para la resolución de casos complejos, asegurando que los problemas críticos se escalen sin demoras y que la supervisión del proyecto disponga de visibilidad total sobre el estado de cada requerimiento.

Asimismo, el proyecto contará con una mesa de servicios dedicada para la recepción, registro, clasificación y seguimiento de incidentes o solicitudes técnicas derivadas del uso de las soluciones adquiridas. Esta mesa deberá operar con disponibilidad acorde al nivel de criticidad de las herramientas (incluyendo atención 24/7 cuando la herramienta lo requiera), registrar cada caso en un sistema de atención con trazabilidad completa y garantizar la generación de reportes periódicos para la supervisión.

Durante la vigencia del contrato, el provvedor deberá asegurar que todas las soluciones, plataformas y licencias se mantengan actualizadas a sus versiones más recientes, incluyendo parches de seguridad, mejoras funcionales y actualizaciones críticas del fabricante. Cualquier actualización deberá ser previamente validada en coordinación con el equipo técnico del ColCERT, confirmando su compatibilidad y evitando interrupciones operacionales.

Finalmente, al término del proyecto, el contratista deberá entregar a la supervisión toda la documentación relacionada con el soporte prestado, los reportes de incidentes atendidos, las actualizaciones aplicadas, los certificados de soporte del fabricante y las recomendaciones para asegurar la continuidad operativa posterior a la finalización del contrato

ACUERDO DE NIVELES DE SERVICIO ANS

Entrega y activación de licenciamientos

Objetivo. Garantizar continuidad operativa sin brechas de cobertura, entregando licencias a tiempo, con soporte de fabricante y trazabilidad documental.

Compromisos.

- Entrega y activación de cada licencia hasta 15 días calendario antes del vencimiento previo o dentro del plazo acordado para nuevas adquisiciones; documentación en orden (derecho de uso, versión y soporte vigente). Buenas prácticas exigen plazos claros y remedios ante demoras.
- Soporte del fabricante incluido en cada licencia (nivel estándar o superior) y acceso a actualizaciones durante los 12 meses de vigencia. [crowdstrike.com]

Métricas.

- Tasa de activación a tiempo ≥ 98% (licencias activas dentro de la ventana comprometida). Basado en prácticas de gestión contractual y control de SLAs (entrega y performance).
- Cumplimiento documental (100% licencias con evidencia de soporte vigente).

Objetivo. Asegurar cobertura ininterrumpida 24/7/365, con detección, análisis y contención guiada.

Disponibilidad del servicio.

- Uptime de la plataforma ≥ 99,9% mensual para los componentes cloud, excluyendo mantenimientos programados y causas de fuerza mayor, con esquema de créditos por indisponibilidad por debajo del umbral (cuando aplique). Este umbral es consistente con SLAs de SaaS de referencia y compromisos típicos de disponibilidad. [unlimited.humio.com], [odoo.com], [dev.to]

Métricas operativas MDR/SOC.

- MTTD (Mean Time To Detect): objetivo en minutos para incidentes P1/P2 en horas críticas (p. ej., ≤15 min); la literatura de MDR y operación SOC prioriza MTTD/MTTR como KPI centrales y sitúa expectativas de respuesta en “minutos”, no horas.
- MTTR (Mean Time To Respond/Recover): objetivo ≤4 horas para P1 con acciones de contención guiada y medidas de erradicación inicial; benchmarks de respuesta y resolución se alinean con prácticas ITSM y marcos de incidentes.
- Cacería gestionada 24/7 (Falcon OverWatch) activa con alertamiento y guía de remediación; OverWatch está diseñado para priorizar amenazas críticas y apoyar la contención en coordinación con el equipo del cliente.

Soporte y atención de casos (prioridades).

- P1 – Crítico (brecha activa, indisponibilidad mayor o propagación rápida): ack 5–15 min, acción inicial ≤60 min, actualizaciones cada 15–30 min.
- P2 – Alto (degradación relevante sin paro total): ack ≤30 min, acción inicial ≤4 h, actualizaciones cada 30–60 min.
- P3 – Medio y P4 – Bajo: respuesta y resolución conforme a matriz ITIL (p. ej., P3 en 1–3 días hábiles; P4 en 3–5 días hábiles), con frecuencia de actualización acorde a impacto/urgencia.

Mesa de servicios y escalamiento.

- Service Desk 24/7 para registro, clasificación y seguimiento; matriz de escalamiento técnico y jerárquico con tiempos máximos por prioridad (incluye escalamiento al fabricante cuando aplique).

CUMPLIMIENTO NORMATIVO Y ALINEACIÓN CON POLÍTICAS DE SEGURIDAD

El contratista debe alinear sus procesos y procedimientos con las políticas de seguridad y protección de datos del Ministerio TIC, garantizando la confidencialidad, integridad y disponibilidad de la información. El cumplimiento de la normativa vigente y la firma de acuerdos de confidencialidad por parte del personal técnico son actividades críticas para la protección de los datos y la confianza institucional.

1.3. ASPECTO LEGAL

El Artículo 113 de la Constitución Política señala cuáles son las Ramas del Poder Público para la realización de las funciones del Estado y contempla además que *"Los diferentes órganos del Estado tienen funciones separadas, pero colaboran armónicamente para la realización de sus fines".*

De la misma manera, el artículo 6° de la Ley 489 de 1998, dispone que, en virtud del principio de coordinación y colaboración, las autoridades administrativas deben garantizar la armonía en el ejercicio de sus respectivas funciones con el fin de lograr los fines y cometidos estatales.

En concordancia con lo anterior, artículo 32 de la Ley 80 de 1993 señala: "De los Contratos Estatales. Son contratos estatales todos los actos jurídicos generadores de obligaciones que celebren las entidades a que se refiere el presente estatuto, previstos en el derecho privado o en disposiciones especiales, o derivados del ejercicio de la autonomía de la voluntad, así como los que, a título enunciativo, se definen a continuación (…)". Así mismo, y en ejercicio de la autonomía de la voluntad, las entidades estatales señaladas en el artículo 2º de la Ley 80 de 1993, podrán celebrar directamente contratos entre ellas, siempre que las obligaciones de este tengan relación directa con el objeto de la entidad ejecutora bajo la modalidad de Contratos Interadministrativos, entre otros. La presente contratación se adelantará bajo modalidad de selección por CONTRATACIÓN DIRECTA, como quiera que el objeto de esta se ajusta a la causal de que trata el literal c) del numeral 4º del artículo 2 de la Ley 1150 de 2007, (modificado por el artículo 92 de la Ley 1474 de 2011) que establece: "…4. Contratación directa. La modalidad de selección de contratación directa solamente procederá en los siguientes casos: … c) Contratos interadministrativos, siempre que las obligaciones derivadas del mismo tengan relación directa con el objeto de la entidad ejecutora señalado en la ley o en sus reglamentos…"; y acorde con el artículo 2.2.1.2.1.4.4. del Decreto 1082 de 2015 que señala: "... Convenios o contratos interadministrativos. En ese orden y dada la compatibilidad y las funciones asignadas a las entidades estatales que participaran en el contrato, el fundamento jurídico aplicable es el definido para un contrato interadministrativo

2. COMPORTAMIENTO DEL GASTO HISTÓRICO

Con el ánimo de identificar experiencias de contratación similares que permitan definir parámetros para la estructuración del proceso, se identificaron en el Sistema Electrónico de Contratación Pública SECOP II, procesos adelantados por diferentes entidades públicas y por el Ministerio TIC/ Fondo Único de Tecnologías de la Información y las Comunicaciones, por diferentes modalidades de selección cuyo objeto de contratación fue similar a la del presente proceso contratación, guardando su especificidad cada uno.

A. ¿Cómo ha adquirido la Entidad Estatal en el pasado este bien, obra o servicio? Al realizar la búsqueda por medio de la herramienta SECOP II, pudo determinarse que el Ministerio de Tecnologías de la Información y las Comunicaciones / Fondo único de tecnologías de la información y las comunicaciones ha realizado en el pasado contratación de selección de objetos que incorporan el componente de capacitación:

ENTIDAD	REFERENCIA DEL PROCESO	OBJETO	VALOR	DURACIÓN (meses)	ESTADO DEL PROCESO
FUTIC/ MINTIC	FTIC-CD-1232-2023	Aunar esfuerzos para desarrollar un ecosistema de seguridad digital que impulse procesos de innovación y desarrollo tecnológico, mediante el estudio de escenarios que promuevan la gestión del conocimiento de los riesgos cibernéticos y las afectaciones de los incidentes de seguridad digital entre los diferentes grupos poblacionales del territorio colombiano	6.099.490.000	48 DÍAS	Proceso adjudicado y celebrado Modalidad: Convenio interadministrativo
MINTIC / FUTIC	FTIC-CD-1225-2023	Aunar esfuerzos técnicos, administrativos y financieros para el fortalecimiento de las competencias en seguridad digital de las personas en general para aumentar la confianza en el uso del entorno digital, en desarrollo de las actividades del Grupo de Respuestas a Emergencias Cibernéticas de Colombia - COLCERT coordinado por el Ministerio de Tecnologías de la Información y las Comunicaciones.	$ 3.209.433.454	51	Proceso adjudicado y celebrado Modalidad: Convenio interadministrativo
MINTIC	MTIC-SAPMC 002-202	Capacitar a un grupo de servidores del Ministerio de Tecnologías de la Información y las Comunicaciones en temáticas aprobadas en el Plan Institucional de Capacitación 2022, para el fortalecimiento de sus competencias según lo establecido	$205.103.521	47	Selección Abreviada de Menor Cuantía

		en las políticas de gestión y desempeño de talento humano e integridad			

El gobierno nacional ha desarrollado instrumentos de política pública e iniciativas para crear una cultura de la seguridad digital que permita proteger las actividades, las personas y la sociedad, sin inhibir los beneficios y oportunidades de las TIC.

Desde 2020 Colombia actualizó su política nacional de Seguridad Digital, para incluir un enfoque centrado en la generación de confianza en el uso del entorno digital, en línea con las recomendaciones de la OCDE, dicha política se materializó con la expedición del CONPES 3995 – Política de Confianza y Seguridad Digital, que incluyó un ambicioso plan de acción para:

a. Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado.
b. Actualizar el marco de gobernanza en materia de seguridad digital.
c. Adoptar modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías. Por otro lado, en el marco de la implementación de la Política de Confianza y Seguridad Digital se expidió el Decreto 338 de 2022 mediante el cual:

- Se actualizó el marco para la gobernanza nacional de la seguridad digital.
- Se fortalecieron los equipos nacionales de respuesta a incidentes de seguridad digital.
- Se definieron instrumentos para la identificación de infraestructuras críticas del sector público.

Esta normativa, también, determina los roles y compromisos de los diferentes entes responsables de la ciberseguridad en el país y la forma en que se deben coordinar; además, formaliza el Comité Nacional de Seguridad Digital que tiene como propósito adoptar un esquema de múltiples partes interesadas y brindar confianza a la ciudadanía. De esta forma, define sus participantes y la manera en que operará, así mismo, se formalizan e impulsan las estructuras de los equipos y/o grupos de respuesta a emergencias cibernéticas de Colombia tales como: El Grupo de Respuesta a Emergencias Cibernéticas de Colombia -ColCERT, Csirt del Gobierno de Colombia y Csirt de defensa, entre otros.

B. **¿Cómo adquieren otras Entidades Estatales y las empresas privadas este bien, obra o servicio?**

Se adelantó la revisión de demanda histórica, con el fin de definir algunos de los parámetros para la estructuración del proceso aquí pretendido. Se identificaron en el Sistema Electrónico de Contratación Pública SECOP II, procesos adelantados por diferentes entidades públicas, en diferentes modalidades de selección sobre plataformas SOC/NOC cuyo objeto de contratación fue similar a la del presente proceso contratación.

ENTIDAD	OBJETO	NO. PROCESO	VALOR	FECHA DE PUBLICACIÓN
Alcaldía Local de Kennedy	Formación E Incentivos Seguridad	FDLK-LP-014-2023	$ 929.292.532	7/09/2023
Instituto Para El Desarrollo De Antioquia Idea	Sistema De Gestión De Seguridad De La Información	SAMC 014 DE 2023	$ 85.412.250	7/09/2023

	Ciberseguridad			
Municipio Bucaramanga	Adquisición, Municipio Bucaramanga De implementación, configuración, migración, capacitación, soporte y puesta en funcionamiento de un sistema de información en ambiente web multiplataforma (web y móvil), que permita gestión.	SSYA-SAMC-00-4 2023	$ 296.818.497	4/09/2023
Comando General De Las Fuerzas Militares	Contratar la capacitación y entrenamiento en ciberseguridad y ciberdefensa	259COGFM DIADF 2023	$ 240.000.000	14/08/2023
Secretaria Distrital De Seguridad, Convivencia Y Justicia	Capacitación Para La Secretaría Distrital De Seguridad, Convivencia Y Justicia, En Los Temas Determinados Dentro De Los Ejes Temáticos Del Plan Institucional De Capacitación.	SCJ-SAMC-001 2023	$ 486.437.718	10/07/2023

En la consulta de las diferentes plataformas de Gestión de contratos públicos, se evidencia que diversas entidades han contratado en capacitación en ciberseguridad, sin embargo no se han presentado contratos de la magnitud de la contratación de un centro de monitoreo de ciberseguridad nivel nacional, es por esto que la entidad requiere un proveedor con experiencia extensa en temas de ciberseguridad y infraestructura de software para garantizar una solución integral y acorde al alcance del proyecto.

Dinámica de producción, distribución y entrega de bienes, obras o servicios

La dinámica de la entrega de servicios TIC puede variar dependiendo de la empresa y su enfoque. Un modelo de entrega de servicios de tecnología se enfoca en generar valor para la empresa, habilitando servicios o productos que permitan una entrada en el mercado más rápida y creando una cultura de mejora continúa centrada en el cliente. Esto implica un cambio organizacional y favorece la generación de ideas, la experimentación y el aprendizaje.

La dinámica de producción y distribución de los proyectos tecnológicos involucra una serie de etapas clave que van desde la concepción de la idea hasta la entrega final del producto o servicio al usuario final. Este proceso abarca no solo aspectos técnicos, sino también económicos, logísticos, y de marketing, entre otros. A continuación, te describo las

principales fases involucradas en esta dinámica.

Una fase inicial de Investigación y Desarrollo, en la cual se involucran etapas de Innovación y Evaluación, una fase de Desarrollo y Producción, una fase de Logística y cadena de suministro y finalmente unas etapas de soporte y transferencia de conocimiento. La dinámica de producción y distribución de proyectos tecnológicos es un proceso complejo que involucra múltiples fases, desde investigación y desarrollo inicial hasta el mantenimiento y la mejora del producto a largo plazo, los agentes deben ser ágiles, innovadoras y capaces de adaptarse a las cambiantes necesidades del mercado y la tecnología.

En el mercado colombiano existen diversas personas jurídicas que cumplen con estándares de capacitación en Ciberseguridad que pueden prestan el servicio requerido por el Ministerio de las Tecnologías de la Información y las Comunicaciones, que a través de su experiencia en ámbitos públicos y privados se han caracterizado por su cumplimiento dentro de los términos de calidad y eficiencia. En el Sistema de contratación Pública – SECOP, así como en el sistema integrado de información societaria (SIIS) de la Superintendencia de Sociedades de Colombia se pueden identificar posibles proveedores, empresas, universidades o personas jurídicas que realicen formación en Ciberseguridad.

En la consulta de diversas plataformas de Gestión de Contratos Públicos, se observa que varias entidades han optado por contratar soluciones de ciberseguridad para capacitar a su personal para prevenir ataques informáticos. Estas contrataciones, aunque relevantes, no han alcanzado la magnitud necesaria para fortalecer la seguridad informática, lo cual representa una brecha importante en la protección integral de los sistemas de información en un contexto de creciente sofisticación de ciberataques. Aunque se han tomado medidas puntuales, la falta de un enfoque centralizado y de gran escala limita la capacidad de respuesta ante incidentes de seguridad a nivel nacional, un aspecto clave para garantizar la resiliencia digital de las entidades públicas.

Dado este panorama, la entidad reconoce la necesidad de contar con un proveedor que posea una experiencia extensa en el campo de la ciberseguridad, así como en la gestión y desarrollo de infraestructuras de software avanzadas.

Experiencia del contratista en de procesos similares:

En el marco del proceso de contratación que adelanta la **Corporación Agencia Nacional de Gobierno Digital – AND**, se realizó el correspondiente **estudio de mercado** con el fin de identificar las condiciones existentes de oferta, precios, capacidades técnicas y especialización disponibles, particularmente en **procesos de tecnología y seguridad digital**, garantizando la eficiencia, transparencia y razonabilidad del proceso contractual.

El estudio de mercado se sustentó en el análisis de **procesos de contratación similares en materia de tecnologías de la información y seguridad digital**, desarrollados por entidades públicas y/o privadas, cuyos objetos contractuales guardan correspondencia con el alcance técnico, los estándares de seguridad, los niveles de servicio y la criticidad de los activos digitales involucrados. Este análisis permitió obtener referencias objetivas sobre precios de mercado, modalidades de contratación, plazos de ejecución, perfiles profesionales especializados y buenas prácticas del sector.

Asimismo, la revisión de contrataciones similares en **tecnología y seguridad digital** contribuye a **mitigar riesgos asociados a sobrecostos, obsolescencia tecnológica, brechas de seguridad y dependencia de proveedores**, fortaleciendo la planeación contractual y promoviendo la participación de oferentes con capacidades técnicas comprobadas. Lo anterior se encuentra alineado con los principios de **eficiencia, economía, transparencia y responsabilidad** que rigen la contratación pública.

En consecuencia, el estudio de mercado constituye un insumo técnico esencial para la determinación del presupuesto referencial y la definición de las condiciones del proceso de contratación, asegurando que la decisión de la **Corporación Agencia Nacional de Gobierno Digital – AND** se adopte con base en información verificable, comparable y pertinente al contexto institucional y a las exigencias propias de los **entornos tecnológicos y de seguridad digital**.

En conclusión, la se posiciona como un actor clave en el ámbito del desarrollo de contenidos digitales, lo que lo convierte en un socio estratégico para el desarrollo de programas académicos dirigidos al sector público.

El alcance de este requisito se define en el artículo 92 del Decreto 1474 de 2011 el cual modificó el inciso primero del literal c) del numeral 4 del artículo 2 de la Ley 1150 de 2007, donde se exige que las obligaciones derivadas del contrato tengan relación directa con el objeto de la entidad ejecutora señalado en la ley o en sus reglamentos.

A continuación, una muestra de los contratos:

Entidad	Referencia del Proceso	Objeto	Valor contrato	Modalidad de Contratacion	Duracion	Unidad de Duracion	LINK SECOP
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CD-1225-2025.	32000892501 Aunar esfuerzos técnicos, administrativos y financieros para proveer los servicios de soporte, evolución, mantenimiento, operación, uso y apropiación de los Servicios Ciudadanos Digitales - SCD - y su ecosistema (1. Interoperabilidad, 2. Autenticación Digital, 3 Carpeta Ciudadana Digital, 4 Firma Digital, 5. GOV.CO, 6. SIGMI, 7. Portal de Lenguaje Común de Intercambio, 8. Digitalización de tramites, 9. Asistente Inteligente, 10. Mi Colombia Digital y 11. Analítica de las Soluciones),	$19.026.716.769	Contratación directa	209	día(s)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.9092497
ALCALDIA LOCAL DE SAN CRISTOBAL	FDLSC-CD-368-2025	AUNAR ESFUERZOS TÉCNICOS, ADMINISTRATIVOS Y LOGÍSTICOS PARA LA IMPLEMENTACIÓN DE SOLUCIONES	$4.623.543.052,	Contratación Directa (con ofertas)	0,	día(s)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.4281555

		TECNOLÓGICAS INTEGRALES, QUE INCLUYEN LA ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE KITS DE VIDEOVIGILANCIA, ASÍ COMO LA ADECUACIÓN DE ESPACIOS LOCATIVOS, INSTALACIÓN DE INFRAESTRUCTURA DE RED Y PUESTA EN FUNCIONAMIENTO DE SIETE (7) NODOS DIGITALES, CON EL FIN DE FORTALECER LA SEGURIDAD CIUDADANA, LA CONECTIVIDAD, EL ACCESO A SERVICIOS DIGITALES, LA MODERNIZACIÓN INSTITUCIONAL					
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CD-669-2023	Aunar esfuerzos para realizar el soporte, evolución, mantenimiento, operación de los Servicios Ciudadanos Digitales (Interoperabilidad, Autenticación Digital, Carpeta Ciudadana Digital), GOV.CO y el soporte y operación de Mi Colombia Digital que aporte al Estado colombiano la capacidad y eficiencia requerida para el proceso de transformación digital	$18.250.711.291,	Contratación directa	198,	día(s)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.4281555
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CD-650-2022-1	Aunar esfuerzos técnicos, administrativos y financieros para el soporte, evolución y mantenimiento del modelo de Servicios Ciudadanos Digitales que aporte al Estado colombiano la capacidad y eficiencia requerida para el proceso de transformación digital.	$26.403.717.181,	Contratación directa	335,	día(s)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.2728018

Superintendencia de Transporte**	654-2025	799_Aunar esfuerzos técnicos, administrativos y financieros para modernizar y desarrollar una estrategia integral de mejora que permita fortalecer la ciberseguridad en la Superintendencia de Transporte, con el fin de protegerla información institucional, garantizando su accesibilidad, confidencialidad, integridad y disponibilidad.	$397.425.500,	Contratación directa	45,	día(s)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.9136239
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CI-807-2018	Aunar esfuerzos técnicos, administrativos y financieros para la implementación de una prueba de concepto del Ecosistema de Servicios Ciudadanos Digitales para el desarrollo de nuevos productos y procesos en la administración pública, con la adopción de buenas prácticas en la Gestión, Seguridad y Privacidad de TI que eleven la interacción entre el ciudadano y el Estado.	$7.746.088.274,	Contratación Directa (con ofertas)	11,	Mes(es)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.342189
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CD-657-2021	Aunar esfuerzos técnicos, administrativos y financieros para implementar un modelo de Servicios Ciudadanos Digitales que brinde al Estado capacidad y eficiencia para su transformación digital y aumentar las herramientas tecnológicas para la prestación de los servicios de las entidades públicas.	$15.670.708.494,	Contratación Directa (con ofertas)	352,	día(s)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.1652193

ANSV	ANSV-125-2025	CONTRATAR EL LICENCIAMIENTO EN LA NUBE Y EL DESARROLLO A LA MEDIDA DE UN SISTEMA DE INFORMACIÓN ESCALABLE Y SOSTENIBLE, INCLUIDA SU ADAPTACIÓN, PARAMETRIZACIÓN, MIGRACIÓN Y PUESTA EN PRODUCCIÓN, CON EL PROPÓSITO DE AUTOMATIZAR LOS PROCESOS MISIONALES DE LA ANSV Y FACILITAR LA INTERACCIÓN CON ENTIDADES DEL ORDEN TERRITORIAL EN MATERIA DE CAMPAÑAS, ESTRATEGIAS, ASÍ COMO MONITOREAR Y MEDIR EL AVANCE DE LA POLÍTICA PÚBLICA DE SEGURIDAD VIAL A NIVEL NACIONAL Y TERRITORIAL	$12.998.100.000,	Contratación directa	12,	Mes(es)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.9019648
DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA ENTIDAD	DAFP-CD-033-2024 LÍNEA PAA 30	Prestar servicios de operación y soporte para asegurar el correcto funcionamiento, disponibilidad, seguridad y continuidad de la Infraestructura como servicio- IaaS y de la Plataforma como servicio - Paas usada para la gestión de los Servicios de Información, Aplicativos, Portales y Micro sitios de la Nube Privada del Departamento Administrativo de la Función Pública.	$522.652.248,	Contratación directa	7,	Mes(es)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.5890109
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CD-916-2020	Aunar esfuerzos técnicos, administrativos y financieros para implementar un modelo de Servicios Ciudadanos Digitales que brinde al Estado capacidad y eficiencia para su transformación digital y aumentar las herramientas	$7.918.967.781,	Contratación Directa (con ofertas)	5,	Mes(es)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.1373738

		tecnológicas para la prestación de los servicios de las entidades públicas					
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CD-651-2022	Aunar esfuerzos técnicos, administrativos y financieros para la Implementación de una Plataforma Integral Convergente para la Gestión de la Información de las Ciudades y Territorios Inteligentes en Colombia, a través de la planeación, diseño, adquisición, desarrollo, despliegue y personalización de una serie de herramientas hardware y software que posibiliten la integración y articulación de soluciones IoT y Smart Cities desplegadas en los territorios.	$12.899.028.000,	Contratación directa	321,	día(s)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.2721788
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CD-1225-2025	32000892501 Aunar esfuerzos técnicos, administrativos y financieros para proveer los servicios de soporte, evolución, mantenimiento, operación, uso y apropiación de los Servicios Ciudadanos Digitales - SCD - y su ecosistema (1. Interoperabilidad, 2. Autenticación Digital, 3 Carpeta Ciudadana Digital, 4 Firma Digital, 5. GOV.CO, 6. SIGMI, 7. Portal de Lenguaje Común de Intercambio, 8. Digitalización de tramites, 9. Asistente Inteligente, 10. Mi Colombia Digital y 11.Analítica de las Soluciones),	$19.026.716.769,	Contratación directa	245,	día(s)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.8046440

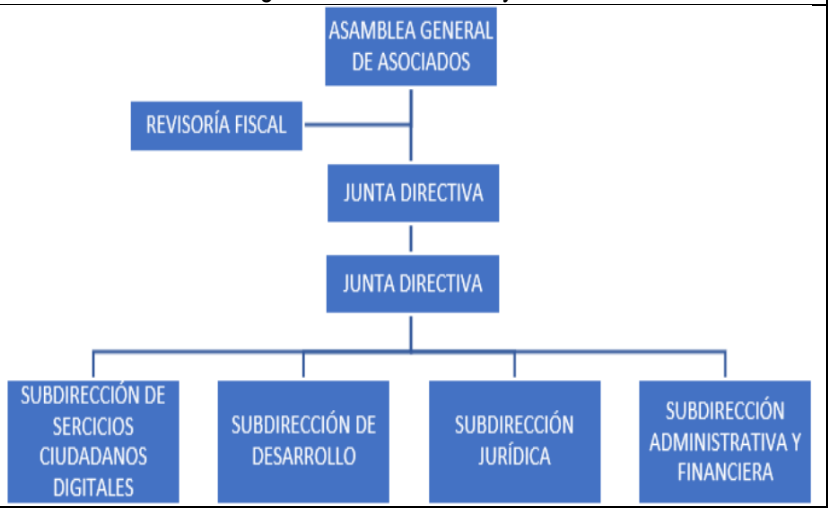
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CI-807-2018	Aunar esfuerzos técnicos, administrativos y financieros para la implementación de una prueba de concepto del Ecosistema de Servicios Ciudadanos Digitales para el desarrollo de nuevos productos y procesos en la administración pública, con la adopción de buenas prácticas en la Gestión, Seguridad y Privacidad de TI que eleven la interacción entre el ciudadano y el Estado.	$7.746.088.274,	Contratación Directa (con ofertas)	11,	Mes(es)	
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CD-762-2022	Contratar el Diseño, Desarrollo, Implementación, Administración, Operación, de una solución tecnológica que mediante la vinculación de los Servicios Ciudadanos Digitales y disponiendo los recursos humanos, técnicos, materiales y físicos, permitan el correcto funcionamiento de la solución tecnológica que se implemente para el Registro de Deudores Alimentarios Morosos (REDAM).	$5.496.640.890,	Contratación directa	5,	Mes(es)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.3117796
ANI	CI-015-2023	AUNAR ESFUERZOS TÉCNICOS, ADMINISTRATIVOS, TECNOLÓGICOS, OPERATIVOS FINANCIEROS Y JURÍDICOS ENTRE LA AGENCIA NACIONAL DE INFRAESTRUCTURA Y LA AGENCIA NACIONAL DIGITAL PARA EL FORTALECIMIENTO INTEGRAL DE LA CAPACIDAD DE CÓMPUTO, SEGURIDAD DE LA INFORMACIÓN, ALMACENAMIENTO, REDES, VIRTUALIZACIÓN Y CONEXOS DE LA INFRAESTRUCTURA TECNOLÓGICA, PARA	$22.036.988.010,	Contratación directa	1,	Año(s)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.5368834

		PARA SOPORTAR LOS SERVICIOS Y PROCESOS TI DE LA AGENCIA NACIONAL DE INFRAESTRUCTURA EN VIRTUD DEL CONVENIO MARCO 939 - 2023					
FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CI-807-2018	Aunar esfuerzos técnicos, administrativos y financieros para la implementación de una prueba de concepto del Ecosistema de Servicios Ciudadanos Digitales para el desarrollo de nuevos productos y procesos en la administración pública, con la adopción de buenas prácticas en la Gestión, Seguridad y Privacidad de TI que eleven la interacción entre el ciudadano y el Estado.	$7.746.088.274,	Contratación Directa (con ofertas)	11,	Mes(es)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.342189
Superintendencia de Transporte**	653-2025	800_Aunar esfuerzos técnicos, administrativos y financieros en atención al componente de mejoramiento de la infraestructura tecnológica prevista en el Convenio Marco suscrito entre la Agencia Nacional Digital y la Supertransporte, que permita el fortalecimiento de la función de Inspección, Vigilancia y Control de la Superintendencia en las regiones	$1.050.000.000,	Contratación directa	45,	día(s)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.9134889

FONDO UNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	FTIC-CI-807-2018	Aunar esfuerzos técnicos, administrativos y financieros para la implementación de una prueba de concepto del Ecosistema de Servicios Ciudadanos Digitales para el desarrollo de nuevos productos y procesos en la administración pública, con la adopción de buenas prácticas en la Gestión, Seguridad y Privacidad de TI que eleven la interacción entre el ciudadano y el Estado.	$7.746.088.274,	Contratación Directa (con ofertas)	11,	Mes(es)	https://community.secop.gov.co/Public/Tendering/OpportunityDetail/Index?noticeUID=CO1.NTC.342189

Teniendo en cuenta la naturaleza del contrato a suscribir, así como las actividades de ciencia y tecnología a desarrollar, con el objetivo de exponer la idoneidad jurídica, técnica, administrativa y financiera de la CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL para asociarse con el Ministerio de las Tecnologías de la Información y la Comunicaciones, se presenta el siguiente estudio:

ANÁLISIS DE IDONEIDAD		
CAPACIDAD JURÍDICA	NATURALEZA JURÍDICA Y DENOMINACIÓN ESTATUTARIA	La Corporación Agencia Nacional De Gobierno Digital, es una entidad descentralizada indirecta, con el carácter de asociación civil, de participación pública y naturaleza privada, sin ánimo de lucro, con patrimonio propio, organizada bajo las leyes colombianas, dentro del marco de la Constitución Política y las normas de Ciencia y Tecnología en especial del Decreto Ley 393 de 1991 y regida por ellas, y por las regulaciones previstas para las corporaciones en el Código Civil y por sus Estatutos. Su régimen contractual para las actividades de Ciencia y Tecnología será el indicado en el Decreto Ley 393 de 1991, y en lo demás, en lo regulado por la Ley 80 de 1993, Ley 1150 de 2007 y normas concordantes.
	OBJETO	La Corporación tiene como objeto articular los Servicios Ciudadanos Digitales de que trata el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector TIC, subrogado por el artículo 1 del Decreto 620 de 2020, acorde con la evolución de los modelos de servicios digitales ciudadanos y del sistema de planeación y gestión pública, y desarrollar las actividades de ciencia, tecnología e innovación asociadas a la creación de un ecosistema de información pública, incorporando la debida gestión de riesgos asociada a la información, que permita apoyar proyectos de ciencia, tecnología e innovación, así como identificar planes, programas y proyectos que ofrezcan soluciones a problemáticas o cuellos de botella en el sector público colombiano, introduciendo con ello mejoras significativas en los procesos estatales, mediante el uso y desarrollo de soluciones de software, analítica de datos, entre otras.

	CONFORMACIÓN	ASOCIADOS: Ministerio de las Tecnologías de la Información y las Comunicaciones y Departamento Administrativo de la Función Pública. En relación con este punto, es necesario resaltar el hecho de que el MinTIC sea uno de los asociados de la AND, ya que ello la consolida como su aliado estratégico para el cumplimiento de los objetivos que la Ley 1341 de 2009 le asignó.
	LÍNEAS DE ACCIÓN POTENCIALES	Investigación científica y desarrollo tecnológico mediante el desarrollo de nuevos productos, procesos y servicios basados seguridad digital.
		Creación de un ecosistema de información pública, incorporando la debida gestión de riesgos asociada a la información, para apoyar proyectos de ciencia, tecnología e innovación y seguridad digital. Difusión científica y tecnológica mediante la publicación, divulgación y asesoría en ciencia y tecnología relacionada con tecnologías de la información y las comunicaciones
		Proyectos de innovación que incorporen tecnología encaminada a mejorar la calidad de los servicios ofrecidos por las diversas entidades públicas a través de la tecnología tanto nacional como internacional, en lo ateniente a tecnologías de la información y las comunicaciones.
		Impulsora y facilitadora de las acciones requeridas para avanzar en los objetivos de desarrollo sostenible, facilitando el goce efectivo de derechos a través del uso de tecnologías de la información y las comunicaciones.
CAPACIDAD ADMINISTRATIVA Y ORGANIZACIONAL	ESTRUCTURA ORGANIZACIONAL	

La CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL – AND es el articulador y prestador de los servicios ciudadanos digitales y por ende la entidad encargada de proveer y gestionar de manera integral los mismos. En virtud de anterior, el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, en el marco del proceso para la ejecución de la Fase 4 del Proyecto, pretende ejecutar el presente proyecto, teniendo en cuenta adicionalmente las siguientes previsiones contenidas en el Decreto No. 1310 de 2022, así:

- ARTÍCULO 2.2.23.15. Responsabilidades y deberes de las Fuentes de Información. (...) 3. Garantizar que los sistemas de información de las Fuentes de la Información se integren al modelo de interoperabilidad de los servicios ciudadanos digitales en el marco de la política de gobierno digital expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Teniendo en cuenta que desde el año 2020 el Ministerio de Tecnologías de la Información y las Comunicaciones ha venido celebrando de manera sucesiva convenios / contratos interadministrativos con la Corporación Agencia Nacional de Gobierno Digital, con los amplios beneficios que esto ha traído consigo en materia de fomento, uso y aprovechamiento de las TIC en el sector público, generación de valor público a través de la transformación digital del Estado, impacto positivo en aras del gobierno trasparente, accesible, interoperando e integrado, uso y operación de los servicios digitales, entre otros; aunado a que acuerdo con lo establecido en el Decreto 620 de 2020, la CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL – AND es el articulador y prestador de los servicios ciudadanos digitales base y por ende la entidad encargada de proveer y gestionar de manera integral los mismos, de tal manera que cuenta con la idoneidad y experiencia para ejecutar el contrato a celebrar, se propone, que sea la Corporación Agencia Nacional de Gobierno Digital a través de un nuevo contrato interadministrativo quien continúe ejecutando los servicios ciudadanos digitales y sus proyectos asociados.

Teniendo en cuenta lo anterior se considera que:

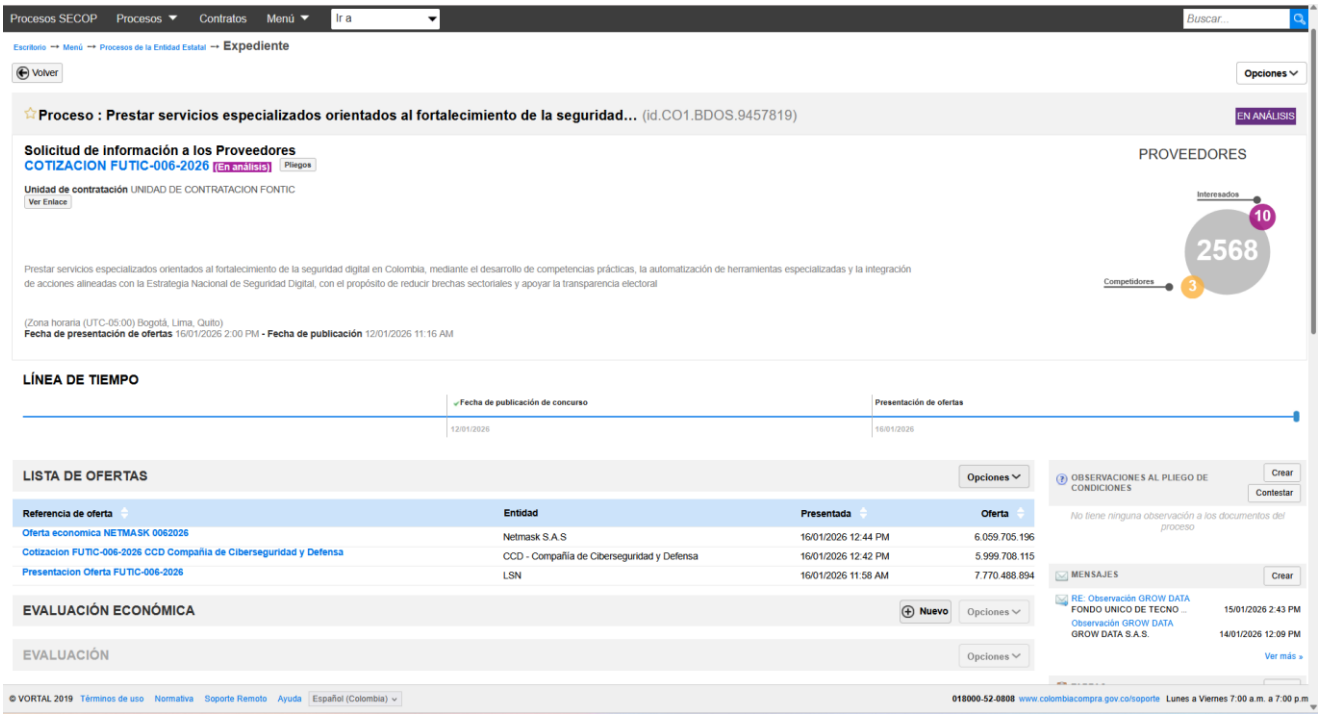
a. De acuerdo con el artículo 2.2.17.1.4 del Decreto No. 620 de 2020, la CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL- AND es la encargada de proveer y gestionar de manera integral los servicios ciudadanos digitales, además de apoyar técnica y operativamente al Ministerio de Tecnologías de la Información y las Comunicaciones para garantizar el pleno funcionamiento de tales servicios.
b. La CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL- AND, tiene una amplia experiencia en el desarrollo de proyectos de gran magnitud orientados a la transformación digital del Estado Colombiano,
c. Como parte de los proyectos ejecutados por la CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL- AND se encuentra los señalados en el capítulo 14.- Criterios para seleccionar al Ejecutor

La CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL- AND apoyará al Min. Tic garantizando los medios necesarios que permitan la ejecución del proyectoEn cumplimiento de lo anterior, por medio de los artículos 2.2.17.1.5. y 2.2.17.1.4 numeral segundo del Decreto 1078 de 2015, se dispuso que, para efectos de lo establecido en el título 17 de la parte 2 del libro 2 del citado decreto, la Agencia Nacional Digital tendrá el rol articulador y, en ese sentido, será la encargada de proveer y gestionar de manera integral los servicios ciudadanos digitales, además de apoyar técnica y operativamente al Ministerio de Tecnologías de la Información y las Comunicaciones para garantizar el pleno funcionamiento de tales servicios.

Con base en sus estatutos general, de contratación y de extensión y proyección social, La CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL- AND cuenta con el marco normativo para acreditar la competencia para ejecutar proyectos interadministrativos y convenios de cooperación, de acuerdo con el numeral 4 del artículo 2 de la Ley 1150 de 2007 y el artículo 95 de la Ley 489 de 1998, no estando sujeta integralmente a la Ley 80 de 1993, sino contratando bajo derecho civil y comercial, conforme a principios de transparencia, responsabilidad, selección objetiva y economía**5. ESTUDIO DEL MERCADO**

Con el objetivo de identificar posibles proveedores en el marco del presente proceso de selección, se llevó a cabo un sondeo de mercado mediante el evento de Cotización FUTIC-006-2026, a través de la plataforma SECOP II. En este evento, el MINTIC convocó a los interesados a presentar cotizaciones e información para conocer la oferta del sector, el cual se abrió el día 12 de enero de 2026 y se cerró el 16 de enero de 2026.

Se recibieron un total de tres (3) cotizaciones. Los posibles proveedores se relacionan a continuación:



De conformidad con los lineamientos metodológicos aplicados en el Estudio del Sector y en atención a los requerimientos técnicos definidos para el programa “Ciberseguridad 360°”, se presenta a continuación la determinación del presupuesto del proyecto a partir de la información de los oferentes NETMASK SAS, LSN y COMPAÑÍA CIBERSEGURIDAD Y DEFENSA. El presente apartado describe las fuentes de información, la metodología de cálculo, las estructuras de costos por oferente, y el procedimiento para arribar al valor de referencia del presupuesto oficial del proyecto, respetando la premisa de trabajar sobre valores antes de impuestos para garantizar comparabilidad.

Todos los valores se cotizan en pesos colombianos (COP).

A efectos de garantizar la razonabilidad técnica y económica del proceso, la determinación del presupuesto oficial se sustenta en el modelo estadístico por cuartiles descrito en la cartilla de Colombia Compra Eficiente.

Con la información recibida y de acuerdo con lo indicado en la Guía de Colombia Compra Eficiente, Con la muestra de precios normalizada, se calcularon las medidas de posición central típicas del enfoque por cuartiles: primer cuartil (Q1), mediana (Q2) y tercer cuartil (Q3), a partir de las cuales se determinó el rango intercuartílico. El RIC permitió identificar la concentración real de la distribución de precios del mercado y establecer, mediante el criterio de Tukey, los límites inferior y superior para detección de atípicos (límite inferior = Q1 – 1,5×RIC; límite superior = Q3 + 1,5×RIC). Los valores que quedaron por fuera de esos límites fueron revisados con criterio técnico (especificaciones no equivalentes, errores de transcripción, vigencias o condicionamientos no aplicables) y, cuando correspondió, se excluyeron de la muestra depurada. Continuando con el ejercicio estadístico y mediante promedio simple, el área obtuvo unos precios finales como insumo para la proyección del mercado. Lo anterior, con el propósito de validar que la cotización y propuesta presentada por la Agencia Nacional de Gobierno Digital se encuentra dentro del rango del estudio realizado.

				NETMASK SAS	LSN	COMPAÑÍA CIBERSEGURIDAD Y DEFENSA							
	ITEM	Actividades	Producto	Valor sin IVA	Valor sin IVA	Valor sin IVA	Q1	Q2 Mediana	Q3	Rango	Inferior	Maximo	Promedio
1	CONVOCATORIA	"Apoyo inicio formal del proyecto, despliegue de piezas gráficas y publicidad. "	Realizar toda la publicidad para el proyecto, la cual que debe incluir el logo oficial de MINTIC, de acuerdo al manual de manejo de imagen del Ministerio. Garantizar que la plataforma web interactiva y comprobada para la formación virtual cumpla los que requisitos establecidos en el anexo técnico y este en servicio durante toda la ejecución del convenio. Desarrollar el contenido académico con los módulos descritos en el anexo técnico. Atender las sugerencias hechas por la supervisión a los cursos de formación, sin que ello afecte el contenido de estos, considerando además las recomendaciones que realice el área de Comunicaciones o el Cooperante para un mayor incentivo de participantes. El cooperante hará entrega de los certificados a los usuarios que hayan culminado exitosamente el curso a sus correos electrónicos y mantendrá la opción de descargué por parte del estudiante en la plataforma por un plazo por quince (15) días después de haber terminado el curso. Entregar el registro de beneficiarios en los formatos y tiempos definidos por el Ministerio TIC. Gestionar las bases de datos acorde con política de tratamiento de datos	$ 20.200.000,00	$ 320.000.000,00	$ 20.000.000,00	$ 20.100.000	$ 20.200.000	$ 170.100.000	$ 150.000.000	-$ 204.900.000	$ 395.100.000	$ 120.066.667
		El aliado deberá garantizar las gestiones que conlleven a que el público objetivo adelante de manera efectiva el proceso de inscripción a las convocatorias.		5.250.000,00	$ 259.000.000,00	$ 25.000.000,00	$ 25.125.000	$ 25.250.000	$ 142.125.000	$ 117.000.000	-$ 150.375.000	$ 317.625.000	$ 103.083.333
		VALIDACIÓN DE INSCRITOS: El aliado debe evaluar que los inscritos cumplan con los criterios para acceder a la formación		$ 25.250.000,00	$ 249.000.000,00	$ 25.000.000,00	$ 25.125.000	$ 25.250.000	$ 137.125.000	$ 112.000.000	-$ 142.875.000	$ 305.125.000	$ 99.750.000
2	DISEÑO DE CURSOS	Diseño curricular de los programas especializados será responsabilidad del aliado seleccionado y será un ítem importante durante la adjudicación del proyecto. Sin embargo, MINTIC propone que se manejen unos niveles de formación: Nivel Medio y Nivel avanzado, acorde con los contenidos mínimos.		$ 101.000.000,00	$ 425.006.000,00	$ 100.000.000,00	$ 100.500.000	$ 101.000.000	$ 263.003.000	$ 162.503.000	-$ 143.254.500	$ 506.757.500	$ 208.668.667
3	PLATAFORMA WEB	Plataforma web interactiva y comprobada para la formación virtual, que permitirá experiencias de aprendizaje tanto síncronas como asíncronas y la simulación de escenarios reales. Esta herramienta facilitará la creación de programas formativos, el seguimiento en tiempo real del avance y la gestión eficiente de los participantes, con la configuración definida en el alcance técnico.		$ 1.717.008.080,00	$ 778.954.000,00	$ 1.700.008.000,00	$ 1.239.481.000	$ 1.700.008.000	$ 1.708.508.040	$ 469.027.040	$ 535.940.440	$ 2.412.048.600	$ 1.398.656.693
4	CERTIFICADOS	Entrega de certificados: A los participantes que cumplan satisfactoriamente con el programa se les otorgará un certificado de formación en ciberseguridad alineado con los requerimientos del MINTIC.		$ 151.500.000,00	$ 410.000.000,00	$ 150.000.000,00	$ 150.750.000	$ 151.500.000	$ 280.750.000	$ 130.000.000	-$ 44.250.000	$ 475.750.000	$ 237.166.667

5	CAMPAÑAS DE COMUNICACIÓN PARA CONVOCATORIA Y REGISTRO	Diseño y desarrollo de piezas para convocatoria, envio de piezas a potenciales empresas (trabajo en conjunto con MINTIC), platafroma de inscripción.	personales del Ministerio TIC y sus procedimientos correspondientes.	$ 50.500.000,00	$ 345.000.000,00	$ 50.000.000,00	$ 50.250.000	$ 50.500.000	$ 197.750.000	$ 147.500.000	-$ 171.000.000	$ 419.000.000	$ 148.500.000
6	ACOMPAÑAMIENTO EMPRESAS	Se espera que para la metodología de enseñanza se propone que se tenga en cuenta: clases en línea, Seminarios web, laboratorios virtuales.		$ 103.020.000,00	$ 349.564.600,00	$ 102.000.000,00	$ 102.510.000	$ 103.020.000	$ 226.292.300	$ 123.782.300	-$ 83.163.450	$ 411.965.750	$ 184.861.533
7	EQUIPO ADMINISTRATIVO y LOGÍSTICO	Equipo base del proyecto, acorde con lo definido en el Anexo Técnico.		$ 56.409.005,00	$ 905.678.000,00	$ 55.850.500,00	$ 56.129.753	$ 56.409.005	$ 481.043.503	$ 424.913.750	-$ 581.240.873	$ 1.118.414.128	$ 339.312.502
8	Actualización de licenciamientos	Cubrimiento de licenciamientos a renovar o actualización de herramientas acorde con lo establecido en el anexo técnico y las capaidades definidas mínimas.	El contratista deberá proporcionar al Ministerio / Fondo Único de TIC dentro de los tres (3) días hábiles siguientes a la suscripción del acta de inicio y de común acuerdo con el supervisor del contrato, la metodología de trabajo, el plan de trabajo y cronograma de actividades para la ejecución del proyecto, incluyendo el certificado del licenciamiento para su uso; en todo caso, la entrega de las herramientas tecnológicas tendrá lugar dentro de los 15 días calendario siguientes al acta de inicio. Dar cumplimiento a los servicios derivados del despliegue de las herramientas y soluciones de seguridad digital y generar los insumos y entregables en cada una de ellas, los cuales se encuentran descritos en el Anexo Técnico. Asegurar que todas las soluciones, herramientas y plataformas proporcionadas estén debidamente licenciadas por el fabricante, por un periodo mínimo de doce (12) meses, incluidas las actualizaciones a las versiones más recientes durante todo el período de vigencia del licenciamiento. Realizar la transferencia de conocimiento, tanto	$ 3.013.840.000,00	$ 1.688.916.000,00	$ 2.984.000.000,00	$ 2.336.458.000	$ 2.984.000.000	$ 2.998.920.000	$ 662.462.000	$ 1.342.765.000	$ 3.992.613.000	$ 2.562.252.000

			técnica como funcional a las personas que la entidad designe, así como los entrenamientos de acuerdo con los lineamientos establecidos en el Anexo Técnico. Establecer programas de entrenamiento para el personal del centro de operaciones ColCERT, manteniéndolos actualizados sobre las últimas tendencias y técnicas en ciberseguridad. Prever el plan de recuperación y contingencia del servicio contratado ante los eventos que puedan afectar el cumplimiento de la ejecución de este tecnológicas definidas en el Anexo Técnico										
9	Solución DFIR – Torre Forense	Torre Forense, Dispositivos externos de evidencia forense y almacenamiento adicional	Entregar informes preliminares y finales para las actividades de despliegue de la solución y los resultados de la gestión de seguridad digital que se está realizando con cada entidad beneficiaria. Cumplir con los requisitos técnicos y funcionales de la Plataforma definida en el documento de	$ 106.050.000,00	$ 586.430.000,00	$ 105.000.000,00	$ 105.525.000	$ 106.050.000	$ 346.240.000	$ 240.715.000	-$ 255.547.500	$ 707.312.500	$ 265.826.667

		Licenciamiento MAGNET AXIOM CYBER	anexo técnico. Configuración y el afinamiento inicial de la solución, en conjunto con el equipo técnico de ColCERT, para la visualización en las entidades de la muestra y el principal en el ColCERT. Entregar la información de las entidades seleccionadas que se recolecte durante la ejecución del contrato a la terminación, asegurando que es propiedad del Ministerio. El personal técnico asignado por el proveedor deberá firmar un acuerdo de confidencialidad para proteger la información de ColCERT al momento de su vinculación. El servicio de soporte debe ser 24/7 durante los meses del proyecto, así mismo contar con un servicio se SOC que soporte la solución MDR (monitoreo, detección y respuesta gestionada) y garantizar la continuidad del servicio durante el convenio. Enfocar la gestión e identificación de incidentes de seguridad digital, estableciendo procedimientos alineados con NIST 800-61 R3, comunicados al Equipo ColCERT y a las entidades vinculadas. Configurar tableros de control en la solución XDR para visualizar en tiempo real las actividades de monitoreo, con accesos consolidados para ColCERT y particulares para cada entidad. El plazo máximo de entrega e instalación de la solución, que incluye de agentes y la visualización de monitoreo, es de 30 días calendario, según lo determine ColCERT."	$ 118.523.500,00	$ 124.234.000,00	$ 117.350.000,00	$ 117.936.750	$ 118.523.500	$ 121.378.750	$ 3.442.000	$ 112.773.750	$ 126.541.750	$ 120.035.833
10	oporte y mantenimiento sistema de videwall RGBlink	Ref: Q16PRO GEN2-8U / matriz de 3X6 (Pantalla industrial de 55 pulgadas LG Ref 55VSH7J		$ 84.840.000,00	$ 88.040.000,00	$ 84.000.000,00	$ 84.420.000	$ 84.840.000	$ 86.440.000	$ 2.020.000	$ 81.390.000	$ 89.470.000	$ 85.626.667
			TOTAL	$ 5.573.390.585,00	$ 6.529.822.600,00	$ 5.518.208.500,00							**$ 5.873.807.228**

Sobre la muestra ya depurada se estimaron estadísticas robustas al efecto de valores extremos. De forma preferente, se empleó la media podada a un porcentaje simétrico de los extremos, entendida como un promedio que descarta una fracción equivalente de observaciones altas y bajas para representar de mejor forma el "núcleo" de la oferta de mercado. En aquellos casos en que el tamaño muestral fuese reducido o la distribución resultase marcadamente asimétrica, se privilegió la mediana (Q2) como medida central. El resultado de esta estimación se presenta como valor de referencia antes de impuestos.

De conformidad con la práctica de estudios de mercado, el presupuesto oficial recomendado se expresa antes de impuestos, a fin de mantener la comparabilidad homogénea entre ofertas y fuentes consultadas. En consecuencia, el Presupuesto oficial se fija en **$5.873.807.228 COP**, derivado del estadístico robusto seleccionado (media podada/mediana) aplicado sobre la muestra depurada. Los tributos aplicables, tasas y retenciones se liquidarán en la fase contractual de acuerdo con la normatividad vigente y la naturaleza jurídica de las partes, sin alterar el método de determinación del valor de referencia aquí documentado.

De conformidad con la determinación del presupuesto oficial realizada anteriormente, se estimó un valor de referencia de $5.873.807.228 antes de IVA, equivalente a $6.989.830.602 IVA incluido, según la estructura de costos definida para el objeto a contratar. En contraste, la propuesta presentada por la Agencia Nacional de Gobierno Digital asciende a $5.900.000.000 IVA incluido, valor que se ubica por debajo del monto total calculado en la estimación presupuestal. En consecuencia, desde la perspectiva financiera, la oferta resulta compatible con el presupuesto determinado, sin superar el techo presupuestal establecido para la vigencia y manteniéndose dentro de los parámetros de costo previstos para la contratación.

Riesgos presupuestales y medidas de mitigación

- **Variaciones en la demanda efectiva:** Fluctuaciones en el número real de participantes (rango 3.000–5.000) pueden impactar costos variables. Se mitigará aplicando escalas de precios por tramo y cláusulas de ajuste.
- **Capacidades tecnológicas:** Sobrecostos por ampliación de infraestructura de plataforma. Se mitigará con pruebas de carga, SLA de disponibilidad y dimensionamiento progresivo.
- **Ejecución logística:** Riesgo de mayores costos operativos en territorios. Se mitigará con planeación territorial y alianzas locales.
- **Tiempos de integración de datos:** Demora en la entrega/validación de insumos (p. ej., bases de inscritos). Se mitigará con hitos y entregables quincenales de gestión de convocatoria e inscripción.

Para garantizar trazabilidad y control interno, cada partida deberá imputarse al componente correspondiente y soportarse con evidencia verificable (órdenes de compra, entregables aprobados, reportes de avance, actas de comité). Se recomienda un tablero de control mensual con corte quincenal para: (i) avance físico por ítem, (ii) ejecución presupuestal, (iii) relación costo-resultado (indicadores de convocatoria, permanencia y certificación), y (iv) alertas tempranas de desvíos.

De acuerdo con los valores presentados en los formatos de cotización:

- NETMASK SAS presentó una propuesta con un valor total de $ 6.059.705.196,15
- **LSN** presentó una propuesta por $**7.770.488.894** COP.
- **COMPAÑÍA CIBERSEGURIDAD Y DEFENSA** presentó una propuesta por $**5.999.708.115** COP

Estas propuestas reflejan un rango representativo del mercado que varía según el enfoque estratégico, la cobertura territorial, la infraestructura técnica y los niveles de ejecución propuestos. Con base en estos antecedentes y considerando los costos asociados a los componentes definidos en el Anexo Técnico, se establece como valor estimado del mercado es por la suma de $**$6.609.967.401,72** COP. Este valor incluye todos los costos directos e indirectos requeridos para la ejecución del proyecto y se fija como valor de referencia máximo, sujeto a la disponibilidad presupuestal del Fondo Único de Tecnologías de la Información y las Comunicaciones (Fondo Único TIC) y a los actos administrativos que regulen el proceso contractual

.

6. ANÁLISIS DE LA PROPUESTA DEL ALIADO:

Para el presente contrato interadministrativo, la CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL conforme las siguientes consideraciones:

Programa de Formación					
No.	**Item**	**Descripción**	5000 personas formadas (certificados)		
			Valor Unitario	**Valor IVA**	**Valor Total (IVA incluido)**
1	**CONVOCATORIA**	Apoyo inicio formal del proyecto, despliegue de piezas gráficas y publicidad.	145.566.610	34.145.254	179.711.865
		El aliado deberá garantizar las gestiones que conlleven a que el público objetivo adelante de manera efectiva el proceso de inscripción a las convocatorias.	84.913.856	19.918.065	104.831.921
		VALIDACIÓN DE INSCRITOS: El aliado debe evaluar que los inscritos cumplan con los criterios para acceder a la formación	133.436.060	31.299.816	164.735.876
2	**DISEÑO DE CURSOS**	Diseño curricular de los programas especializados será responsabilidad del aliado seleccionado y será un ítem importante durante la adjudicación del proyecto. Sin embargo, MINTIC propone que se manejen unos niveles de formación: Nivel Medio y Nivel avanzado, acorde con los contenidos mínimos.	valor embebido con la adquisición de los cursos de la plataforma web	-	
3	**PLATAFORMA WEB**	Plataforma web interactiva y comprobada para la formación virtual, que permitirá experiencias de aprendizaje tanto síncronas como asíncronas y la simulación de escenarios reales. Esta herramienta facilitará la creación de programas formativos, el seguimiento en tiempo real del avance y la gestión eficiente de	1.224.100.761	232.579.145	1.456.679.906

		los participantes, con la configuración definida en el alcance técnico.			
4	**CERTIFICADOS**	Entrega de certificados: A los participantes que cumplan satisfactoriamente con el programa se les otorgará un certificado de formación en ciberseguridad alineado con los requerimientos del MINTIC.	Certificados están inmersos en el valor de la plataforma Web y podrán ser descargados una vez se finalicen el curso	-	
5	**CAMPAÑAS DE COMUNICACIÓN PARA CONVOCATORIA Y REGISTRO**	Diseño y desarrollo de piezas para convocatoria, envio de piezas a potenciales empresas (trabajo en conjunto con MINTIC), platafroma de inscripción.		-	89.855.932
6	**ACOMPAÑAMIENTO EMPRESAS**	Se espera que para la metodología de enseñanza se propone que se tenga en cuenta: clases en línea, Seminarios web, laboratorios virtuales.	61.800.000	11.742.000	73.542.000
7	**EQUIPO ADMINISTRATIVO y LOGÍSTICO**	Equipo base del proyecto, acorde con lo definido en el Anexo Técnico.	25.750.000	4.892.500	30.642.500
Total (IVA incluido)		**Totales**	**2.100.000.000**		

Herramientas de Apoyo y Fortalecimiento de la operación

No.	Item	Descripción	Valor Unitario	Valor IVA	Valor Total (IVA incluido)
1	**Actualización de licenciamientos**	Cubrimiento de licenciamientos a renovar o actualización de herramientas acorde con lo establecido en el anexo técnico y las capaidades definidas mínimas.	$ 1.478.761.915	$ -	$ 1.478.761.915
			$ 1.463.090.698	$ 277.987.232	$ 1.741.077.930
2	**Solución DFIR – Torre Forense**	Torre Forense, Dispositivos externos de evidencia forense y almacenamiento adicional	$ 184.768.735	$ 35.106.060	$ 219.874.795
		Licenciamiento MAGNET AXIOM CYBER	$ 247.417.434	$ 47.009.312	$ 294.426.746
3	**Soporte y mantenimiento sistema de videwall RGBlink**	Ref: Q16PRO GEN2-8U / matriz de 3X6 (Pantalla industrial de 55 pulgadas LG Ref 55VSH7J	$ 55.343.373	$ 10.515.241	$ 65.858.614
Total (IVA incluido)			**$**		**3.800.000.000**

Total oferta económica (IVA incluido)	**$**	**5.900.000.000**

La propuesta presentada por la CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL, se fundamenta en la necesidad identificada por ColCERT de fortalecer sus capacidades institucionales en materia de seguridad digital, en un contexto caracterizado por el incremento y sofisticación de las amenazas cibernéticas, la creciente dependencia de los servicios digitales y las obligaciones normativas aplicables a las entidades del sector público colombiano.

En el marco de la iniciativa Ciberseguridad 360, se establecen dos componentes fundamentales. El componente técnico se orienta a fortalecer la infraestructura tecnológica que soporta los servicios asociados al portafolio de ColCERT, contribuyendo a ampliar sus capacidades operativas para anticipar riesgos y mejorar la eficiencia en la gestión de incidentes de seguridad digital, conforme a los alcances definidos en el Anexo Técnico.

De manera complementaria, el componente de formación de talento humano especializado busca desarrollar procesos de formación práctica y certificable, orientados al fortalecimiento de competencias técnicas y a la consolidación de una cultura institucional resiliente y sostenible en ciberseguridad, en respuesta a la demanda creciente de capacidades especializadas en esta materia. En este contexto, la contratación de la Agencia Nacional Digital – AND se orienta a la implementación del modelo Ciberseguridad 360, de conformidad con los componentes, actividades y alcances establecidos en el Anexo Técnico.

La ejecución del proyecto permitirá habilitar las capacidades técnicas y formativas previstas, mediante la configuración y puesta en operación de las herramientas tecnológicas definidas, la ejecución de los procesos de formación correspondientes y el acompañamiento técnico durante el periodo contractual, sin que ello implique la sustitución de las funciones misionales de ColCERT ni la asunción de responsabilidades que excedan el alcance del contrato.
Adicionalmente, el proyecto se encuentra alineado con los lineamientos de la Estrategia Nacional de Seguridad Digital, particularmente en lo relacionado con el fortalecimiento de capacidades institucionales, la gestión de riesgos cibernéticos, el uso eficiente de herramientas tecnológicas y la mejora continua de los procesos asociados a la seguridad digital. La implementación del modelo Ciberseguridad 360 contribuirá a que ColCERT avance en el fortalecimiento de su madurez institucional en esta materia, en coherencia con sus prioridades y capacidades internas.

En dicho sentido, se establece que servicio requerido *"**Prestar servicios especializados orientados al fortalecimiento de la seguridad digital en Colombia, mediante el desarrollo de competencias prácticas, la automatización de herramientas especializadas y la integración de acciones alineadas con la Estrategia Nacional de Seguridad Digital, con el propósito de reducir brechas sectoriales y apoyar la transparencia electoral**."* se desarrollará atendiendo EL ANEXO TÉCNICO y la propuesta económica presentada por la CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL,en virtud del contrato que se pretende celebrar.

En concordancia con lo mencionado, el valor estiamdo del contrato corresponderá a la suma **CINCO MIL NOVECIENTOS MILLONES DE PESOS MTCE ($5.900.000.000) IVA INCLUIDO** demás impuestos, tasas, contribuciones, costos directos e indirectos que conlleven la celebración y ejecución del contrato**,** valor que en todo caso está sustentado en las actividades, bienes y servicios que se deben desarrollar de acuerdo con el anexo técnico, dentro de las cuales serán certificadas durante la ejecución del proyecto, dentro de la presente vigencia de conformidad a la propuesta económica presentada por el aliado, la cual se encuentra ajustado a los precios del mercado.

El valor estimado del presupuesto fue determinado a partir de un análisis integral del alcance del proyecto, considerando las especificaciones técnicas, los costos de mercado vigentes, la experiencia requerida, los recursos humanos y

materiales necesarios, así como los riesgos asociados a la correcta ejecución del objeto contractual. Dicho análisis se basó en estudios comparativos, referencias de proyectos similares y cotizaciones representativas del sector, garantizando que el monto estimado sea razonable, suficiente y acorde con los estándares de calidad exigidos.

En este sentido, el presupuesto estimado se mantiene como un referente adecuado y técnicamente sustentado, al reflejar de manera más precisa los costos reales necesarios para garantizar la ejecución eficiente, oportuna y conforme a los requerimientos establecidos. Por lo anterior, la evaluación económica debe realizarse de forma conjunta con el análisis técnico y de cumplimiento.

Ahora bien, es de resaltar que tanto la CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL, ha ejecutado convenios y contratos con entidades públicas, en especial con el Ministerio de Tecnologías de la Información y Las Comunicaciones siendo un aliado estratégico para adelantar proyectos de relevancia tecnológica para el país, los cuales se han adelantado de acuerdo con el plan de trabajo propuesto en su momento, demostrando con esto tener idoneidad técnica, experiencia y capacidad de desarrollar el proyecto, por lo anterior se pretende ejecutar actividades similares en esta vigencia presupuestal, vale la pena indicar que la propuesta de la Corporación Colombia Digital se encuentra ajustada a los valores del mercado, con objetos similares asociados a la seguridad digital e infraestructura tecnológica.

Por lo anterior, el MinTic considera que la Corporación Colombia Digital cuenta con la capacidad y experiencia necesaria para la ejecución del proyecto mencionado por lo que suscribirá un contrato interadministrativo de conformidad con el literal c) numeral 4 del artículo 2 de la Ley 1150 de 2007 y el artículo 2.2.1.2.1.4.4 del Decreto 1082 de 2015, teniendo en cuenta la capacidad técnica, experiencia e idoneidad de la Corporación

7. CONCLUSIONES

De acuerdo con la información comparativa desarrollada en los numerales anteriores y el análisis del sector adelantado por el Fondo Único de Tecnologías de la Información y Comunicaciones a través de la Coordinación de GIT ColCERT, de los valores del sector previa determinación de la idoneidad de los cotizantes con la identificación de empresas con la experiencia suficiente para la correcta realización de las actividades enmarcadas en los programas, proyectos y servicios de la entidad. El presente proceso de selección le permitirá a la Coordinación GIT ColCERT contar con un aliado que le permita apoyar en la implementación de un proyecto de ciencia, tecnología e innovación enfocado en la solución de retos en materia de ciberseguridad de un grupo de pymes del país, mejorando así los niveles de seguridad digital y fortaleciendo las capacidades y el portafolio de productos y servicios de empresas del sector de tecnologías de la información nacionales.

De esta manera, se esperan desarrollar todas las fases correspondientes con este proyecto que incluyen la identificación y clasificación de retos de innovación en materia de ciberseguridad, el fortalecimiento de las capacidades de empresas de TI para solucionar esos retos y el desarrollo de proyectos de innovación que atiendan las necesidades de seguridad digital encontradas, beneficiando de esta manera, no solo a empresas de la industria TI, sino generando valiosas conexiones con empresas de otros sectores que sin duda mejorarán las capacidades del país para enfrentar los desafíos que trae la digitalización y la lucha contra los delitos cibernéticos

(firmado digitalmente)
ANGELA JANETH CORTÉS HÉRNANDEZ
Coordinadora del Git De COLCERT

Elaboró: Jairo Alexander Martinez Martinez – Abogado GIT ColCERT
Andres Oliverio Sandoval Sandoval – Contratista GIT ColCER

REGISTRO DE FIRMAS ELECTRONICAS

3. Estudio del Sector

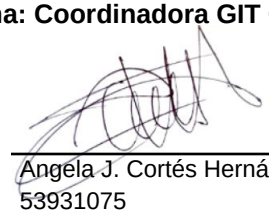
Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20260128-145248-c7a117-49408511
Estado: Finalizado

Creación: 2026-01-28 14:52:48
Finalización: 2026-01-28 15:09:16

Escanee el código para verificación

Firma: Coordinadora GIT ColCERT



Angela J. Cortés Hernández
53931075
acortes@mintic.gov.co

Ministerio TIC

Elaboración: Contratista GIT ColCERT

Andres Oliverio Sandoval Sandoval
1072665899
asandoval@mintic.gov.co
Contratista
ColCERT

Elaboración: Abogado GIT ColCERT

JAIRO ALEXANDER MARTINEZ MARTINEZ
1015401530
jmartinezm@mintic.gov.co

REPORTE DE TRAZABILIDAD

3. Estudio del Sector

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20260128-145248-c7a117-49408511
Creación: 2026-01-28 14:52:48
Estado: Finalizado
Finalización: 2026-01-28 15:09:16

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	JAIRO ALEXANDER MARTINEZ MARTINEZ jmartinezm@mintic.gov.co	Aprobado	Env.: 2026-01-28 14:52:54 Lec.: 2026-01-28 14:58:11 Res.: 2026-01-28 14:58:19 IP Res.: 191.95.55.234 Canal: Email
Elaboración	Andres Oliverio Sandoval Sandoval asandoval@mintic.gov.co Contratista ColCERT	Aprobado	Env.: 2026-01-28 14:58:20 Lec.: 2026-01-28 15:04:00 Res.: 2026-01-28 15:04:10 IP Res.: 190.68.151.202 Canal: Email
Firma	Angela J. Cortés Hernández acortes@mintic.gov.co Ministerio TIC	Aprobado	Env.: 2026-01-28 15:04:10 Lec.: 2026-01-28 15:09:10 Res.: 2026-01-28 15:09:15 IP Res.: 191.156.234.16 Canal: Email