REPÚBLICA DE COLOMBIA

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

GIT COLCERT

ANÁLISIS DEL SECTOR

OBJETO: 3020021-Adquisición de Software por Catálogo II mediante un servicio de Ciberinteligencia Proactiva utilizando Google Threat Intelligence Enterprise, para el despliegue y continuidad de la línea de Análisis Situacional del portafolio de servicios del Equipo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT.

Bogotá D.C, Diciembre de 2025

CONTENIDO

1. INTRODUCCIÓN

El Equipo de Respuesta a Emergencias Cibernéticas de Colombia – **ColCERT**, como componente fundamental del Sistema de Seguridad Digital del Estado, tiene la responsabilidad de **proteger la infraestructura crítica, los activos tecnológicos gubernamentales y la información de interés nacional** frente a amenazas en constante evolución dentro del ciberespacio. Su misión incluye la **anticipación, identificación, caracterización, correlación y mitigación de incidentes**, así como la coordinación nacional ante riesgos y campañas cibernéticas de alto impacto

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 por ejemplo, se registraron 7.1 mil millones de intentos de ciberataques en el primer semestre de 2025[1], ubicando a Colombia como el tercer país con mayor número de ataques en América Latina. A su vez en la gestión de incidentes de seguridad digital en Colombia durante 2025 ColCERT clasificó los incidentes en tres categorías: Orden Nacional (18.48%), Territorial (50.71%) y Privado (30.81%). Los principales incidentes reportados fueron el uso no autorizado de datos y el phishing, mientras que el 70% de los ataques de ransomware afectaron principalmente a los sectores gubernamental y educativo. De acuerdo con los datos del

[1] Según el más reciente informe de FortiGuard Lab 2025.

primer semestre, el uso no autorizado de recursos representó el 36.49% y el phishing el 31.75% de los incidentes más reportados, manteniéndose la distribución por categoría previamente mencionada. En cuanto al análisis y la gestión de vulnerabilidades, se evaluaron 198 entidades y 8,085 sitios web y servidores pertenecientes a los sectores Gobierno, TIC y Minero, identificándose como vulnerabilidades recurrentes el uso de PHP sin soporte (55%) y la utilización de versiones desactualizadas de Bootstrap en el diseño web (25%). Adicionalmente, se llevaron a cabo sesiones de concientización sobre riesgos cibernéticos que impactaron a 7,917 funcionarios, contratistas y colaboradores. Finalmente, el Análisis Situacional del Observatorio evidenció un aumento en la generación y gestión de alertas, advertencias e informes, lo cual refleja una mejora sustancial en la capacidad de detección y vigilancia de amenazas digitales. Estos puntos resumen Los principales aspectos tratados; para información adicional, se encuentra disponible la posibilidad de solicitarla.

La gestión de transferencia de conocimiento ha funcionado como un componente clave de formación continua para funcionarios, contratistas y colaboradores de entidades públicas y privadas en Colombia, orientada a fortalecer hábitos de seguridad digital y capacidades de gestión de incidentes, con impacto directo en la continuidad operativa y la protección de la información. Entre 2022 y 2025 se han desarrollado 117 sesiones que han capacitado a 8.352 personas, con una progresión que evidencia madurez y escalamiento: en 2022 se realizaron 23 sesiones para 1.260 participantes; en 2023 se ejecutaron 27 sesiones con 1.695 asistentes; en 2024 el programa se expandió a 42 sesiones que involucraron a 3.180 personas, y en el transcurso de 2025 se registran 25 sesiones con 2.217 participantes. El promedio de participación es de 71 asistentes por sesión, con una tendencia ascendente año a año que sugiere mayor atracción y pertinencia de los contenidos.

La participación institucional muestra un equilibrio y alcance nacional. De las 117 sesiones realizadas, 56 se impartieron a entidades del orden nacional, 44 a entidades del orden territorial y 17 al sector privado, lo que equivale aproximadamente a un 48 %, 38 % y 15 % del total, respectivamente. Esta distribución demuestra la objetiva capacidad de articulación con equipos técnicos de diferentes niveles de entidades de gobierno y con actores privados, asegurando que las competencias desarrolladas traspasen tanto funciones misionales como cadenas de provisión de servicios.

Desde una perspectiva de valor público, las cifras describen un mecanismo efectivo de cierre de brechas de conocimiento y de estandarización de buenas prácticas. El crecimiento sostenido en sesiones y alcance, junto con la diversificación institucional, indican que el programa no sólo sensibiliza, sino que transfiere capacidades aplicables a la prevención, detección y respuesta a incidentes, contribuyendo a la construcción de una cultura de seguridad digital en entornos familiares, personales y laborales, así como a la mejora continua del nivel de preparación del Estado y sus aliados.

En conclusión, incrementar el nivel de formación en ciberseguridad resulta esencial ante el crecimiento de amenazas cibernéticas, motivado por el desconocimiento sobre detección de riesgos, la falta de habilidades especializadas y la continua evolución tecnológica. Un programa formativo efectivo debe abordar estas causas, proporcionando a personas y organizaciones las competencias necesarias para desenvolverse adecuadamente en un entorno cada vez más digitalizado. Sólo mediante el compromiso sostenido de todos los actores sociales será posible garantizar una Colombia digital segura, inclusiva y adaptativa a los retos del siglo XXI.

Por lo anterior, El Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic / Fondo Único de TIC contó con la licencia El Workshop de Google Threat Intelligence (GTI) Enterprise tuvo una duración aproximada de 2 semanas, con un total de 15 horas de capacitación, distribuidas en sesiones teórico-prácticas, para la fecha no se encuentra vigente.

Como resultado del desarrollo del Workshop de Google Threat Intelligence (GTI) Enterprise, Servinformación entregará los siguientes elementos al finalizar las sesiones, los cuales consolidan los principales resultados del entrenamiento:

- Material de capacitación utilizado durante el Workshop, incluyendo presentaciones técnicas, guías de apoyo y escenarios de laboratorio empleados en las demostraciones.
- Documentación técnica consolidada, que incluirá las configuraciones, capturas y procedimientos vistos durante las sesiones prácticas (ASM, DTM, Private Scanning e integración con SecOps).
- Diagrama de arquitectura e integración interna de GTI Enterprise, mostrando la relación con los módulos y fuentes de inteligencia de Mandiant, VirusTotal y Google Cloud Threat Intelligence.
- Guía de mejores prácticas y KPIs operativos, enfocada en la sostenibilidad y aprovechamiento del servicio dentro del entorno de MINTIC.
- Informe final del Workshop, que consolida los materiales, resultados de las sesiones, recomendaciones estratégicas y registro de asistencia de participantes.

Por lo anterior, es necesario realizar la adquisición de un licenciamiento, en las condiciones señaladas en el IAD para la compra de software por catálogo II No. CCE-SNG-IA-002-2024, a efectos que el ColCert pueda cumplir con su misionalidad que es la a**nticipación, identificación, caracterización, correlación y mitigación de incidentes cibernéticos** para brindar seguridad digital.

1 DEFINICIÓN DE LA NECESIDAD

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[2] Modificado por el Art. 4 de la Ley 1978 de 2019[3], 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 (…)".

[2] 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.

[3] 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

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".*

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, 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, 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 y de conformidad con artículo 2.2.21.1.5.2 del Decreto 338 de 2022.

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.

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 por ejemplo, se registraron 7.1 mil millones de intentos de ciberataques en el primer semestre de 2025[4], ubicando a Colombia como el tercer país con mayor número de ataques en América Latina. A su vez en la gestión de incidentes de seguridad digital en Colombia durante 2025 ColCERT clasificó los incidentes en tres categorías: Orden Nacional (18.48%), Territorial (50.71%) y Privado (30.81%). Los principales incidentes reportados fueron el uso no autorizado de datos y el phishing, mientras que el 70% de los ataques de ransomware afectaron principalmente a los sectores gubernamental y educativo. De acuerdo con los datos del primer semestre, el uso no autorizado de recursos representó el 36.49% y el phishing el 31.75% de los incidentes más reportados, manteniéndose la distribución por categoría previamente mencionada. En cuanto al análisis y la gestión de vulnerabilidades, se evaluaron 198 entidades y 8,085 sitios web y servidores pertenecientes a los sectores Gobierno, TIC y Minero, identificándose como vulnerabilidades recurrentes el uso de PHP sin soporte (55%) y la utilización de versiones desactualizadas de Bootstrap en el diseño web (25%).

[4] Según el más reciente informe de FortiGuard Lab 2025.

Adicionalmente, se llevaron a cabo sesiones de concientización sobre riesgos cibernéticos que impactaron a 7,917 funcionarios, contratistas y colaboradores. Finalmente, el Análisis Situacional del Observatorio evidenció un aumento en la generación y gestión de alertas, advertencias e informes, lo cual refleja una mejora sustancial en la capacidad de detección y vigilancia de amenazas digitales. Estos puntos resumen Los principales aspectos tratados; para información adicional, se encuentra disponible la posibilidad de solicitarla.

La gestión de transferencia de conocimiento ha funcionado como un componente clave de formación continua para funcionarios, contratistas y colaboradores de entidades públicas y privadas en Colombia, orientada a fortalecer hábitos de seguridad digital y capacidades de gestión de incidentes, con impacto directo en la continuidad operativa y la protección de la información. Entre 2022 y 2025 se han desarrollado 117 sesiones que han capacitado a 8.352 personas, con una progresión que evidencia madurez y escalamiento: en 2022 se realizaron 23 sesiones para 1.260 participantes; en 2023 se ejecutaron 27 sesiones con 1.695 asistentes; en 2024 el programa se expandió a 42 sesiones que involucraron a 3.180 personas, y en el transcurso de 2025 se registran 25 sesiones con 2.217 participantes. El promedio de participación es de 71 asistentes por sesión, con una tendencia ascendente año a año que sugiere mayor atracción y pertinencia de los contenidos.

La participación institucional muestra un equilibrio y alcance nacional. De las 117 sesiones realizadas, 56 se impartieron a entidades del orden nacional, 44 a entidades del orden territorial y 17 al sector privado, lo que equivale aproximadamente a un 48 %, 38 % y 15 % del total, respectivamente. Esta distribución demuestra la objetiva capacidad de articulación con equipos técnicos de diferentes niveles de entidades de gobierno y con actores privados, asegurando que las competencias desarrolladas traspasen tanto funciones misionales como cadenas de provisión de servicios.

Desde una perspectiva de valor público, las cifras describen un mecanismo efectivo de cierre de brechas de conocimiento y de estandarización de buenas prácticas. El crecimiento sostenido en sesiones y alcance, junto con la diversificación institucional, indican que el programa no sólo sensibiliza, sino que transfiere capacidades aplicables a la prevención, detección y respuesta a incidentes, contribuyendo a la construcción de una cultura de seguridad digital en entornos familiares, personales y laborales, así como a la mejora continua del nivel de preparación del Estado y sus aliados.

En conclusión, incrementar el nivel de formación en ciberseguridad resulta esencial ante el crecimiento de amenazas cibernéticas, motivado por el desconocimiento sobre detección de riesgos, la falta de habilidades especializadas y la continua evolución tecnológica. Un programa formativo efectivo debe abordar estas causas, proporcionando a personas y organizaciones las competencias necesarias para desenvolverse adecuadamente en un entorno cada vez más digitalizado. Sólo mediante el compromiso sostenido de todos los actores sociales será posible garantizar una Colombia digital segura, inclusiva y adaptativa a los retos del siglo XXI.

De conformidad de lo anterior, El Equipo de Respuesta a Emergencias Cibernéticas de Colombia – **ColCERT**, como componente fundamental del Sistema de Seguridad Digital del Estado, tiene la responsabilidad de **proteger la infraestructura crítica, los activos tecnológicos gubernamentales y la información de interés nacional** frente a amenazas en constante evolución dentro del ciberespacio. Su misión incluye la **anticipación, identificación, caracterización, correlación y mitigación de incidentes**, así como la coordinación nacional ante riesgos y campañas cibernéticas de alto impacto.

En desarrollo de esta misión, ColCERT debe mantener capacidades robustas y actualizadas que le permitan realizar **Análisis Situacional**, entendidos como procesos de vigilancia, comprensión contextual y toma de decisiones basadas en inteligencia sobre el ecosistema de amenazas que puede afectar a entidades del Estado y sectores estratégicos. Sin embargo, el entorno actual presenta desafíos crecientes que exigen un fortalecimiento significativo de esta línea operacional. Entre los factores que justifican esta necesidad se destacan los siguientes:

1. **Incremento en la complejidad de las amenazas cibernéticas**

El panorama nacional y global presenta una proliferación de:

- campañas de ransomware avanzadas,
- operaciones persistentes de actores estatales y grupos APT,
- explotación de vulnerabilidades zero-day,
- ataques a la cadena de suministro,
- herramientas de ataque automatizadas basadas en IA,
- y amenazas híbridas que combinan desinformación, ingeniería social y explotación técnica.

Estas amenazas superan las capacidades tradicionales de monitoreo y respuesta reactiva. ColCERT requiere herramientas especializadas que permitan **identificar patrones no evidentes, correlacionar señales débiles y anticipar comportamientos maliciosos**, incluso antes de que los ataques se materialicen.

2. ***Necesidad de detección temprana y correlación avanzada***

El ciclo de vida de los incidentes cibernéticos se ha acortado drásticamente. Gran parte de las campañas modernas aprovechan:

- automatización,
- infraestructura masiva distribuida,
- técnicas de evasión sofisticadas,
- y despliegues coordinados que pueden comprometer múltiples entidades al mismo tiempo.
-

Para proteger el Estado colombiano, ColCERT debe contar con **capas profundas de inteligencia de amenazas**, capaces de:

- detectar indicadores de compromiso (IoC) emergentes,
- reconocer tácticas, técnicas y procedimientos (TTPs) de actores relevantes,
- correlacionar eventos dispersos entre varias fuentes nacionales e internacionales,
- y generar alertas tempranas que permitan adoptar medidas preventivas.

Esto implica la necesidad de una plataforma que integre **inteligencia técnica (CTI), datos OSINT, análisis automatizado y fuentes globales en tiempo real**.

Las entidades públicas han adoptado de manera acelerada tecnologías como:

- servicios en la nube,
- arquitecturas híbridas,
- dispositivos IoT,
- sistemas industriales OT/SCADA,
- y servicios expuestos a internet para interoperabilidad y ciudadanía digital.

Este crecimiento ha ampliado la superficie de ataque del Estado colombiano. La línea de Análisis Situacional debe contar con capacidades que permitan:

- identificar activos expuestos,
- mapear vulnerabilidades asociadas,
- comprender su relación con campañas globales en curso,
- y priorizar alertas de acuerdo con el riesgo real para el país.

Sin estas capacidades, el ColCERT tendría limitaciones para emitir alertas estratégicas, boletines de seguridad o recomendaciones de mitigación efectivas.

La cantidad de información que procesa ColCERT diariamente es creciente:

- telemetría global,
- reportes de incidentes,
- feeds de amenazas,
- datos OSINT,
- logs de infraestructura,
- investigaciones de terceros,
- información de comunidades internacionales de ciberseguridad.

Sin herramientas avanzadas, la enorme carga de datos puede convertirse en una barrera. Se requiere **automatización asistida por inteligencia artificial** para:

- clasificar,
- priorizar,
- correlacionar,
- y transformar datos crudos en inteligencia accionable.

La automatización reduce tiempos y permite que los analistas enfoquen su trabajo en actividades de mayor valor como threat hunting, atribución y análisis estratégico.

Las amenazas cibernéticas son persistentes y de carácter continuo. Por ello, la línea de Análisis Situacional no puede operar bajo modelos de interrupción o dependencia de herramientas puntuales.

La continuidad operativa implica garantizar:

- disponibilidad permanente de fuentes de inteligencia,
- acceso en tiempo real a indicadores y alertas globales,
- soporte especializado para su interpretación y correlación,
- y mecanismos de continuidad tecnológica a largo plazo.

Una interrupción en estas capacidades representa un riesgo directo para la seguridad digital del Estado colombiano.

La selección de Google Threat Intelligence (GTI) porque representa la fusión más potente y completa de inteligencia de amenazas en el ciberespacio disponible en el mercado para un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), ofreciendo al Equipo de Respuesta a Emergencia Cibernéticas de Colombia ColCERT una ventaja operativa crucial que ninguna otra solución iguala al combinar simultáneamente la escala global, la experiencia especializada y la verificación técnica inmediata. Mientras que competidores como Microsoft Defender Threat Intelligence (MDTI) ofrecen una

La selección de Google Threat Intelligence (GTI) porque representa la fusión más potente y completa de inteligencia de amenazas en el ciberespacio disponible en el mercado para un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), ofreciendo al Equipo de Respuesta a Emergencia Cibernéticas de Colombia ColCERT una ventaja operativa crucial que ninguna otra solución iguala al combinar simultáneamente la escala global, la experiencia especializada y la verificación técnica inmediata. Mientras que competidores como Microsoft Defender Threat Intelligence (MDTI) ofrecen una excelente visibilidad para entornos basados en su propia nube, la fortaleza de GTI reside en su independencia y universalidad, capturando datos de la red de Google a una escala que va más allá de un ecosistema de productos específico, dándonos una visibilidad de manera preventiva a nivel global. Además, si bien otras plataformas como Recorded Future son excelentes para priorizar amenazas y escanear la *Dark Web*, GTI nos proporciona algo más valioso en una crisis, la experiencia de respuesta de Mandiant, una división especialziada reconocida mundialmente por su análisis de Técnicas, Tácticas y Procedimientos (TTPs - *quién, cómo y por qué* atacan los adversarios), que es la pieza faltante que transforma los datos en estrategia de defensa en tiempo real. La tercera gran ventaja es el acceso directo a la base de datos de VirusTotal, la enciclopedia de *malware* más grande del mundo, que nos permite verificar y contextualizar cualquier Indicador de Compromiso (IoC) en segundos, superando a otras fuentes que solo proporcionan *feeds* de datos sin esta capacidad de análisis instantáneo. La adopción de una

plataforma avanzada de ciberinteligencia como Google Threat Intelligence Enterprise (GTIE), en el marco del despliegue y fortalecimiento de la línea de Análisis Situacional de ColCERT.

3. Complejidad técnica de la plataforma y del entorno operativo nacional

GTIE integra:

- Telemetría global de múltiples fuentes
- Datos históricos y tiempo real
- Mecanismos de Machine Learning
- Módulos de hunting, correlación, modelado de amenazas y análisis de artefactos

El ecosistema tecnológico de ColCERT, por su parte, incluye:

- Infraestructura híbrida (on-premise, nube gubernamental, servicios externos)
- Herramientas SIEM, SOAR, TIP y sistemas de monitoreo
- Múltiples flujos de información provenientes de entidades públicas y privadas
- Procesos internos de gestión de incidentes y análisis de inteligencia

Esta combinación de elementos exige una fase de **acompañamiento profesional** para garantizar un despliegue técnicamente sólido, consistente con las mejores prácticas internacionales y adaptado a la realidad particular del Estado colombiano.

4. Configuración avanzada y adaptación a casos de uso del Gobierno de Colombia

Un servicio de ciberinteligencia proactiva no es un producto de uso genérico. Debe adaptarse a los **casos de uso operativos, tácticos y estratégicos** del ColCERT.

1.1.1 **Diseño e implementación de casos de uso críticos:**

- Monitoreo de campañas APT dirigidas a entidades públicas
- Identificación de amenazas a infraestructura crítica nacional
- Alertas tempranas sobre filtración de credenciales gubernamentales
- Seguimiento de campañas de phishing específicas de servicios del Estado
- Correlación de IOCs con datos internos del Gobierno
- Priorización basada en impacto nacional

1.1.2 Ajuste fino de reglas, dashboards y correlaciones

Para que la plataforma entregue productos de inteligencia útiles y no información cruda sin contexto.

1.1.3 Construcción de modelos de riesgo adaptados a Colombia

Incorporando:

- Tácticas de actores hostiles con interés en el país
- Tipologías de ataques más frecuentes contra el sector público
- Estacionalidad de campañas (elecciones, periodos fiscales, coyunturas geopolíticas)

Sin este acompañamiento, el uso del software sería superficial y el retorno de inversión limitado

5. Acompañamiento en investigaciones de amenazas complejas

Las amenazas que enfrenta el país incluyen:

- Grupos APT con capacidades ofensivas avanzadas
- Campañas de desinformación coordinadas
- Operaciones de espionaje digital
- Ransomware de alto impacto
- Compromisos de cadenas de suministro
- Exfiltración de datos en dark web

La investigación de este tipo de campañas requiere:

- Analistas con experiencia en ciberinteligencia estratégica
- Capacidades de atribución técnica y contextual
- Uso avanzado de herramientas de correlación
- Interpretación de patrones geopolíticos que afectan al país

Estos servicios permiten apoyar al ColCERT en situaciones de alto impacto, donde el tiempo de respuesta y la precisión son fundamentales.

Por lo anterior, el ColCERT en aras de cumplir su misionalidad y cumplir sus necesidades requiere lo siguiente:

Solución Cloud.

Con base en lo enunciado en el contexto, se requiere adquirir la suscripción y servicios asociados a la plataforma Google Threat Intelligence - Edición Enterprise. Esta solución debe ser nativa de nube (SaaS) y contemplar los siguientes módulos y capacidades:

- Inteligencia de Amenazas Unificada: Herramienta que consolide inteligencia de primera línea (tipo Mandiant), inteligencia de comunidad global (tipo VirusTotal) y telemetría de infraestructura de nube (Google). Debe permitir la investigación ilimitada de Indicadores de Compromiso (IoCs) y ofrecer perfiles detallados de actores de amenaza.
- Gestión de Superficie de Ataque (Attack Surface Management - ASM): Módulo para el descubrimiento y monitoreo continuo de activos externos expuestos a internet, identificando vulnerabilidades, "Shadow IT" y malas configuraciones antes que los atacantes.
- Monitoreo de Amenazas Digitales (Digital Threat Monitoring - DTM): Capacidad para monitorear la web superficial, profunda y oscura (Deep/Dark Web) en busca de suplantaciones de marca, fugas de credenciales y menciones maliciosas contra la entidad.
- Análisis con Inteligencia Artificial: Incorporación de modelos de IA Generativa (como Gemini) para resumir amenazas complejas, realizar búsquedas en lenguaje natural y automatizar el análisis de código malicioso.
- Investigación y Sandbox Privado: Capacidad de detonar y analizar archivos y URLs sospechosos en un entorno seguro y privado, sin compartir la información con la comunidad pública.

Esta plataforma despliega una vigilancia 24/7 automatizada sobre el panorama global de amenazas, elemento fundamental para la generación de inteligencia proactiva de alto valor. Esta información será utilizada por el servicio de análisis situacional y publicada para que las entidades ajusten inmediatamente su postura de seguridad, reduciendo el riesgo de ser víctimas de actores de amenaza avanzados.

Criterios sugeridos para la definición del alcance y características técnicas de la necesidad.

Requisitos de negocio (Entidad).

El ColCERT busca adoptar un enfoque de "Dominancia de Inteligencia". La plataforma tecnológica debe permitir no sólo consumir datos, sino entender el contexto del adversario.

Funcionalidades Técnicas Requeridas:

- Threat Landscape & Graph: Acceso a perfiles de amenazas, campañas activas y visualización gráfica de relaciones entre indicadores.
- Inteligencia de Vulnerabilidades: Priorización de vulnerabilidades basada en riesgo real de explotación (EPSS) y no solo en severidad teórica (CVSS).
- Reglas YARA y Hunting: Capacidad para crear y gestionar reglas YARA para búsqueda proactiva de amenazas en repositorios globales de malware (Livehunt y Retrohunt).

- API y APIficación: La solución debe contar con una API robusta (mínimo 30,000 solicitudes/día) para integrarse con sistemas SIEM (ej. Google SecOps, Splunk), SOAR y EDR, facilitando la interoperabilidad y automatización.

1.1.4 Infraestructura

La arquitectura de la solución es 100% SaaS, eliminando la necesidad de hardware local.

A. Servicios de Implementación y Puesta en Marcha:

- Configuración inicial del *tenant* de Google Threat Intelligence.
- Definición de activos críticos para el módulo de ASM.
- Configuración de palabras clave y dominios para el monitoreo de marca (DTM).

Como resultado del desarrollo del Workshop de Google Threat Intelligence (GTI) Enterprise, Servinformación entregará los siguientes elementos al finalizar las sesiones, los cuales consolidan los principales resultados del entrenamiento:

- Material de capacitación utilizado durante el Workshop, incluyendo presentaciones técnicas, guías de apoyo y escenarios de laboratorio empleados en las demostraciones.
- Documentación técnica consolidada, que incluirá las configuraciones, capturas y procedimientos vistos durante las sesiones prácticas (ASM, DTM, Private Scanning e integración con SecOps).
- Diagrama de arquitectura e integración interna de GTI Enterprise, mostrando la relación con los módulos y fuentes de inteligencia de Mandiant, VirusTotal y Google Cloud Threat Intelligence.
- Guía de mejores prácticas y KPIs operativos, enfocada en la sostenibilidad y aprovechamiento del servicio dentro del entorno de MINTIC.
- Informe final del Workshop, que consolida los materiales, resultados de las sesiones, recomendaciones estratégicas y registro de asistencia de participantes.

Por lo anterior, es necesario realizar la adquisición de un licenciamiento, en las condiciones señaladas en el IAD para la compra de software por catálogo II No. CCE-SNG-IA-002-2024, a efectos de garantizar la continuidad de la iniciativa Mi Colombia Digital y en el apoyo que se brinda a las entidades territoriales que hacen parte de esta

Aunado a lo anterior, y teniendo en cuenta lo establecido en el IAD para la compra de software por catálogo II No. CCE-SNG-IAD-002-2024, la entidad procedió también a publicar en la Tienda Virtual del Estado Colombiano (TVEC), el 28 de octubre de 2025 la consulta de información (RFI) asociada al evento no. 203450

el cual remitieron información a fecha de cierre 1 de diciembre de 2025, las compañías XERTICA COLOMBIA S.A.S, Network & Accesories SAS e Información Localizada.

Las tres respuestas recibidas por parte de los proveedores no presentaron observaciones que implicaran modificaciones a los aspectos técnicos y mediante las mismas, se manifiesta el cumplimiento del requerimiento RFI – SC – GOOGLE – Evento 203450.

En consecuencia, teniendo en cuenta que existe el Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024, vigente hasta el 21 de noviembre de 2027 y que tiene como fecha máxima para ejecutar órdenes de compra hasta el 21 de noviembre de 2028, el cual contempla un catálogo de productos Google entre los que se encuentra el licenciamiento requerido, es procedente realizar la adquisición a través de este instrumento. https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/instrumento-de-agregacion-de-demanda-iadsda-de

Finalmente, se informa que la presente contratación se encuentra incluida en el Plan Anual de Adquisiciones de la Entidad con el código 3020021- Adquisición de Software por Catálogo II mediante un servicio de Ciberinteligencia Proactiva utilizando Google Threat Intelligence Enterprise, para el despliegue y continuidad de la línea de Análisis Situacional del portafolio de servicios del Equipo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, y se realizará con cargo al presupuesto del Fondo Único de TIC para la vigencia 2025, para lo cual se ha solicitado el Certificado de Disponibilidad Presupuestal No. 326925 del 19/12/2025 a través del Coordinador del Grupo de Presupuesto del Ministerio.

2. ASPECTOS GENERALES

En cumplimiento de lo dispuesto en el artículo 2.2.1.1.1.6.1 del Decreto 1082 de 2015, las Entidades Estatales deben elaborar un estudio del sector con el propósito de analizar las condiciones del mercado relacionadas con el objeto a contratar, identificando la oferta disponible, los precios de referencia, las condiciones técnicas, financieras y legales, así como los riesgos asociados al proceso de contratación, garantizando la pluralidad de oferentes, la eficiencia y la selección objetiva.

En desarrollo de dicho mandato normativo, para la **adquisición del licenciamiento Google Workspace**, se realizó un análisis de los factores **internacionales, económicos, financieros, técnicos y legales** que inciden en el comportamiento del sector de software colaborativo y de correo institucional en la nube. El estudio parte de la existencia del **Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024**, administrado por **Colombia Compra Eficiente**, el cual consolida la oferta de productos de software de uso común, entre ellos las licencias de **Google Workspace** en sus diferentes modalidades (*Enterprise Starter, Enterprise Standard y Enterprise Plus*).

Los resultados del presente análisis permiten confirmar que el mercado dispone de proveedores habilitados, con condiciones técnicas homogéneas, precios competitivos y un marco regulatorio claro, lo que garantiza la transparencia, eficiencia y oportunidad en la adquisición de las licencias requeridas.

En este contexto, el presente estudio del sector se desarrolla con el fin de soportar la adquisición proyectada y asegurar la adecuada planeación de la contratación, conforme a los principios de la función administrativa y a las directrices del Instrumento de Agregación de Demanda (IAD/SDA) de Software por Catálogo II No. CCE-SNG-IAD-002-2024.

3.1 ASPECTO INTERNACIONAL

A nivel internacional, las herramientas colaborativas basadas en la nube —como Google Workspace, Microsoft 365 y, en menor medida, Zoho Workplace— han sido adoptadas por diversos organismos gubernamentales para optimizar la productividad, la comunicación y la gestión documental. Estas plataformas cuentan con certificaciones internacionales de seguridad de la información, tales como ISO/IEC 27001, SOC 2 e ISO/IEC 27701, lo que contribuye a su idoneidad para entornos públicos que manejan información sensible.

En el plano internacional, aunque los datos exactos de participación pueden variar, se observa que los grandes proveedores de nube (como Google, Microsoft y Amazon) concentran una parte relevante del gasto en servicios de nube y herramientas SaaS, lo que refleja el peso creciente de los modelos de productividad en la nube.

En la práctica, casos como el de la Tesorería General de la República de Chile (TGR), que implementó 2.200 licencias de Google Workspace y gestionó más de 11.000 reuniones virtuales en un mes, y el del Tribunal Regional del Trabajo de la 3ª Región en Minas Gerais (Brasil), que migró ~5.000 cuentas y 30 TB de datos, confirman la adopción real en el sector público latinoamericano.

1.2 ASPECTO ECONÓMICO

El mercado global de software colaborativo y de productividad en la nube presenta un crecimiento sostenido, impulsado por la digitalización del trabajo, la adopción del modelo SaaS (*Software as a Service*) y la búsqueda de soluciones que reduzcan costos de infraestructura y soporte. De acuerdo con proyecciones de IDC 2025, el mercado mundial de servicios en la nube registra una tasa de crecimiento promedio anual cercana al 14%, reflejando la consolidación de plataformas como Google Workspace, Microsoft 365 y Zoho Workplace. Estas soluciones concentran una participación significativa en los segmentos gubernamental, educativo y corporativo por su escalabilidad, seguridad y modelo flexible de licenciamiento. Dicha dinámica es posible gracias a la interacción de los agentes que componen el sector, una cadena de valor que inicia con los fabricantes de tecnología (OEMs) y desarrolladores globales, pasa por los mayoristas y canales integradores que nacionalizan y adaptan la oferta, y finaliza en las entidades compradoras que consumen el servicio.

También cabe resaltar que el sector de servicios de tecnología de la información y las comunicaciones (TIC), específicamente al subsector de desarrollo y provisión de software, servicios en la nube y soluciones digitales empresariales. Este rubro forma parte del sector terciario de la economía, correspondiente a las actividades de servicios. Dentro de esta clasificación, los productos incluidos en el sector abarcan una amplia gama de

soluciones que van más allá del almacenamiento básico, integrando suites completas de colaboración y productividad (correo, ofimática, videoconferencia), infraestructura como servicio (IaaS), plataformas como servicio (PaaS), herramientas de ciberseguridad y aplicativos de gestión empresarial, los cuales son esenciales para la modernización operativa.

En el contexto colombiano, el mercado de software y servicios en la nube se ha fortalecido mediante la utilización de instrumentos de agregación de demanda administrados por Colombia Compra Eficiente, los cuales permiten a las entidades públicas acceder a precios preferenciales y a condiciones económicas homogéneas. Este entorno cuenta con la participación activa de gremios y asociaciones como la Federación Colombiana de la Industria de Software y TI (Fedesoft), la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y la Cámara de la Industria Digital de la ANDI, entidades que juegan un rol crucial en la articulación entre la industria privada y las necesidades del Estado. En particular, el Acuerdo Marco de Software por Catálogo II (IAD/SDA No. CCE-SNG-IAD-002-2024) constituye el principal mecanismo para la adquisición de licencias de correo y colaboración en la nube, al consolidar la oferta de los principales proveedores habilitados y generar economías de escala en las compras del Estado.

Respecto a las cifras totales de ventas y eficiencia del gasto, el Ministerio TIC, a través del Fondo Único de Tecnologías de la Información y las Comunicaciones (FUTIC), ha demostrado que el uso de este instrumento genera ahorros superiores al 60% frente a los valores de mercado, según los resultados obtenidos en las vigencias 2019–2024. Esta optimización del gasto público se explica por la reducción en costos de infraestructura física, mantenimiento, soporte y administración técnica, además de eliminar los gastos de transacción asociados a múltiples procesos de contratación. De igual forma, la utilización del IAD/SDA asegura condiciones económicas estables, control presupuestal efectivo y transparencia en la contratación, al concentrar la demanda en un único proceso regulado.

De igual forma, la utilización del IAD/SDA asegura condiciones económicas estables, control presupuestal efectivo y transparencia en la contratación, al concentrar la demanda en un único proceso regulado.

En términos de demanda, la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de su Grupo Interno de Trabajo de Servicios Ciudadanos Digitales realizó una encuesta aplicada a 568 entidades beneficiarias del programa “Mi Colombia Digital” lo que permitió evidenciar un incremento del 58 % en la necesidad de almacenamiento superior a 1 TB por usuario, lo que confirma la sostenibilidad económica y técnica de mantener un esquema de licenciamiento escalable y de pago por uso, ajustado a las necesidades reales de las entidades públicas.

El proceso aplica al sector de servicios de tecnología de la información y las comunicaciones (TIC), específicamente al subsector de desarrollo y provisión de software, servicios en la nube y soluciones digitales

empresariales. Este sector forma parte del sector terciario de la economía, correspondiente a las actividades de servicios.

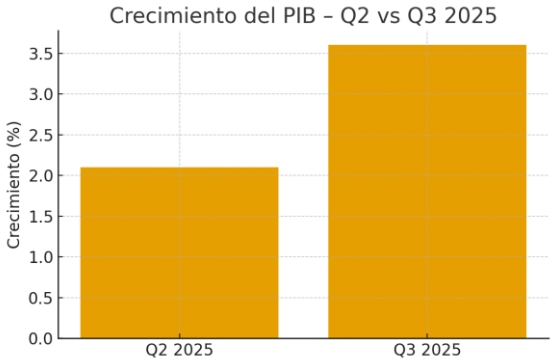
Las siguientes son actividades desarrolladas por el sector en Colombia y se muestran los productos y servicios ofrecidos por el sector:

Código CIIU	Actividad Económica
4651	Comercio al por mayor de computadores, equipo periférico y programas de informática
4741	Comercio al por menor de computadores, equipos periféricos, programas de informática y equipos de telecomunicaciones en establecimientos especializados
5820	Edición de programas de informática (software)
6201	Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas)
6202	Actividades de consultoría informática y actividades de administración de instalaciones informáticas
6209	Otras actividades de tecnologías de información y actividades de servicios informáticos
6311	Procesamiento de datos, alojamiento (hosting) y actividades relacionadas
6312	Portales web
6399	Otras actividades de servicio de información n.c.p

Fuente: https://linea.ccb.org.co/descripcionciiu/

Producto Interno Bruto (PIB): tercer trimestre 2025

Según el DANE (2025), el Producto Interno Bruto presentó un crecimiento real del 3,6% en el tercer trimestre de 2025 respecto al mismo trimestre del año anterior. Este comportamiento refleja una recuperación progresiva de las actividades productivas, impulsada principalmente por los sectores de comercio, transporte, agricultura y servicios públicos esenciales.



Fuente: Departamento Administrativo Nacional de Estadística. (2025). Boletín técnico PIB – III trimestre 2025.

De acuerdo con las cifras del Departamento Administrativo Nacional de Estadística (DANE), la economía colombiana registró un crecimiento del 3,6% en su serie original durante el tercer trimestre de 2025, en comparación con el mismo periodo del año anterior. Así mismo, frente al trimestre inmediatamente anterior, el PIB presentó un incremento del 1,2% en su serie ajustada por efecto estacional y calendario.

Crecimiento del Sector Información y Comunicaciones:

Si bien la información específica del crecimiento del valor agregado del sector Información y Comunicaciones para el tercer trimestre de 2025 no está detallada en los informes del DANE, el crecimiento general del PIB del 3,6% para el tercer trimestre supera el 2,1% reportado para el segundo trimestre de 2025, lo que indica una aceleración en la dinámica económica nacional.

Con respecto al índice de precios al consumidor (IPC), en septiembre de 2025, la variación mensual de fue de 0,32%, con una variación anual de 5,18%.

Comportamiento de la División Información y Comunicación:

La división Información y comunicación se ubicó por encima del promedio nacional 0,32%, registrando una variación mensual de 1,43% en septiembre de 2025. Esta división contribuyó con 0,04 puntos porcentuales a la variación total mensual del IPC.

Mayor Contribución Relacionada al Sector:

La subclase que más contribuyó al alza en el IPC a nivel general, y que está directamente relacionada con el sector, fue:

- Servicios de comunicación fija y móvil y provisión a internet, con una variación del 1,59% y una contribución de 0,04 puntos porcentuales.

El Producto Interno Bruto (PIB) de Colombia registró un crecimiento total del 3,6% en el tercer trimestre de 2025, evidenciando una expansión impulsada principalmente por el sector servicios. De hecho, las actividades con mayor dinamismo fueron las artísticas, de entretenimiento y servicios a los hogares, que lideraron con un crecimiento del 9,2%. Asimismo, el componente de Administración Pública, Educación y Salud contribuyó significativamente al alza, con una expansión del 6,8%. Por otra parte, sectores clave como el Comercio, Transporte y Alojamiento mantuvieron una sólida expansión del 5,6%, mientras que la Industria Manufacturera creció moderadamente a un 4,1%. Sin embargo, el panorama no fue positivo para todos los sectores: la Construcción experimentó una contracción del -1,5%, y peor aún, el sector de Explotación de Minas y Canteras (petróleo y carbón) fue el más afectado, con una caída de -5,7%, lo que demuestra los desafíos que enfrentan las actividades extractivas y de inversión en el país.

Desempeño del Sector de Información y Comunicaciones en el PIB de Colombia (Q3 2025)

El Producto Interno Bruto (PIB) de Colombia experimentó un crecimiento general del 3,6% en el tercer trimestre de 2025. Dentro de este panorama, el sector de Información y Comunicaciones mantuvo un aporte positivo y constante, aunque su ritmo de crecimiento fue más moderado en comparación con las actividades líderes como las artísticas y el sector público. Específicamente, el crecimiento anual (Serie Original) de este sector fue del 3,0% en el Q3 de 2025, al compararse con el mismo trimestre del año anterior. Además, al observar su desempeño inmediato, el crecimiento trimestral (Serie Ajustada) fue del 2,3% en comparación con el segundo trimestre de 2025, lo que confirma que el sector se mantiene en una senda de expansión saludable.

Tabla 2. Información y comunicaciones Tasas de crecimiento en volumen1 Segundo trimestre 2025pr

Actividad económica	Serie original (Variación Anual: Q3 2025 / Q3 2024)
Producto Interno Bruto (PIB)	**3,6%**
Actividades artísticas, de entretenimiento y de recreación y otras actividades de servicios...	9,2%
Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Salud	6,8%

Actividad económica	Serie original (Variación Anual: Q3 2025 / Q3 2024)
Comercio al por mayor y al por menor; Transporte y almacenamiento; Alojamiento y servicios de comida	5,6%
Actividades financieras y de seguros	4,6%
Industrias manufactureras	4,1%
Información y comunicaciones	3,0%
Agricultura, ganadería, caza, silvicultura y pesca	2,4%
Construcción	-1,5%
Explotación de minas y canteras	-5,7%

Fuente: Departamento Administrativo Nacional de Estadística (DANE). (2025). *Producto Interno Bruto (PIB) Trimestral, Cifras Preliminares III Trimestre de 2025*. Recuperado de https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-nacionales-trimestrales

Índice de Precios al Consumidor (IPC).

La inflación en Colombia, medida por el IPC, alcanzó una variación anual del 5,18% en septiembre de 2025, marcando el cierre del tercer trimestre y completando el tercer mes consecutivo de aumentos en la tasa de inflación. De manera específica, la variación mensual de septiembre fue del 0,32%, siendo superior a las expectativas de los analistas. En términos acumulados, la inflación entre enero y septiembre de 2025 se situó en 4,55%. Los mayores incrementos de precio en este mes se observaron en divisiones como Información y Comunicación (principalmente servicios de telefonía e internet), Educación y Bebidas Alcohólicas y Tabaco. A pesar del incremento en el ritmo mensual, la tasa anual de 5,18% es notablemente menor a la registrada en el mismo periodo del año anterior (septiembre de 2024), cuando fue de 5,81%.

Serie de Variación	Periodo	Tasa de Variación
Mensual	Septiembre de 2025 / Agosto de 2025	**0,32%**

Serie de Variación	Periodo	Tasa de Variación
Acumulada Trimestral (Año corrido)	Enero a Septiembre de 2025	**4,55%**
Anual (Inflación)	Septiembre de 2024 a Septiembre de 2025	**5,18%**

Fuente: Departamento Administrativo Nacional de Estadística (DANE). (2025). *Índice de Precios al Consumidor (IPC): Variación mensual, acumulada y anual, septiembre 2025*. Recuperado de https://www.dane.gov.co/index.php/estadisticas-por-tema/precios-y-costos/indice-de-precios-al-consumidor-ipc

El siguiente gráfico, que compara las variaciones del Índice de Precios al Consumidor (IPC) entre septiembre de 2024 y septiembre de 2025 revela tendencias mixtas: por un lado, la inflación anual (el indicador de los últimos doce meses) muestra una clara desaceleración, pasando del 5,81% en 2024 al 5,18% en 2025, lo que indica un alivio en la presión inflacionaria a largo plazo. No obstante, al analizar la variación mensual, el incremento de precios en septiembre de 2025 (0,32%) fue superior al registrado en el mismo mes de 2024 (0,24%), sugiriendo un repunte en el ritmo de subida de los precios al consumidor. Finalmente, la variación acumulada en lo corrido del año (enero a septiembre) se mantuvo prácticamente estable entre ambos periodos, con 4,58% en 2024 y 4,55% en 2025, confirmando que la dinámica inflacionaria general del año ha sido muy similar hasta el final del tercer trimestre.

Cuadro 2. IPC Variación y contribución año corrido Por principales subclases septiembre 2025

Subclase	Variación (%)	Contribución Puntos porcentuales
Arriendo imputado	0,38	0,05
Servicios de comunicación fija y móvil y provisión a internet	1,59	0,04
Frutas frescas	2,38	0,03
Arriendo efectivo	0,36	0,03
Educación preescolar y básica primaria	1,98	0,03
Educación secundaria	2,36	0,02
Electricidad	0,53	0,02
Cerveza y refajo	1,57	0,02
Carne de res y derivados	0,63	0,02
Yuca para consumo en el hogar	12,25	0,01

Fuente: Boletín Técnico Índice de Precios al Consumidor (IPC) septiembre 2025 – DANE: https://www.dane.gov.co/files/operaciones/IPC/sep2025/bol-IPC-sep2025.pdf

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

1.3 ASPECTO FINANCIERO

Determinación del Presupuesto y Normativa Tributaria

El costo estimado del contrato se determina con base en los precios establecidos en el Acuerdo Marco de Precios de Software por Catálogo II (IAD/SDA), vigente hasta 2027, lo que garantiza transparencia, competitividad y estabilidad en los valores de mercado. Este esquema evita sobrecostos por procesos individuales y centraliza la negociación con proveedores globales como Google, obteniendo condiciones financieras favorables para el Estado.

Conforme con la necesidad identificada y en aplicación de la Tasa Representativa del Mercado (TRM) vigente a 15 de diciembre de 2025, equivalente a $3.788,53 pesos colombianos por dólar (USD), se efectuó el cálculo del valor estimado de la adquisición de licencias Google Workspace en sus diferentes modalidades.

Así pues, dado que el licenciamiento a adquirir se enmarca dentro de un modelo de comunicación y colaboración 100% en nube, cuya administración y acceso puede realizarse desde cualquier plataforma heterogénea (celulares, tabletas, ordenadores, etc.), se advierte que la misma está enmarcada dentro del concepto de "computación en la nube" de acuerdo con el Oficio de Registro No. 1058335 del 22 de junio del 2017, emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y replicado por la DIAN en su Concepto Unificado No. 17056 del 25 de agosto de 2017.

Como resultado, el valor estimado de la compra asciende a la suma desuma **DOS MIL DOSCIENTOS OCHENTA Y CUATRO MILLONES QUINIENTOS CUARENTA MIL SETECIENTOS CUATRO PESOS. ($2.284.540.704) M/CTE,** incluido impuesto de timbre y todos los costos administrativos, fiscales, tasas, impuestos y estampillas nacionales y locales.

Nota: Es de aclarar que de acuerdo a la clausula 9 del INTRUMENTO DE AGREGACIÓN DE DEMANDA SISTEMA DINÁMICO DE ADQUSICIÓN (IAD/SDA) DE SOFTWARE POR CATÁLOGO II No. CCE-SNG-IAD-002-2024, el simulador al calcular la cotización incorpora de manera discriminada el valor del IVA, con el fin de determinar el valor oficial de la adquisición. No obstante, se advierte que una vez revisado lo dispuesto en el numeral 20 del artículo 476 del decreto 624 de 1989, este tipo de adquisición de software son exentos del pago del impuesto de IVA.

Definición y Establecimiento de las Cantidades

Para dar cumplimiento a los principios de planeación y economía, la Entidad estableció las cantidades requeridas mediante un análisis técnico de la demanda interna, considerando los siguientes factores:

- Histórico de Consumo y Planta de Personal: Se realizó un cruce de información entre el inventario actual de cuentas activas y la planta de personal (funcionarios y contratistas) proyectada para la vigencia, identificando el número exacto de usuarios que requieren servicios de correo y colaboración.
- Perfiles de Usuario: Se segmentaron las necesidades en diferentes perfiles (ej. Business Starter, Standard, Plus) para asegurar que cada usuario reciba las herramientas estrictamente necesarias para su labor, optimizando así el costo por licencia.
- Proyección de Crecimiento: Se incluyó un margen técnico basado en la tasa de crecimiento de la entidad y la entrada de nuevos proyectos de inversión, asegurando la disponibilidad del servicio durante toda la ejecución del contrato sin incurrir en desabastecimiento ni en compras excesivas de licencias ociosas.

Modelo de Abastecimiento Estratégico

El modelo de abastecimiento estratégico seleccionado corresponde a la Agregación de Demanda mediante el uso de Instrumentos de Agregación de Demanda (IAD). Esta decisión se fundamenta en los lineamientos de Colombia Compra Eficiente, dado que:

- Estandarización: El bien a adquirir (licencias de software de ofimática y colaboración) posee características técnicas uniformes y de común utilización por parte de las entidades estatales.
- Economías de Escala: Al utilizar el Acuerdo Marco de Precios, la Entidad se beneficia de la negociación en bloque realizada por el Estado Colombiano, accediendo a descuentos por volumen que no serían posibles en un proceso de selección individual (Licitación o Selección Abreviada).
- Eficiencia Administrativa: Este modelo reduce los tiempos de contratación y los costos administrativos asociados a la estructuración de procesos complejos, permitiendo una adquisición ágil a través de la Tienda Virtual del Estado Colombiano (TVEC).

Análisis de Adquisiciones: Entidad y Sector Público

Como parte del análisis del sector, se evaluó el comportamiento de la compra tanto a nivel interno como externo:

- Adquisiciones previas de la Entidad: Históricamente, la Entidad ha satisfecho esta necesidad mediante la suscripción de Órdenes de Compra derivadas de los Acuerdos Marco de Precios anteriores (Nube Pública y Software I), lo cual ha demostrado ser un mecanismo eficiente que garantiza la continuidad del servicio y la interoperabilidad con los sistemas de gestión documental existentes.
- Comportamiento de otras Entidades: Al revisar los datos abiertos de la Tienda Virtual del Estado Colombiano y el SECOP II, se evidencia que las entidades del orden nacional con necesidades similares (ministerios, superintendencias y departamentos administrativos) adquieren mayoritariamente estos servicios a través del Acuerdo Marco de Software por Catálogo. Esta tendencia

del mercado confirma que es el canal idóneo, pues estandariza los niveles de servicio (SLA) y facilita el control fiscal sobre los recursos tecnológicos.

Item	Código del producto	Nombre	Descripción	Asistencia	Perfil	Unidad	Zona	Información adicional	Cantidad	Precio unitario
1	THREAT-INTEL-ENTERPRISE	Google Threat Intelligence Enterprise	Licencia Google Threat Intelligence Enterprise	N/A	N/A	N/A	N/A	Categoria: Google	1	$ 2.273.118.000,00
IMPUESTO TIMBRE										$ 11.422.704
VALOR TOTAL										$ 2.284.540.704,00

1.4 ASPECTO TÉCNICO

Implementar una solución integral de Ciberinteligencia y servicios especializados que permitan al ColCERT:

- ✓ Anticiparse a los ataques. La comprensión de las TTPs de los actores de amenazas relevantes para el sector Gobierno y Telecomunicaciones asegura que la defensa se enfoque donde el riesgo es real.
- ✓ Visibilidad completa del riesgo digital externo. Esto cubre la superficie de ataque expuesta de las entidades, la protección de su marca digital ante suplantaciones y los riesgos inherentes a la cadena de suministro.
- ✓ Producir información accionable a través de la publicación oportuna de alertas, advertencias e informes coyunturales y semanales. Esto permite a las entidades públicas y privadas ajustar proactivamente su postura de seguridad, recibiendo inteligencia predictiva antes de que un incidente de seguridad digital llegue a materializarse.
- ✓ Operación Especializada y Accionable con un equipo de expertos dedicados (Analistas de Ciberinteligencia) que curan la inteligencia y la transforman. Esto garantiza la generación de reportes accionables de alto valor para la toma de decisiones estratégicas.

Extracción y generación continua de Indicadores de Compromiso (IoCs) derivados de la inteligencia activa. Estos IoCs seran publicados para consulta de la ciudadanía y las entidades, fortaleciendo la defensa colectiva. Paralelamente, se mantiene un monitoreo constante de los dominios gubernamentales para identificar y rastrear las Campañas Maliciosas desplegadas por Amenazas Persistentes Avanzadas (APTs) que buscan impactar la seguridad digital en Colombia.

- **Condiciones técnicas de la solución Cloud**

Con base en lo enunciado en el contexto, se requiere adquirir la suscripción y servicios asociados a la plataforma Google Threat Intelligence - Edición Enterprise. Esta solución debe ser nativa de nube (SaaS) y contemplar los siguientes módulos y capacidades:

- ✓ Inteligencia de Amenazas Unificada: Herramienta que consolide inteligencia de primera línea (tipo Mandiant), inteligencia de comunidad global (tipo VirusTotal) y telemetría de infraestructura de nube (Google). Debe permitir la investigación ilimitada de Indicadores de Compromiso (IoCs) y ofrecer perfiles detallados de actores de amenaza.
- ✓ Gestión de Superficie de Ataque (Attack Surface Management - ASM): Módulo para el descubrimiento y monitoreo continuo de activos externos expuestos a internet, identificando vulnerabilidades, "Shadow IT" y malas configuraciones antes que los atacantes.
- ✓ Monitoreo de Amenazas Digitales (Digital Threat Monitoring - DTM): Capacidad para monitorear la web superficial, profunda y oscura (Deep/Dark Web) en busca de suplantaciones de marca, fugas de credenciales y menciones maliciosas contra la entidad.
- ✓ Análisis con Inteligencia Artificial: Incorporación de modelos de IA Generativa (como Gemini) para resumir amenazas complejas, realizar búsquedas en lenguaje natural y automatizar el análisis de código malicioso.
- ✓ Investigación y Sandbox Privado: Capacidad de detonar y analizar archivos y URLs sospechosos en un entorno seguro y privado, sin compartir la información con la comunidad pública.

El Equipo, ha verificado los Acuerdos Marco de Precios vigentes en el portal Colombia Compra Eficiente, evidenciando que el insumo pretendido se encuentra en el Instrumento de Agregación de Demanda (IAD/SDA) de Software por Catálogo II No. CCE-SNGIAD-002-2024, específicamente el servicio de Ciberinteligencia Proactiva utilizando Google Threat Intelligence Enterprise.

Esta plataforma despliega una vigilancia 24/7 automatizada sobre el panorama global de amenazas, elementofundamental para la generación de inteligencia proactiva de alto valor. Esta información será utilizada por el servicio de análisis situacional y publicada para que las entidades ajusten inmediatamente su postura de seguridad, reduciendo el riesgo de ser víctimas de actores de amenaza avanzados.

Criterios sugeridos para la definición del alcance y características técnicas de la necesidad.

Requisitos de negocio (Entidad)

El ColCERT busca adoptar un enfoque de "Dominancia de Inteligencia". La plataforma tecnológica debe permitir no sólo consumir datos, sino entender el contexto del adversario.

Funcionalidades Técnicas Requeridas:

- ✓ Threat Landscape & Graph: Acceso a perfiles de amenazas, campañas activas y visualización gráfica de relaciones entre indicadores.
- ✓ Inteligencia de Vulnerabilidades: Priorización de vulnerabilidades basada en riesgo real de explotación (EPSS) y no solo en severidad teórica (CVSS).
- ✓ Reglas YARA y Hunting: Capacidad para crear y gestionar reglas YARA para búsqueda proactiva de amenazas en repositorios globales de malware (Livehunt y Retrohunt).
- ✓ API y APIficación: La solución debe contar con una API robusta (mínimo 30,000 solicitudes/día) para integrarse con sistemas SIEM (ej. Google SecOps, Splunk), SOAR y EDR, facilitando la interoperabilidad y automatización.

Infraestructura

La arquitectura de la solución es 100% SaaS, eliminando la necesidad de hardware local.

A. Servicios de Implementación y Puesta en Marcha:

- Configuración inicial del *tenant* de Google Threat Intelligence.
- Definición de activos críticos para el módulo de ASM.
- Configuración de palabras clave y dominios para el monitoreo de marca (DTM).

Transferencia de Conocimiento:

El proponente debe realizar transferencia de conocimiento al equipo técnico del ColCERT, con el propósito de identificar las funcionalidades del licenciamiento.

Así mismo el proponente deberá garantizar el acceso a los informes técnicos especializados (ej. Mandiant) y a la información técnica especializa de la Google Threat Intelligence Enterprise Edition

Soporte Técnico:

Se requiere soporte técnico directo del fabricante y del partner implementador durante la vigencia de la suscripción.

Adicionalmente, la presente contratación se encuentra clasificada de acuerdo con el Catálogo de Bienes y Servicios de Naciones Unidas – UNSPSC, conforme a la siguiente codificación:

Clasificación UNSPSC	Segmento		Familia		Clase	
80101500	80	Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	10	Servicios de asesoría de gestión	15	Servicios de consultoría de negocios y administración corporativa
80111600	80	Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	11	Servicios de recursos humanos	16	Servicios de personal temporal
81111500	81	Servicios Basados en Ingeniería, Investigación y Tecnología	11	Servicios informáticos	15	Ingeniería de software o hardware
81111600	81	Servicios Basados en Ingeniería, Investigación y Tecnología	11	Servicios informáticos	16	Programadores de computador
81111700	81	Servicios Basados en Ingeniería, Investigación y Tecnología	11	Servicios informáticos	17	Sistemas de manejo de información MIS
81111800	81	Servicios Basados en Ingeniería, Investigación y Tecnología	11	Servicios informáticos	18	Servicios de sistemas y administración de componentes de sistemas
81112000	81	Servicios Basados en Ingeniería, Investigación y Tecnología	11	Servicios informáticos	20	Servicios de datos

81112100	81	Servicios Basados en Ingeniería, Investigación y Tecnología	11	Servicios informáticos	21	Servicios de internet

Esta codificación garantiza la correcta identificación del objeto contractual en el Sistema Electrónico para la Contratación Pública (SECOP II) y asegura la trazabilidad y compatibilidad con los mecanismos de adquisición definidos en el Instrumento de Agregación de Demanda (IAD/SDA) de Software por Catálogo II No. CCE-SNG-IAD-002-2024.

En conclusión, desde el punto de vista técnico, la solución propuesta satisface los requerimientos técnicos de disponibilidad, seguridad y alineación con los lineamientos del Ministerio TIC, asegurando la continuidad de los servicios institucionales en la nube y el cumplimiento de los estándares tecnológicos y de gobierno digital vigentes.

1.5 **ASPECTO LEGAL**

El artículo segundo del Decreto Ley 4170 de 2011 *"Por el cual se crea la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, se determinan sus objetivos y estructura", establece como objetivo de la Agencia Nacional de Contratación Pública lo siguiente: "La Agencia Nacional de Contratación Pública – Colombia Compra Eficiente–, como ente rector, tiene como objetivo desarrollar e impulsar políticas públicas y herramientas, orientadas a la organización y articulación, de los partícipes en los procesos de compras y contratación pública con el fin de lograr una mayor eficiencia, transparencia y optimización de los recursos del Estado".*

Así mismo, el artículo 3, numeral 7 ibidem señala como una de sus funciones la de *"Diseñar, organizar y celebrar los acuerdos marco de precios y demás mecanismos de agregación de demanda de que trata el artículo 2° de la Ley 1150 de 2007, de acuerdo con los procedimientos que se establezcan para el efecto.".*

Por su parte, la Ley 1150 de 2007, Título I, Artículo 2 establece como modalidades de selección para la escogencia de contratistas, las siguientes:

"ARTÍCULO 2o. DE LAS MODALIDADES DE SELECCIÓN. La escogencia del contratista se efectuará con arreglo a las modalidades de selección de licitación pública, selección abreviada, concurso de méritos y contratación directa, con base en las siguientes reglas:

"(…)

2.Selección abreviada. La Selección abreviada corresponde a la modalidad de selección objetiva prevista para aquellos casos en que, por las características del objeto a contratar, las circunstancias

de la contratación o la cuantía o destinación del bien, obra o servicio puedan adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual.

El Gobierno Nacional reglamentará la materia. Serán causales de selección abreviada las siguientes:

a) La adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades, que corresponden a aquellos que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos.
Para la adquisición de estos bienes y servicios las entidades deberán, siempre que el reglamento así lo señale, hacer uso de procedimientos de subasta inversa o de instrumentos de compra por catálogo derivados de la celebración de acuerdos marco de precios o de procedimientos de adquisición en bolsas de productos;

(…)"

El Artículo 1° del Decreto 310 de 2021. establece:

"Artículo 1: Las Entidades Estatales sometidas al Estatuto General de Contratación de la Administración Pública, están obligadas a adquirir Bienes y Servicios de Características Técnicas Uniformes de Común Utilización a través de los Acuerdos Marco de Precios previamente justificados, diseñados, organizados y celebrados por la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente-. (…).

(…).

En virtud de lo anterior, la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente busca ofrecer a las Entidades del Estado un Acuerdo Marco de Precios que permita contratar servicios de forma fácil y ágil, permitiendo generar información sobre el costo de estos y evitando costos de intermediación.

En cumplimiento de lo anterior, El ColCERT requiere Adquisición de Software por Catálogo II mediante un servicio de Ciberinteligencia Proactiva utilizando Google Threat Intelligence Enterprise, para el despliegue y continuidad de la línea de Análisis Situacional del portafolio de servicios del Equipo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERTde conformidad con las condiciones exigidas en el RFI por el ColCERT teniendo en cuenta la vigencia del Instrumento de Agregación de Demanda No. CCE-SNG-IAD-002-2024, (proceso CCENEG-075-02-2024) cuyo objeto es "(i) Seleccionar los Proveedores de Software. (ii) Definir las condiciones de contratación de Software por parte de las entidades estatales que contraten bajo el amparo del mecanismo de agregación de demanda.

Los proveedores se obligan a proporcionar a nivel nacional los productos de software y los servicios complementarios que las entidades compradoras requieren para su funcionamiento y misionalidad, bajo las condiciones técnicas definidas en los documentos del proceso. .

4. ANÁLISIS DE LA DEMANDA Y DE LA OFERTA
4.1. ANALISIS DE LA DEMANDA
4.1.1. Contrataciones Previas de la Entidad

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), a través del Fondo Único de Tecnologías de la Información y las Comunicaciones (FUTIC), ha adelantado desde la vigencia 2019 diferentes procesos de adquisición de licencias Google Workspace mediante el Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024, administrado por Colombia Compra Eficiente.

Estas contrataciones han permitido optimizar el gasto público, consolidar las compras de software bajo un único mecanismo regulado y garantizar la continuidad del servicio de correo institucional y herramientas colaborativas en la nube, dentro del marco del programa Mi Colombia Digital.

A continuación, se presenta el resumen de las contrataciones previas relacionadas con la adquisición de licencias Google:

Año del proceso	Número de Orden de Compra	Cantidad de licencias	Valor unitario COP $	Valor Simuladores (Licencias Enterprise)	Valores Contratados (Licencias Enterprise)	Valor diferencia	Diferencia Porcentual (%)
2019	43756 de 2019	30653	$171.697,00	**$5.263.028.141,00**	**$2.412.380.515,57**	$ 2.850.647.625,43	**54,16%**
2020	61867 de 2020	30000	$262.076,40	**$7.862.292.000,00**	**$2.553.210.000,00**	$ 5.309.082.000,00	**67,53%**
2021	83120 de 2021	36100	$279.974,16	**$10.107.067.176,00**	**$3.388.252.862,00**	$ 6.718.814.314,00	**66,48%**

2022	102778 de 2022	36100	$461.382,72	**$16.655.916.192,00**	**$4.931.816.662,00**	$ 11.724.099.530,00	**70,39%**
2023	113508 de 2023	36100	$402.362,88	**$14.525.299.968,00**	**$5.076.011.253,00**	$ 9.449.288.715,00	**65,05%**
2024	140174 de 2024	40010	$ 1,562,875 $ 520,958 $ 260,479 (según tipo de licencia)	**$ 17.728.200.750,00**	**$ 6,135,205,300,00**	$ 11,592,995,450.00	**65.39%**

De acuerdo con el análisis de la información anterior, se evidencia que entre las vigencias 2019 y 2024 el Ministerio TIC ha mantenido una demanda constante de licencias de productividad y correo institucional en la nube, con una tendencia progresiva en el número de usuarios y una reducción promedio del 65 % frente a los valores techo del mercado, gracias a la aplicación del Instrumento de Agregación de Demanda (IAD/SDA).

Estos resultados demuestran la eficiencia del modelo de contratación por catálogo, que ha permitido obtener condiciones económicas favorables, estandarizar la prestación del servicio y garantizar la sostenibilidad del ecosistema colaborativo institucional.

.

4.2 ANÁLISIS DE LA OFERTA

4.2.1 Descripción general

El valor estimado del contrato se encuentra basado en la información disponible en el Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024, administrado por Colombia Compra Eficiente, el cual consolida la oferta de productos de software de uso común para las entidades estatales.
Dentro de este instrumento se encuentran habilitados varios proveedores autorizados por Google Cloud, quienes cuentan con la experticia técnica y la certificación necesaria para la prestación del servicio de licenciamiento Google Workspace.

El análisis del valor se realizó tomando como referencia los precios publicados en la Tienda Virtual del Estado Colombiano y las simulaciones efectuadas en el catálogo electrónico, con base en las modalidades de licenciamiento Enterprise Starter, Enterprise Standard y Enterprise Plus, correspondientes a la suscripción anual por usuario.

El valor total estimado de la contratación asciende a **DOS MIL DOSCIENTOS OCHENTA Y CUATRO MILLONES QUINIENTOS CUARENTA MIL SETECIENTOS CUATRO PESOS. ($2.284.540.704) M/CTE,** incluido impuesto de timbre y todos los costos administrativos, fiscales, tasas, impuestos y estampillas nacionales y locales

Nota: Es de aclarar que de acuerdo a la clausula 9 del INTRUMENTO DE AGREGACIÓN DE DEMANDA SISTEMA DINÁMICO DE ADQUSICIÓN (IAD/SDA) DE SOFTWARE POR CATÁLOGO II No. CCE-SNG-IAD-002-2024, el simulador al calcular la cotización incorpora de manera discriminada el valor del IVA, con el fin de determinar el valor oficial de la adquisición. No obstante, se advierte que una vez revisado lo dispuesto en el numeral 20 del artículo 476 del decreto 624 de 1989, este tipo de adquisición de software son exentos del pago del impuesto de IVA

.

Distribución estimada del valor:

Item	Código del producto	Nombre	Descripción	Asistencia	Perfil	Unidad	Zona	Información adicional	Cantidad	Precio unitario
1	THREAT-INTEL-ENTERPRISE	Google Threat Intelligence Enterprise	Licencia Google Threat Intelligence Enterprise	N/A	N/A	N/A	N/A	Categoria: Google	1	$ 2.273.118.000,00
IMPUESTO TIMBRE										$ 11.422.704
VALOR TOTAL										$ 2.284.540.704,00

En conclusión, El Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic / Fondo Único de TIC contó con la licencia El Workshop de Google Threat Intelligence (GTI) Enterprise durante 2 semanas, con un total de 15 horas de capacitación, distribuidas en sesiones teórico-prácticas, para la fecha no se encuentra vigente.

Como resultado del desarrollo del Workshop de Google Threat Intelligence (GTI) Enterprise, Servinformación entregará los siguientes elementos al finalizar las sesiones, los cuales consolidan los principales resultados del entrenamiento:

- Material de capacitación utilizado durante el Workshop, incluyendo presentaciones técnicas, guías de apoyo y escenarios de laboratorio empleados en las demostraciones.
- Documentación técnica consolidada, que incluirá las configuraciones, capturas y procedimientos vistos durante las sesiones prácticas (ASM, DTM, Private Scanning e integración con SecOps).
- Diagrama de arquitectura e integración interna de GTI Enterprise, mostrando la relación con los módulos y fuentes de inteligencia de Mandiant, VirusTotal y Google Cloud Threat Intelligence.
- Guía de mejores prácticas y KPIs operativos, enfocada en la sostenibilidad y aprovechamiento del servicio dentro del entorno de MINTIC.
- Informe final del Workshop, que consolida los materiales, resultados de las sesiones, recomendaciones estratégicas y registro de asistencia de participantes.

Por lo anterior, es necesarioAdquisición de Software por Catálogo II mediante un servicio de Ciberinteligencia Proactiva utilizando Google Threat Intelligence Enterprise, para el despliegue y continuidad de la línea de Análisis Situacional del portafolio de servicios del Equipo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, en las condiciones señaladas en el IAD para la compra de software por catálogo II No. CCE-SNG-IA-002-2024, a efectos de garantizar la misionalidad del ColCERT bajo las condiciones técnicas definidas en los documentos del proceso.

Los pagos se realizarán conforme al cronograma y los términos establecidos en la Orden de Compra que se genere en la Tienda Virtual del Estado Colombiano, dentro del plazo y condiciones del IAD/SDA CCE-SNG-IAD-002-2024.

El proveedor seleccionado deberá constituir la garantía de cumplimiento en los términos del artículo 7 de la Ley 1150 de 2007 y los artículos 2.2.1.2.3.2.1.2.1. y 2.2.1.2.3.4.1. del Decreto 1082 de 2015, por un valor equivalente al diez por ciento (10%) del monto total de la orden, conforme a lo establecido en la cláusula 15.2 del IAD/SDA.

Los recursos que respaldan esta contratación provienen del rubro presupuestal del Fondo Único de Tecnologías de la Información y las Comunicaciones (FUTIC), dentro del proyecto: “Fortalecimiento de las capacidades de prevención, detección y recuperación de incidentes de seguridad digital de los ciudadanos, del sector público y del sector privado. Nacional” con código BPIN 2022011000093

De conformidad con los antecedentes contractuales de las vigencias 2019–2024, la adquisición mediante el IAD/SDA de Colombia Compra Eficiente ha demostrado ser el mecanismo más eficiente, transparente y competitivo para la obtención de licenciamiento Google Workspace, garantizando condiciones técnicas homogéneas, soporte especializado y optimización del gasto público.

4.2.2 Aplicación del modelo de abastecimiento estratégico al análisis de la oferta

Con base en el **modelo de abastecimiento estratégico**, el análisis de la oferta del mercado se desarrolla en los siguientes componentes:

- **Evaluación del mercado proveedor:** El mercado de servicios de productividad en la nube presenta una **oferta concentrada en proveedores internacionales** (Google, Microsoft, Amazon), con altos estándares de seguridad, escalabilidad, disponibilidad y cumplimiento normativo.
- **Condiciones comerciales:** Los precios y configuraciones de licencias se encuentran **estandarizados y regulados** mediante el instrumento de agregación, lo que garantiza igualdad de condiciones para todas las entidades públicas y evita asimetrías de información.
- **Riesgos del suministro:** Se identificó un **riesgo medio**, derivado de la dependencia tecnológica de un proveedor único, mitigado mediante la utilización de cláusulas contractuales de continuidad del servicio, soporte técnico y respaldo de información institucional.
- **Estrategia de abastecimiento:** Mantener la contratación mediante el **Instrumento de Agregación de Demanda** garantiza **eficiencia, transparencia y sostenibilidad**, alineándose con las **buenas prácticas del modelo de abastecimiento estratégico** y las políticas de Colombia Compra Eficiente.
- **Análisis del costo total de propiedad (TCO):** El modelo SaaS reduce los costos asociados a infraestructura, mantenimiento y soporte interno, incrementando la eficiencia y el retorno del gasto público.

4.3 Conclusión

En conclusión, El Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic / Fondo Único de TIC contó con la licencia El Workshop de Google Threat Intelligence (GTI) Enterprise tendrá una duración aproximada de 2 semanas, con un total de 15 horas de capacitación, distribuidas en sesiones teórico-prácticas, para la fecha no se encuentra vigente.

Como resultado del desarrollo del Workshop de Google Threat Intelligence (GTI) Enterprise, Servinformación entregará los siguientes elementos al finalizar las sesiones, los cuales consolidan los principales resultados del entrenamiento:

- Material de capacitación utilizado durante el Workshop, incluyendo presentaciones técnicas, guías de apoyo y escenarios de laboratorio empleados en las demostraciones.

- Documentación técnica consolidada, que incluirá las configuraciones, capturas y procedimientos vistos durante las sesiones prácticas (ASM, DTM, Private Scanning e integración con SecOps).

- Diagrama de arquitectura e integración interna de GTI Enterprise, mostrando la relación con los módulos y fuentes de inteligencia de Mandiant, VirusTotal y Google Cloud Threat Intelligence.

- Guía de mejores prácticas y KPIs operativos, enfocada en la sostenibilidad y aprovechamiento del servicio dentro del entorno de MINTIC.
- Informe final del Workshop, que consolida los materiales, resultados de las sesiones, recomendaciones estratégicas y registro de asistencia de participantes.

Por lo anterior, es necesario la Adquisición de Software por Catálogo II mediante un servicio de Ciberinteligencia Proactiva utilizando Google Threat Intelligence Enterprise, para el despliegue y continuidad de la línea de Análisis Situacional del portafolio de servicios del Equipo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, en las condiciones señaladas en el IAD para la compra de software por catálogo II No. CCE-SNG-IA-002-2024, a efectos de garantizar la misionalidad del ColCERT bajo las condiciones técnicas definidas en los documentos del proceso

(Firma Electrónicamente)
ANGELA JANETH CORTES HERNANDEZ
Coordinadora GIT ColCERT

Elaboró: Jairo Alexander Martinez Martinez – Abogado GIT ColCERT

REGISTRO DE FIRMAS ELECTRONICAS

ANALISIS DEL SECTOR GOOGLE

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

Id Acuerdo: 20251223-181009-de0943-77614937

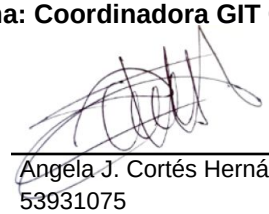
Estado: Finalizado

Creación: 2025-12-23 18:10:10

Finalización: 2025-12-23 18:11:17

Escanee el código para verificación

Firma: Coordinadora GIT ColCERT



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

Ministerio TIC

Elaboración: Aboagdo GIT ColCERT

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

REPORTE DE TRAZABILIDAD

ANALISIS DEL SECTOR GOOGLE

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

Id Acuerdo: 20251223-181009-de0943-77614937
Creación: 2025-12-23 18:10:10
Estado: Finalizado
Finalización: 2025-12-23 18:11:17

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	JAIRO ALEXANDER MARTINEZ MARTINEZ jmartinezm@mintic.gov.co	Aprobado	Env.: 2025-12-23 18:10:16 Lec.: 2025-12-23 18:10:30 Res.: 2025-12-23 18:10:35 IP Res.: 191.95.53.187 Canal: Email
Firma	Angela J. Cortés Hernández acortes@mintic.gov.co Ministerio TIC	Aprobado	Env.: 2025-12-23 18:10:35 Lec.: 2025-12-23 18:11:14 Res.: 2025-12-23 18:11:17 IP Res.: 190.145.189.98 Canal: Email