Datos del área gestora:	**Dependencia solicitante:**	Viceministerio de Transformación Digital
	Nombre del Viceministro o Jefe o Director o Subdirector de la Dependencia solicitante	Giovanni Andrés López Cabezas

1. Descripción de la necesidad que la entidad pretende satisfacer

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

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

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

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

[1] LEY 1341 DE 2009 (julio 30), "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones". DIARIO OFICIAL. AÑO CXLIV. N. 47426. 30, JULIO, 2009. PÁG. 4.

[2] LEY 1978 DE 2019 (julio 25) "Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones". Año CLV NO. 51.025, Bogotá, D. C., jueves, 25 de julio de 2019. PAG. 1

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[3], 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

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

(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%). 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.

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

Ajuste fino de reglas, dashboards y correlaciones

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

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.

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, 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.

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.

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 de 19 de diciembre de 2025 a través del Coordinador del Grupo de Presupuesto del Ministerio.

2. Descripción del objeto a contratar, con sus especificaciones y la identificación del contrato a celebrar.

2.1. Descripción del Objeto a contratar	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
Clasificación UNSPSC	La presente contratación se encuentra incluida dentro de los siguientes códigos del clasificador de bienes y servicios UNSPSC:

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

2.2. Especificaciones del contrato

2.2.1 Obligaciones generales del contratista:	1. Cumplir con lo establecido en las políticas de tratamiento de Datos personales, Seguridad y Privacidad de la información, seguridad digital y continuidad de la operación de los servicios y tratamiento de la Información de la entidad, en particular, lo estipulado en las leyes 1266 de 2008 y 1581 de 2012 respecto de la protección de datos personales. 2. Salvaguardar los activos de información del Ministerio/Fondo Único de TIC, durante toda la ejecución del contrato. 3. Suscribir el documento de compromiso de confidencialidad al momento de suscribir el acta de inicio.

	4. Cumplir con la cláusula 27 del Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024 que requieran las entidades estatales. 5. Reportar de manera oportuna a la Mesa de Servicio, o a quien haga sus veces, cualquier incidente que afecte o pueda afectar la Seguridad y Privacidad de la Información, la Seguridad Digital o la continuidad de los servicios de la Entidad. 6. Cumplir a cabalidad con lo establecido el objeto contractual, en los términos y condiciones establecidos en este documento y en su oferta, observando en todo momento la Constitución Política, las leyes colombianas y el régimen de contratación pública. Por ningún motivo podrá suspender o abandonar la ejecución del contrato sin la justificación previa y aceptación expresa de la Entidad contratante. 7. Ejercer la dirección, gestión y control de todas las actividades a su cargo de manera oportuna y dentro del plazo establecido, garantizando el cumplimiento del objeto contractual. 8. Responder, sin perjuicio de la respectiva garantía, por el cumplimiento y calidad de los servicios prestados durante el término previsto en el presente contrato. 9. Responder ante terceros por los daños que se ocasionen y que provengan de causas imputables a su actuación u omisión. 10. Salvaguardar toda la información confidencial que conozca o maneje durante la ejecución del contrato, salvo requerimiento expreso de Autoridad competente. Toda la información y/o documentos que se produzcan en desarrollo del presente contrato serán de uso exclusivo del Fondo Único de TIC, y el contratista se obliga a no divulgarlos ni utilizarlos para fines distintos a los previstos en este contrato, de conformidad con la Ley 1581 de 2012 y el Decreto reglamentario 1377 de 2013, so pena de las acciones civiles, administrativas o penales a que haya lugar. 11. Entregar al supervisor del control de ejecución del contrato, el informe de las actividades realizadas durante el mes o periodo, al igual que los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos en cada actividad encomendada cuando así se requiera, en los términos y formatos definidos por la Entidad. 12. Atender los requerimientos, observaciones y/o recomendaciones que formule el supervisor dentro de los cinco (5) días hábiles siguientes a su notificación, garantizando la correcta ejecución del contrato y cumplimiento de sus obligaciones**.** 13. Reportar, de manera inmediata al supervisor, la ocurrencia de cualquier novedad, anomalía o eventualidad que se presente durante la ejecución contractual. 14. Informar sobre peticiones o amenazas de que sea objeto por quienes actúen por fuera de la ley, con el propósito de obligarlo a hacer o a omitir algún acto o hecho, al Fondo Único de Tecnologías de la Información y las Comunicaciones a través del funcionario responsable de la supervisión y control de ejecución, y a las demás autoridades competentes para que se adopten las medidas y correctivos que fueren necesarios. 15. Presentar la factura electrónica previamente validada por la DIAN, como requisito necesario para el pago de los bienes y/o servicios contratados, conforme con las disposiciones señaladas en el Decreto 358 del

	5 de marzo de 2020, en concordancia con lo dispuesto en la Resolución No. 000042 del 5 de mayo de 2020, en los casos que aplique. 16. Cumplir con las obligaciones generales que se encuentran establecidas en la cláusula 7 del Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024, así como las que se deriven de la normativa aplicable.
2.2.2 Obligaciones para la prestación de servicios tecnológicos y aprovisionamiento de infraestructura	Teniendo en cuenta que se trata de una operación secundaria a través del Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024 únicamente se pretende adquirir licencia Google Threat Intelligence Enterprise con soporte técnico y configuración y parametrización de los productos. Las obligaciones específicas de los proveedores se encuentran establecidas en la cláusula 7 del Instrumento de Agregación, su anexo modificatorio, y en los demás documentos que forman parte del IAD. No se requiere en el presente caso la contratación y/o aprovisionamiento de infraestructura para la prestación de servicios tecnológicos adicional a la ya existente.
2.2.3 Obligaciones específicas del contratista:	Teniendo en cuenta que se trata de una operación secundaria a través del Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024, el proveedor para la ejecución de la orden de compra a generar deberá cumplir con las obligaciones específicas de los proveedores que se encuentran establecidas en la cláusula 7 del Instrumento de Agregación, su anexo modificatorio, y en los demás documentos que forman parte del IAD.
2.2.4 Obligaciones particulares del Ministerio o del Fondo Único de TIC	1. Pagar oportunamente el valor del contrato, de conformidad con lo estipulado en este mismo documento y en el Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024 2. Designar al funcionario que ejercerá la supervisión y el control de ejecución del contrato, quien estará en permanente contacto con el contratista, para la coordinación de cualquier asunto que así se requiera. 3. Suscribir, a través del supervisor del control de ejecución del contrato, los documentos y actas que sean necesarias durante el desarrollo del contrato. 4. Suministrar la información necesaria sobre los diferentes aspectos que sean requeridos para el logro de los objetivos propuestos, siempre y cuando no sea obligación del contratista suministrarla. 5. Informar de manera inmediata, acerca de cualquier circunstancia que amenace vulnerar los derechos del contratista, al igual que cualquier perturbación que afecte el desarrollo normal del contrato. 6. Guardar la confidencialidad y velar por la protección de los productos y servicios propuestos por el contratista cuando a ello hubiere lugar. 7. Cumplir con las obligaciones establecidas en la cláusula 27 del Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024.
2.2.5 Plazo de ejecución del contrato	El plazo de ejecución de la orden de compra es hasta el 31 de diciembre de 2025, contado a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución.

	Nota: Google Threat Intelligence Enterprise adquirida por el Ministerio TIC en 2025 tendrán vigencia de un (1) año contado a partir recibo a satisfacción por parte de la entidad (recibo del usuario y confirmación de acceso a la plataforma)..
2.2.6 Lugar de ejecución del contrato:	El lugar de ejecución y el domicilio contractual será la ciudad de Bogotá, D.C.
2.2.7 Valor del contrato / presupuesto oficial:	El valor estimado para la adquisición de Google Threat Intelligence Enterprise asciende a la suma **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. Este valor incluye IVA SI ☐ NO ☐ No es sujeto de IVA: **X** **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.
2.2.8 Forma de pago y requisitos:	De conformidad con la cláusula 11 del Instrumento de Agregación de Demanda (IAD/SDA) una adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024, se pueden dar en dos escenarios: A. Cuando la orden de compra solo incluye productos de software que no se enmarcan ni requieren ningún servicio. Se entenderá efectivamente entregado (i) cuando se perfeccionen los requisitos legales de la orden de compra y (ii) posteriormente sean suministradas de manera inmediata las licencias, claves o cuentas, el aprovisionamiento en plataforma o cualquier requerimiento adicional para que la entidad compradora pueda instalar, acceder y hacer uso del software. B. Cuando la orden de compra incluye productos de software que se enmarcan o requieren servicios. Un servicio es efectivamente prestado cuando el Proveedor lo pone a disposición de la Entidad Compradora en las condiciones técnicas establecidas en los anexos, aun si la Entidad Compradora no usa el servicio. El Proveedor puede facturar el Software por catálogo adquirido de la siguiente manera: i) Periódicamente o, ii) De contado, dependiendo de las condiciones del producto adquirido en los términos señalados en el Catálogo. Para las dos formas de pago descritas, el Proveedor deberá facturar los productos adquiridos de conformidad con el consumo prestado o las obligaciones monetarias adquiridas en el período. El Proveedor, de acuerdo con las disposiciones tributarias, deberá realizar el manejo de las facturas electrónicas según la Resolución 042 de 2020 y la regulación aplicable, o aquellas que las modifiquen, adicionen o sustituyan. El Proveedor debe presentar a la Entidad Compradora para el pago:

	i. Factura debidamente diligenciada, conforme con los requisitos establecidos en el Estatuto Tributario. ii. De conformidad con la Ley 1231 de 2008, las partes (Entidad Compradora y Proveedor) acuerdan que el Proveedor indicará en sus facturas que la Entidad Compradora deberá pagar las sumas pactadas dentro de los **TREINTA (30) DÍAS CALENDARIO** siguientes a la aceptación de la factura la cual debe estar debidamente elaborada, documentada (se refiere a todos los soportes exigidos por la Entidad Compradora para el trámite). Al ser un trámite realizado entre la Entidad Compradora y el Proveedor, Colombia Compra Eficiente no será parte en este aspecto. iii. Certificado suscrito por el representante legal o el revisor fiscal en el cual manifieste que el Proveedor está a paz y salvo con sus obligaciones laborales frente al Sistema de Seguridad Social Integral y demás aportes de conformidad con el artículo 50 de la Ley 789 de 2002 o aquellas que la modifiquen. iv. Soporte del pago del Impuesto de Timbre, conforme a lo dispuesto en la Circular Externa No. 010 del 5 de marzo de 2025, expedida por el Ministerio de Hacienda y Crédito Público y en cumplimiento de lo previsto en el artículo 519 del Estatuto Tributario Nacional. v. Los demás documentos requeridos por la Entidad Compradora que hagan parte de su Sistema de Gestión de Calidad o de Control Interno para el procedimiento de pagos a terceros. El Proveedor debe publicar una copia de la factura en la Tienda Virtual del Estado Colombiano dentro de los ocho (8) días hábiles siguientes a la fecha de su presentación. En caso de que la Entidad Compradora solicite entregas parciales, deberá acordarlo con el proveedor y definir los pagos parciales y proporcionales a que haya lugar. El Proveedor deberá presentar con cada entrega la factura correspondiente. Las Entidades Compradoras deben aprobar o rechazar la factura dentro de los **tres (3) días hábiles** siguientes a su presentación. Una vez aprobadas, las Entidades Compradoras deben pagar las facturas dentro de los **treinta (30) días calendario** siguientes. Si al realizar la verificación completa de una factura se establece que esta no cumple con la totalidad de los requisitos, la Entidad Compradora solicitará las correcciones al Proveedor dentro de los **tres (3) días hábiles** siguientes al rechazo; el término de **treinta (30) días calendario** empezará a contar a partir de la aprobación de la nueva factura. La Entidad Compradora deberá entregar el Comprobante de Pago, incluyendo detalle de descuentos y retenciones realizados al Proveedor y publicarlo en la Tienda Virtual del Estado Colombiano en un plazo no mayor a **ocho (8) días hábiles** siguientes al pago efectivo. En el evento en que la Entidad Compradora aplique ANS los mismos deben estar incluidos en la factura presentada por el proveedor para el mes en que se afectó el ANS.

En el escenario en el cual, por alguna razón, la Entidad Compradora y el Proveedor acuerden la terminación anticipada de la Orden de Compra, la Entidad Compradora realizará el pago de los productos y servicios a las mismas efectivamente entregados o prestados.

El plan de pagos proyectado es el siguiente:

Concepto de pago	Fecha estimada de pago	Valor a pagar (hasta)
Un único pago por el 100% del valor de la orden de compra.	30 de diciembre de 2025	**$2.284.540.704**
Total, Hasta		**$2.284.540.704**

El pago se autorizará una vez se reciba la confirmación de activación de las licencias a nombre del MinTIC / FUTIC

Nota 1: 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..

Nota 2: El valor a pagar corresponderá con el valor de la oferta adjudicataria.

La suma de **SEISCIENTOS CINCUENTA Y UN MILLONES CUATROCIENTOS TREINTA Y CINCO MIL PESOS MCTE ($ 651.435.000)** son recursos propios.

La suma de **MIL SEISCIENTOS TREINTA Y TRES MILLONES CIENTO CINCO MIL SETECIENTOS CUATRO PESOS MCTE ($1.633.105.704)** son recursos nación.

La fuente de los recursos que soportan la presente contratación corresponde a Recursos Nación y Recursos Propios del Fondo Único de TIC y se derivan del proyecto denominado: "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.

El pago se hará con cargo al presupuesto asignado para la presente vigencia fiscal de conformidad con el Certificado de Disponibilidad Presupuestal No. 326925 del 19/12/2025expedido por la Coordinadora del Grupo Interno de Trabajo de Presupuesto.

El Fondo Único TIC realizará los pagos, previa disponibilidad del PAC y liquidez de la Tesorería

Nota: Se anexa CDP No. 326925 del 19/12/2025

2.2.9 Justificación del anticipo.	No aplica
2.2.10 Supervisión.	La supervisión de la ejecución de este contrato será ejercida por la Coordinado GIT ColCERT o quien haga sus veces, o quien designe la/el ordenador(a) del gasto, quien tendrá a su cargo la correcta ejecución técnica, jurídica y financiera del contrato. Para cumplir con su labor de verificación, la supervisión ejercerá funciones de inspección, vigilancia y control sobre todos los documentos y actuaciones que realicen los funcionarios de las entidades participantes en el contrato y que tengan relación alguna con la ejecución de este. En ningún caso el supervisor goza de la facultad de modificar el contenido y alcance del contrato suscrito entre el contratista y el Fondo Único de TIC, ni de eximir, a ninguno de ellos, de sus obligaciones y responsabilidades. Las atribuciones, responsabilidades y obligaciones serán las establecidas en el manual de supervisión e interventoría vigente del Ministerio de Tecnologías de Información y las Comunicaciones, así como las dispuestas en los artículos 82 y 83 de la Ley 1474 de 2011 y el Manual de Contratación de la entidad.
2.2.11 Otras especificaciones	Se incluye todas las especificaciones contenidas en el Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024, como también las siguientes: **-SOLUCIÓN DE CONTROVERSIAS**: Las partes disponen que, en caso de presentarse controversias contractuales, estas serán resueltas de mutuo acuerdo, sin perjuicio de poder acudir a las instancias y procedimientos contemplados en las normas vigente. **-LIQUIDACIÓN**: De conformidad con lo establecido en el artículo 60 de la Ley 80 de 1993, tratándose de un contrato de ejecución instantánea que se lleva a cabo mediante la colocación de una orden de compra por la existencia de un Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo, el presente contrato no será objeto de liquidación. **-CLÁUSULAS EXORBITANTES:** 1. **MODIFICACIÓN, TERMINACIÓN E INTERPRETACIÓN UNILATERALES.** - El presente contrato podrá ser terminado, modificado e interpretado unilateralmente por el **FONDO ÚNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES** con sujeción a lo previsto en los artículos 15, 16 y 17 de la Ley 80 de 1993. 2. **CADUCIDAD.** - **EL FONDO ÚNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES** o el MINTIC podrá declarar la caducidad administrativa de este contrato mediante resolución motivada, a través de la cual lo dará por terminado y ordenará su liquidación en el estado en que se encuentre, de conformidad con lo contemplado en el artículo 18 de la Ley 80 de 1993.

	-CONFIDENCIALIDAD: El CONTRATISTA deberá salvaguardar la información confidencial que obtenga o conozca en el desarrollo de sus actividades salvo requerimiento expreso de autoridad competente. Toda la información y/o documentos que se produzcan en desarrollo del presente contrato serán de uso exclusivo del Fondo Único de TIC, obligándose desde ya el contratista a no utilizarlos para fines distintos a los previstos en este contrato, ni a divulgar la información que se le suministre ni los resultados de su trabajo conservando la confidencialidad de estos, de conformidad con la Ley, so pena de las acciones civiles, administrativas o penales a que haya lugar. Por lo anterior, deberá suscribir el documento de compromiso de confidencialidad, al momento de suscribir el acta de inicio.
2.3. Tipo del contrato a celebrar	Compraventa

3. Fundamentos jurídicos de la modalidad de selección

De conformidad con lo establecido en el Decreto 4170 de 2011, *"Por el cual se crea la Agencia Nacional de Contratación Pública —Colombia Compra Eficiente—,* se determinan sus objetivos y estructura*",* es el ente rector, que 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*.", y como una de sus funciones, a la luz de lo preceptuado en el artículo 3 numeral 7, es la de "*Diseñar, organizar y celebrar los acuerdos marco de precios y demás mecanismos de agregación de demanda de que trata el artículo 20 de la Ley 1150 de 2007, de acuerdo con los procedimientos que se establezcan para el efecto*", en consecuencia, comprar a través de los instrumentos generados por Colombia compra Eficiente se entiende como una buena práctica de compras públicas.

El artículo 2.2.1.2.1.2.7 del Decreto 1082 de 2015, modificado por el artículo 1 del Decreto 310 de 2021 *"Por el cual se reglamenta el artículo 41 de la Ley 1955 de 2019, sobre las condiciones para implementar la obligatoriedad y aplicación de los Acuerdos Marco de Precios y se modifican los artículos 2.2.1.2.1.2.7. Y 2.2.1.2.1.2.12 del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional"* "Por el cual se reglamenta el sistema de compras y contratación pública" determina la *"Procedencia del Acuerdo Marco de Precios", y establece que: "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-. La implementación de nuevos Acuerdos Marco de Precios organizados y celebrados por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente de uso obligatorio por parte de las entidades territoriales, estará precedida de un estudio de agregación de demanda que realizará aquella, el cual tenga en cuenta las particularidades propias de los mercados regionales, la necesidad de promover el desarrollo empresarial en las entidades territoriales a través de las MYPIMES y evitar en lo posible, la concentración de proveedores en ciertas ciudades del país, salvo que exista la respectiva justificación técnica, económica.* (…)".

En efecto, la norma del Decreto 310 de 2021 "*Por el cual se reglamenta el artículo 41 de la Ley 1955 de 2019, sobre las condiciones para implementar la obligatoriedad y aplicación de los Acuerdos Marco de Precios y se modifican los artículos 2.2.1.2.1.2.7. Y 2.2.1.2.1.2.12 del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional*" antes referida, señala lo siguiente:

" *a. Para el año 2021 deberán ingresar a la Tienda Virtual del Estado Colombiano - TVEC: i) Las entidades del sector central y del sector descentralizado de la Rama Ejecutiva del orden nacional, que a la fecha de expedición del presente Decreto aún no hayan*

ingresado; ii) la Rama Judicial; iii) la Rama Legislativa; iv) las entidades del sector central y descentralizado del nivel departamental; v) las entidades del sector central y descentralizando de los municipios (o distritos) que sean capitales de departamento; vi) las entidades del sector central y del sector descentralizado del Distrito Capital; vii) los órganos de control nacionales, departamentales y de ciudades capitales de departamento; viii) la Organización Electoral; ix) los órganos autónomos e independientes de creación constitucional que estén sometidos al Estatuto General de Contratación de la Administración Pública; x) las Corporaciones Autónomas de que trata la Ley 99 de 1993 y el Artículo 331 de la Constitución Política de Colombia; xi) las entidades del sector central y descentralizado de los municipios de categoría 1, 2 y 3; y xii) las Áreas Metropolitanas, las Asociaciones de Municipios y las Regiones Administrativas Especiales de que trata la ley 1454 de 2011."

De igual forma, conforme lo señala el artículo 8 del Decreto 142 de 2023, *"Las entidades estatales sometidas al Estatuto General de Contratación de la administración pública están obligadas a adquirir Bienes y Servicios Uniformes y No 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"-.*

Asimismo, la Ley 1150 de 2007 en su artículo 2 determinó que las modalidades de selección de contratistas serían la licitación pública, la selección abreviada, el concurso de méritos, la contratación directa y la mínima cuantía. Según lo establecido en el artículo 2, numeral 2 de la Ley 1150 de 2007, serán causales de selección abreviada: 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.

La Agencia Nacional de Contratación Pública – Colombia Compra Eficiente – creada mediante Decreto 4170 de 2011, 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"*. Y como una de sus funciones señala el artículo 3°, numeral 7. *"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*".

Verificado el sistema de compras públicas de Colombia Compra Eficiente, se encuentra que existe el Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024, 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"* el cual se encuentra vigente desde el 22/11/2024 hasta el 21/11/2027 y puede ser consultado en el siguiente enlace: https://www.colombiacompra.gov.co/archivos/portfolio-item/iad-sda-de-software-por-catalogo-ii

En conclusión, la amplia diferencia entre el valor calculado por los simuladores de Colombia Compra Eficiente y el presupuesto proyectado para la contratación se debe a que dichos simuladores utilizan precios de referencia estándar, sin contemplar los descuentos que por volumen otorgan los proveedores ni las condiciones preferenciales asociadas al instrumento de agregación de demanda. En contraste, el proceso contractual ejecutado bajo el instrumento incorpora economías de escala y una optimización del gasto público, lo que permite acceder a precios significativamente menores que los proyectados inicialmente. Esta situación

se puede observar claramente en las órdenes de compra efectuadas por el Ministerio en vigencias anteriores, donde los descuentos aplicados por los proveedores al momento de cotizar permiten el ahorro significativo de recursos públicos al Estado.

4. Análisis que soporta el valor estimado del contrato
Anexo obligatorio
(si hay estudio de mercado)
Número de Folios:

El valor se estima de conformidad al simulador

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

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..

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.

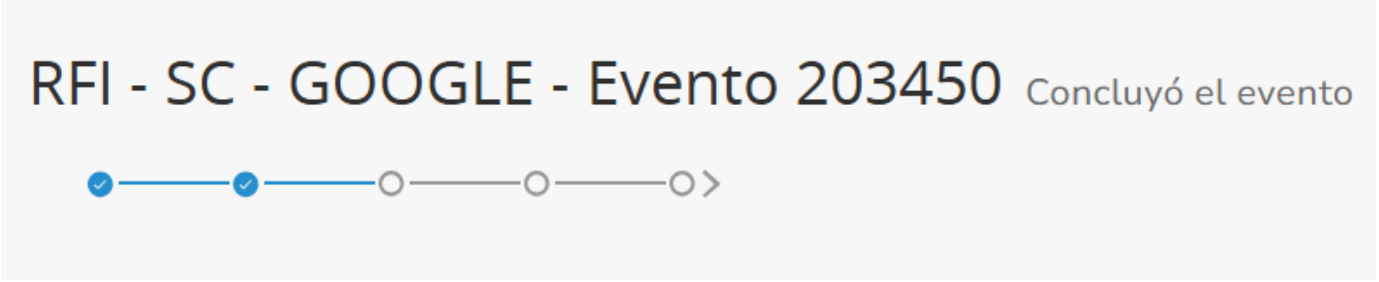
- Guía de mejores prácticas y KPIs operativos, enfocada en la sostenibilidad y aprovechamiento del servicio dentro del entorno de MINTIC.

- Informe final del Workshop, que consolida los materiales, resultados de las sesiones, recomendaciones estratégicas y registro de asistencia de participantes.

Por lo anterior, es 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.

De acuerdo con lo anterior, la entidad descargó el simulador de productos Google para estructurar la compra, disponible en el minisitio del IAD para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024, a través del enlace https://operaciones.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/iadsda-de-software-por-catalogo-ii , el cual le permite a las Entidades Compradoras estructurar y recrear el escenario del valor aproximado de la orden de compra, teniendo en cuenta para ello el precio techo del proveedor que cotizó el menor valor de los productos a adquirir por la entidad, siendo este formato el que se utiliza para solicitar las cotizaciones a los proveedores que hacen parte del Acuerdo Marco de Precios.

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 a publicar en la Tienda Virtual del Estado Colombiano (TVEC), el 27 de noviembre de 2025 la consulta de información (RFI) asociada al evento no. 203450 y en 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.

Según la información publicada por el Banco de la República de Colombia en su portal (estadisticas-economicas), se toma la TRM oficial publicada por el Banco de la República para el 15 de diciembre de 2025 (3.788,53 COP/USD), por ser la tasa certificada y vigente según la Superintendencia Financiera de Colombia, y la única reconocida legalmente para efectos contables y financieros. No se utiliza el promedio ni el valor máximo del periodo, ya que estos solo reflejan tendencias y no corresponden a una tasa oficial.

La cláusula 9 del IAD de Software por Catálogo II indica de forma precisa, la TRM a utilizar, así: *"Para solicitudes de Cotización realizadas entre el primero (1) y el quince (15) de cada mes la TRM es la del cierre del último día del mes anterior; y (ii) para solicitudes de Cotización realizadas entre el 16 y el último día de cada mes la TRM es la del cierre del 15 del mismo mes".*

Se anexa tabla con el listado de los valores de la TRM para el periodo citado, tomados de la fuente Banco de la República Archivo: TRM_30112025.xlsx

Conforme con la necesidad a satisfacer y en aplicación de la Tasa Representativa del Mercado (TRM) vigente para el 15 de diciembre de 2025, se realizó el cálculo del valor unitario en pesos colombianos, obteniéndose como valor estimado de la compra, la suma de **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, según se detalla en el siguiente cuadro.

Valor TRM: $ 3.788, 53

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

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..

A continuación, y teniendo en cuenta que el MinTIC, ha contratado y ejecutado de manera satisfactoria varios procesos para el suministro de servicios de licenciamiento equivalentes a los requeridos en el proceso actual para Licencia Google Threat Intelligence Enterprise. El siguiente análisis, evidencia que los resultados de los simuladores de procesos anteriores son significativamente superiores a los valores contratados históricamente, obteniendo los siguientes resultados:

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 (%)
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%**

Estas diferencias evidencian los beneficios derivados del Instrumento de Agregación de Demanda (IAD), particularmente en términos de economías de escala, ya que la brecha entre el valor simulado y el contratado alcanza en algunos casos más de once mil setecientos millones de pesos, lo que representa ahorros superiores al 66,94% frente al valor simulado por cada vigencia.
El comportamiento analizado también permite evidenciar el impacto positivo y el alcance estratégico del instrumento para las entidades territoriales beneficiarias, que de realizar procesos de adquisición de manera individual habrían incurrido en costos considerablemente mayores y en un número elevado de trámites contractuales.

Los porcentajes de diferencia observados en la tabla responden tanto a las condiciones macroeconómicas de cada vigencia como al comportamiento del mercado en función del volumen y nivel de licenciamiento contratado. Estos resultados evidencian la eficiencia y conveniencia del modelo de contratación consolidada, así como el impacto estratégico y beneficioso del proceso adelantado en el marco de la iniciativa Mi Colombia Digital, liderada por el MinTIC a través de la Dirección de Gobierno Digital.

A continuación, los enlaces públicos a los procesos correspondientes y referidos en la tabla anterior:

Año del proceso	Número de Orden de Compra	URL
2022	102778 de 2022	https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/ordenes-compra/102778
2023	113508 de 2023	https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/ordenes-compra/113508
2024	140174 de 2024	https://operaciones.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/ordenes-compra/140174

5. Selección objetiva: Artículo 5 Ley 1150 de 2007

5.1. Requisitos mínimos habilitantes

Capacidad Jurídica	**VERIFICACIÓN DE INHABILIDADES, MULTAS, SANCIONES E INCOMPATIBILIDADES DEL PROVEEDOR**

	La entidad compradora es responsable de realizar la verificación de las inhabilidades, multas, sanciones e incompatibilidades en que pueda estar en curso el proveedor que presento la cotización más económica antes del momento de la adjudicación de la Orden de Compra, para lo cual es conveniente revisar la información consignada en el aplicativo RUES, sin que ello sea la única fuente de verificación. En ese sentido, en caso tal de identificar que el proveedor se encuentra incurso en alguna de las causales de inhabilidad o incompatibilidad previstas en la legislación vigente, deberá informarlo de inmediato a la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente para el trámite respectivo y tomar las acciones que considere necesarias por la entidad compradora.
Capacidad Financiera	NO APLICA
Capacidad Organizacional	NO APLICA
Capacidad residual de contratación	NO APLICA
Experiencia mínima requerida del proponente	NO APLICA
Experiencia mínima del personal requerido para la contratación	NO APLICA
Requisitos mínimos técnicos (características mínimas técnicas de los bienes o servicios a contratar con las que deben contar los proponentes para participar en el proceso)	NO APLICA

5.2. Justificación de los factores de selección que permiten identificar la oferta más favorable:

La entidad seleccionará al proveedor que ofrezca las condiciones más favorables para la entidad, en virtud de lo establecido en la Cláusula 6 del Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024, y en particular lo previsto el numeral 6.5.3 para lo cual, la Entidad deberá seleccionar al Proveedor que cotiza con el menor precio para el Software que se pretende adquirir, siempre que su cotización cumpla con las cantidades y condiciones solicitadas en el formato de solicitud de cotización.

El Fondo Único de TIC como entidad compradora y para la selección del proveedor en la operación secundaria, desarrollará cada una de las actividades y/o obligaciones establecidas el Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024.

5.3. Criterios de desempate:

En caso de presentarse un empate entre dos (2) o más ofertas, la Entidad dará aplicación a las reglas previstas en el artículo 35 de la Ley 2069 de 2020 en concordancia con lo establecido en el Decreto 1860 de 2021 y conforme con los criterios para su acreditación previstos el Anexo a la Guía de Compra del Acuerdo Marco de Precios o Instrumento de Agregación de Demanda relacionado con los Criterios de Desempate en la Operación Secundaria, disponible a través del enlace: https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/instrumento-de-agregacion-de-demanda-iadsda-de

6. Análisis de Riesgo y forma de Mitigarlo

Los riesgos previsibles identificados para el proceso de contratación del Instrumento de Agregación de Demanda (IAD/SDA) para la adquisición de software por catálogo II No. CCE-SNG-IAD-002-2024, que pueden afectar la ejecución del contrato y el plan de tratamiento a estos riesgos se encuentran identificados en el documento "*Estudios y Documentos Previos de la Invitación Pública*

para seleccionar los Proveedores del IAD/SDA de Software por Catálogo II – CCENEG-075-02-2024 en el capítulo 9. Riesgos asociados al sistema dinámico, forma de mitigarlos y asignación de riesgos y 10. Garantías" Ver el documento en el siguiente enlace:
https://community.secop.gov.co/Public/Tendering/OpportunityDetail/IndexnoticeUID=CO1.NTC.6329069&isFromPublicArea=True&isModal=False

Se adjunta matriz: SI

7. Análisis que sustenta la exigencia de garantías destinadas a amparar los perjuicios de naturaleza contractual o extracontractual, derivados del incumplimiento del ofrecimiento o del contrato según el caso.

De conformidad con lo establecido en el numeral 15.2 de la minuta del Instrumento de Agregación de demanda, el proveedor que resulte adjudicatario del presente proceso de selección debe constituir una garantía de cumplimiento a favor de Ministerio TIC y el Fondo Único de TIC (con sus respectivos NIT), que cumpla con las siguientes condiciones:

Los Proveedores deben constituir una garantía de cumplimiento dentro de los **TRES (3) DÍAS HÁBILES** siguientes a la colocación de la Orden de Compra a favor de la Entidad Compradora, por el valor, amparos y vigencia establecidos en la siguiente tabla:

AMPARO	SUFICIENCIA	VIGENCIA
Cumplimiento del contrato	10% del Valor de la Orden de Compra	Duración de la Orden de Compra y seis (6) meses más.
Calidad y correcto funcionamiento de los bienes	10% del Valor de la Orden de Compra	Duración de la Orden de Compra y seis (6) meses más.
Calidad del servicio	10% del Valor de la Orden de Compra	Duración de la Orden de Compra y seis (6) meses más.

El amparo de calidad del servicio deberá solicitarse por parte de la Entidad Compradora cuando la orden de compra cuente con servicios.

El valor de los amparos de la garantía de cumplimiento es calculado de acuerdo con el valor de la Orden de Compra.
La vigencia de la garantía y sus amparos debe iniciar desde la colocación de la Orden de Compra.

Los Proveedores deberán ampliar la garantía dentro de los tres (3) días hábiles siguientes a la fecha en la que la Orden de Compra sea modificada, adicionada y/o prorrogada. En todo caso, las garantías deberán cumplir con la vigencia establecida por el Acuerdo Marco.

En caso de declaratoria de incumplimiento que afecte la garantía de cumplimiento, el Proveedor deberá ajustar la suficiencia de la garantía, en los amparos respectivos, de forma tal que cumpla con lo señalado en la tabla de esta sección después de haber sido afectada.

Colombia Compra Eficiente puede suspender del Catálogo de la Tienda Virtual del Estado Colombiano a los Proveedores que no hayan ajustado la cuantía y/o la vigencia de las garantías dentro de los plazos señalados en esta cláusula, mientras tal ajuste se dé y esté aprobado en debida forma, en caso tal que así lo considere pertinente.				
8. Indicar si la contratación esta cobijada por un Acuerdo Internacional o un tratado de Libre comercio vigente para el Estado Colombiano bajo los parámetros establecidos por el *Manual para el Manejo de Acuerdos Comerciales en Procesos de Contratación* emitido por Colombia Compra Eficiente, en desarrollo del artículo 2.2.1.2.5.2 del Decreto 1082 de 2015				
NO APLICA				
9. Certificado de disponibilidad presupuestal (CDP):	No.	**326925**	Fecha:	19/12/2025
10. Vigencias futuras:	No. Oficio		Año	Cuantía por año
	No. de aprobación			
(Incluir cuadro adicional con la programación de valores por vigencia específicamente del contrato a realizar)				

CONTRATACIÓN DIRECTA DECRETO 1082 DE 2015						
11. Nombre o Razón Social de la(s) persona(s) natural(es) o jurídica(s) a contratar:						
	Contacto		Dirección		Teléfono	
11.1. Perfil de la persona a contratar:						
12. Firmas autorizadas:						
Firma responsable: Jefe de la Dependencia Solicitante Nombre: Giovanni Andrés López Cabezas Cargo: Viceministro de Transformación Digital Fecha: Diciembre de 2025			Firma responsable Nombre: Angela Janeth Cortes Hernandez Cargo: Coordinador GIT ColCERt Fecha: Diciembre de 2025			

ANEXOS

Listado de documentos anexos al formato general de estudios previos

Documentos Anexos
Documentos:
• Estudios del sector o Análisis de sector o Estudio mercado
• Matriz de riesgos
• Análisis de garantías (si aplica)

REGISTRO DE FIRMAS ELECTRONICAS

Estudio previo Licenciamiento GOOGLE ajustado

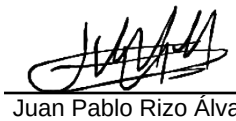
Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20251223-180157-7e4580-91319724
Estado: Finalizado

Creación: 2025-12-23 18:01:57
Finalización: 2025-12-23 18:41:43

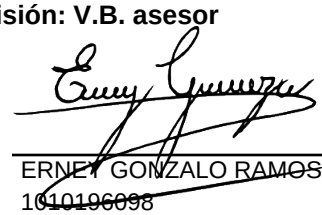
Escanee el código para verificación

Revisión: V.B. asesor



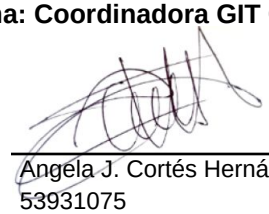
Juan Pablo Rizo Álvarez
1091664205
jrizo@mintic.gov.co
Asesor
Viceministerio de Transformación Digital

Revisión: V.B. asesor



ERNEY GONZALO RAMOS GUATAQUIRA
1010196098
eramosg@mintic.gov.co
Asesor
Viceministerio de Transformación Digital

Firma: Coordinadora GIT ColCERT



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

Ministerio TIC

Elaboración: Abogado GIT ColCERT

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

REGISTRO DE FIRMAS ELECTRONICAS

Estudio previo Licenciamiento GOOGLE ajustado

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

Id Acuerdo: 20251223-180157-7e4580-91319724

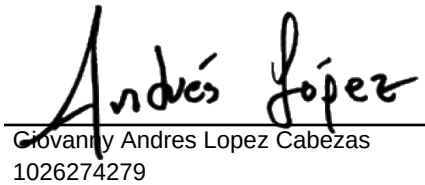
Estado: Finalizado

Creación: 2025-12-23 18:01:57

Finalización: 2025-12-23 18:41:43

Escanee el código para verificación

Firma: Viceministro de Transformación Digital



Giovanny Andres Lopez Cabezas
1026274279
galopezc@mintic.gov.co
Viceministro de Transformación Digital
Ministerio de Tecnologías de la Información y las Comunicaciones

REPORTE DE TRAZABILIDAD

Estudio previo Licenciamiento GOOGLE ajustado

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

Id Acuerdo: 20251223-180157-7e4580-91319724
Creación: 2025-12-23 18:01:57
Estado: Finalizado
Finalización: 2025-12-23 18:41:43

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 18:02:01 Lec.: 2025-12-23 18:02:32 Res.: 2025-12-23 18:02:38 IP Res.: 191.95.53.187 Canal: Email
Firma	Angela J. Cortés Hernández acortes@mintic.gov.co Ministerio TIC	Aprobado	Env.: 2025-12-23 18:02:39 Lec.: 2025-12-23 18:08:03 Res.: 2025-12-23 18:08:07 IP Res.: 190.145.189.98 Canal: Email
Revisión	ERNEY GONZALO RAMOS GUATAQUIRA eramosg@mintic.gov.co Asesor Viceministerio de Transformación Digital	Aprobado	Env.: 2025-12-23 18:08:07 Lec.: 2025-12-23 18:10:01 Res.: 2025-12-23 18:24:06 IP Res.: 190.145.189.98 Canal: Email
Revisión	Juan Pablo Rizo Álvarez jrizo@mintic.gov.co Asesor Viceministerio de Transformación Digital	Aprobado	Env.: 2025-12-23 18:24:07 Lec.: 2025-12-23 18:24:48 Res.: 2025-12-23 18:24:55 IP Res.: 186.102.0.234 Canal: Email
Firma	Giovanny Andres Lopez Cabezas galopezc@mintic.gov.co Viceministro de Transformación Digital Ministerio de Tecnologías de la Información y las	Aprobado	Env.: 2025-12-23 18:24:55 Lec.: 2025-12-23 18:41:35 Res.: 2025-12-23 18:41:43 IP Res.: 190.145.189.98 Canal: Email