Datos del área gestora:	**Dependencia solicitante:**	**DIRECCIÓN DE ECONOMÍA DIGITAL SUBDIRECCIÓN DE INDUSTRIA TI**
	Nombre del servidor que diligencia el estudio previo:	**MARÍA LUCÍA FLÓREZ JIMÉNEZ**

1.- Análisis sobre la Pertinencia y Necesidad de la suscripción del convenio

El artículo 2 de la Constitución Política, determina que los fines esenciales del Estado son: "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 en todas las decisiones que los afecta y en la vida económica, política y administrativa." Igualmente, el artículo 209 de la Constitución Política, indica que la función administrativa está al servicio de los intereses generales y desarrollada con fundamentos en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Al igual que la carta política colombiana en el Articulo 208, determina que los ministros y los directores de departamentos administrativos son los jefes de la administración en su respectiva dependencia. Bajo la dirección del presidente de la República, les corresponde formular las políticas atinentes a su despacho, dirigir la actividad administrativa y ejecutar la ley. El Estatuto General de Contratación de la Administración Pública, desde su entrada en vigor, aplica para los contratos que la Nación y sus entidades descentralizadas celebren en ocasión al desarrollo de actividades de Ciencia y Tecnología los artículos 2, 8, 9, 17 y 19 del Decreto ley 591 de 1991 y en el Decreto ley 393 de 1991.

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, el cual 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 FTIC, 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".

En complemento, el artículo 18 de la Ley 1341 de 2009, modificado por el artículo 14 de la ley 1978 establece como funciones del MINISTERIO TIC, entre otras, las siguientes: "1. Diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. 2. Definir, adoptar y promover las políticas, planes y programas tendientes a incrementar y facilitar el acceso de todos los habitantes del territorio nacional, a las tecnologías de la información y las comunicaciones y a sus beneficios para lo cual debe: a) Diseñar, formular y proponer políticas, planes y programas que garanticen el acceso y la implantación de las Tecnologías de la Información y las Comunicaciones, con el fin de fomentar su uso como soporte del crecimiento y aumento de la competitividad del país en los distintos sectores; b) Formular políticas, planes y programas que garanticen a través del uso de Tecnologías de la Información y las Comunicaciones: el mejoramiento de la calidad de vida de la comunidad, el acceso a mercados para el sector productivo, y el acceso equitativo a oportunidades de educación, trabajo, salud, justicia, cultura y recreación, entre otras. (…); 14. Propender por la utilización de las TIC para mejorar la competitividad del país (…).

Con el fin de dar cumplimiento a lo expuesto, dentro de la estructura del MinTIC se cuenta con la Dirección de Economía Digital, que en virtud de las modificaciones introducidas por el Decreto 1064 de 2020, que en su artículo 29 le asisten las funciones relacionadas con "(...) 2. Promocionar e incentivar en el país la innovación en materia de Tecnologías de la Información y las Comunicaciones. (...) 9. Definir, diseñar y promover políticas y acciones relacionadas con la adopción de buenas prácticas para la industria de Tecnologías de la Información y las Comunicaciones. 10. Definir, diseñar y promover la creación de mecanismos de fomento para la industria de Tecnologías de la Información y las Comunicaciones. (...)"

Además, la estructura organizacional de la entidad dispone que la Subdirección de Industria de Tecnologías de la Información hace parte de la Dirección de Economía Digital, esta subdirección ostenta un marco misional establecido por el artículo 31 del Decreto 1064 de 2020 el cual le asigna como funciones: "*1. Apoyar la formulación de políticas y estrategias, y poner en marcha programas, planes y proyectos que promuevan y generen emprendimiento digital en el Estado y la comunidad, e incrementen la productividad económica del país. 2. Fomentar el desarrollo de emprendimientos de base tecnológica, en sus diferentes fases de desarrollo, promover su visibilización y difusión del ecosistema emprendedor colombiano. 4. Diseñar e implementar modelos de conocimiento prácticos y competitivos, que se puedan adoptar en el sector público y privado y que fomenten el emprendimiento y la creatividad en la industria TI. 5. Diseñar y proponer nuevas formas de negocio digital de vanguardia y competitivos, acorde con el entorno económico, social, cultural y tecnológico del País. 6. Diseñar y proponer nuevas formas de financiamiento de negocios para la industria y la comunidad del emprendimiento digital.* ***8. Diseñar e implementar estrategias especializadas para la industria de tecnologías de información que dinamicen la creación de nuevas empresas innovadoras en el sector, y el fortalecimiento de las existentes. 10. Apoyar la formulación y ejecutar políticas, estrategias, programas planes y proyectos de Investigación, Desarrollo e Innovación, buscando que se genere verdadero valor a la oferta de la Industria TI.*** *11. Elaborar estudios de viabilidad para la implementación de infraestructura apta y pertinente a las tendencias, para fomentar la industria TI. 12. Proponer modelos de calidad de información tecnológica globalmente reconocidos por parte de las empresas que hacen parte de la Industria TI que permitan fortalecer el sector público y privado del país. 13. Las demás que le sean asignadas, inherentes a la naturaleza de la dependencia."* En negrilla y subrayado fuera del texto.

Así mismo, en el marco del Plan Nacional de Desarrollo (PND) 2022-2026 "Colombia, Potencia Mundial de la Vida", se establece la "Transformación productiva, internacionalización y acción climática", enfocada en generar una transición hacia actividades productivas diversificadas, incentivando el desarrollo sostenible y la competitividad y teniendo en cuenta un componente de inclusión social que debe ir a la par con la inclusión productiva. Esto requiere desarrollar una producción industrial sostenible, cerrar brechas tecnológicas, impulsar cadenas de valor para la integración regional, fortalecer las capacidades humanas y generar empleos de calidad. En el ámbito de la transformación digital, el PND 2022-2026 destaca la importancia de la ciberseguridad como un elemento crítico para la modernización del Estado y la competitividad del sector privado. El plan propone la implementación de políticas robustas de ciberseguridad para proteger las infraestructuras críticas, fortalecer la resiliencia cibernética y garantizar la privacidad y protección de datos personales. Entre las metas específicas se incluyen la creación de capacidades técnicas y operativas en ciberseguridad, el fomento de la cooperación público-privada en la gestión de riesgos cibernéticos, y el impulso a la educación y la formación en competencias digitales. Además, el PND enfatiza la necesidad de una regulación dinámica y adaptable que permita enfrentar las nuevas amenazas cibernéticas, asegurando así un entorno digital seguro que propicie la innovación y el desarrollo económico sostenible del país.

En ese sentido, con el catalizador "Economía productiva a través de la reindustrialización y la bioeconomía", se establece como objetivo generar un impulso a la industria digital del país mediante el desarrollo de una estrategia que involucre aspectos técnicos, de financiamiento, cultura empresarial, emprendimiento e innovación. Esto puede

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

Pública

lograrse mediante el fortalecimiento de los productos y servicios de las industrias de TI, a partir de la generación de conocimiento y el fomento a la innovación para el desarrollo de modelos de negocio de base tecnológica que habilite el acceso a mercados de alto valor agregado, como el de la industria de la ciberseguridad.

Por otro lado, el CONPES 3854 del 11 de abril de 2016, establece la Política Nacional de Seguridad Digital, que crea las condiciones para que las partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, siendo uno de los principales aportes el desarrollo de estrategias que establecieron un marco institucional para la seguridad digital con un enfoque de gestión de riesgos, con una visión preventiva antes que reactiva ante las posibles amenazas.

Así mismo, el documento CONPES 3854 de 2016, establece también una serie de lineamientos estratégicos para fortalecer la seguridad digital en Colombia. Este reconoce la importancia de crear un entorno seguro y confiable para el uso de tecnologías de la información y la comunicación (TIC), esencial para el desarrollo económico y social del país. Entre sus objetivos principales se encuentran la protección de las infraestructuras críticas, la promoción de la colaboración entre el sector público y privado, y el fomento de una cultura de seguridad digital entre los ciudadanos. El CONPES 3854 de 2016 destaca la necesidad de mejorar las capacidades técnicas y operativas del país en materia de ciberseguridad, así como la importancia de la cooperación internacional para enfrentar amenazas cibernéticas globales. Además, establece acciones concretas para prevenir, detectar y responder a incidentes de seguridad digital, para garantizar la integridad, disponibilidad y confidencialidad de la información en Colombia.

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.

Además, dando continuidad a lo relacionado con Ciberseguridad, el documento CONPES 3995 de 01 julio de 2020, titulado "Política Nacional de Confianza y Seguridad Digital", dicha política pública busca fortalecer la seguridad digital y fomentar la confianza en el entorno digital del país. Que tiene como objetivo general, fortalecer la confianza digital y la seguridad en Colombia para garantizar que el país sea una sociedad inclusiva y competitiva en el entorno digital. Unas de las metas principales es preparar a Colombia para los desafíos de la cuarta revolución industrial (4RI) mediante la implementación de tecnologías avanzadas, maximizar la generación de valor socioeconómico a través del uso seguro y eficiente del internet y el ciberespacio e impulsar la confianza digital entre los ciudadanos y las organizaciones, asegurando la protección de datos y la privacidad. Este CONPES 3995, se espera que contribuya significativamente al desarrollo económico y social de Colombia, al proporcionar un entorno digital seguro y confiable que fomente la innovación y el crecimiento económico. Además, busca que Colombia avance hacia una mayor inclusión digital y competitividad en el ámbito internacional.

Necesidad y Pertinencia del Proyecto

La ciberseguridad se ha convertido en una prioridad estratégica para Colombia en esta era digital, donde la protección de datos y la infraestructura tecnológica son esenciales para el desarrollo económico y social del país. Con el auge de la digitalización, también se han incrementado las amenazas cibernéticas, por eso el gobierno ha implementado políticas y normativas para salvaguardar la información y los sistemas críticos, alineada con el Plan Nacional de Desarrollo 2022–2026, la estrategia de seguridad busca proteger los activos digitales y fomentar una cultura de seguridad y confianza en el uso de tecnologías de la información.

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

Pública

Desde la Ley 1273 de 2009, que tipifica los delitos informáticos, hasta los documentos CONPES de Política Nacional enfocados hacia la Ciberseguridad y Ciberdefensa, Colombia está fortaleciendo su capacidad de respuesta y de adaptación ante posibles ataques cibernéticos, garantizando así un entorno digital seguro y confiable para todos sus ciudadanos y organizaciones.

Dentro de los principales hallazgos asociados a encuestas en la materia realizadas en Colombia, se identificaron los siguientes aspectos5 (PWC, 2024):

- Tendencia en el aumento en el número de brechas y los costos en términos de seguridad digital.
- Solo una cuarta parte de las organizaciones en Colombia cuenta con un plan estructurado de gestión de riesgos para abordar los desafíos de los proveedores de servicios en la nube.
- Más del 30 % de las empresas no sigue sistemáticamente lo que deberían ser prácticas estándar de ciberdefensa.
- Gestionan los riesgos de mejor manera optimizan las soluciones de seguridad y posicionado las empresas tener una mayor productividad y un crecimiento más rápido, superando a la competencia mientras implementan nuevas tecnologías.
- En Colombia los riesgos de ciberseguridad se ubican detrás de los riesgos derivados de la volatilidad macroeconómica, mientras a nivel global, el riesgo cibernético se ubica detrás de los riesgos digitales y tecnológicos.

En consecuencia, y, a partir de lo descrito con las anteriores cifras, de manera estructural una de las debilidades que ha generado impactos en las empresas en Colombia es la falta de una estrategia y una arquitectura de seguridad robusta a nivel interno, que identifique y mitigue los riesgos a los que se exponen estas unidades económicas, y tenga un presupuesto para ello. De otra parte, a pesar de que los ciberataques pueden costar millones de pesos en la mayoría de las empresas aún no existe claridad frente al nivel de exposición a estos riesgos e iniciativas concretas para mitigarlos, por tal motivo, es importante incluir la ciberseguridad en los procesos y cada actividad empresarial que represente manejo de datos y transacciones digitales, objetivo y alcance del proyecto **RETOS DE INNOVACIÓN TECNOLÓGICA EN CIBERSEGURIDAD**.

De esta forma, la ciberseguridad ha tomado cada vez mayor relevancia en el sector industrial y empresarial en Colombia, por lo que se han implementado estratégicas innovaciones para proteger sistemas, equipos y redes. Así, la relación entre la ciberseguridad y la innovación se ha implementado bajo dos corrientes: la ciberseguridad permite que la innovación sea considerada en casi todos los sectores de la economía digital al generar un ambiente de confianza en los usuarios de las tecnologías de la información y, por el otro, las diversas innovaciones tecnológicas permiten a las empresas dedicadas a ciberseguridad generar dispositivos y sistemas para proteger las empresas, redes y datos.

Bajo los anteriores principios, se enmarca el proyecto por desarrollar, relacionado con actividades del sector de servicios especializados en Tecnologías de la Información y las Comunicaciones -TIC, tal como es la identificación, formulación y puesta en marcha de soluciones digitales innovadoras, fundamentados en la necesidad de comprender los retos tecnológicos que enfrentan las MIPYMES del país en materia de ciberseguridad y las capacidades del sector de las industrias de tecnologías de la información para atender de manera innovadora estos retos, contribuyendo de este modo al fortalecimiento de un ecosistema que aproveche el conocimiento y las tendencias tecnológicas para estimular las dinámicas de oferta y demanda en torno al negocio de la ciberseguridad.

Así, el convenio se enfoca como un proyecto en Ciencia, Tecnológica e Innovación, fundamentado en la necesidad de comprender los retos tecnológicos de las MIPYMES del país en materia de ciberseguridad y las capacidades del

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

sector de las industrias de tecnologías de la información para atender de manera innovadora estos retos, contribuyendo así al fortalecimiento de un ecosistema que aproveche el conocimiento, la innovación y las tendencias tecnológicas para estimular la oferta y demanda en torno al negocio de la ciberseguridad, alineado, de esta forma, con el Decreto 393 de 1991 *"Por el cual se dictan normas sobre asociación para actividades científicas y tecnológicas, proyectos de investigación y creación de tecnologías"*, que en su artículo 2, literal h) el cual menciona, lo siguiente: *"Asesorar la negociación, aplicación y adaptación de tecnologías nacionales y extranjeras",* apartado según el cual resulta valida de la celebración de convenios de cooperación entre una entidad gestora (Aliado) y el Ministerio.

En consecuencia, el objeto del proyecto busca comprender los retos tecnológicos que enfrentan las MIPYMES del país en materia de ciberseguridad y las capacidades del sector de las industrias de tecnologías de la información para atender de manera innovadora estos retos, contribuyendo de este modo al fortalecimiento de un ecosistema que aproveche el conocimiento y las tendencias tecnológicas para estimular las dinámicas de oferta y demanda en torno al negocio de la ciberseguridad.

El Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC- en Colombia tiene un rol determinante en el tema de ciberseguridad debido a que es la entidad encargada de diseñar, coordinar y promover políticas públicas relacionadas con la tecnología y la comunicación en el país, esto incluye garantizar que el entorno digital seguro y resiliente frente a amenazas cibernéticas a la que se puedan enfrentar las diferentes empresas del país.

De igual forma, el liderazgo del MinTIC frente al tema de ciberseguridad es fundamental para asegurar una gestión efectiva de los riesgos y desafíos en el entorno digital, implementando acciones y estrategias encaminadas en proteger tanto a ciudadanos como las empresas en el ámbito digital, y adoptando buenas prácticas para fortalecer la protección cibernética a nivel nacional.

CIENCIA, TECNOLOGÍA E INNOVACIÓN

Teniendo en cuenta lo anterior se logra evidenciar que el presente proyecto se enmarca en las actividades de ciencia tecnología e innovación descritas en el artículo 2 de la Ley 591 de 1991 que establece: "*Para los efectos del presente Decreto, entiéndese por actividades científicas y tecnológicas las siguientes:*

1. ***Investigación científica y desarrollo tecnológico, desarrollo de nuevos productos y procesos, creación y apoyo a centros científicos y tecnológicos y conformación de redes de investigación e información.***
2. *Difusión científica y tecnológica, esto es, información, publicación, divulgación y asesoría en ciencia y tecnología.*
3. *Servicios científicos y tecnológicos que se refieren a la realización de planes, estudios, estadísticas y censos de ciencia y tecnología; a la homologación, normalización, metodología, certificación y control de calidad; a la prospección de recursos, inventario de recursos terrestres y ordenamiento territorial; a la promoción científica y tecnológica; a la realización de seminarios, congresos y talleres de ciencia y tecnología, así como a la promoción y gestión de sistemas de calidad total y de evaluación tecnológica.*
4. ***Proyectos de innovación que incorporen tecnología, creación, generación, apropiación y adaptación de la misma, así como la creación y el apoyo a incubadoras de empresas, a parques tecnológicos y a empresas de base tecnológica.***
5. ***Transferencia tecnológica que comprende la negociación, apropiación, desagregación, asimilación, adaptación y aplicación de nuevas tecnologías nacionales o extranjeras****.*
6. *Cooperación científica y tecnológica nacional e internacional." (negrita fuera de texto)*

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

Pública

Lo anterior en concordancia con los artículos 1 y 2 del Decreto 393 de 1991, donde establece que para adelantar actividades científicas y tecnológicas proyectos de investigación y creación de tecnologías, la Nación y sus entidades descentralizadas podrán asociarse con los particulares bajo dos modalidades: 1. Mediante la creación y organización de sociedades civiles y comerciales y personas jurídicas sin ánimo de lucro como corporaciones y fundaciones o **2. Mediante la celebración de convenios especiales de cooperación.**

Dentro de los objetos de estos negocios jurídicos, se puede pactar el desarrollo de las actividades señaladas en los instrumentos auxiliares, como el Manual Metodológico general para la identificación, preparación, programación y evaluación de Proyectos de Ciencia, Tecnología e Innovación de COLCIENCIAS hoy MINCIENCIAS, Manual de Frascati[1], Camberra, Oslo, Patentes, BTP, CONPES 3582 de 2009 y 3834 de 2015, Instructivo para el uso del clasificador de política transversal de ACTIC´S, entre otros.

En primer lugar, según las definiciones contenidas tanto en el Manual de Frascati 2015, como en los documentos CONPES 3582 de 2009[2] y 3834 de 2015[3], la investigación y el desarrollo experimental (I+D), comprenden el trabajo creativo llevado a cabo de manera sistemática para incrementar el volumen de conocimientos, incluido el conocimiento del hombre, la cultura y la sociedad y el uso de esos conocimientos para crear nuevas aplicaciones[4].

Estas mismas definiciones son recogidas en la Guía Sectorial No. 2[5] de programas y proyectos de ciencia, tecnología e innovación, para la identificación, preparación, programación y evaluación de proyectos, por medio de la cual se presentan los lineamientos conceptuales para mejorar los procesos de identificación, preparación, formulación y evaluación de los proyectos en materia de ciencia, tecnología e innovación. El objetivo de la guía es "(...) orientar la identificación, formulación y evaluación de proyectos de ciencia, tecnología e innovación (CTeI), y de proyectos de otros sectores que incluyan actividades de Ciencia, Tecnología e Innovación (ACTI), que sean financiados con recursos de inversión del gobierno nacional, las entidades territoriales, el Sistema General de Regalías SGR- y otras fuentes de recursos públicos y privados"

A su vez, Colciencias hoy MinCiencias, mediante la Guía No 2, definió las actividades de ciencia y tecnología (ACT) como todas las actividades sistemáticas que están estrechamente relacionadas con la generación, producción, avance, promoción, difusión, diseminación, y aplicación de conocimiento científico y técnico y que aplican a todos los campos de la ciencia y la tecnología (UNESCO, 1984[6]). Para el caso Colombia a esta definición de ACT se le incorporaron las actividades de innovación, que el Manual de Frascati[7] denomina otras actividades industriales.

Las actividades de ciencia, tecnología e innovación (ACTI) comprenden:

a. Investigación y desarrollo experimental
b. Formación y capacitación científica y tecnológica
c. Servicios científicos y tecnológicos
d. Actividades de innovación

[1] https://www.fecyt.es/es/publicacion/manual-de-frascati-2015
[2] Política Nacional de Ciencia, Tecnología e Innovación.
[3] Lineamientos de política para estimular la inversión privada en Ciencia, Tecnología e Innovación a través de deducciones tributarias
[4] Frascati Manual 2015. Guidelines for collecting and reporting data on research and experimental development. Página 46.
[5] https://www.colciencias.gov.co/sites/default/files/guiasectorialctei.pdf
[6] UNESCO. (1984). Manual for Statistics on Scientific and Technological Activities, ST-84/WS/12. Paris: UNESCO, http://www.uis.unesco.org/ev.php?ID=6090_201&ID2=DO_TOPIC.
7 OCDE. (2002). Manual de Frascati - Propuesta de norma práctica para encuestas de investigación y desarrollo experimental (6ta ed.). Paris: Fundación Española Ciencia y Tecnología, OCDE.

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

Pública

e. Administración y otras actividades de apoyo a la I+D[8]

Las actividades relativas a la innovación se refieren a la implementación de un producto (bien o servicio), proceso, método de mercadeo, o método organizacional nuevo o significativamente mejorado, en las prácticas de los negocios, la organización del trabajo o las relaciones externas (OCDE, 2005, Manual de Oslo[9]).

De acuerdo con lo anterior, las actividades de innovación pueden ser: (i) actividades relativas a las innovaciones en productos y procesos; (ii) actividades relativas a las innovaciones en mercadotecnia y organización. Teniendo en cuenta los adelantos del Manual de Oslo y las actividades definidas por el DANE en las Encuestas de Desarrollo e Innovación Tecnológica (EDIT), las actividades identificadas para lograr estos objetivos son:

Adquisición de conocimientos externos a la empresa: Adquisición de patentes, invenciones no patentadas, licencias, divulgación del know-how, marcas de fábrica, estudios de diseño y modelos orientados a la innovación. Se incluye también la adquisición de servicios informáticos, así como otros servicios científicos y técnicos que apoyen la innovación. Esta adquisición también está reflejada en la contratación de personal que posee conocimientos especializados o en la contratación de investigaciones y servicios de consultoría, que apoyen la innovación.

Adquisición de máquinas, equipos y otros bienes de capital: Son aquellas adquisiciones de maquinaria y equipos con desempeño tecnológico mejorado (incluso software integrado), vinculados con las innovaciones implementadas en la empresa.

Comercialización: Actividades relacionadas con el lanzamiento de productos tecnológicamente nuevos o mejorados, entre ellas se incluyen la investigación de mercado y la publicidad de lanzamiento. Así mismo, comprende las actividades tendientes a mejorar las posibilidades de penetración en segmentos específicos del mercado mediante cambios en la presentación o en los métodos de entrega del producto. También incluye las actividades vinculadas a la elaboración y la introducción de nuevos métodos de comercialización que no eran utilizados anteriormente por la empresa.

Capacitación: Comprende la capacitación en temas estrechamente relacionados con las tecnologías centrales en el proceso productivo del establecimiento necesarias para la introducción de una innovación de producto o proceso. Estas tecnologías pueden ser blandas (gestión y administración) o duras (tecnología de procesos productivos), que involucran un grado de complejidad significativo -no evidente- que requiere de un personal capacitador altamente especializado.

Innovaciones de organización: Se entiende por estas cuando se desarrollan cambios en formas de organización y gestión del establecimiento, cambios en la organización y en el proceso productivo, incorporación de estructuras organizativas significativamente mejoradas e implementación de orientaciones estratégicas corporativas nuevas o sustancialmente modificadas.

De otra parte y conforme a la actualización realizada en de la versión 2018 del Manual de Oslo[10], se tiene que "La innovación es fundamental para mejorar el nivel de vida y puede afectar a las personas, Instituciones, sectores

8 El término I+D contempla tres tipos de actividades: investigación básica, investigación aplicada y desarrollo experimental. El rápido desarrollo de la ciencia y la tecnología ha implicado que en muchas ocasiones la distinción entre estás categorías se dificulte y por esta razón su uso ha venido disminuyendo.
9 OCDE, & Eurostat. (2005). Manual de Oslo - Guía para la recogida e interpretación de datos sobre innovación, 3ra edición. Paris, Luxembourg: OCDE, European Communities.
10 OCDE Manual de Oslo, edición 4, octubre de 2018, página 28

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

Pública

económicos completos, y países de múltiples maneras. La innovación y el uso de datos de innovación en la investigación pueden ayudar a los responsables políticos a mejorar y comprender los cambios económicos y sociales, evaluar la contribución de la innovación a los objetivos económicos y supervisar y evaluar la eficacia y la eficiencia de sus políticas.

El manual proporciona la base para un lenguaje común para discutir la innovación, los factores que apoyan Innovación, y resultados de innovación.

En ese marco, establece que las siguientes son actividades de I+D[11]:

- ingeniería, diseño y otras actividades de trabajo creativo
- actividades de capital de marketing y de marca
- de propiedad intelectual (PI) y las actividades relacionadas
- las actividades de formación de los empleados
- desarrollo de software de bases de datos y las actividades
- actividades relacionadas con la adquisición o arrendamiento de bienes tangibles
- actividades de gestión de la innovación.

Como se puede apreciar, el proyecto tiene un fuerte enfoque en la transferencia de conocimiento y metodologías, así como en la innovación organizacional, lo que permite clasificarlo como dentro de las actividades de Ciencia, tecnología e Innovación establecidas.

Es importante destacar que el desarrollo técnico de cada uno de los objetivos que enmarcarán la ejecución del presente convenio se encuentra debidamente desarrollados en el anexo técnico (Ver Anexo Técnico).

2.- Naturaleza Jurídica de la Entidad con la que se va a suscribir el convenio.

Por Acta No. 1 del 12 de noviembre de 2010 de la Asamblea Constitutiva de Manizales, inscrito en Cámara de Comercio el 28 de diciembre de 2010, con el No. 15941 del Libro I del Registro de Entidades sin Ánimo de Lucro, se constituyó la entidad sin ánimo de lucro de naturaleza Corporativa denominada CENTRO DE BIOINFORMÁTICA Y BIOLOGÍA COMPUTACIONAL DE COLOMBIA CON SIGLA: CBBC. Posteriormente, por Acta No. 7 del 28 de abril de 2014 de la Asamblea de Asociados de Manizales, se decretó la reforma parcial de estatutos con la que se cambió el nombre a CENTRO DE BIOINFORMÁTICA Y BIOLOGÍA COMPUTACIONAL DE COLOMBIA o BIOS o CBBC.

De acuerdo con el certificado de existencia y representación legal, BIOS tiene como objeto "*prestar servicios de procesamiento y almacenamiento de datos, desarrollo de software y soporte técnico y científico a empresas, universidades, organizaciones públicas, centros y grupos de investigación; en las áreas de las ciencias de la vida, ciencias de la computación y ciencias que demanden servicios del CBBC y su interrelación para el estudio de la biodiversidad. Parágrafo. Para el adecuado desarrollo de su objeto, además de la posibilidad de usar todos los instrumentos contractuales y operacionales que la ley permite, desplegara actividades académicas en alianza con universidades, en consecuencia, de conformidad con lo previsto en el artículo 125 de la ley 30 de 1992 el CBBC, podrá ofrecer, previo convenio con las universidades y conjuntamente con estas, programas de formación avanzada, todo de conformidad con lo previsto en las normas de ciencia y tecnología y en el decreto 393 de 1991.*"(...)

[11] OCDE Manual de Oslo, edición 4, octubre de 2018, capítulo 3

La clasificación de las actividades económicas - CIIU de BIOS son:

Actividad principal Código CIIU: J6202 - Actividades de consultoría informática y actividades de administración de instalaciones informáticas.

Actividad secundaria Código CIIU: J6311 - Procesamiento de datos, alojamiento (hosting) y actividades relacionadas

Otras actividades Código CIIU:

J6201 - Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas)
N8299 - Otras actividades de servicio de apoyo a las empresas n.c.p.

3.- Descripción del objeto del convenio.

Objeto.	33200401811 - Aunar esfuerzos técnicos, administrativos y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.
3.1- Códigos de clasificación UNSPSC:	El objeto antes señalado se encuentra enmarcado en los siguientes códigos de clasificación UNSPSC:

Grupo	Segmento	Familia	Clase	Código
Servicios (F)	Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	Servicios de asesoría de gestión	Servicios de asesoramiento sobre tecnologías de la información	80101507
			Gerencia de proyectos	80101600
	Servicios basados en ingeniería, investigación, y tecnología	Entrega de servicios de tecnología de información	Servicios de administración de acceso	81161500
		Servicios Informáticos	Sistema Recuperación Información	81111900
		Servicios Informáticos	Servicios de sistemas y administración de componentes de sistemas	81111800

4.- Compromisos	**Descripción de los compromisos.**

Pública

a)Compromisos generales del ejecutor /cooperante.	1. Garantizar que el objeto del convenio se cumpla en las condiciones de calidad y oportunidad definidas en el anexo técnico y los demás documentos que hacen parte integral del mismo. 2. Cumplir con lo establecido en el convenio descrito en los términos y condiciones aquí pactadas observando siempre la constitución política, las leyes colombianas y elrégimen de contratación pública. Por ningún motivo suspenderá o abandonará elcumplimiento del convenio, sin previa justificación aceptada por la Entidad contratante. 3. Ejercer la dirección y el control de las actividades encomendadas, en tiempo y en el término establecido, para obtener la correcta realización del objeto contratado. 4. Presentar ante el supervisor por parte del Ministerio TIC/Fondo Único TIC un informe mensual de ejecución con corte al último día de cada mes, dentro de los cinco (5) días calendario siguientes a la fecha de corte. Los informes de deberán presentar desde el primer mes de inicio y hasta la finalización del convenio. 5. Presentar ante la supervisión del convenio por parte del Ministerio TIC/Fondo Único TIC un informe final de gestión que contenga la ejecución técnica, administrativa y financiera, así como las observaciones y recomendaciones de implementación del proyecto, que dé cuenta de todo el período del convenio, el cual deberá ser presentado dentro de los quince (15) días hábiles siguientes a la terminación delconvenio. 6. Atender solicitudes, resolver inconvenientes y realizar las propuestas necesariaspara la buena ejecución del convenio. 7. De conformidad a la Ley 1581 de 2012 y Decreto Reglamentario 1377 de 2013, salvaguardar la información clasificada y reservada que obtenga o conozca con

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

	ocasión de la ejecución de las actividades del convenio, salvo justificación legal orequerimiento de autoridad competente. 8. De conformidad a la Ley 1581 de 2012 y Decreto Reglamentario 1377 de 2013, usar la información y/o documentos producidos en desarrollo de este convenio conforme al objeto establecido, obligándose a no emplearlos para fines distintos a los previstos en este convenio, conservando la confidencialidad de estos, según la ley, so pena de las acciones civiles, administrativas o penales a que haya lugar. 9. Abrir y manejar una cuenta bancaria exclusiva para la administración de los recursos financieros del convenio relacionado con el proyecto. Esta cuenta se utilizará para transacciones financieras asociadas al convenio, asegurando la transparencia y trazabilidad adecuada de los fondos. El aliado garantiza que todos los movimientos de cuenta se realizarán según las normativas financieras aplicables y bajo los principios de eficiencia y responsabilidad fiscal, para asegurar el uso correcto y efectivo de los recursos del convenio para cumplir sus objetivos estipulados. 10. Presentar ante el supervisor del Fondo Único de TIC de manera mensual el informe de legalización de recursos establecido por el Fondo, en función de adelantar el seguimiento mensual a la ejecución financiera de los recursos aportados. Para tal efecto, se deberá presentar la relación de los pagos efectivamente realizados en el marco de la ejecución del objeto convenido, los citados informes deberán tramitarse con sujeción a los procedimientos institucionales dispuestos para tal efecto, en concordancia con el anexo técnico. 11. Presentar al supervisor del convenio por parte del Ministerio TIC/Fondo Único TIC un informe parcial de legalización de recursos con corte al 15 de diciembre de 2024, que tendrá como fecha límite de entrega el veintidós (22) de diciembre de 2024. El citado informe deberá contemplar un reporte de los movimientos, pagos, transacciones y en general todos los aspectos relacionados con la ejecución financiera del convenio, con sujeción a los procedimientos institucionales dispuestos para tal efecto. Este informe es adicional a los que se solicitan en numeral anterior. 12. Reintegrar mensualmente los rendimientos financieros generados con los recursos entregados por el Fondo Único de TIC en la cuenta que este señale para tal efecto y de conformidad con lo establecido en la propuesta que integra este documento y hasta el cierre de la cuenta del convenio. 13. Reintegrar los recursos no comprometidos del convenio a la finalización del término de ejecución previsto, en la cuenta que señale el Fondo Único de TIC, y en todo caso antes de la liquidación de este. 14. Pagar por su cuenta los salarios, prestaciones sociales, contribuciones al sistema integral de seguridad social y aportes parafiscales a quien hubiere lugar, de todos los empleados a su cargo, conforme a las disposiciones vigentes en el régimen legal colombiano. 15. Atender, en un término no mayor a cinco días hábiles, los requerimientos, instrucciones y/o recomendaciones que durante el desarrollo del convenio le imparta el Fondo a través del supervisor de este, para una correcta ejecución y cumplimiento de sus obligaciones. 16. Reportar de manera inmediata al supervisor, la ocurrencia de cualquier novedad o anomalía durante la ejecución del convenio.

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

Pública

	17. Responder, en los términos establecidos por la ley, a las peticiones, quejas, reclamos, sugerencias y denuncias -PQRSD- asignadas a través del sistema de información documental INTEGRATIC, o del que disponga la Entidad, sin tareas pendientes a su cargo, cuyo trámite será considerado por el supervisor del convenio para la autorización de cobro y expedición de paz y salvos.
b) Compromisos específicos del ejecutor /cooperante	1. Aportar una contrapartida en especie cuantificados hasta la suma de CIENTO NOVENTA Y OCHO MILLONES CIENTO TREINTA MIL CINCUENTA Y SEIS PESOS ($198.130.056), en función de atender los conceptos asociados en la propuesta técnica que hace parte integral del presente documento. 2. Elaborar y presentar para revisión y aprobación en el primer Comité Operativo del Convenio el plan de trabajo, de conformidad con el objeto del convenio de los requerimientos establecidos en el anexo técnico y los demás documentos que hacen parte integral del presente documento dentro de los primeros cinco (5) días hábiles posteriores al inicio del convenio. 3. Desarrollar la Fase 1. “Planeación y alistamiento” descrita en el anexo técnico con sus actividades y entregables. 4. Desarrollar la Fase 2. “Definición de retos tecnológicos” descrita en el anexo técnico con sus actividades, entregables y plazos. 5. Desarrollar la Fase 3. “Fortalecimiento de solucionadores tecnológicos” descrita en el anexo técnico con sus actividades, entregables y plazos. 6. Desarrollar la Fase 4. “Implementación de retos tecnológicos**”** descrita en el anexo técnico con sus actividades, entregables y plazos. 7. Desarrollar la Fase 5. “Difusión y cierre**”** descrita en el anexo técnico con sus actividades, entregables y plazos. 8. Contratar un equipo base con dedicación 100% y exclusiva al proyecto, que garantice la implementación, el cumplimiento y la calidad del proyecto, así como la correcta y oportuna ejecución de los recursos del convenio. Los perfiles se encuentran descritos en el anexo técnico que hace parte integral del convenio. 9. Diseñar las estrategias de comunicaciones de las convocatorias derivadas del proyecto, desde el inicio de la ejecución, las cuales deben ser aprobadas por el supervisor de MinTIC en articulación con la instancia pertinente del Ministerio. En el caso de todas las piezas de divulgación del proyecto, deberán ajustarse a los manuales de marca e imagen del MinTIC y tener su aprobación. 10. Asistir a las reuniones de seguimiento a la ejecución del convenio que se llevarán con periodicidad mensual, sin perjuicio de las mesas de trabajo y demás reuniones que sean convocadas por la entidad contratante. Parágrafo Primero: Las partes deberán mantenerse mutuamente indemnes de cualquier reclamación proveniente de terceros, cuando la de sus contratistas, o subcontratistas, o dependientes, se le cause daño a dicho tercero; por lo anterior, todos los gastos en que se incurra por la aplicación de esta cláusula serán a cargo de la entidad que ocasionó la afectación al tercero. Parágrafo Segundo: Las partes suscriptoras del convenio se comprometen a no realizar explotación económica o patrimonial de los entregables generados con ocasión de la ejecución del objeto pactado. En complemento, el aliado se compromete a garantizar la

“Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios”

Pública

	tutela de los derechos de autor configurados a partir de la ejecución del convenio, en favor del Fondo Único de Tecnologías de la Información y las Comunicaciones en su calidad de titular de los citados derechos. Lo anterior, según lo establecido por el artículo 20 de la Ley 23 de 1982.
c) Compromisos particulares del Ministerio / Fondo Único de Tecnologías de la Información y las Comunicaciones	1. Desembolsar oportunamente los recursos establecidos para el desarrollo del objeto del convenio. 2. Concurrir en las actividades de conceptualización, estructuración, planificación e intercambio de argumentos a que haya lugar para la buena ejecución del convenio, en el marco de lo establecido en el alcance de objeto y en el anexo técnico. 3. Facilitar el intercambio de información necesaria para lograr los cometidos del convenio. 4. Designar el supervisor del convenio, quien se encargará de la supervisión y el seguimiento técnico, administrativo, jurídico y financiero al desarrollo de las actividades del convenio, de acompañar el proceso, y de las gestiones necesarias para alcanzar el éxito del objeto del convenio. 5. Aprobar por parte de la supervisión del MinTIC los informes y/o entregables a que haya lugar, para efectos de trámite de los desembolsos. 6. Cumplir con todos los requisitos de ley, destinados al cumplimiento del objeto convenido, aplicando las disposiciones legales vigentes.
5.- Plazo de ejecución del convenio	El plazo de ejecución del convenio será hasta el treinta y uno (31) de diciembre de 2024, contado a partir de la suscripción del acta de inicio, previo el cumplimiento de los requisitos de perfeccionamiento y ejecución del convenio.
6.- Lugar de ejecución del convenio:	Para todos los efectos legales el presente convenio se ejecutará en Bogotá, D.C y todo el territorio nacional, fijando como domicilio contractual la ciudad de Bogotá, D.C.
7.- Supervisión / interventoría	La supervisión será ejercida por el Subdirector de Industria de Tecnologías de la Información o quien designe el ordenador del gasto. En ningún caso el supervisor goza de la facultad de modificar el contenido y alcance del convenio suscrito, 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. Para cumplir con su labor de verificación, la supervisión por parte del MINTIC, ejercerá entre otras, las siguientes funciones: 1. Realizar el seguimiento y control técnico, administrativo, financiero, contable y jurídico a la ejecución del Convenio. 2. Verificar que el cooperante cumpla con el objeto y compromisos del convenio, en términos de cantidad, calidad y oportunidad, conforme a lo estipulado en el convenio. 3. Requerir al cooperante sobre el cumplimiento de los compromisos estipulados en el convenio, en el anexo técnico y en la propuesta presentada y aceptada por la Entidad. 4. Suscribir los documentos y actas a que haya lugar durante la ejecución del convenio.

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

	5. Informar a la Secretaría General del Ministerio TIC/Fondo Único TIC con respecto a las demoras o incumplimiento de los compromisos del cooperante. 6. Recibir la correspondencia, informes y documentos que presente el cooperante y hacer las observaciones que estime convenientes. 7. Solicitar la suscripción de adiciones, prórrogas o modificaciones, previa la debida y detallada sustentación propendiendo por el cumplimiento a cabalidad del objeto convenido. 8. Certificar el cumplimiento de las actividades a cargo del cooperante y autorizar los desembolsos a cargo del Fondo Único TIC. 9. Elaborar y entregar a la Subdirección de Gestión Contractual para revisión y ajustes, el proyecto de acta de liquidación del convenio una vez éste se termine, adjuntando el balance económico y los soportes correspondientes. 10. Suscribir y entregar el acta de liquidación del convenio a la Subdirección de Gestión Contractual dentro de los términos de ley. 11. Verificar el cumplimiento de las obligaciones del cooperante relacionadas con el sistema de seguridad social integral y parafiscales, de conformidad con el artículo 23 de la Ley 1150 de 2007. 12. Solicitar la información que requiera respecto de cualquiera de los compromisos, o con el desarrollo del objeto del presente convenio. 13. Publicar en la plataforma SECOP II los documentos generados en todas las etapas del Convenio. 14. Las demás contempladas en la ley y el Manual de Contratación vigente del MinTIC.
8.- Comité	Para la adecuada ejecución del convenio, se creará un Comité Operativo, que actuará como máximo órgano de decisión y de dirección del proyecto. Dicho Comité estará integrado así: Por parte del Ministerio/ Fondo Único de TIC: 1. Delegado del Viceministro de Transformación Digital 2. El supervisor del convenio Por parte del aliado: 3. El representante legal o su delegado Las recomendaciones y decisiones que se tomen al interior de este Comité Operativo deberán ser unánimes. El comité tendrá las siguientes funciones: 1. Velar de manera conjunta que se cumpla lo acordado por las partes del Convenio. 2. Emitir recomendaciones a la ejecución del plan de trabajo y cronograma del convenio, proponer ajustes al mismo y dar orientaciones generales para el cumplimiento del objeto del convenio. 3. Aprobar el plan de trabajo del convenio y las modificaciones que se generen a éste. 4. Evaluar periódicamente y realizar el seguimiento al cumplimiento de lo dispuesto en el plan de trabajo y en el anexo técnico.

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

Pública

	5. Revisar y aprobar los términos de referencia y el reporte del estado de las convocatorias, invitaciones y/o cualquier otro mecanismo que se utilice para la implementación del plan de trabajo del convenio. 6. Hacer recomendaciones técnicas sobre la adecuada gestión y seguimiento del convenio. 7. Servir como espacio de discusión y debate de los asuntos que sean abordados para el desarrollo del convenio, así como ser la instancia inicial para la resolución de las controversias que puedan llegar a presentarse. 8. Realizar seguimiento a los compromisos adquiridos en el marco del Comité Operativo. 9. Las demás requeridas para la correcta ejecución del convenio. El Comité Técnico Operativo de ejecución del convenio se reunirá por convocatoria del supervisor del MinTIC / Fondo Único de Tecnologías de la Información y las Comunicaciones y/o del supervisor de BIOS, como mínimo una vez al mes desde el cumplimiento de requisitos de inicio; de forma extraordinaria, se reunirá por convocatoria de cualquiera de las partes. Se deberá dejar constancia de sus recomendaciones y compromisos adquiridos, mediante las correspondientes actas. La Secretaría del Comité estará a cargo de BIOS quien deberá elaborar las respectivas actas, dentro de los cinco (5) días hábiles siguientes a su realización.
9.- Tipo de convenio a celebrar	Convenio Especial de Cooperación
10.- Fundamentos jurídicos de la modalidad de selección	En virtud de lo señalado en la Ley 1150 de 2007, establece: las actividades de Ciencia, tecnología e innovación pueden ser contratadas a través de la causal de contratación directa las cuales están definidas en el literal (a), artículo 2 del Decreto-Ley 393 de 1991, literal (b) del artículo 2 del Decreto-Ley 591 de 1991, así mismo, Así mismo, la Circular Externa No. 6 del 27 de septiembre de 2013 emitida por Colombia Compra Eficiente establece que: "*Los contratos para la ejecución de programas, proyectos y actividades de ciencia, tecnología e innovación, pueden celebrarse en la modalidad de contratación directa de acuerdo con lo dispuesto en el literal (e), numeral 4, del artículo 2 de la Ley 1150 de 2007.* Acorde con el convenio en ejecución las actividades de Ciencia, tecnología e innovación son las siguientes: (i) Crear, fomentar, desarrollar y financiar empresas que incorporen innovaciones científicas o tecnológicas aplicables a la producción nacional, al manejo del medio ambiente o al aprovechamiento de los recursos naturales; (ii) Organizar, crear y apoyar centros científicos, tecnológicos y de innovación, parques tecnológicos, incubadoras de empresas y empresas de base tecnológica; (iii) Formar y capacitar el recurso humano para el avance y la gestión de la ciencia, tecnología e innovación; (iv) Establecer y conformar redes de investigación e información científica, tecnológica y de innovación; (v) Crear fondos de desarrollo científico, tecnológico y de innovación a nivel nacional y regional, fondos especiales de garantías y fondos para la renovación y el mantenimiento de equipos científicos; (vi) Realizar seminarios, cursos, congresos, talleres y eventos nacionales o internacionales de ciencia, tecnología e innovación; (vii) Financiar publicaciones y otorgar premios y distinciones a investigadores, grupos de

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

investigación e investigaciones; (viii) Adelantar proyectos de investigación científica, desarrollo tecnológico e innovación; desarrollo de nuevos productos y procesos; (ix) Difundir información científica, tecnológica y de innovación, esto es, información, publicación, divulgación y asesoría en ciencia, tecnología e innovación; (x) Desarrollar servicios científicos y tecnológicos que se refieren a la realización de planes, estudios, estadísticas y censos de ciencia y tecnología; y la realización de actividades de homologación, normalización y metrología, certificación y control de calidad; a la prospección de recursos, inventario de recursos terrestres y ordenamiento territorial; a la promoción científica, tecnológica y d innovación; así como a la creación, fomento, difusión, promoción, implementación y gestión de sistemas de calidad total y de evaluación tecnológica; (xi) Desarrollar proyectos de innovación que incorporen tecnología, creación, generación, apropiación y adaptación de la misma; (xii) Transferencia tecnológica que comprende la asesoría, negociación, apropiación, desagregación, asimilación, adaptación y aplicación de nuevas tecnologías nacionales o extranjeras; (xiii) Cooperación en ciencia, tecnología e innovación nacional o internacional; (xiv) Apropiación social de la ciencia, la tecnología y la innovación a través dela integración de la cultura científica, tecnológica e innovadora a la cultura regional y nacional; (xv) Elaborar y desarrollar proyectos de investigación y desarrollo experimental (I+D), formación y capacitación científica y tecnológica, servicios científicos y tecnológicos y actividades de innovación e innovación social.

En consecuencia, y de acuerdo con lo anterior, los contratos para la ejecución, financiamiento y administración de programas, proyectos y actividades de ciencia, tecnología e innovación que se celebren a través de la modalidad de contratación directa de acuerdo con lo dispuesto en el literal (e), numeral 4, del artículo 2 de la Ley 1150 de 2007, deben tener por objeto alguna de las actividades antes enunciadas. Si bien las actividades de Ciencia, tecnología e innovación pueden ser contratados directamente, las Entidades Estatales sólo podrán ejecutar actividades de ciencia, tecnología e innovación mediante los algunos tipos de contrato entre ellos el Convenio especial de cooperación el cual es celebrado para asociar recursos, capacidades y competencias, y puede incluir el financiamiento y administración de proyectos. El convenio especial de cooperación está regulado en los artículos 6, 7 y 8 del Decreto-Ley 393 de 1991 y en el artículo 17 del Decreto-Ley 591 de 1991".

En ese orden y dada la compatibilidad y las funciones de la naturaleza jurídica de BIOS se suscribirá el convenio de cooperación amparado en el Decreto 393 y 591 de 1991, como se indica a continuación:

Actividad de CTI de acuerdo con los Decretos 393 y 591 de 1991	Relación de la actividad de CTI con el proyecto
1. *Investigación científica y desarrollo tecnológico, desarrollo de nuevos productos y procesos, creación y apoyo a centros científicos y tecnológicos y conformación de redes de investigación e información.*	Las actividades específicas e implementar soluciones tecnológicas innovadoras en el proyecto, radica en el impulso a la creación, desarrollo y adaptación de tecnologías que aborden retos concretos del sector de ciberseguridad. Así se convoca a varias empresas del sector TIC que apoyen en desarrollar prototipos funcionales que respondan a necesidades específicas, estimulando así la generación de

4. *Proyectos de innovación que incorporen tecnología, creación, generación, apropiación y adaptación de la misma, así como la creación y el apoyo a incubadoras de empresas, a parques tecnológicos y a empresas de base tecnológica.*	nuevas ideas y la aplicación directa de la tecnología en contextos reales. Esta actividad refleja cómo la innovación y la tecnología pueden ser herramientas para el desarrollo económico y la seguridad que promueve la creación de soluciones son teóricas, aplicables y capaces de transformar la dinámica actual del sector, y de los entornos de seguridad digital	
5. *Transferencia tecnológica que comprende la negociación, apropiación, desagregación, asimilación, adaptación y aplicación de nuevas tecnologías nacionales o extranjeras.*	Adicionalmente, se resalta que las empresas que hacen parte de la industria TIC fomentarán la innovación y colaboración en el desarrollo de soluciones tecnológicas que aborden restos en ciberseguridad, seleccionando soluciones tecnológicas ganadoras para su implementación y financiación, garantizando que se ajuste a la arquitectura propuesta y cumpla con los estándares de calidad y funcionalidad esperados Se realizará en la ejecución del proyecto una etapa de transferencia de conocimiento en una de las fases de ejecución del convenio.	

Los convenios especiales de cooperación, según el artículo 7 del Decreto ley 393 de 1991, se someten a las siguientes reglas: i. No existe régimen de solidaridad entre quienes lo celebren, pues cada una responderá por las obligaciones que asume específicamente en virtud del convenio. ii.) Debe precisarse en ellos la propiedad de todos los resultados que se obtengan y los derechos de las partes sobre los mismos. Y, cuando la naturaleza del convenio lo exija debe pactarse las medidas conducentes para la transferencia de tecnología (art. 19 Decreto ley 591 de 1991). iii.) Deben definirse las obligaciones contractuales, especialmente las de orden laboral, que asumen cada una de las partes. iv.) Los recursos aportados para la ejecución del convenio podrán manejarse mediante encargo fiduciario o cualquier otro sistema de administración. v.) Se rigen por las normas del Derecho Privado, en armonía con los artículos 13 y 40 de la Ley 80 de 1993, por las disposiciones comerciales y civiles pertinentes, salvo lo regulado en la ley de contratación pública y en las especiales en ciencia y tecnología (decretos 393 y 591 de 1991).

Finalmente, según el artículo 8 ibídem, el convenio especial de cooperación siempre deberá constar por escrito, contendrá como mínimo cláusulas que determinen su objeto, término de duración, mecanismos de administración, sistemas de contabilización, causales de terminación y cesión; y no requiere para su celebración y validez requisitos distintos de los propios de la contratación entre particulares. Ahora bien, El artículo13 de la ley 1978 de 2019 modificó el artículo 17 de la ley 1341 estableció como objetivos del MINISTERIO TIC, 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 (…) 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 (…)".
11.- Valor del convenio	El Valor total del proyecto se estima en DOS MIL OCHENTA Y CINCO MILLONES OCHENTA Y DOS MIL NOVECIENTOS SESENTA Y NUEVE PESOS M/CTE ($2.085.082.969) aportados así: A. Aporte del MinTIC/FONDO ÚNICO El aporte del fondo será de MIL OCHOCIENTOS OCHENTA Y SEIS MILLONES NOVECIENTOS CINCUENTA Y DOS MIL NOVECIENTOS TRECE PESOS ($1.886.952.913). B. De acuerdo con la propuesta del día 13 de agosto de 2024 se agrega el aporte de la contrapartida de CIENTO NOVENTA Y OCHO MILLONES CIENTO TREINTA MIL CINCUENTA Y SEIS PESOS ($198.130.056) en especie representados en recurso humano para el desarrollo de actividades técnicas y de administración del proyecto. La fuente de los recursos son el 100%, recursos propios del Fondo Único de TIC, aportados de la: Ficha: FITI - BPIN: 2018011000589 Producto: Servicio de asistencia técnica a empresas de la industria de Tecnologías de la Información para mejorar sus capacidades de comercialización e innovación Actividad: Generar instrumentos que permitan el desarrollo de productos/servicios TI de las empresas de la industria de TI en concordancia con las necesidades del mercado, aprovechando las ventajas competitivas. CDP No. 223424 del 21 de agosto de 2024
12.- Análisis que soporta el valor estimado del Convenio	
Al no existir antecedentes concretos de proyectos de retos de innovación en temas relacionados con ciberseguridad, y para lograr una estimación precisa, el MinTIC de acuerdo con los componentes definidos en el anexo técnico, realizó un estudio de mercado, desarrollado entre el 24 de julio y el 02 de agosto de 2024. Este proceso se realizó para recoger propuestas económicas de organizaciones capacitadas para la ejecución de este tipo de proyectos y poder así, establecer un presupuesto razonable con los precios del mercado. Teniendo en cuenta que en el país se encuentran actores estratégicos en esta materia que tienen la capacidad de implementar proyectos con el impacto previsto y que cuentan con una estructura profesional que les permite realizar actividades de ciencia, tecnología e innovación, consultoría y ejecución de proyectos. El Ministerio TIC realizó un ejercicio de identificación de potenciales cotizantes, obteniendo como resultado las siguientes organizaciones que recibieron invitación para presentar cotización: • **FUNDACIÓN TECNALIA COLOMBIA:** Es un Centro de Innovación y Productividad, sin ánimo de lucro, dedicado a formular y desarrollar proyectos I+D+i con nuevas tecnologías y actividades de transferencia para responder a las necesidades del desarrollo sostenible, con una amplia experiencia de más de 12 años en el mercado nacional nos ha permitido impactar diferentes sectores logrando transferir conocimiento y generar capacidades para la innovación en el territorio nacional y regional.	

- **CINTEL:** Es un Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones – CINTEL, reconocida por la ejecución de proyectos orientados a apoyar la transformación digital de las empresas públicas y privadas. Así mismo, la Entidad presenta gran experiencia en proyectos de innovación y desarrollo tecnológico del sector TIC en Colombia, y actualmente lidera diversas iniciativas enfocadas a dinamizar la industria y la apropiación social de la tecnología.

- **BOOST BUSINESS CONSULTING:** Es una empresa de consultoría dedicada a la prestación de servicios empresariales de alto impacto, especializados en transformación digital, estrategia e innovación empresarial, modelos de negocio, auditoria, asesoría fiscal, tributaria, estándares internacionales de información financiera; construimos valor con experiencia.

- **CORPORACIÓN CONNECT BOGOTÁ REGIÓN:** Es una empresa que busca articular los actores del ecosistema de ciencia, tecnología, innovación y emprendimiento para trabajar colaborativamente en iniciativas y proyectos, basados en innovación, que transformen al país y la región, impactando en su desarrollo y competitividad.

- **FEDERACION COLOMBIANA DE LA INDUSTRIA DE SOFTWARE Y TECNOLOGIAS INFORMATICAS RELACIONADAS - FEDESOFT:** Se define como la Federación Colombiana de la Industria del Software y Tecnologías Informáticas. Esta una organización gremial trabaja por el fortalecimiento de la industria del software nacional, para que esta sea competitiva, reconocida, exitosa en el entorno internacional. Así mismo, Fedesoft trabaja en el desarrollo de políticas públicas, el impulso de la formación y la competitividad de las firmas del sector, la generación de información sectorial especializada y la exploración de oportunidades globales que posicionan a Colombia como proveedor tecnológico de talla mundial.

- **E-TRAINING**: Es una empresa con experiencia en la construcción y el desarrollo de procesos de transformación digital de la educación, orientada en crear soluciones innovadoras para la generación de proyectos educativos que fomentan la competitividad, empleabilidad y proyección institucional.

- **CYMETRIA GROUP S.A.S.:** Es una empresa enfocada a realizar negocios digitales y talento tecnológico para empresas, profesionales y startups en Latinoamérica

- **VT SAS:** Es una Firma consultora en gestión de innovación y desarrollo tecnológico con un amplio portafolio, que permite articular soluciones integrales para establecer las capacidades de innovación en las organizaciones. Dentro de su portafolio, se enfoca en diseñar y desarrollar sistemas de gestión de innovación, usando conceptos y aplicaciones de clase mundial, diseñados a la medida e implementados modularmente, lo cual permite a las organizaciones contar con resultados relevantes en el corto plazo, mientras se construyen las bases de un sistema que produzca innovaciones de muy alto impacto en el largo plazo.

- **INTERSOFTWARE:** Es una corporación que busca impulsar por el dinamismo del sector productivo, promoviendo el desarrollo y crecimiento económico de las empresas miembros, creando y aprovechando sinergias poderosas dentro de nuestra red.

- **TECNOLOGÍA E INNOVACIÓN INVERSIONES SAS - INVENTTA**: Es una empresa que desarrolla soluciones tecnológicas por medio de la innovación, disponen de un talentoso y multidisciplinario equipo de especialistas que combinan diversas y exitosas metodologías de innovación con visiones amplias, integrales y sistémicas

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

A estas diez (10) organizaciones, se les realizó una solicitud de información económica, remitiéndoseles, mediante correo electrónico, el anexo técnico del proyecto que especifica las actividades por desarrollar durante la ejecución prevista, las calidades de las actividades contempladas y los tiempos de ejecución proyectados; esto con el propósito de trasladar a los destinatarios las características mínimas requeridas para la ejecución y con ello garantizar el entendimiento de los fines y necesidades planteadas. Adicionalmente, se remitió un anexo de cotización, para que diligenciaran los valores propuestos para la ejecución de las estrategias del proyecto requiriendo además la identificación de los costos totales y los asociados a impuestos.

Como resultado de estas invitaciones, en el estudio de mercado para el proyecto de retos de ciberseguridad, se recibieron cotizaciones de siete (7) de las diez (10) organizaciones distintas invitadas, en la que cada una presentó su cotización para desarrollar los componentes requeridos por el proyecto.

Una vez recibidas las mismas, desde la Subdirección de Industria de Tecnologías de la Información, se inicia el proceso de revisión y análisis de las siete (7) cotizaciones recibidas, resumidas así:

COTIZACIONES RETOS CIBERSEGURIDAD 2024

No.	ENTIDAD OFERENTE	VALOR TOTAL
1	BOOST BUSINESS CONSULTING SAS	$2.572.274.250
2	CINTEL	$3.701.499.097
3	CORPORACIÓN CONNECT BOGOTÁ REGIÓN	$2.316.928.691
4	CYMETRIA GROUP S.A.S.	$4.029.340.000
5	FEDERACION COLOMBIANA DE LA INDUSTRIA DE SOFTWARE Y TECNOLOGIAS INFORMATICAS RELACIONADAS - FEDESOFT	$2.496.868.000
6	TECNOLOGÍA E INNOVACIÓN INVERSIONES SAS - INVENTTA	$697.340.000
7	FUNDACIÓN TECNALIA COLOMBIA	$878.750.000

Aplicando la metodología de desviación estándar, se establecieron rangos mínimos y máximos para identificar valores fuera del rango o desviados de la muestra. Con esta metodología, se determinó que cuatro (4) de las siete (7) propuestas (CINTEL, CYMETRIA GROUP S.A.S., TECNOLOGÍA E INNOVACIÓN INVERSIONES SAS – INVENTTA y FUNDACIÓN TECNALIA COLOMBIA) se encontraban por fuera del intervalo estándar establecido, por lo que fueron descartadas para el análisis.

Una vez excluidas estas propuestas, se consideraron las tres (3) ofertas restantes: la de BOOST BUSINESS CONSULTING SAS por $2.572.274.250, la de CORPORACIÓN CONNECT BOGOTÁ REGIÓN por $2.316.928.691, y la de FEDESOFT por $2.496.868.000. A continuación, se presenta el detalle de las cotizaciones:

COMPONENTE	BOOST	CONNECT	FEDESOFT
Componente 1. Identificación, clasificación y conformación de retos tecnológicos.	$209.321.000	$82.966.800	$65.450.000
Componente 2. Mapeo, selección y fortalecimiento de solucionadores tecnológicos.	$715.398.250	$404.885.600	$1.456.808.000
Componente 3. Diseño e implementación de soluciones innovadoras.	$768.145.000	$1.289.484.000	$605.710.000
Componente 4. Difusión tecnológica para el ecosistema de ciberseguridad.	$879.410.000	$539.592.291	$368.900.000
TOTAL GENERAL	**$2.572.274.250**	**$2.316.928.691**	**$2.496.868.000**

Con base en la tabla anterior, se calcula el valor promedio por cada uno de los componentes de las tres (3) cotizaciones válidas para la estimación del presupuesto del proyecto, así, se obtuvo un valor promedio de $2.462.023.647. A continuación, se presenta el detalle del cálculo:

COMPONENTE	PROMEDIO
Componente 1. Identificación, clasificación y conformación de retos tecnológicos.	$119.245.933
Componente 2. Mapeo, selección y fortalecimiento de solucionadores tecnológicos.	$859.030.617
Componente 3. Diseño e implementación de soluciones innovadoras.	$887.779.667
Componente 4. Difusión tecnológica para el ecosistema de ciberseguridad.	$595.967.430
TOTAL GENERAL	**$2.462.023.647**

Después de implementar la metodología sugerida por Colombia Compra Eficiente, en donde se calcularon los limites superiores e inferiores para descartar valores atípicos, se puede concluir que la oferta económica presentada por el Centro de Bioinformática y Biología Computacional de Colombia por valor de DOS MIL OCHENTA Y CINCO MILLONES OCHENTA Y DOS MIL NOVECIENTOS SESENTA Y NUEVE PESOS M/CTE ($2.085.082.969), se encuentra por debajo del resultado del análisis de mercado por DOS MIL CUATROCIENTOS SESENTA Y DOS MILLONES VEINTITRÉS MIL SEISCIENTOS CUARENTA Y SIETE PESOS M/CTE ($2.462.023.647), representado aproximadamente en un 85% de este estudio, por lo que el valor de la propuesta se ajusta a los precios de mercado.

Ahora bien, la propuesta del CENTRO DE BIOINFORMÁTICA Y BIOLOGÍA COMPUTACIONAL DE COLOMBIA – BIOS, por un valor total de DOS MIL OCHENTA Y CINCO MILLONES OCHENTA Y DOS MIL NOVECIENTOS SESENTA Y NUEVE PESOS M/CTE ($2.085.082.969), corresponde a, MIL OCHOCIENTOS OCHENTA Y SEIS MILLONES NOVECIENTOS CINCUENTA Y DOS MIL NOVECIENTOS TRECE PESOS M/CTE. ($1.886.952.913) de aporte en efectivo del FUTIC y a CIENTO NOVENTA Y OCHO MILLONES CIENTO TREINTA MIL CINCUENTA Y SEIS PESOS ($198.130.056) de aporte en especie del aliado representados en recurso humano para el desarrollo de actividades técnicas y de administración del proyecto.

A continuación, se detallan los rubros de contrapartida, correspondientes al personal de BIOS que se vinculará al proyecto.

CONCEPTO	JUSTIFICACIÓN	VALOR
TALENTO HUMANO	Dos (2) profesionales con maestría en el núcleo de formación de ingeniería eléctrica, electrónica, computación y afines, y amplia experiencia en desarrollo de metodologías ágiles para la ejecución de las actividades del proyecto	$ 142.243.225
	Profesional para el apoyo y seguimiento a los retos de seguridad	$ 22.862.794
	Profesional con maestría para la elaboración del plan operativo del proyecto	$ 33.024.037

Pública

TOTAL CONTRAPARTIDA	$ 198.130.056

13.- Forma de desembolso de los aportes.

a) Forma de desembolsos y requisitos:

Conforme a las condiciones del flujo de caja establecido para el cumplimiento del objeto del convenio, el Fondo Único de Tecnologías de la Información y las Comunicaciones girará al ejecutor/cooperante el valor de su aporte al convenio, en la siguiente forma:

Desembolso y fecha estimada	Valor	Requisitos para desembolso
Primer desembolso 35% 04/10/2024	$660.433.520	**FASE I PLANEACIÓN Y ALISTAMIENTO** • **Entregable 1.1** Plan de trabajo detallado que incluya todas las fases del proyecto y con un cronograma que considere los momentos de los entregables, los hitos, entregas de informes, desembolsos y demás aspectos del proyecto.
		• **Entregable 1.2** Matriz que recopile cada uno de los perfiles seleccionados junto con las hojas de vida de cada perfil. **FASE II DEFINICIÓN DE RETOS TECNOLÓGICOS** • **Entregable 2.1** Plan operativo de la convocatoria que incluya, entre otros elementos, la estrategia de comunicación y divulgación, los mecanismos para la identificación y vinculación de empresas, la metodología e instrumentos para la inscripción y validación de empresas y el cronograma del proceso. • **Entregable 2.2** Términos de referencia de la convocatoria. El CONTRATISTA podrá hacer entregas parciales de los entregables descritos para ser aprobados por el MINTIC, sin embargo, el desembolso se hará solo hasta que la totalidad de los entregables sean aprobados en sus versiones finales.

Pública

	Segundo desembolso 65% 15/11/2024	$1.226.519.393	**FASE II DEFINICIÓN DE RETOS TECNOLÓGICOS** • **Entregable 2.4** Un banco de al menos cien (100) retos con sus respectivas fichas de caracterización estructuradas, una para cada empresa, que incluya un planteamiento de las temáticas necesarias a desarrollar en los procesos de transferencia de conocimientode la Fase 2. **FASE III FORTALECIMIENTO DE SOLUCIONADORES TECNOLÓGICOS** • **Entregable 3.4** Documento con el resultado del mapeo sobre las tecnologías e innovaciones de punta en ciberseguridad (vigilancia tecnológica), que incluya la identificación de herramientas, prácticas, modelos de negocio innovadores y tendencias para tener en cuenta en los procesos de transferencia de conocimiento. • **Entregable 3.5** Plan de transferencia de conocimiento para las 45 empresas de tecnologías de la información vinculadas,

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

			sobre los micro cursos, el bootcamp y las mentorías especializadas, que incluya, entre otros elementos, los contenidos a desarrollar, las metodologías a implementar, las herramientas tecnológicas a utilizar, el cronograma y la intensidad horaria de las actividades, los mecanismos de control, evaluación y validación de la efectividad de latransferencia. **FASE IV. IMPLEMENTACIÓN DE RETOS TECNOLÓGICOS** • **Entregable 4.1** Modelo o formato de ficha para la presentación de propuesta de soluciónde retos. • **Entregable 4.3** Documento de lineamientos operativos para la selección de las diez (10) MIPYMES y sus retos, los criterios para los emparejamientos de solucionador-retador, las condiciones contractuales, técnicas yjurídicas para estos emparejamientos, el mecanismo de operación del desarrollo de lassoluciones, entre otros. **FASE V. DIFUSIÓN Y CIERRE** • **Entregable 5.1** Plan de organización y desarrollo del evento que incluya, entre otros aspectos, la planeación logística,cotizaciones y proveedores, las listas de invitados y conferencistas, los temas y actividades por desarrollar y la agenda académica.
	Cada desembolso estará sujeto a la disponibilidad de PAC y liquidez de parte de Tesorería del Fondo TIC, así mismo deberá atender los lineamientos establecidos por el Fondo Único TIC para la legalización de recursos como se explica a continuación: Para presentar las legalizaciones se deberá tener en cuenta los lineamientos establecidos por el área financiera con sus respectivos soportes que evidencien la ejecución y giros de los contratos/convenios suscritos con el equipo y aliados, (facturas, comprobantes de pago, órdenes de compra, extractos bancarios, etc.). Se deberá legalizar el 80% del primer desembolso, como condición para realizar el segundo desembolso.		

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

	Las fechas antes indicadas y los valores establecidos son una proyección de desembolsos; no obstante, se encuentran sujetos a la fecha de suscripción del futuro convenio y a la propuesta del proponente seleccionado.
b. Justificación del aporte inicial.	No aplica

14.- Criterios para seleccionar al Ejecutor/Cooperante:

El cooperante fue seleccionado teniendo en cuenta el principio rector que impone a las entidades estatales el deber de coordinar las actuaciones para el cumplimiento de los fines del estado y atendiendo la finalidad de los convenios de cooperación, es más que el cumplimiento de compromisos dirigidos a un bien común en torno al cual se suscribe el convenio. Para seleccionar al cooperante se verificó su idoneidad, considerando, entre otros, los rasgos del estudio de sector y la caracterización de la cotización recibida en el estudio de mercado adelantado por el área técnica. Estos ejercicios permitieron establecer que BIOS, cuenta con cualidades que permitirían fortalecer las condiciones necesarias para la adecuada ejecución del proyecto a saber:

Su calidad de socio estratégico del gobierno nacional y entidades territoriales para la planificación, estructuración, financiación y ejecución de proyectos sostenibles que transforman territorios.

Esta condición en un factor que genera sinergias territoriales e institucionales y que coadyuva al cumplimiento de la meta de impacto y a la descentralización del esquema de acompañamiento estructurado para esta iniciativa.

La correlación entre las competencias de la entidad aliada y el objeto del futuro convenio de cooperación.

BIOS posee experiencia probada en materia de ejecución de proyectos de alto impacto que impliquen procesos de innovación, desarrollo tecnológico y el estudio de escenarios que promuevan gestión del conocimiento. se desea destacar la siguiente experiencia con el MinTIC que resulta fundamental para el objeto del convenio que se pretende suscribir:

#	PROYECTO	OBJETO	ENTIDAD	FECHA INICIO	DURACIÓN	VALOR
1	Centro de inteligencia artificial aplicada	Aunar esfuerzos técnicos administrativos y financieros para el desarrollo de proyectos de ciencia tecnología e innovación con énfasis en los sectores estratégicos de las Direcciones del gobierno en línea, políticas y Desarrollo de TI, I+D+I, que permitan el desarrollo de los objetivos planteados en el plan estratégico del Min TIC	MinTIC	23/08/2017	12 meses	$ 7.944.877.927
2	Diseñar el Centro de Servidos Compartidos de Transformación Digital (CSCTD) para la atención de retos institucionales o empresariales a partir del uso de nuevas tecnologías tales como Inteligencia Artificial, el rediseño de los centros de excelencia y	"Diseñar el Centro de Servidos Compartidos de Transformación Digital (CSCTD) para la atención de retos institucionales o empresariales a partir del uso de nuevas tecnologías tales como Inteligencia Artificial, el rediseño de los centros de excelencia y apropiación en BigData, IoT de conformidad a las Hojas de Ruta Regionales de Transformación Digital, garantizando la	FONTIC	19/12/2019	12 meses	$ 1.970.966.877

Pública

	apropiación en BigData, IoT de conformidad a las Hojas de Ruta Regionales de Transformación Digital	formulación y ejecución de proyectos que brinden soluciones a los sectores de la economía que coadyuven al desarrollo de las empresas en sus diferentes iniciativas regionales y nacionales. Toda la información resultante usará las capacidades e infraestructura computacional de alto desempeño con la que actualmente cuenta BIOS"				
3	Implementación de la Red Nacional de Supercomputación	El objetivo principal del convenio especial de cooperación es aunar esfuerzos técnicos, administrativos y financieros, para realizar las acciones y estrategias correspondientes para la creación y articulación de la Red Nacional de Servicios de Computación de Alto Rendimiento.	MinTIC	18/02/2021	10 meses	$ 1.231.948.648
4	Resolución 00528: Por la cual se ordena un gasto como aporte	Por la cual se ordena un gasto como aporte al Centro de Bioinformática y Biología Computacional de Colombia o BIOS o CBBC con NIT 900.404.482-6.	MINTIC	24/07/2023	5 meses	$ 1.500.000.000
5	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.	Aunar esfuerzos para desarrollar un ecosistema de seguridad digital que impulse procesos de innovación y desarrollo tecnológico, mediante el estudio de escenarios que promuevan la gestión del conocimiento de los riesgos cibernéticos y las afectaciones de los incidentes de seguridad digital entre los diferentes grupos poblacionales del territorio colombiano.	MINTIC	17/11/2023	1 mes y medio	$ 5.100.000.000

Adicionalmente, BIOS está equipado con tecnología de vanguardia, incluyendo potentes sistemas informáticos, redes de alta velocidad y acceso a recursos especializados en ciberseguridad, capacidades que le permiten simulaciones complejas y tareas intensivas de analítica de datos que resultan fundamentales para soportar planes de capacitación en materia de ciberseguridad. Desde dicha óptica, poseer infraestructura de supercomputación disponible le permite abordar problemas complejos de ciberseguridad mediante el uso de técnicas de paralelismo, acelerando el tiempo de entrenamiento y de análisis de datos, condiciones especialmente útiles cuando se trata de grandes volúmenes de información y análisis de malware, condiciones objetivas que permiten a BIOS simular entornos de red y sistemas informáticos reales para que los beneficiarios del convenio practiquen sus habilidades en escenarios más cercanos a situaciones del mundo real, contribuyendo a mejorar la preparación para enfrentar amenazas reales y desarrollar habilidades prácticas.

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

BIOS es un reconocido actor del ecosistema de ciencia y tecnología de la nación, capaz de articular actores públicos y privados para la gestión de conocimiento y el impulso de procesos de alto impacto, sumando dentro sus aliados para la estructuración de planes, mejoramiento de capacidades y formación del recurso humano, con la Universidad Nacional de Colombia, la Universidad de Caldas y la Universidad Tecnológica de Pereira, contando además con acceso a recursos especializados en materia de ciberseguridad al amparo de acuerdos con actores de mercado reconocidos tales como IBM, Bulkware, Td Synnex y Lenovo, entre otros, relacionamiento que confieren a dicho Centro la capacidad para satisfacer la necesidad del Ministerio. Sin perjuicio de lo anterior, BIOS posee además otras potencialidades.

3. **Especialidad, unicidad y vínculo especial con el Ministerio de Tecnologías de la Información y las Comunicaciones**

BIOS es una entidad única en Colombia que combina una amplia gama de especialidades, incluyendo bioinformática, ciencia de datos, ciberseguridad, computación de alto rendimiento (HPC) e infraestructura tecnológica. Su misión, centrada en la generación de valor a través de la incorporación efectiva de tecnologías avanzadas en el ecosistema de tecnología del país, hace que BIOS sea un actor fundamental en el sector tecnológico y de ciberseguridad. Aquí cabe resaltar que BIOS fue creada por iniciativa de la Nación como corporación sin ánimo de lucro de carácter privado, contando con participación de MinTIC en su Junta Directiva, siendo históricamente el principal aportante del Centro.

4. **Liderazgo en Ciberseguridad**

BIOS es el líder promotor del HUB de Ciberseguridad (ubicado en el municipio de Villamaría) en concurso con la Gobernación del Departamento de Caldas. Para tal efecto, BIOS cuenta con la manifestación de un número importante de actores, tanto de la academia como del sector real, interesadas en ofrecer coordinadamente sus productos y servicios a través del HUB para fortalecer las capacidades técnicas y humanas del país en materia de ciberseguridad, así: **i.** Actores empresariales: Dragonjar, Kavantic, Data & Service, IBM, TD Synnex, Global AST, People Contact, Bulwark, IT Forensic, Fygp, Innerconsulting, Lenovo, Hispasec; **ii.** Actores académicos: Universidad de Manizales, Universidad Católica de Manizales, Universidad Católica Luis Amigó, Universidad Nacional Abierta y a Distancia, Universidad Autónoma de Manizales y Universidad de Caldas; y **iii.** Actores gremiales: Acopi, Fenalco, Fundacion Universidad Empresa, Red de Emprendimiento y ARCIS.

5. **Respaldo y soporte profesional en Ciberseguridad**

El talento humano es uno de sus mayores activos de BIOS, contando con profesionales de la ingeniería, expertos en programación, ciencia de datos, y ciberseguridad, tanto en su equipo interno, como provenientes de las universidades públicas del Eje Cafetero que concurren al Centro. En el ámbito de la ciberseguridad, BIOS ostenta un relacionamiento que le permiten acceder a conocimiento especializado desde una visión crítica fundada en las diversas tecnologías disponibles en el mercado, otorgándole la capacidad de procurar soluciones agiles en beneficio de la Nación.

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

Pública

También es importante recalcar que el aporte de contrapartida que hará BIOS al Convenio, por $198.130.056 (ciento noventa y ocho millones ciento treinta mil cincuenta y seis pesos) en especie, están representados en recurso humano con experticia en metodologías de proyectos ágiles para los temas de TI, lo que brinda respaldo profesional especializado en favor del proyecto.

6. Experiencia en materia de proyectos de alto impacto

BIOS ha demostrado su experiencia y capacidad para manejar proyectos de gran envergadura en el ámbito de la ciberseguridad, la bioinformática, la ciencia de datos y las tecnologías avanzadas. Sus proyectos en formación incluyen la creación de aulas virtuales para ofrecer cursos avanzados de tecnología propios y de las universidades vinculadas, la capacitación de empresarios en tecnología y la formación avanzada de investigadores en diversas tecnologías avanzadas. Además, ha sido ejecutor habitual y cumplido de los proyectos estratégicos de MinTIC desde 2011 y de regalías de ciencia y tecnología desde 2021.

Es de anotar también que el Ministerio TIC tiene como antecedente más cercano el Convenio Especial de Cooperación de Proyectos de Ciencia, Tecnología e Innovación No. 1257 de 2023 suscrito entre Fondo Único de Tecnologías de la Información y las Comunicaciones y el Centro de Bioinformática y Biología Computacional de Colombia.

7. Experiencia certificada en el desarrollo de proyectos con esta magnitud de impacto que dan cuenta de su capacidad operativa para abordar el proyecto a saber:

El portafolio de servicios incluido en la propuesta de BIOS permitirá que la ejecución del objeto del convenio de cooperación se promueva y ejecute en un extenso margen de la actividad económica regional.

Ahora bien, BIOS aportará como contrapartida en especie, representados en los costos directos e indirectos de equipo de apoyo a la Asistencia y Administración del Proyecto, el valor que asciende a un total de CIENTO NOVENTA Y OCHO MILLONES CIENTO TREINTA MIL CINCUENTA Y SEIS PESOS ($198.130.056).

15.- Análisis de Riesgo y forma de Mitigarlo.

Se entienden como riesgo un evento que puede generar efectos adversos y de distinta magnitud en el logro de los objetivos del Convenio o en la ejecución de éste.

La metodología planteada por Colombia Compra Eficiente indica que es necesario como punto inicial identificar el contexto en el cual interactúa la Entidad Estatal, lo que permitirá la identificación de los riesgos previsibles para el proceso de contratación objeto de estructuración. En consecuencia, previo a la elaboración de la matriz de riesgos se procedió a analizar el documento de estudios previos, la necesidad en él identificada, la estimación del presupuesto oficial, entre otros aspectos señalados por el Decreto 1082 de 2015, la documentación e información histórica remitida por el área originadora en virtud de lo indicado en la circular 011 de 2022 emitida por la Secretaría General del Ministerio de Tecnologías de la Información y las Comunicaciones.

Se deben evaluar los riesgos combinando la probabilidad de ocurrencia y el impacto del evento para:

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

(a) Asignar una categoría a cada Riesgo de acuerdo con la probabilidad de ocurrencia así: raro, improbable, posible, probable y casi cierto y valorarlos de 1 a 5 siendo raro el de valor más bajo y casi cierto el de valor más alto.

Tabla 1 - Probabilidad del Riesgo

	Categoría	Valoración
Probabilidad	Raro (puede ocurrir excepcionalmente)	1
	Improbable (puede ocurrir ocasionalmente)	2
	Posible (puede ocurrir en cualquier momento futuro)	3
	Probable (probablemente va a ocurrir)	4
	Casi cierto (ocurre en la mayoría de las circunstancias)	5

(b) Determinar el impacto del Riesgo, utilizando la Tabla 2, analizando los siguientes criterios: (i) la calificación cualitativa del efecto del Riesgo, y (ii) la calificación monetaria del Riesgo, la cual corresponde a la estimación de los sobrecostos ocasionados por la ocurrencia del Riesgo como un porcentaje del valor total del presupuesto del contrato. Se debe escoger la mayor valoración resultante de los criterios (i) y (ii) para determinar el impacto del Riesgo.

Tabla 2 - Impacto del Riesgo

Valoración	Insignificante	Menor	Moderado	Mayor	Catastrófico
	1	2	3	4	5
Calificación cualitativa	Obstruye la ejecución del contrato de manera intrascendente	Dificulta la ejecución del contrato de manera baja, aplicando medidas mínimas se puede lograr el objeto contractual	Afecta la ejecución del contrato sin alterar el beneficio para las partes	Obstruye la ejecución del contrato sustancialmente, pero, aun así permite la consecución del objeto contractual	Perturba la ejecución del contrato de manera grave imposibilitando la consecución del objeto contractual
Calificación monetaria	Los sobrecostos no representan más del uno por ciento (1%) del valor del contrato	Los sobrecostos no representan más del cinco por ciento (5%) del valor del contrato	Genera un impacto sobre el valor del contrato entre el cinco (5%) y el quince por ciento (15%).	Incrementa el valor del contrato entre el quince (15%) y el treinta por ciento (30%)	Impacto sobre el valor del contrato en más de treinta por ciento (30%)

(c) Para cada Riesgo se deben sumar las valoraciones de probabilidad e impacto, para obtener la valoración total del Riesgo

Tabla 3 – Valoración del Riesgo

Valoración del Riesgo	Categoría
8, 9 y 10	Riesgo extremo
6 y 7	Riesgo alto
5	Riesgo medio
2, 3 y 4	Riesgo bajo

(d) Finalmente, la valoración completa del riesgo permite establecer una categoría a cada uno de ellos para su correcta gestión.

Pública

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

GARANTÍA DE CUMPLIMIENTO

De conformidad lo establecido por el artículo "2.2.1.2.3.1.7. Garantía de cumplimiento" del decreto 1082 de 2015, y dado que se evidencia la necesidad, en términos de ejecución del futuro convenio especial de cooperación, de amparar a la entidad mediante garantías, se considera que se deberá exigir para cubrir cualquier hecho constitutivo de incumplimiento los amparos que a continuación se señalan, correspondiendo al asociado la obligación de presentar la garantía de cumplimiento en original al MINTIC, dentro de los tres (3) días hábiles siguientes contados a partir de la firma del convenio. Esta garantía tendrá las siguientes características:

CARACTERISTICA	CONDICIÓN
TIPO DE GARANTÍA	Cualquiera de las clases permitidas por el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, a saber: (i) Contrato de seguro, contenido en una póliza para Entidades Estatales; (ii) Patrimonio autónomo; (iii) Garantía Bancaria.
TOMADOR	Asociado
BENEFICIARIO / ASEGURADO	Fondo Único de Tecnologías de la Información y las Comunicaciones (Nit. 800.131.648-6) y Ministerio de Tecnologías de la Información y las Comunicaciones (Nit. 899.999.053-1)
AMPAROS	

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

Pública

AMPARO	VIGENCIA	VALOR ASEGURADO
Cumplimiento general del convenio	Por el plazo de ejecución del convenio y seis (6) meses más. En todo caso, este amparo deberá mantenerse vigente hasta la liquidación del contrato.	Por el veinte por ciento (20%) del valor total del convenio
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales.	Por el plazo de ejecución del contrato y tres (3) años más.	Por el cinco por ciento (5%) del valor total del convenio.
Calidad del servicio	Por seis (6) meses contados a partir de la terminación del convenio.	Por el diez (10%) por ciento del valor total del conveni.

Nota 1: El asociado está obligado a restablecer el valor de la garantía cuando esta se vea reducida por razón de las reclamaciones que efectúe la Entidad, así como, a ampliar las garantías en los eventos de adición y/o prórroga del convenio.

Nota 2: El asociado deberá presentar el certificado de no expiración de la póliza por falta de pago de la prima, lo anterior bajo los términos del artículo 2.2.1.2.3.2.5 del Decreto 1082 de 2015.

PÓLIZA DE RESPONSABILIDAD CIVIL EXTRACONTRACTUAL -RCE.

De acuerdo con el Artículo 2.2.1.2.3.1.8 del decreto 1082 de 2015, cubrimiento de la responsabilidad civil extracontractual, "La Entidad Estatal debe exigir en los contratos de obra, y en aquellos en que por su objeto o naturaleza lo considere necesario con ocasión de los Riesgos del contrato, el otorgamiento de una póliza de responsabilidad civil extracontractual que la proteja de eventuales reclamaciones de terceros derivadas de la responsabilidad extracontractual que surja de las actuaciones, hechos u omisiones de su contratista. La Entidad Estatal debe exigir que la póliza de responsabilidad extracontractual cubra también los perjuicios ocasionados por eventuales reclamaciones de terceros derivadas de la responsabilidad extracontractual que surjan de las actuaciones, hechos u omisiones de los subcontratistas autorizados o en su defecto, que acredite que el subcontratista cuenta con un seguro propio con el mismo objeto y que la Entidad Estatal sea el asegurado". Así las cosas, y de acuerdo con el contenido de las obligaciones específicas a cargo del futuro asociado, se recomienda la exigencia de una garantía, con las siguientes características:

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

<table>
<tr><th>CARACTERISTICA</th><th>CONDICIÓN</th></tr>
<tr><td>TIPO DE GARANTÍA</td><td>Contrato de seguro, el cual reúna los requisitos y términos establecidos en el Decreto 1082 de 2015.</td></tr>
<tr><td>TOMADOR</td><td>o Asociado</td></tr>
<tr><td>ASEGURADO</td><td>Fondo Único de Tecnologías de la Información y las Comunicaciones (Nit. 800.131.648-6), Ministerio de Tecnologías de la Información y las Comunicaciones (Nit. 899.999.053-1) y el asociado.</td></tr>
<tr><td>BENEFICIARIO</td><td>Fondo Único de Tecnologías de la Información y las Comunicaciones (Nit. 800.131.648-6), Ministerio de Tecnologías de la Información y las Comunicaciones (Nit. 899.999.053-1) y terceros afectados.</td></tr>
<tr><td>AMPAROS</td><td>
<table>
<tr><th>AMPARO</th><th>VIGENCIA</th><th>VALOR ASEGURADO</th></tr>
<tr><td>El amparo Responsabilidad Civil Extracontractual - RCE deberá constituirse de acuerdo con las coberturas y requisitos establecidos en el Decreto 1082 de 2015 sin sublimitarse.

El seguro deberá incluir los siguientes amparos:
o Predios, Laborales y Operaciones
o Cobertura expresa de perjuicios por daño emergente y lucro cesante.
o Cobertura expresa de perjuicios extrapatrimoniales.
o Cobertura expresa de la responsabilidad surgida por actos de contratistas y subcontratistas.
o Cobertura expresa de amparo patronal.
o Cobertura expresa de vehículos propios y no propios.</td><td>La vigencia de esta garantía deberá ser igual al periodo de ejecución del convenio.</td><td>El valor asegurado corresponderá a 300 SMLMV</td></tr>
</table>
</td></tr>
</table>

Nota 1: El asociado está obligado a restablecer el valor del seguro cuando esta se vea reducida por razón de las reclamaciones que efectúe la Entidad y/o terceros afectados, así como, a ampliar las garantías en los eventos de adición y/o prórroga del convenio.

Nota 2: El asociado deberá entregar a la Entidad el respectivo soporte de pago de la póliza.

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

17. Indicación 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 159 del Decreto 1150 de 2013.

Para el análisis de la aplicación de los Acuerdos Comerciales y los tratados de libre comercio vigentes para el Estado Colombiano, se verificó según la información publicada en las páginas web del Ministerio de Comercio, Industria y Turismo y en el SECOP, el cumplimiento de los factores establecidos en el Literal D y Anexo 3 del Manual para el Manejo de Acuerdos Comerciales en Procesos de Contratación emitido por Colombia Compra Eficiente, determinándose que a la presente contratación no le aplican los tratados de libre comercio y acuerdos internacionales teniendo en cuenta que se trata de Contratación Directa.

18.- Certificado de disponibilidad presupuestal (CDP):	No. 223424		Fecha: 21 de agosto de 2024	
19.- Vigencias futuras:	No. Oficio	N. A.	Año	Cuantía por año
			N. A.	N. A.
	No. de aprobación	N. A.	N. A.	N. A.
			N. A.	N. A.
			N. A.	N. A.

20.- Firmas autorizadas:	
Firma responsable Jefe de la Dependencia Solicitante María Lucía Flórez Jiménez Cargo: Directora Economía Digital Fecha: Septiembre 2024	Firma responsable Supervisor Andrés Enrique Galindo Bernal Cargo: Subdirector de Industria TI Fecha: Septiembre 2024

Nota: En el evento que las personas autorizadas sean la misma, diligenciar únicamente en el siguiente recuadro:

ANEXOS

Cronograma de flujo de desembolsos

Concepto	Fecha	Valor
Primer desembolso	04/10/2024	$660.433.520
Segundo desembolso	15/11/2024	$1.226.519.393
	Total, aporte FUTIC	$1.886.952.913

Listado de documentos anexos al Formato de Estudios Previos

Documentos Anexos	
Documentos	No. de folios
Certificado de Disponibilidad Presupuestal (Cuando el convenio lleve erogación presupuestal a	

Pública

cargo del Ministerio –Fondo Único de Tecnologías de la Información y las Comunicaciones).	
Análisis del Sector	
Anexo Técnico	
Análisis de garantías (si aplica)	

"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

Memorias de cálculo	
Propuesta técnica BIOS	
Fotocopia de la Cédula del Representante Legal.	

REGISTRO DE FIRMAS ELECTRONICAS

Estudio Previo Ciberseguridad 17.09.2024

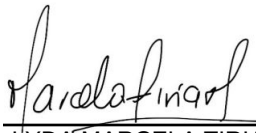
Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20240917-144104-9277b1-16009130
Estado: Finalizado

Creación: 2024-09-17 14:41:04
Finalización: 2024-09-18 08:54:53

Escanee el código para verificación

Revisión: Lyda Marcela Tiria Medina Contratista Subdireccion de Industria de TI



LYDA MARCELA TIRIA MEDINA
1052385544
ltiria@mintic.gov.co
CPS- Abogada
Subdirección de Industria de TI

Elaboración: Andrés Ricardo García Soto Contratista SITI



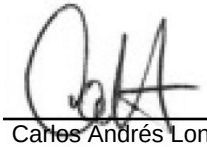
ANDRES RICARDO GARCIA SOTO
86083502
agarcias@mintic.gov.co
CONTRATISTA
SUBDIRECCIÓN DE INDUSTRIA TI - MINTIC

Elaboración: César Mauricio Cortés Alarcón Contratista SITI



Cesar Mauricio Cortes Alarcon
80221518
ccortes@mintic.gov.co
Contratista DED SITI
Ministerio TIC

Elaboración: Carlos Andrés Londoño Zuluaga Contratista SITI



Carlos Andrés Londoño Zuluaga
16079899
clondono@mintic.gov.co
Contratista
Subdirección de Industria de Tecnologías de la Información

REGISTRO DE FIRMAS ELECTRONICAS

Estudio Previo Ciberseguridad 17.09.2024

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

Id Acuerdo: 20240917-144104-9277b1-16009130

Estado: Finalizado

Creación: 2024-09-17 14:41:04

Finalización: 2024-09-18 08:54:53

Escanee el código para verificación

Firma: Maria Lucía Flórez Jiménez- Directora de Economía Digital



María Lucía Flórez Jiménez
1010198800
mlflorez@mintic.gov.co
Directora de Economía Digital
MinTIC

Firma: Andres Enrique Galindo Bernal Subdirector de Industria de TI



ANDRES ENRIQUE GALINDO BERNAL
79900265
aegalindo@mintic.gov.co
Subdirector de Industria de TI
MinTIC

Revisión: Carlos Felipe Gomez Pelaez Contratista Subdireccion de Industria de TI



Carlos Felipe Gomez Pelaez
CC94472127
cgomezp@mintic.gov.co

REPORTE DE TRAZABILIDAD

Estudio Previo Ciberseguridad 17.09.2024

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

Id Acuerdo: 20240917-144104-9277b1-16009130
Creación: 2024-09-17 14:41:04
Estado: Finalizado
Finalización: 2024-09-18 08:54:53

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	Carlos Andrés Londoño Zuluaga clondono@mintic.gov.co Contratista Subdirección de Industria de Tecnologías	Aprobado	Env.: 2024-09-17 14:41:14 Lec.: 2024-09-17 14:43:08 Res.: 2024-09-17 14:43:26 IP Res.: 186.81.88.13
Elaboración	Cesar Mauricio Cortes Alarcon ccortes@mintic.gov.co Contratista DED SITI Ministerio TIC	Aprobado	Env.: 2024-09-17 14:43:26 Lec.: 2024-09-17 14:43:46 Res.: 2024-09-17 14:45:39 IP Res.: 186.119.99.108
Elaboración	ANDRES RICARDO GARCIA SOTO agarcias@mintic.gov.co CONTRATISTA SUBDIRECCIÓN DE INDUSTRIA TI - MINTIC	Aprobado	Env.: 2024-09-17 14:45:39 Lec.: 2024-09-17 14:45:54 Res.: 2024-09-17 14:46:24 IP Res.: 45.189.119.65
Revisión	LYDA MARCELA TIRIA MEDINA ltiria@mintic.gov.co CPS- Abogada Subdirección de Industria de TI	Aprobado	Env.: 2024-09-17 14:46:24 Lec.: 2024-09-17 15:09:18 Res.: 2024-09-17 15:09:22 IP Res.: 181.51.34.76
Revisión	Carlos Felipe Gomez Pelaez cgomezp@mintic.gov.co	Aprobado	Env.: 2024-09-17 15:09:22 Lec.: 2024-09-17 15:49:08 Res.: 2024-09-17 16:17:30 IP Res.: 190.145.189.98
Firma	ANDRES ENRIQUE GALINDO BERNAL aegalindo@mintic.gov.co Subdirector de Industria de TI MinTIC	Aprobado	Env.: 2024-09-17 16:17:30 Lec.: 2024-09-17 16:18:39 Res.: 2024-09-17 16:18:49 IP Res.: 190.145.189.98
Firma	María Lucía Flórez Jiménez mlflorez@mintic.gov.co Directora de Economía Digital MinTIC	Aprobado	Env.: 2024-09-17 16:18:49 Lec.: 2024-09-18 08:54:50 Res.: 2024-09-18 08:54:53 IP Res.: 190.145.189.98

ANALISIS DEL SECTOR

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
DIRECCIÓN DE ECONOMIA DIGITAL

PROYECTO RETOS DE INNOVACIÓN TECNOLÓGICA EN CIBERSEGURIDAD

2024

Contenido

1. INTRODUCCIÓN 3
2. ASPECTOS GENERALES DEL MERCADO 4
2.1. Aspecto económico 10
2.2. Análisis Técnico 9
2.3. Análisis regulatorio 20
3. ANALISIS DE LA DEMANDA 15
4. ANÁLISIS DE LA OFERTA 19
5. ESTUDIO DE MERCADO 38

ANALISIS DE SECTOR

OBJETO: 33200401811 – Aunar esfuerzos técnicos, administrativos, y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.

Duración estimada del proyecto: Desde la suscripción del acta de inicio y hasta el 31 de diciembre de 2024

Presupuesto estimado del Convenio: El Valor total del proyecto se estima en DOS MIL OCHENTA Y CINCO MILLONES OCHENTA Y DOS MIL NOVECIENTOS SESENTA Y NUEVE PESOS M/CTE ($2.085.082.969).

1. INTRODUCCIÓN

De conformidad con los artículos 38 y 58 de la Ley 489 de 1998, los ministerios son entidades de la rama ejecutiva del poder público del orden nacional, del sector central encargadas de formular y adoptar las políticas, planes generales, programas y proyectos del sector administrativo que dirigen. Por su parte, el Ministerio de Tecnologías de la Información y las Comunicaciones, de acuerdo con lo establecido por el artículo 17 de la Ley 1341 de 2009, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. Entre sus funciones está la de incrementar y facilitar el acceso de todos los habitantes del territorio nacional a las Tecnologías de la Información y las Comunicaciones, fortaleciendo su capacidad de respuesta y de adaptación ante la Ciberseguridad y Ciberdefensa, garantizando así un entorno digital seguro y confiable para todos sus ciudadanos y organizaciones.

En consecuencia, el presente proceso, está sujeto a lo establecido en la Constitución Política, el Estatuto General de Contratación de la Administración Pública contenido en la Ley 80 de 1993, la Ley 1150 de 2007, el Decreto 1082 de 2015, y demás normas que los reglamentan, modifican o adicionan al estudio previo, sus anexos y demás documentos del proceso desde la perspectiva legal, comercial, financiera, organizacional, técnica, y de Análisis de Riesgo; el Estatuto Anticorrupción contenido en la Ley 1474 de 2011. Así mismo, el Estatuto General de Contratación de la Administración Pública, desde su entrada en vigor, aplica para los contratos que la Nación y sus entidades descentralizadas celebren en ocasión al desarrollo de actividades de Ciencia y Tecnología los artículos 2, 8, 9, 17 y 19 del Decreto ley 591 de 1991 y en el Decreto ley 393 de 1991.

Es así, y con el propósito de satisfacer las necesidades identificadas por el MinTIC – Fondo Único de TIC, se desarrolla el presente documento con los aspectos generales del mercado tendiente a la identificación del sector económico al que pertenecen los actores que detentan las condiciones técnicas financieras y experiencia suficiente para ejecutar las actividades que integran el proyecto denominado **RETOS DE INNOVACIÓN TECNOLÓGICA EN CIBERSEGURIDAD**. Este enfoque es esencial para analizar los ingresos que permitan su sostenimiento y desarrollo a largo plazo, su interacción con el mercado y responden a las exigencias de un entorno económico globalizado y digitalmente conectado.

Por consiguiente, este análisis contribuye, a establecer el contexto de las oportunidades disponibles en el mercado según la atención de las necesidades definidas por la entidad. Para los efectos previamente mencionados, el presente documento aborda cuatro (4) capítulos: (i) Aspectos generales del mercado, incluyendo el económico, técnico y regulatorio (ii) Análisis de la demanda, mostrando la necesidad y cómo satisfacerla (iii) Análisis de la oferta, por medio de la cual se describe quienes y cómo pueden proveer los servicios requeridos y iv) el Estudio de mercado, con el análisis de la información obtenida y la justificación de la selección de la propuesta.

Este enfoque es esencial para analizar los ingresos que permitan su sostenimiento y desarrollo a largo plazo, su interacción con el mercado y responden a las exigencias de un entorno económico globalizado y digitalmente conectado.

Es así, como el presente documento forma parte integral del estudio previo para la contratación directa cuyo objeto es: Aunar esfuerzos técnicos, administrativos, y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información. y se proyecta siguiendo los lineamientos emitidos por Colombia Compra Eficiente, a través de la Guía para Elaboración de Estudios del Sector.

2. ASPECTOS GENERALES

2.1 Aspectos Generales en el Sector de Ciberseguridad

La definición de ciberseguridad es un término relativamente nuevo, que surgió durante la revolución de las tecnologías de la información y comunicación (TIC), y su concepto se ha visto impactado durante los últimos años. Dentro de un concepto en general se define "*es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica"* [1] (Kaspersky,2022).

La ciberseguridad durante en esta era digital se convierte en una prioridad estratégica para Colombia, donde la protección de datos y la infraestructura tecnológica son esenciales para el desarrollo económico de las diferentes empresas país. Las amenazas cibernéticas también aumentaron con el auge de la digitalización, por lo que el gobierno nacional ha implementado políticas y normativas para salvaguardar la información y los sistemas críticos que se puedan presentar.

De esta forma, la ciberseguridad ha tomado cada vez mayor relevancia en el sector industrial y empresarial, por lo que se han implementado estratégicas innovaciones para proteger sistemas, equipos y redes. Así, la relación entre la ciberseguridad y la innovación se ha implementado bajo dos corrientes: la ciberseguridad permite que la innovación sea considerada en casi todos los sectores de la economía digital al generar un ambiente de confianza en los usuarios de las tecnologías de la información y, por el otro, las diversas innovaciones tecnológicas permiten a las empresas dedicadas a ciberseguridad generar dispositivos y sistemas para proteger las empresas, redes y datos.

Bajo los anteriores principios, se enmarca el proyecto por desarrollar, relacionado con actividades del sector de servicios especializados en Tecnologías de la Información y las comunicaciones -TIC, tal como es la identificación, formulación y puesta en marcha de soluciones digitales, fundamentados en la necesidad de comprender los retos tecnológicos que enfrentan las MIPYMES del país en materia de ciberseguridad y las capacidades del sector de las industrias de tecnologías de la información para atender de manera innovadora estos retos, contribuyendo de este modo al fortalecimiento de un ecosistema que aproveche el conocimiento y las tendencias tecnológicas para estimular las dinámicas de oferta y demanda en torno al negocio de la ciberseguridad.

Alineados bajo el anterior objetivo, y considerando como el sector de las Tecnologías de la Información y las Comunicaciones se consolida como un sector estratégico, de alto crecimiento y desarrollo tanto a nivel mundial como en el país, el gobierno, por medio del Plan Nacional de Desarrollo 2022 -2026 "Colombia Potencia Mundial de la Vida" en su catalizador Habilitadores que potencian la seguridad humana y las oportunidades de bienestar- eje: Seguridad y Justicia, establece: Habilitadores que permiten contar con un entorno en donde predomine la legitimidad, la transparencia y la integridad. Contribuyen a tener un ecosistema digital confiable y seguro en el cual se puedan desarrollar actividades

1 Kaspersky Lab. (2022). ¿Qué es la ciberseguridad? AO Kaspersky Lab. Recuperado de https://latam.kaspersky.com/resource-center/definitions/what-is-cybersecurity

sociales y económicas, y *"Se diseñará e implementará una estrategia para adelantar las medidas enfocadas a salvaguardar la infraestructura crítica cibernética del país.* ***Se protegerá la información de las entidades gubernamentales y de las personas de posibles ataques cibernéticos y delitos informáticos****, bajo principios de resiliencia y rápida recuperación".*

De otra parte, y enmarcado dentro del eje estratégico de Transformación Productiva, Internacionalización y Acción Climática, se plantea desde el PND en el Cierre de brechas tecnológicas en el sector productivo, bajo la implementación con una Política de Reindustrialización, se plantea incrementar la (...) "innovación empresarial a partir del escalamiento de capacidades, condiciones y servicio de ***extensión tecnológica que permitan el cierre de brechas tecnológicas para el desarrollo productivo regional, incluyendo el uso de datos y de tecnologías digitales".***

Todo lo anterior, mediante la aplicación de esquemas de seguridad digital, y el uso de los conceptos de ciberseguridad y ciberdefensa. De igual forma, para la identificación, gestión, tratar y mitigar los riesgos en el entorno digital, se asegura una responsabilidad compartida, y la participación de alianzas que involucren los sectores público- privado.

En conclusión, el enfoque de innovación abierta adoptado por el presente proyecto promueve no solo la creación de nuevas soluciones tecnológicas, sino también facilita un ambiente de transparencia y confianza en el sector empresarial, esencial para abordar y solucionar eficazmente las experiencias negativas por los principales riesgos en la materia, e identificar los componentes de una estrategia integral que contribuya en mejorar el desempeño de las empresas en el mercado.

2.2 Aspectos Económicos

2.2.1 Estructura del Análisis Económico del Sector

Para adelantar el estudio del sector al que pertenecen los servicios que integran el proyecto- analizando aspectos generales económicos, técnicos, internacionales y legales abordados de manera posterior en el documento-, y que la Entidad requiere para la suscripción del Convenio, se identificaron los servicios requeridos en el marco de la ejecución, para lo cual se identifican con los códigos enunciados en el Clasificador de Bienes y servicios de las Naciones Unidas – UNSPSC- en el tercer nivel, como se indica a continuación:

Grupo	Segmento	Familia	Clase	Código
Servicios (F)	Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	Servicios de asesoría de gestión	Servicios de asesoramiento sobre tecnologías de la información	80101507
			Gerencia de proyectos	80101600
	Servicios basados en ingeniería, investigación, y tecnología	Entrega de servicios de tecnología de información	Servicios de administración de acceso	81161500
		Servicios Informáticos	Sistema Recuperación Información	81111900
		Servicios Informáticos	Servicios de sistemas y administración de componentes de sistemas	81111800

2.2.2 Aspectos Económicos Ciberseguridad en el Mundo

La velocidad con la que los gobiernos y las empresas se apoyan en la tecnología para administrar y desempeñar sus funciones desde la prestación de bienes y servicios públicos hasta los procesos comerciales crece a un ritmo exponencial.

Esta situación ha acelerado la adopción de una variedad de plataformas y dispositivos conectados en entornos con poca protección contra la intrusión cibernética, generando la oportunidad para que información sea robada, manipulada o dañada en perjuicio de sus propietarios.

En el actual contexto digital, la interconectividad con el apoyo de las tecnologías de la información (TI) y la infraestructura digital ha generado mayor interdependencia y vulnerabilidad en el mundo frente a amenazas que atentan contra la integridad, seguridad y confiabilidad de la información, lo que representa grandes gastos económicos bajo un enfoque reactivo más que proactivo, organizado y estructurado.

De acuerdo con el informe líder Cost of a Data Breach Report -2021, informe de referencia líder a nivel mundial, para el analizó una base de 537 fugas reales de información, y realizó su cálculo en términos de costos de 2020 a 2021 a nivel mundial, obteniendo como resultado: una filtración de datos pasó de USD $3.86 millones a USD $4.24 millones, siendo las regiones con el mayor aumento promedio del costo son América Latina (aumento del 52.4%), Sudáfrica (aumento del 50%), Australia (aumento del 30.2%), Canadá (aumento del 20%). Además de los costos económicos, los ataques informáticos también tienen afectaciones a la infraestructura crítica, la cohesión social, y en términos empresariales, cada ataque cibernético exitoso dirigido a una pyme podría ocasionar para algunas significaría un daño que ocasionaría el cierre de la empresa[2] (2022, UNAM).

Entre otros datos que soportan las anteriores afirmaciones[3] (EDWIN DACARET,2023), y que reflejan las implicaciones en termino económicos de la importancia del sector de ciberseguridad en las empresas se encuentran las siguientes:

- Los delitos cibernéticos muestran que un mínimo de 422 millones de personas se vio afectadas, con 800.944 denuncias registradas en 2022, y casi 33.000 millones de cuentas fueron estimadas a ser vulneradas en 2023, con un costo en 8 billones de dólares (según los registros de delitos en Internet del FBI)4.

- Se espera que en los próximos cinco años se produzca un aumento del 15 % en los costes de la ciberdelincuencia, alcanzando los 10,5 billones en 2025 (Según Cybercrime Magazine).
- El indicador 'Costo estimado del cibercrimen' del mercado de la ciberseguridad ha aumentado continuamente en los últimos años, este indicador global aumentará continuamente entre 2023 y 2028 en un total de 5,7 billones de dólares (+69,94%). Después del undécimo año consecutivo de aumento, se estima que el indicador alcanzará los 13,82 billones de dólares estadounidenses y, por tanto, una nueva alza en 2028.

De otra parte, y como un *factor positivo* la necesidad de ciberseguridad impulsa la innovación y el desarrollo tecnológico, manifestado en nuevas tecnologías y métodos para proteger sistemas y datos, lo que refleja un impacto económico representativo a nivel global, y significativo en la industria en costos, pero necesarios para protegerse de las amenazas cibernéticas. **Sus impactos económicos** se pueden observar en varios aspectos, tales como:

- **Costos de Inversión en Seguridad,** los gobiernos y las empresas pueden invertir grandes sumas de dinero en soluciones de ciberseguridad, que incluyen software, hardware, servicios de consultoría y equipos especializados.

---

2 UNAM. 2022. Vigilancia tecnológica en CIBERSEGURIDAD. https://www.icat.unam.mx/wp-content/uploads/2022/09/Vigilancia_Tecnologica_en_Ciberseguridad_Boletin.pdf

3 https://es.linkedin.com/pulse/ciberseguridad-costos-y-roi cisoglobalatam#:~:text=Statista%20pronostica%20que%20el%20indicador,estadounidenses%20(%2B69%2C94%25).

4 https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

- **Costos de Incidentes de Seguridad,** los efectos representados en los ataques cibernéticos pueden resultar en costos directos e indirectos significativos como: la pérdida de datos, el daño a sistemas y la interrupción de operaciones, interrupción de servicios y operaciones empresariales, resultando en pérdidas de productividad y, por ende, en pérdidas económicas (directos), la pérdida de confianza de los clientes, daños en la imagen empresarial u organizaciones y posibles sanciones regulatorias (indirectos).
- **Crecimiento del Mercado de Ciberseguridad,** a partir de la creciente demanda de protección contra amenazas cibernéticas se espera que el valor global del mercado de ciberseguridad crezca significativamente en los próximos años.
- **Nuevos costos y tipos de Seguro**: Las pólizas de seguro para ciberseguridad se han convertido en una opción cada vez más común para las empresas, lo que también refleja la importancia económica del riesgo cibernético. Los costos de estos seguros pueden variar según el nivel de cobertura y la exposición al riesgo.
- **Cumplimiento de regulaciones, l**as leyes y regulaciones sobre protección de datos y ciberseguridad, han generado costos adicionales a las empresas en términos de cumplimiento, implementación de medidas de seguridad y posibles sanciones por incumplimiento, como el GDPR en Europa o la CCPA en California[5].
- **Demanda de Profesionales,** La tendencia mundial se orienta por una alta demanda de profesionales en ciberseguridad, lo que ha generado a un aumento en los salarios y a creación de nuevas oportunidades laborales para este campo.

2.2.3 Aspectos Económicos Ciberseguridad en Colombia

Aunque se presenta el interés y el entusiasmo en el sector industrial TI y en las empresas colombianas por implementar programas de seguridad tecnológica de la información, reflejado en el incremento de los presupuestos destinados a la ciberseguridad, es desafiante que el progreso en este campo para mejorarla, y aún está estancado en muchos casos.
Dentro de los principales hallazgos asociados a encuestas en la materia realizadas en Colombia, se identificaron los siguientes aspectos6 (PWC, 2024):

- Tendencia en el aumento en el número de brechas y los costos en términos de seguridad digital.
- Solo una cuarta parte de las organizaciones en Colombia cuenta con un plan estructurado de gestión de riesgos para abordar los desafíos de los proveedores de servicios en la nube.
- Más del 30 % de las empresas no sigue sistemáticamente lo que deberían ser prácticas estándar de ciberdefensa.
- Gestionan los riesgos de mejor manera optimizan las soluciones de seguridad y posicionado las empresas tener una mayor productividad y un crecimiento más rápido, superando a la competencia mientras implementan nuevas tecnologías.
- En Colombia los riesgos de ciberseguridad se ubican detrás de los riesgos derivados de la volatilidad macroeconómica, mientras a nivel global, el riesgo cibernético se ubica detrás de los riesgos digitales y tecnológicos.

De otra parte, y de acuerdo con la Estrategia Nacional Digital de Colombia 2023 – 2027, en Colombia, al igual que en otros países del mundo, se experimenta un incremento notable en ataques cibernéticos, y para el año 2022 se presentó una variación del 149% en las muestras de malware analizadas respecto al año 2021 (Según el Centro Cibernético Policial en su Balance de Ciberseguridad 2022), de acuerdo con el Índice de Exposición a la Ciberseguridad 2020 de Password Managers, ***Colombia ocupó el puesto 54 de 108 países en su ranking global*** y el quinto país más expuesto de Sudamérica.

5 https://www.entrust.com/es/resources/learn/ccpa-vs-gdpr
6 PwC (2024). Global Digital Trust Insights de 2024 de PwC Colombia Tendencias de la ciberseguridad en Colombia: Poniendo la seguridad en el centro de la innovación. https://www.pwc.com/co/es/publicaciones/digital-trust-insights/2024/digital-trust-insights-2024-pwc-colombia.pdf
7 Línea de la Estrategia: Seguridad y confianza digital para la garantía de las libertades y el desarrollo integral de las personas.

Comprendiendo la importancia de disponer de estadísticas sobre ciberseguridad, puesto que permiten a las empresas evaluar los riesgos potenciales a los que se encuentran expuestas, y a su vez y priorizar las medidas de protección, la Estrategia Nacional Digital de Colombia 2023 – 2026 presenta las siguientes cifras en la materia para Colombia:

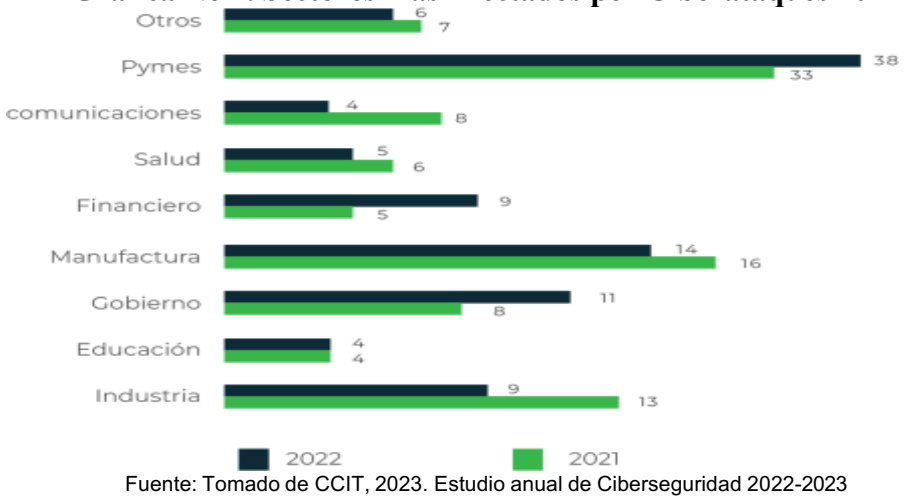
- El sector Industrial, las entidades públicas y los ciudadanos han sido los más afectados por la creciente ciberdelincuencia en el país. El total de delitos cibernéticos denunciados por el público en general para noviembre del 2021 ante la fiscalía general de la Nación, las policías judiciales del Cuerpo Técnico de Investigación (CTI) y la Policía Nacional (DIJIN-SIJIN), correspondió a 46.527 denuncias por distintos delitos, 21 % más que lo registrado en 2020 (Cámara Colombiana de Informática y Telecomunicaciones - CCIT, 2022). Ya en 2022 las denuncias por ciberdelitos crecieron un 26 % con respecto al 2021, siendo el hurto por medios informáticos el delito con mayor número de registros (un total de 25.413) (Cámara Colombiana de Informática y Telecomunicaciones - CCIT, 2023).
- Es necesario mejorar el uso seguro de los dispositivos y tecnologías digitales de los colombianos para que tengan una mayor protección en el entorno digital. De acuerdo con la Encuesta ENTIC de 2021, en el momento de proteger la información de los dispositivos con los que se accede a Internet, la proporción de personas que definen contraseñas seguras es del 60,9 % y la proporción de personas que utilizan algún software de protección como un antivirus es del 43,4 %.
- Aunque el país refleja esfuerzos en el sector de los últimos años, se presentan debilidades en medidas organizativas y el desarrollo de infraestructura en materia de ciberseguridad de acuerdo con el reporte 2020 del Global Cibersecurity Index (GCI) (Unión Internacional de Telecomunicaciones - UIT, 2020), Colombia obtuvo un puntaje de 6,67 de 20 puntos (medidas legales y organizacionales en ciberseguridad), lo que representa una menor puntuación, y de acuerdo con el Child Online Safety Index, el país presenta un bajo desempeño en el desarrollo de infraestructuras de ciberseguridad.

Las MYPES el Sector más afectado por los ciberataques en COLOMBIA

Según los últimos estudios realizados para el sector ciberseguridad en Colombia, en el periodo 2019-2022, el año con mayor incremento en las cifras de ciberdelito, con una diferencia de 14.000 casos respecto 2021, superado por 2020, con un incremento anual de más de 22.000 casos en comparación con el 2019.

De manera relevante los estudios ***indican que las pequeñas y medianas industrias (Sector PYME), sigue siendo el sector más afectado por los ciberataques, identificando como una de sus principales causas:*** débiles estrategias de ciberseguridad implementadas por los responsables, no identificación como factor estratégico, no inclusión e incorporación dentro de la cadena productiva la necesidad de invertir o planear recursos en la operación y las ventajas que representan su aplicación y puesta en marcha.

Grafica No 1. Sectores más Afectados por Ciberataques 2021-2022



Fuente: Tomado de CCIT, 2023. Estudio anual de Ciberseguridad 2022-2023

Una de las grandes amenazas de las pymes en cuanto a su subsistencia y continuidad se relaciona con los ataques de las PYMES en Colombia, aunque solo el 7% sufren un ciberataque en su primer año de trabajo, casi siempre y dependiendo de su magnitud, en algunos casos deben cerrar, ya que las pérdidas superan el capital de inversión inicial. (CCIT, 2023).

Así mismo, los análisis sobre el sector de ciberseguridad en Colombia particularmente atribuyen un escenario en el que se observan múltiples factores que tienen un impacto tanto como económico como productivo en las diferentes empresas del país, entre los que se encuentran los siguientes:

- Sensibilización insuficiente como herramienta de detección temprana y prevención de ataques en fases iniciales.
- Percepción de la ciberseguridad como un gasto elevado en la operación de las Empresas en Colombia.
- Desactualización de los sistemas y del recurso humano por fuga de talentos de Ciberseguridad.

El balance y los análisis del Cibercrimen reflejan la gravedad del problema del ciberdelito en Colombia y la necesidad de fortalecer la ciberseguridad en la industria TIC, así que los gobiernos y las empresas tomen medidas para protegerse de estos delitos, representados en la implementación de medidas de seguridad informática, y complementado con asistencia técnica sobre los riesgos y amenazas del ciberespacio.

En conclusión, los ciberataques representan un impacto económico considerable en las empresas colombianas, afectando tanto a nivel directo (costos inmediatos de respuesta y solución) como indirecto (daño a la imagen y credibilidad empresarial, pérdida de clientes y costos legales), por lo cual, es determínate que las empresas inviertan en medidas de prevención, protección y respuesta para mitigar estos impactos y asegurar la resiliencia cibernética.

2.3 Análisis Técnico

El sector de Ciberseguridad en el contexto mundial aún presenta un ecosistema complejo que implica la interacción entre la producción de servicios y la provisión de bienes tecnológicos que generen un ecosistema de ciberseguridad confiable en las industrias y empresas del país. De esta forma, el proyecto RETOS DE INNOVACIÓN TECNOLÓGICA EN CIBERSEGURIDAD, apunta a capitalizar estos elementos, identificando, definiendo y en su puesta en marcha de retos tecnológicos en materia de ciberseguridad, tomando como grupo objetivo el apoyo y fortalecimiento de las empresas que hacen parte de la Industria TIC, y a su vez un conjunto de MIPYMES colombianas que requieren del apoyo y la solución a situaciones en materia de seguridad digital.

En consecuencia, los servicios requeridos para el proyecto se ubican en el eslabón producción de servicios TIC de la cadena del sector TIC, en la puesta a disposición de una solución tecnológica para la formación virtual y por otra mediante servicios de asistencia en el uso y apropiación de tecnologías[8] (Grafica N°1), tanto para los empresarios que hacen parte de la industria TIC para este sector, como de las empresas identificados dentro del grupo focal MIPYMES. Por lo tanto, esto implica la generación de habilidades digitales para apoyar a las empresas a desarrollar estrategias que permitan a estas adoptar soluciones tecnológicas adecuadas para fortalecer su presencia mercado.

Grafica No 2. Cadena de Valor del Sector TIC



Fuente: Tomado de MinTIC, 2015. Basado en: Guide to Measuring the Information Society (2011). OECD; Clasificación Central de Productos -CPC Vers. 2 A.C. Dane; CRC (2010). Análisis del sector TIC en Colombia: evolución y desafíos, Raúl Katz (2015). El ecosistema y la economía digital en América Latinoamérica

Además de la adopción y adaptación de nuevas tecnologías, RETOS DE INNOVACIÓN TECNOLÓGICA EN CIBERSEGURIDAD, incorpora un enfoque de innovación abierta (Componente Diseño e implementación de soluciones innovadoras). Este enfoque permite integrar una diversidad de ideas, tecnologías y metodologías que pueden conducir a soluciones más creativas y efectivas, donde la interacción entre diferentes stakeholders y un bootcamp – de acuerdo con los alcances del proyecto- puede generar y mejorar las prácticas existentes para la solución de los retos tecnológicos planteados.

Abordando su aplicación, la ciberseguridad se puede presentar en diferentes contextos, desde los negocios hasta la informática móvil, entre sus categorías más comunes se encuentran las siguientes:

8 https://www.researchgate.net/figure/Figura-31-Cadena-de-valor-del-sector-TIC-Fuente-Tomado-de-MinTIC-2015-Basado-en_fig2_336224640

Grafica No 3. Categorías de la Ciberseguridad

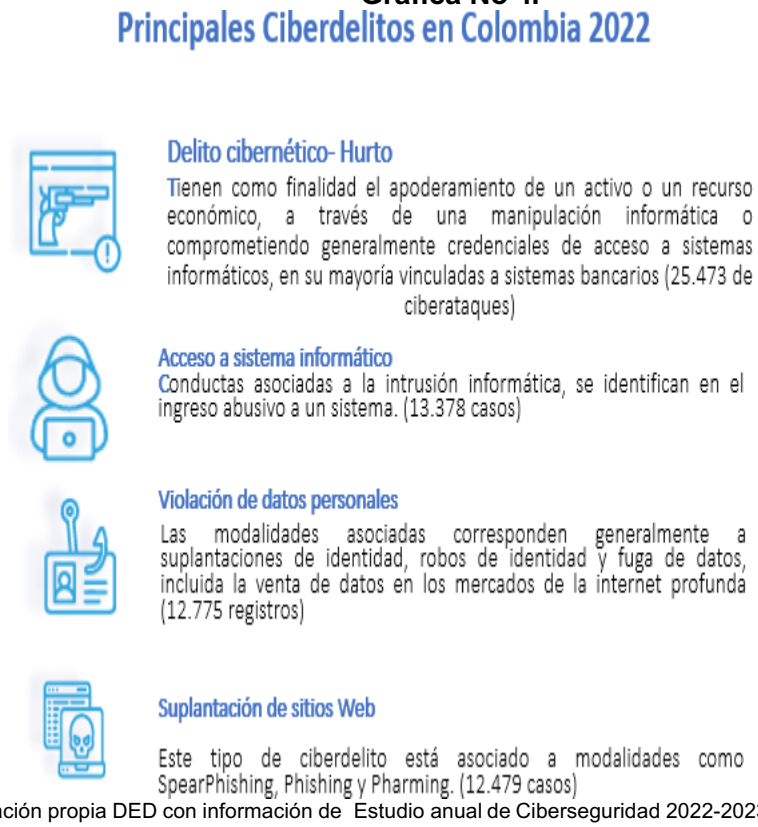


Fuente: Elaboración propia DED con información de CCIT, 2023.
Estudio anual de Ciberseguridad 2022-2023

De otra parte, durante el 2022, las denuncias por ciberdelitos en el país se registraron cada 8 minutos y crecieron un 26%, referentes a infracciones señaladas en Ley 7273 de 20099, siendo el hurto por medios informáticos el delito con mayor número de registros. Dentro de las amenazas más comunes a las que se enfrenta la ciberseguridad en Colombia, se identifican las siguientes:

9 Esta Ley hace referencia a la protección de la información y de los datos"- y se preserven integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Grafica No 4.



Fuente: Elaboración propia DED con información de Estudio anual de Ciberseguridad 2022-2023 (CCIT, 2023)

CONCEPTOS BASICOS RELACIONADOS CON CIBERSEGURIDAD

La aplicación, potencialización y uso de la ciberseguridad en el sector TIC implica usar diversos conceptos que proporcionan un acercamiento en la materia. Aquí algunos detalles técnicos relevantes:

Activo: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 2016, pág. 56).

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO/IEC 27000:2016).

Control: Medida que modifica el riesgo. (NTC ISO 31000:2011). Medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Privacidad: Por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la

entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente. (MSPI).
Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000). Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas10. (DAFP 2022). Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854 2016, pág. 29).

Startup: Es una empresa de reciente creación, que se basa en las tecnologías de la información y la comunicación (TIC) para comercializar sus productos o servicios. Presenta un modelo de negocio escalable y su prioridad es crecer de manera ágil y rápida.

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas. (Basado en DAFP 2022).

2.3 Análisis Regulatorio

Los esfuerzos de las entidades del Estado colombiano por aumentar el número de colombianos y empresas que acceden en el uso y aplicación de la Ciberseguridad y Ciberdefensa, al igual que su reglamentación, han generado un gran despliegue de leyes, programas y proyectos para garantizar la legalidad y puesta en marcha.

En cuanto a los avances referentes normativos asociados a la ejecución del proyecto se destacan los siguientes:

NÚMERO OBJETO	DESAROLLO DEL SUMARIO
Ley 1273 de 2009 modifica el Código Penal	Crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”, y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones

10 Departamento Administrativo de la Función Pública (2022). Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 6. Recuperado de https://www.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf/50bff85a- 70c6-dd15-68f56cd2ea2a8707?t=1677003002032

NÚMERO OBJETO	DESAROLLO DEL SUMARIO
Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales	El cual, de conformidad con su artículo 1, tiene por objeto "(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma (…)".
Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional	Su objetivo es regular el derecho de acceso a la información pública, los procedimientos para ejercer y garantizar el derecho y las excepciones a la publicidad de información, y constituye el marco general de la protección del derecho de acceso a la información pública en Colombia.
Decreto Nacional 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"	Definió la estrategia de seguridad y privacidad de la información, estableciendo que la misma no se limita a este sólo aspecto, sino que comprende la seguridad digital y los requerimientos necesarios para garantizar la continuidad en la prestación de los servicios digitales.
Decreto 1499 de 2017	En su artículo 2.2.22.2.1 relacionado con las Políticas de Gestión y Desempeño Institucional indica que las políticas de Desarrollo Administrativo de que trata la Ley 489 de 1998, formuladas por el Departamento Administrativo de la Función Pública y los demás líderes, se denominarán políticas de Gestión y Desempeño Institucional y comprenderán, entre otras, la de Gobierno Digital, antes Gobierno en Línea, y la de Seguridad Digital.
CONPES 3854 de 2016 - Política Nacional de Seguridad Digital	Se establece un marco institucional claro y preciso en torno a la seguridad digital.
CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital.	Se establecen medidas para desarrollar la confianza digital mejorando la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, fortaleciendo capacidades y actualizando el marco de gobernanza en seguridad digital, y con la adopción de modelos centrados en nuevas tecnologías.
Directiva presidencial 03 de 2021	Emite lineamientos para el uso de servicios en nube, inteligencia artificial, gestión de datos y seguridad digital para entidades públicas de la rama ejecutiva de orden nacional e invita a su aplicación a entidades territoriales, así como a la rama legislativa y judicial.
Resolución 500 del 10 de marzo de 2021, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital",	El Ministerio de Tecnologías de la Información y las Comunicaciones expidió esta resolución en la cual establece los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y establece los lineamientos y estándares para la estrategia de seguridad digital.

Para este apartado, hay que complementar este estudio con lo dispuesto en el artículo 3.2 del Decreto Ley 4170 de 2011 y el inciso primero del artículo 2.2.1.2.5.2 del decreto 1082 de 2015 para desarrollar, implementar y difundir programas que garanticen la debida forma y oportunidad en los procesos contractuales requeridos.

Normatividad Internacional

Un instrumento vinculante para la aplicación y uso de la Ciberseguridad desde el punto legal vigente se relaciona con el marco sobre el tema en el ámbito internacional, y su protocolo para la criminalización de actos cometidos a través de sistemas informáticos, entre la las que se encuentran:

- Convenio sobre la Ciberdelincuencia (CC)). Consejo de Europa.
- (Convenio sobre Cibercriminalidad de Budapest).
- Adoptado en noviembre de 2001 entró en vigor el 1° de julio de 2004
- Resolución AG/RES 2004 (XXXIVO/04) de la Asamblea General de la Organización de los Estados Americanos: estrategia integral para combatir las amenazas a la seguridad cibernética.
-

3. ANALISIS DE LA DEMANDA

Para este apartado se presentan cifras y valores sobre la demanda del sector de la ciberseguridad y ciberdefensa, y luego se aborda la demanda y contratación que ha adelantado y ejecutado el sector público en relación con el sector y objeto de este estudio.

3.1. Cifras y Valores que Demanda el Sector en Ciberseguridad

Análisis especializados en la materia CIBERSEGURIDAD en el mundo un aumento proporcional del sector en ciberseguridad representado en las siguientes cifras[11]:

- El crecimiento del sector en ciberseguridad se encuentra caracterizado y segmentado por t**ipo de producto o categoría** (soluciones (seguridad de aplicaciones, seguridad en la nube, software de seguridad para el consumidor, seguridad de datos, gestión de identidad y acceso, protección de infraestructura, gestión integrada de riesgos, equipos de seguridad de red), servicios (profesionales, gestionados). **por implementación** (local, nube), por industria de usuario final (BFSI, atención médica, aeroespacial y defensa, TI y telecomunicaciones, gobierno, comercio minorista, fabricación), y geografía (América del Norte, Europa, Asia-Pacífico, y Resto del Mundo (América Latina, Medio Oriente y África).
- El tamaño del mercado de ciberseguridad (en el mundo) se estima en USD 182.86 mil millones en 2023, y se espera que alcance los USD 314.28 mil millones para 2028, creciendo a una tasa compuesta anual de 11.44% durante el período de pronóstico (2023-2029).
- El segmento de la nube en ciberseguridad está creciendo, lo anterior soportado, en que las empresas están considerando pasar del software local a soluciones basadas en las nubes, asociadas a posibles soluciones para sus características de seguridad clave, incluido el cumplimiento de estándares, prevención y detección de intrusiones.

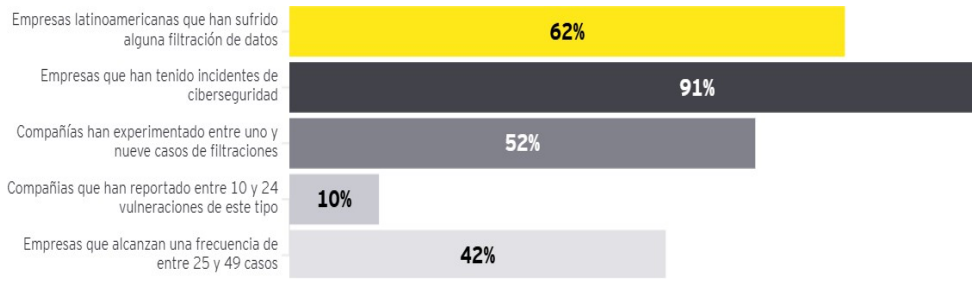
La demanda de productos de ciberseguridad, que abarca áreas como seguridad de endpoints, seguridad de red, seguridad web y del correo electrónico, protección de datos, gestión de identidades y accesos, así como análisis de vulnerabilidades,

11 https://www.mordorintelligence.com/es/industry-reports/cyber-security-market

experimentará un crecimiento del 11,7%, alcanzando los 79.500 millones de dólares en 2023. Aunque este aumento representa un avance significativo para el sector de las tecnologías de la información y comunicación (TIC), se observa una desaceleración en comparación con 2022. En el año anterior, las organizaciones incrementaron el gasto para actualizar sus defensas existentes y añadir nuevas capacidades, especialmente en áreas como la nube, IoT/OT y seguridad de identidades[12].

De manera particular para el caso Latinoamericano, el estudio EY 2023 Global Cybersecurity Leadership Insights reseña que el "62% de las empresas latinoamericanas han sufrido alguna filtración de datos durante el último año, por su parte 52% de las compañías latinoamericanas han experimentado entre uno y nueve casos de filtraciones[13] (Graficas 5 y 6).

Grafica No 6



Fuente: Tomado de EY Global Cybersecurity Leadership Insights Study, 2023.

Finalmente, de acuerdo con el Índice Global de Ciberseguridad más reciente, elaborado por la International Telecommunication Unión de Naciones Unidas, Latinoamérica es la región del mundo más vulnerable a los ataques cibernéticos y presenta el índice más bajo de preparación contra este tipo de delitos (El Tiempo, edición de 23 de septiembre 2023).

3.1.2 Estado de la Ciberseguridad en Colombia

En el año 2021 se presentaron más de 7 billones de intentos de ataques cibernéticos en nuestro país según la Cámara Colombiana de Informática y Telecomunicaciones. En el mismo sentido, la Fiscalía General de la Nación reportó un aumento del 30% en el número de dichos ataques[14] Casos recientes como los ataques sufridos por Keralty o IFX Networks, que prestan servicios a diferentes entidades de gobierno, o los eventos sufridos por el Ministerio de Salud y Protección Social o el Consejo Superior de la Judicatura, demuestra la susceptibilidad en la que se encuentra el país en la materia.[15]

Para el 2022, se reportaron 54.121 denuncias por ciberataques, esto según estadísticas del Centro Cibernético de la Policía Nacional, lo que representa un incremento del 79% frente al año anterior. "Este panorama hace que sea urgente la colaboración entre las agencias gubernamentales y las compañías de ciberseguridad para compartir información sobre las amenazas, desarrollar estrategias de mitigación y apoyar a las víctimas de estos ataques. Desafortunadamente, estas iniciativas aún son "muy incipientes[16]" (Forbes Colombia, 2023).

Cabe señalar, durante el año 2023, se registraron más de 5.000 millones de intentos de ciberataque en Colombia, lo que la ubica el país como la cuarta nación más afectada en América Latina, después de Brasil, México y Venezuela según

12 https://www.ituser.es/seguridad/2023/01/las-empresas-aumentaran-el-gasto-en-ciberseguridad-mas-de-un-13-en-2023
13 www.ey.com/es_co/consulting/is-your-greatest-risk-the-complexity-of-your-cyber-strategy 14https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno
15 https://www.javeriana.edu.co/pesquisa/ciberataque-ifx-networks-colombia/
16 https://forbes.co/2023/10/09/tecnologia/ciberseguridad-colombia-aun-no-esta-preparada-para-avanzar

datos de Fortinet. [17] Por su parte, y de manera particular los riesgos de seguridad digital en el sector financiero, la Asociación Bancaria y de Entidades Financieras de Colombia - Asobancaria, reporta que se registran alrededor de 43 ciberataques por segundo al sistema financiero colombiano. Se trata de un riesgo de grandes proporciones, considerando que hoy en día un 68% de todas las transacciones monetarias del país se realizan a través de canales digitales y servicios de banca en línea.[18]

No obstante, cabe decir que los esfuerzos por mejorar la seguridad de la banca digital han rendido sus frutos. Asobancaria estima que el 99 % de las operaciones financieras a través de canales digitales en el país se realizan seguramente. Por cada 100 dólares de transacciones dentro del sistema bancario, solo 1 tiene reclamación por fraude de parte de los clientes, una estadística muy positiva que refleja la fortaleza de los sistemas de seguridad de la banca nacional. En Colombia, el 34% de las empresas reportan haber experimentado algún tipo de fraude en sus plataformas digitales en los últimos dos años. El 94% de las empresas aseguran estar conscientes de riesgos de fraude, pero solo un 76% monitorea proactivamente sus plataformas. Un 80% considera que cuentan con controles suficientes para detectar fraudes en línea, incluyendo tecnologías de monitorización de transacciones y detección de anomalías en los registros de operaciones financieras (Ibidem).

De igual forma, el Informe Attack Surface Threats de Unit (2023), de la unidad de investigación e inteligencia de amenazas de Palo Alto Networks señala para el caso colombiano: *"Colombia sigue en la mira: 85% de las empresas con trabajo remoto son vulnerables a ataques de ransomware. En Colombia el ciberdelito aumentó un 26% en 2022 en comparación con el año anterior y el 67% de las denuncias de ciberataques se registran por empresas públicas y privadas. Además, el país sigue en la mira de los ciberdelincuentes, no en vano fue víctima recientemente de un ataque de ransomware a gran escala19"*.

Así las cosas, se identifica que los principales problemas de ciberseguridad, tanto en Colombia como los demás países de la región, están relacionados con ciberdelitos por phishing, el whaling, el malware o software malicioso y las descargas automáticas, situaciones que sin duda han acelerado la demanda y la inversión en términos económicos en ciberseguridad en todos los sectores y empresas que conforman la economía nacional.

En consecuencia, y, a partir de lo descrito con las anteriores cifras, de manera estructural una de las debilidades que ha generado impactos en las empresas en Colombia es la falta de una estrategia y una arquitectura de seguridad robusta a nivel interno, que identifique y mitigue los riesgos a los que se exponen estas unidades económicas, y tenga un presupuesto para ello. De otra parte, a pesar de que los ciberataques pueden costar millones de pesos en la mayoría de las empresas aún no existe claridad frente al nivel de exposición a estos riesgos e iniciativas concretas para mitigarlos, por tal motivo, es importante incluir la ciberseguridad en los procesos y cada actividad empresarial que represente manejo de datos y transacciones digitales, objetivo y alcance del proyecto **RETOS DE INNOVACIÓN TECNOLÓGICA EN CIBERSEGURIDAD**.

3.2. Contratación adelantada por el Sector Publico

En respuesta a los riesgos y delitos relacionados con seguridad en el ámbito digital, el gobierno ha fortalecido políticas públicas mediante la expedición de documentos CONPES, y ha puesto en marcha la ejecución de proyectos y suscripción de contratos en aras de enfrentar amenazas de ciberseguridad. Para tal efecto, y en aras por adoptar una metodología adecuada para analizar los antecedentes de demanda de los servicios requeridos para la suscripción de este convenio, el MinTIC usa la herramienta de abastecimiento estratégico proporcionada por la agencia nacional de contratación pública,

17 https://canal1.com.co/noticias/empresas/ciberseguridad-colombia-plataforma-detecta-ciberataques/
18 https://lanotaeconomica.com.co/movidas-empresarial/el-34-de-las-empresas-en-colombia-han-sufrido-algun-tipo-de-fraude-en-plataformas-digitales
19 https://www.infobae.com/inhouse/2023/10/18/colombia-sigue-en-la-mira-85-de-las-empresas-con-trabajo-remoto-son-vulnerables-a-ataques-de-ransomware/Infobae

donde se pueden consultar los procesos de contratación adelantado con clasificadores de bienes y servicios según el servicio requerido por la entidad. Por lo anterior, a continuación, se relacionan procesos de selección de objetos similares al que el MINTIC espera suscribir, referentes a contratación relacionada a servicios de seguridad digital, transformación digital – en términos del fortalecimiento del sector TIC, y la puesta en marcha de restos innovadores- tecnológicos-, servicios tecnológicos de la entidad en materia de tecnología, informática y TIC, entre los que se identifican:

Tabla No. 2

REFERENCIA	DESCRIPCIÓN	No. PROCESO	FECHA PUBLICACIÓN
Empresa colombiana de petróleos	Contrato marco bilateral con la firma Connect Bogotá, para la suscripción para gestionar espacios de networking con la red de emprendedores para la convocatoria y lanzamiento de retos de innovación.	ME 594149 - 3035621	18/08/2023
Contraloría general de la republica	Conceptualización, estructuración, implementación, capacitación y acompañamiento en el desarrollo de las capacidades de la gestión de la innovación en los procesos y el portafolio de programas y proyectos	CGR-130-SBCC	30/08/2023
Interconexión eléctrica s a e s p	Prestación De Servicios De Consultoría De Transformación De Ti, Innovación Y Estrategia Digital	4600005490	21/09/2023
Central administrativa y contable especializada Cenac educación	Capacitación Virtual Offline Para Actividades De Ciencia Tecnología E Innovación Para Las Unidades Centralizadas Por La Cenac De Educación	SIP-MC-614-CENACEDUCACION-2023	14/09/2023
Secretaría Distrital De Movilidad	Realizar la gestión y monitoreo de la seguridad informática sobre la plataforma tecnológica de la secretaría distrital de movilidad a través de un centro de operaciones de seguridad SOC	SDM-LP-009-2021	5/03/2021
Aerocivil	Prestar el servicio para el diseño, implementación y puesta en funcionamiento del servicio de gestión de seguridad tipo SOC (Security Operation Center).	20001084 H3 DE 2020	17/09/2020

Procesos de Selección con objetos contractuales similares en el MINTIC:

La entidad no posee información histórica de contratación refrentes a la implementación de RETOS EN CIBERSEGURIDAD, por lo anterior, se relacionan contratación similar o con objetos relacionados con servicios de ciberseguridad digital, transformación digital del sector TIC, y servicios tecnológicos de la entidad en materia de tecnología, informática y TIC, entre los que se identificaron:

Tabla No. 3

REFERENCIA	DESCRIPCIÓN	No. PROCESO	FECHA PUBLICACIÓN
Ministerio de Ciencia, Tecnología e Innovación	CORPORACIÓN CENTRO DE INNOVACIÓN INVESTIGACIÓN Y EMPRENDIMIENTO	FFJC49-2023	14/09/2023
Corporación Agencia Nacional de Gobierno Digital	Realizar las pruebas de seguridad establecidas en el alcance, con el fin de identificar las debilidades frente a posibles amenazas cibernéticas y así poder mitigarlas a través de controles que permitan una mejora continua en la operación de la agencia nacional digital.	CMA-AND001-202	1/05/2021

REFERENCIA	DESCRIPCIÓN	No. PROCESO	FECHA PUBLICACIÓN
Fondo Único de TIC	Prestar servicios de asistencia y apoyo especializado a las entidades públicas para promover buenas prácticas para la adopción, implementación y apropiación de la Política de Gobierno Digital y el impulso a los procesos de transformación digital.	FTIC-LP-011- 2020	1/04/2020
Fondo de Tecnologías de la Información y las Comunicaciones	Contratar el fortalecimiento de las herramientas de análisis y servicios tecnológicos de la entidad en materia de tecnología, informática y TIC asegurando una información oportuna y de calidad ofreciendo los mecanismos necesarios para el cumplimiento.	FTIC-LP-010 de 201	2/08/2019

4. ANÁLISIS DE LA OFERTA

En términos de oferta en el mundo referente al sector de ciberseguridad, los grandes mega clústeres de ciberseguridad comparten dos características esenciales, o productos y servicios: la primera una cultura de innovación de alta tecnología y startups es un importante motor de crecimiento, con grandes ecosistemas de startups[20] con un importante flujo asociado de capital de riesgo, y de otra parte, muy centradas en productos, con una mayor proporción de empresas basadas en servicios.

Otra de las principales causas del aumento de los ciberataques, y referente al tema de la oferta y la industria TIC a nivel mundial, es la falta de personal capacitado en ciberseguridad en cada sector, muchos de los profesionales con experiencia en ciberseguridad, especialmente en Europa, Asia-Pacífico, América Latina y Medio Oriente, es baja en comparación con la necesidad de profesionales de seguridad para manejar las amenazas cibernéticas para empresas financieros, organizaciones gubernamentales y empresas industriales/del sector privado.

INDUSTRIA Y OFERTA DE LA CIBERSEGURIDAD EN COLOMBIA

Algunas cifras que reflejan el tamaño del mercado de la ciberseguridad en Colombia reflejan que este sector alcanzó 243,86 millones de dólares en 2022, además y según las proyecciones para el período contemplado 2023-2028, se anticipa un crecimiento de casi 555,29 millones de dólares en 2032.

Dentro de los factores clave que determinan las perspectivas del mercado colombiano de la ciberseguridad en su oferta se identifican los siguientes 21:

- **Adopción de la digitalización para el entorno de trabajo por diversos sectores industriales.** El cambio digital de las empresas ha llevado a la expansión del mercado y la industria TI para el componente en ciberseguridad, debido a la creciente demanda de seguridad de tecnologías de información y datos, redes, nube y otros sistemas. En consecuencia, la creciente adopción de espacios basados en la nube híbrida por parte de los sectores BFSI, TI y telecomunicaciones, sanidad y otros se ve representada en una gran amenaza para la información crítica y sensible almacenada en la nube.
- **Integración de nuevas tecnologías y activos electrónicos.** El alto consumo de Internet de las cosas (IoT), el aprendizaje automático, la inteligencia artificial (AI) está detectando las amenazas inciertas de los ciberataques, por lo cual se requiere la generación de soluciones de seguridad cibernética, proporcionando así un impulso al mercado en respuesta a dichos factores.

20
21 https://www.informesdeexpertos.com/informes/mercado-de-la-ciberseguridad-en-colombia

Otros aspectos para considerar que caracteriza y segmenta en la oferta identificada para el sector de la ciberseguridad se ve reflejada en la siguiente tabla (Tabla N°4):

Tabla No.4 Características del Mercado- Sector Ciberseguridad

ASPECTO MERCADO	TIPOLOGIA- DESCRIPCIÓN
Por Componente - ¿Qué tipo?	• **Por Solución:** se dividen en inteligencia de amenazas, antivirus/antimalware, cifrado, mitigación de la denegación de servicio distribuida y filtrado web, gestión unificada de amenazas, cortafuegos, sistemas de detección de intrusiones o sistemas de prevención de intrusiones, prevención de pérdida de datos, recuperación en caso de catástrofe entre otros • **Por Servicios,** se subdividen en seguridad gestionados y profesionales
Despliegue - ¿Cómo?	• **Cloud** • **On-Premises** Mientras que las soluciones en la nube envían la información a un servidor remoto en un centro de datos, con el software on premises todos los datos se almacenan de forma local, a menos que se opte por un servicio de almacenamiento en la nube22.
Tipo de Seguridad ¿En qué?	**Seguridad en la Nube,** • Protección de Datos en la Nube: Asegura la información almacenada en entornos de nube pública, privada o híbrida. • Seguridad de Aplicaciones en la Nube: Incluye herramientas para proteger aplicaciones desplegadas en la nube.
	Seguridad de Endpoints, • Antivirus y Antimalware: Protegen los dispositivos individuales contra software malicioso. • Protección contra amenazas avanzadas: Incluye herramientas como EDR (Endpoint Detection and Response) para detectar y responder a amenazas en endpoints.
	Seguridad de Datos: • Encriptación: Protege la información sensible mediante técnicas de cifrado tanto en tránsito como en reposo. • Gestión de claves: Administra y protege las claves criptográficas utilizadas en la encriptación de datos.
	Seguridad de Redes: • Firewalls: Controlan el tráfico de red entrante y saliente basado en políticas de seguridad. • Sistemas de Prevención/Detección de Intrusiones (IPS/IDS): Monitorean y analizan el tráfico de red en busca de actividades sospechosas. • Segmentación de Red: Divide la red en segmentos para limitar el acceso y contener posibles amenazas.
	Protección de Infraestructuras

22 El término on-premise se puede traducir como in situ o en las propias instalaciones de la empresa, por lo que hace referencia a que la empresa instala toda la infraestructura TI a nivel local en su negocio, como servidores, componentes de red, cortafuegos y, en definitiva, todo el entorno informático y tecnológico

ASPECTO MERCADO	TIPOLOGIA- DESCRIPCIÓN
	Otros: • **Seguridad de Aplicaciones** • **Seguridad en IoT** (Internet de las Cosas). Protección de Dispositivos IoT: Incluye medidas para asegurar dispositivos conectados a la red que pueden ser vulnerables a ataques. • **Gestión de Identidades y Accesos (IAM)** - Autenticación Multifactor (MFA): Requiere múltiples formas de verificación para acceder a sistemas. - Control de Accesos Basado en Roles (RBAC): Define permisos y accesos basados en el rol del usuario dentro de la organización. - Gestión de Identidades: Incluye la provisión, desactivación y auditoría de identidades de usuario. • **Análisis de Vulnerabilidades y Seguridad** - Escaneo de Vulnerabilidades: Identifica debilidades en sistemas y redes que podrían ser explotadas por atacantes. - Pruebas de Penetración (Pentesting): Simula ataques para identificar y corregir vulnerabilidades antes de que puedan ser explotadas en el mundo real. • **Gestión de Incidentes y Respuesta** - Planes de Respuesta a Incidentes: Procedimientos para gestionar y mitigar los efectos de un incidente de seguridad. - Sistemas de Gestión de Información y Eventos de Seguridad (SIEM): Recogen y analizan datos de seguridad para detectar y responder a amenazas.
Tamaño de la organización	• Grandes Empresas • Pequeñas y Medianas Empresas
Uso final	• BFSI • Gobierno y Defensa • Energía y Servicios Públicos • Sanidad • TI y Telecomunicaciones • Fabricación • Comercio minorista • Otros

Fuente: Elaboración propia DED con información de Informesdeexpertos.com[23]

SECTOR TI DE CIBERSEGURIDAD EN COLOMBIA

Conforme las líneas de acción que precave el Plan Nacional de Desarrollo 2022-2026 *"Colombia, Potencia Mundial de la Vida"*, el gobierno busca mejorar las capacidades y fortalecer la cultura de ciberseguridad. Este esfuerzo se plantea como esencial para proteger tanto la información gubernamental como la personal frente a posibles ataques cibernéticos y delitos informáticos. Además, se busca promover un entorno robusto de seguridad digital que asegure la continuidad de los servicios públicos y refuerce la implementación de estándares y buenas prácticas (lo anterior alineado con el Componente 2, y en cumplimiento de este objetivo, referente al fortalecimiento del Sector Industria TIC).

En Colombia la industria TI que desarrolla el componente en ciberseguridad de origen local tiene un bajo nivel de desarrollo. Actualmente la Asociación Colombiana de Ingenieros de Sistemas identifica 165 MiPymes en este sector, en su mayoría se dedican a prestar servicios de consultoría para implementación de productos de grandes empresas

23 Ibidem

internacionales o a ser canal intermediario de las mismas24. Es decir, que hay poco o ningún desarrollo de productos y servicios de origen local, que identifiquen causas estructurales por las cuales se presentan riesgos de seguridad digital.

Algunas empresas del sector TI solo se dedican a proteger a las empresas, en servicios como el análisis de aplicaciones móviles y auditoria para aplicativa web, seguridad en el teletrabajo, protección de sitios web y monitoreo continuo de los procesos de la organización, o la autogestión de usuarios que garantice la identidad de cada colaborador para combatir la suplantación de identidad y ataques de ingeniería social. Así mismo, adicionalmente otras empresas dentro de su portafolio además de los servicios generales ofertados por este sector ofrecen también capacitación a nivel profesional y empresarial, hasta técnicas especializadas tales como Análisis de vulnerabilidades, seguridad de la información, y consultoría en norma ISO 2700125.

Dentro del mercado es importante la presencia de empresas que conforman el sector que se enfoquen en la implementa de procesos prediseñados con una línea de negocio denominada “Seguridad Administrada”, la cual busca realizar análisis previo de vulnerabilidades y la corrección de los eventos encontrados en diferentes áreas de las empresas.

Otra de las características y desafíos a los que se enfrenta la industria TI para este sector en Colombia se asocian con algunos factores, los cuales a su vez reflejan áreas que se deben ser fortalecidos en los siguientes aspectos:

- **Falta de Personal Capacitado,** se presenta una escasez de profesionales altamente capacitados en ciberseguridad en Colombia. Esto puede llevar a una falta de experiencia y habilidades necesarias para enfrentar amenazas sofisticadas.
- **Recursos Limitados,** muchas empresas de ciberseguridad en Colombia pueden operar con presupuestos limitados, lo que restringe su capacidad para invertir en las últimas tecnologías y herramientas de protección.
- **Actualización en Amenazas**, las amenazas cibernéticas están en constante evolución, por lo que las empresas que constituyen el sector deben mantenerse al día con las últimas técnicas y herramientas de ataque, lo que las pone en desventaja frente a otras empresas del mundo con herramientas más avanzados, o en comparación con sus contrapartes en países con industrias de ciberseguridad más maduras.

Siendo una necesidad latente este sector para las empresas nacionales, el mercado de la ciberseguridad en Colombia alcanzó un valor de alrededor de USD 279,71 millones para 2023. Se prevé que el mercado crezca a una tasa anual compuesta del 14,7% entre 2024 y 2032, para alcanzar un valor de 961,11 millones de USD en 2032, por los ataques a empresas y entidades públicas, es decir la demanda por los servicios en seguridad digital tiende a mantenerse y orientarse al crecimiento del mercado.

Dichas organizaciones se enfrentan a competidores internacionales muy fuertes, situación que en muchas ocasiones hace que su posición competitiva resulte débil y por tanto sus opciones de crecimiento limitadas. Por ello se hace necesario que las MiPymes nacionales y los emprendimientos que se dedican a prestar servicios de ciberseguridad se fortalezcan, así el ecosistema TIC podrá hacerse fuerte y sostenible. Este proceso de fortalecimiento debe apuntar a que un número significativo de prestadores de servicios del sector de ciberseguridad desarrollen competencias empresariales, habilidades comerciales y capacidad técnica para enfrentar la dinámica de cambio que caracteriza el negocio.

Por consiguiente, el proceso debe procurar una conexión real entre los sectores con las actividades económicas críticas para el funcionamiento digital del país (tanto en el fortalecimiento de la oferta, en respuesta a las empresas que demandan

24 https://sistemas.acis.org.co/index.php/sistemas/catalog/category/investigacion // https://acis.org.co/portal/content/lista-de-empresas- de-seguridad-inform%C3%A1tica-en-colombia
25 https://marketingdigital.blog/empresas-de-seguridad-informatica/

en el servicio), de tal forma, que el sector empresarial comprenda la importancia de la ciberseguridad y la prioridad que representa para sus organizaciones.

Mediante SECOP II se analizó la base de datos donde relacionan procesos de selección de objetos similares al que el MINTIC espera suscribir, referentes a contratación relacionada donde se observan varios de los proveedores seleccionados:

EMPRESA-PROVEEDOR	DESCRIPCIÓN	ENTIDAD CONTRATANTE	NUMERO DE PROCESO	FECHA
UNION TEMPORAL CYBER & KINETIC SIMS	Adquisición plataforma de simulación en ciberseguridad y ciberdefensa	ESCUELA SUPERIOR DE GUERRA	304-MDN-COGFM-ESDEG-2021	12/03/21
NEXT SECURITY SAS	Renovación y actualización del licenciamiento de los equipos de seguridad perimetral y su arquitectura de ciberseguridad para el instituto tecnológico metropolitano según especificaciones técnicas.	INSTITUTO TECNOLOGICO METROPOLITANO	CV 8030 DE 2022	12/14/22
ESOFT COLOMBIA SAS	Contratar a todo costo la renovación del sistema de ciberseguridad para la gestión de eventos cibernéticos y el sistema DLP de la jefatura de inteligencia naval. Lote2.	ARMADA NACIONAL - DADIN	021-JINAV-DADIN-2022	06/16/22
GAMMA INGENIEROS SAS	Contratar a todo costo la renovación del sistema de ciberseguridad para la gestión de eventos cibernéticos y el sistema DLP de la jefatura de inteligencia naval Lote1.	ARMADA NACIONAL - DADIN	020-JINAV-DADIN-2022	06/17/22
I2 SISTEMAS Y SEGURIDAD INFORMATICA LTDA	Adquisición de un servicio de ciberseguridad basado en análisis de comportamiento de usuarios e identidades con capacidad automatizada y respuesta, de acuerdo con las especificaciones técnicas	COMANDO FAC	161-00-A-COFAC-GOCOP-2021	9/02/21
INTELLIGENT TRAINING DE COLOMBIA S.A	Contratar la realización de un Bootcamp digital que refuerce el fortalecimiento de las habilidades digitales en ciberseguridad e implementación de soluciones en seguridad digital.	SENA DISTRITO CAPITAL GRUPO DE APOYO ADMINISTRATIVO - CGI	CO1.PCCNTR.4026194	09/20/22
IT SECURITY SERVICES S.A.S	Contratar el servicio de alertas de operaciones cibernéticas incluido el desarrollo de prospectiva en materia de seguridad de la información y ciberseguridad.	SUPERINTENDENCIA FINANCIERA DE COLOMBIA	SF.3-027-2021	10/28/21
Heimcore SAS	Adquisición e instalación de software y hardware para la implementación de centro cibernetico de la policía nacional -	DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E	03-2-10099-18	11/13/18

	fortalecimiento centro de capacidades para ciberseguridad de Colombia	INTERPOL		
CAPACITACIÓN Y SERVICIOS ESPECIALIZADOS SAS	Renovación de suscripciones y soporte para una solución de ciberseguridad en el Instituto Nacional de Vias.	INVIAS	1663-2022	12/26/22

Cabe destacar que, en el análisis de la oferta del sector de ciberseguridad, en Colombia, existen varias empresas que se destacan por su capacidad de ofrecer productos y servicios especializados. A continuación, se presentan algunas de las empresas líderes en el sector de ciberseguridad a nivel local:

EMPRESA-PROVEEDOR	SERVICIO O PRODUCTO OFRECIDO	SITIO WEB
Carvajal Tecnología y Servicios	Soluciones de seguridad informática, análisis de vulnerabilidades, protección de datos, y seguridad en la nube.	https://carvajaldigital.co/
GMS (Global Market Solutions)	Auditorías de ciberseguridad, protección contra malware, firewalls, y servicios de seguridad gestionados.	https://www.gms.com.co
Brotec	Soluciones de protección de datos, firewalls, sistemas de detección de intrusiones, y servicios de consultoría en ciberseguridad.	https://www.brotec.com.co
Emergya	Servicios de consultoría en ciberseguridad, auditorías de seguridad, gestión de identidades, y seguridad en la nube.	https://www.emergya.com/es
IFX Networks	Soluciones de seguridad gestionada, firewalls, protección de datos, y recuperación ante desastres.	https://www.ifxnetworks.com

De esta forma, una vez analizada la oferta tenemos que BIOS es un cooperante idóneo para el sector de ciberseguridad en Colombia debido a su enfoque en innovación tecnológica y su capacidad para ofrecer soluciones avanzadas adaptadas a la creciente demanda del mercado. Con una presencia regional fuerte y experiencia en la protección de datos, seguridad en la nube, y gestión de identidades, BIOS está bien posicionado para enfrentar los retos actuales, como el aumento de ciberataques en sectores críticos como el financiero, salud, y gobierno. Además, su enfoque en la colaboración público-privada y su capacidad para implementar arquitecturas de seguridad robustas refuerzan su idoneidad en un mercado que requiere respuestas inmediatas y eficientes.

5. ESTUDIO DE MERCADO

Al no existir antecedentes concretos de proyectos de retos de innovación en temas relacionados con ciberseguridad, y para lograr una estimación precisa, el MinTIC de acuerdo con los componentes definidos en el anexo técnico, realizó un estudio de mercado, desarrollado entre el 24 de julio y el 02 de agosto de 2024. Este proceso se realizó para recoger propuestas económicas de organizaciones capacitadas para la ejecución de este tipo de proyectos y poder así, establecer un

presupuesto razonable con los precios del mercado.

Teniendo en cuenta que en el país se encuentran actores estratégicos en esta materia que tienen la capacidad de implementar proyectos con el impacto previsto y que cuentan con una estructura profesional que les permite realizar actividades de ciencia, tecnología e innovación, consultoría y ejecución de proyectos. El Ministerio TIC realizó un ejercicio de identificación de potenciales cotizantes, obteniendo como resultado las siguientes organizaciones que recibieron invitación para presentar cotización:

- **FUNDACIÓN TECNALIA COLOMBIA:** Es un Centro de Innovación y Productividad, sin ánimo de lucro, dedicado a formular y desarrollar proyectos I+D+i con nuevas tecnologías y actividades de transferencia para responder a las necesidades del desarrollo sostenible, con una amplia experiencia de más de 12 años en el mercado nacional nos ha permitido impactar diferentes sectores logrando transferir conocimiento y generar capacidades para la innovación en el territorio nacional y regional.

- **CINTEL:** Es un Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones – CINTEL, reconocida por la ejecución de proyectos orientados a apoyar la transformación digital de las empresas públicas y privadas. Así mismo, la Entidad presenta gran experiencia en proyectos de innovación y desarrollo tecnológico del sector TIC en Colombia, y actualmente lidera diversas iniciativas enfocadas a dinamizar la industria y la apropiación social de la tecnología.

- **BOOST BUSINESS CONSULTING:** Es una empresa de consultoría dedicada a la prestación de servicios empresariales de alto impacto, especializados en transformación digital, estrategia e innovación empresarial, modelos de negocio, auditoria, asesoría fiscal, tributaria, estándares internacionales de información financiera; construimos valor con experiencia.

- **CORPORACIÓN CONNECT BOGOTÁ REGIÓN:** Es una empresa que busca articular los actores del ecosistema de ciencia, tecnología, innovación y emprendimiento para trabajar colaborativamente en iniciativas y proyectos, basados en innovación, que transformen al país y la región, impactando en su desarrollo y competitividad.

- **FEDERACION COLOMBIANA DE LA INDUSTRIA DE SOFTWARE Y TECNOLOGIAS INFORMATICAS RELACIONADAS - FEDESOFT:** Se define como la Federación Colombiana de la Industria del Software y Tecnologías Informáticas. Esta una organización gremial trabaja por el fortalecimiento de la industria del software nacional, para que esta sea competitiva, reconocida, exitosa en el entorno internacional. Así mismo, Fedesoft trabaja en el desarrollo de políticas públicas, el impulso de la formación y la competitividad de las firmas del sector, la generación de información sectorial especializada y la exploración de oportunidades globales que posicionan a Colombia como proveedor tecnológico de talla mundial.

- **E-TRAINING**: Es una empresa con experiencia en la construcción y el desarrollo de procesos de transformación digital de la educación, orientada en crear soluciones innovadoras para la generación de proyectos educativos que fomentan la competitividad, empleabilidad y proyección institucional.

- **CYMETRIA GROUP S.A.S.:** Es una empresa enfocada a realizar negocios digitales y talento tecnológico para empresas, profesionales y startups en Latinoamérica.

- **VT SAS:** Es una Firma consultora en gestión de innovación y desarrollo tecnológico con un amplio portafolio, que permite articular soluciones integrales para establecer las capacidades de innovación en las organizaciones. Dentro de su portafolio, se enfoca en diseñar y desarrollar sistemas de gestión de innovación, usando conceptos y aplicaciones de clase mundial, diseñados a la medida e implementados modularmente, lo cual permite a las organizaciones contar con resultados relevantes en el corto plazo, mientras se construyen las bases de un sistema que

produzca innovaciones de muy alto impacto en el largo plazo.

- **INTERSOFTWARE:** Es una corporación que busca impulsar por el dinamismo del sector productivo, promoviendo el desarrollo y crecimiento económico de las empresas miembros, creando y aprovechando sinergias poderosas dentro de nuestra red.

- **TECNOLOGÍA E INNOVACIÓN INVERSIONES SAS - INVENTTA**: Es una empresa que desarrolla soluciones tecnológicas por medio de la innovación, disponen de un talentoso y multidisciplinario equipo de especialistas que combinan diversas y exitosas metodologías de innovación con visiones amplias, integrales y sistémicas.

A estas diez (10) organizaciones, se les realizó una solicitud de información económica, remitiéndoseles el anexo técnico del proyecto que especifica las actividades a desarrollar durante la ejecución prevista, las calidades de las actividades contempladas y los tiempos de ejecución proyectados; esto con el propósito de trasladar a los destinatarios las características mínimas requeridas para la ejecución y con ello garantizar el entendimiento de los fines y necesidades planteadas. Adicionalmente, se remitió un anexo de cotización, para que diligenciaran los valores propuestos para la ejecución de las estrategias del proyecto requiriendo además la identificación de los costos totales y los asociados a impuestos.

Como resultado de estas invitaciones, en el estudio de mercado para el proyecto de retos de ciberseguridad, se recibieron cotizaciones de siete (7) de las diez (10) organizaciones distintas invitadas, en la que cada una presentó su cotización para desarrollar los componentes requeridos por el proyecto.

Una vez recibidas las mismas, desde la Subdirección de Industria de Tecnologías de la Información, se inicia el proceso de revisión y análisis de las siete (7) cotizaciones recibidas, resumidas así:

COTIZACIONES RETOS CIBERSEGURIDAD 2024

No.	ENTIDAD OFERENTE	VALOR TOTAL
1	BOOST BUSINESS CONSULTING SAS	$2.572.274.250
2	CINTEL	$3.701.499.097
3	CORPORACIÓN CONNECT BOGOTÁ REGIÓN	$2.316.928.691
4	CYMETRIA GROUP S.A.S.	$4.029.340.000
5	FEDERACION COLOMBIANA DE LA INDUSTRIA DE SOFTWARE Y TECNOLOGIAS INFORMATICAS RELACIONADAS - FEDESOFT	$2.496.868.000
6	TECNOLOGÍA E INNOVACIÓN INVERSIONES SAS - INVENTTA	$697.340.000
7	FUNDACIÓN TECNALIA COLOMBIA	$878.750.000

Aplicando la metodología de desviación estándar, se establecieron rangos mínimos y máximos para identificar valores fuera del rango o desviados de la muestra. Con esta metodología, se determinó que cuatro (4) de las siete (7) propuestas (CINTEL, CYMETRIA GROUP S.A.S., TECNOLOGÍA E INNOVACIÓN INVERSIONES SAS – INVENTTA y FUNDACIÓN TECNALIA COLOMBIA) se encontraban por fuera del intervalo estándar establecido, por lo que fueron descartadas para el análisis.

Una vez excluidas estas propuestas, se consideraron las tres (3) ofertas restantes: la de BOOST BUSINESS CONSULTING SAS por $2.572.274.250, la de CORPORACIÓN CONNECT BOGOTÁ REGIÓN por $2.316.928.691, y la de FEDESOFT por $2.496.868.000. A continuación, se presenta el detalle de las cotizaciones:

COMPONENTE	BOOST	CONNECT	FEDESOFT
Componente 1. Identificación, clasificación y conformación de retos tecnológicos.	$209.321.000	$82.966.800	$65.450.000
Componente 2. Mapeo, selección y fortalecimiento de solucionadores tecnológicos.	$715.398.250	$404.885.600	$1.456.808.000
Componente 3. Diseño e implementación de soluciones innovadoras.	$768.145.000	$1.289.484.000	$605.710.000
Componente 4. Difusión tecnológica para el ecosistema de ciberseguridad.	$879.410.000	$539.592.291	$368.900.000
TOTAL GENERAL	**$2.572.274.250**	**$2.316.928.691**	**$2.496.868.000**

Con base en la tabla anterior, se calcula el valor promedio por cada uno de los componentes de las tres (3) cotizaciones válidas para la estimación del presupuesto del proyecto, así, se obtuvo un valor promedio de $2.462.023.647. A continuación, se presenta el detalle del cálculo:

COMPONENTE	PROMEDIO
Componente 1. Identificación, clasificación y conformación de retos tecnológicos.	$119.245.933
Componente 2. Mapeo, selección y fortalecimiento de solucionadores tecnológicos.	$859.030.617
Componente 3. Diseño e implementación de soluciones innovadoras.	$887.779.667
Componente 4. Difusión tecnológica para el ecosistema de ciberseguridad.	$595.967.430
TOTAL GENERAL	**$2.462.023.647**

En resumen, el estudio de mercado realizado nos permite determinar que, para este proyecto, deberá contarse con un presupuesto de DOS MIL CUATROCIENTOS SESENTA Y DOS MILLONES VEINTITRÉS MIL SEISCIENTOS CUARENTA Y SIETE PESOS M/CTE. ($2.462.023.647).

6. ANÁLISIS DEL ALIADO EJECUTOR

Para el presente convenio, la entidad aliada y ejecutora del proyecto será el Centro de Bioinformática y Biología Computacional de Colombia - BIOS, conforme las siguientes consideraciones:

BIOS posee experiencia probada en materia de ejecución de proyectos de alto impacto que impliquen procesos de innovación, desarrollo tecnológico y el estudio de escenarios que promuevan gestión del conocimiento. se desea destacar la siguiente experiencia con el MinTIC que resulta fundamental para el objeto del convenio que se pretende suscribir:

#	PROYECTO	OBJETO	ENTIDAD	FECHA INICIO	DURACIÓN	VALOR
1	Centro de inteligencia artificial aplicada	Aunar esfuerzos técnicos administrativos y financieros para el desarrollo de proyectos de ciencia tecnología e innovación con énfasis en los sectores estratégicos de las Direcciones del gobierno en línea, políticas y Desarrollo de TI, I+D+I, que permitan el desarrollo de los objetivos planteados en el plan estratégico del Min TIC	MinTIC	23/08/2017	12 meses	$ 7.944.877.927
2	Diseñar el Centro de Servidos Compartidos de Transformación Digital (CSCTD) para la atención de retos institucionales o empresariales a partir del uso de nuevas tecnologías tales como Inteligencia Artificial, el rediseño de los centros de excelencia y apropiación en BigData, IoT de conformidad a las Hojas de Ruta Regionales de Transformación Digital	"Diseñar el Centro de Servidos Compartidos de Transformación Digital (CSCTD) para la atención de retos institucionales o empresariales a partir del uso de nuevas tecnologías tales como Inteligencia Artificial, el rediseño de los centros de excelencia y apropiación en BigData, IoT de conformidad a las Hojas de Ruta Regionales de Transformación Digital, garantizando la formulación y ejecución de proyectos que brinden soluciones a los sectores de la economía que coadyuven al desarrollo de las empresas en sus diferentes iniciativas regionales y nacionales. Toda la información resultante usará las capacidades e infraestructura computacional de alto desempeño con la que actualmente cuenta BIOS"	FONTIC	19/12/2019	12 meses	$ 1.970.966.877
3	Implementación de la Red Nacional de Supercomputación	El objetivo principal del convenio especial de cooperación es aunar esfuerzos técnicos, administrativos y financieros, para realizar las acciones y estrategias correspondientes para la creación y articulación de la Red Nacional de Servicios de Computación de Alto Rendimiento.	MinTIC	18/02/2021	10 meses	$ 1.231.948.648
4	Resolución 00528: Por la cual se ordena un gasto como aporte	Por la cual se ordena un gasto como aporte al Centro de Bioinformática y Biología Computacional de Colombia o BIOS o CBBC con NIT 900.404.482-6.	MINTIC	24/07/2023	5 meses	$ 1.500.000.000

#	PROYECTO	OBJETO	ENTIDAD	FECHA INICIO	DURACIÓN	VALOR
5	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.	Aunar esfuerzos para desarrollar un ecosistema de seguridad digital que impulse procesos de innovación y desarrollo tecnológico, mediante el estudio de escenarios que promuevan la gestión del conocimiento de los riesgos cibernéticos y las afectaciones de los incidentes de seguridad digital entre los diferentes grupos poblacionales del territorio colombiano.	MINTIC	17/11/2023	1 mes y medio	$ 5.100.000.000

Adicionalmente, BIOS está equipado con tecnología de vanguardia, incluyendo potentes sistemas informáticos, redes de alta velocidad y acceso a recursos especializados en ciberseguridad, capacidades que le permiten simulaciones complejas y tareas intensivas de analítica de datos que resultan fundamentales para soportar planes de capacitación en materia de ciberseguridad. Desde dicha óptica, poseer infraestructura de supercomputación disponible le permite abordar problemas complejos de ciberseguridad mediante el uso de técnicas de paralelismo, acelerando el tiempo de entrenamiento y de análisis de datos, condiciones especialmente útiles cuando se trata de grandes volúmenes de información y análisis de malware, condiciones objetivas que permiten a BIOS simular entornos de red y sistemas informáticos reales para que los beneficiarios del convenio practiquen sus habilidades en escenarios más cercanos a situaciones del mundo real, contribuyendo a mejorar la preparación para enfrentar amenazas reales y desarrollar habilidades prácticas.

BIOS es un reconocido actor del ecosistema de ciencia y tecnología de la nación, capaz de articular actores públicos y privados para la gestión de conocimiento y el impulso de procesos de alto impacto, sumando dentro sus aliados para la estructuración de planes, mejoramiento de capacidades y formación del recurso humano, con la Universidad Nacional de Colombia, la Universidad de Caldas y la Universidad Tecnológica de Pereira, contando además con acceso a recursos especializados en materia de ciberseguridad al amparo de acuerdos con actores de mercado reconocidos tales como IBM, Bulkware, Td Synnex y Lenovo, entre otros, relacionamiento que confieren a dicho Centro la capacidad para satisfacer la necesidad del Ministerio. Sin perjuicio de lo anterior, BIOS posee además otras potencialidades:

- **Especialidad, unicidad y vínculo especial con el Ministerio de Tecnologías de la Información y las Comunicaciones**

BIOS es una entidad única en Colombia que combina una amplia gama de especialidades, incluyendo bioinformática, ciencia de datos, ciberseguridad, computación de alto rendimiento (HPC) e infraestructura tecnológica. Su misión, centrada en la generación de valor a través de la incorporación efectiva de tecnologías avanzadas en el ecosistema de tecnología del país, hace que BIOS sea un actor fundamental en el sector tecnológico y de ciberseguridad. Aquí cabe resaltar que BIOS fue creada por iniciativa de la Nación como corporación sin ánimo de lucro de carácter privado, contando con participación de MinTIC en su Junta Directiva, siendo históricamente el principal aportante del Centro.

- **Liderazgo en Ciberseguridad**

BIOS es el líder promotor del HUB de Ciberseguridad (ubicado en el municipio de Villamaría) en concurso con la Gobernación del Departamento de Caldas. Para tal efecto, BIOS cuenta con la manifestación de un número importante de actores, tanto de la academia como del sector real, interesadas en ofrecer coordinadamente sus productos y servicios a través del HUB para fortalecer las capacidades técnicas y humanas del país en materia de ciberseguridad, así: i. Actores empresariales: Dragonjar, Kavantic, Data & Service, IBM, TD Synnex, Global AST, People Contact, Bulwark, IT Forensic, Fygp, Innerconsulting, Lenovo, Hispasec; ii. Actores académicos: Universidad de Manizales, Universidad Católica de Manizales, Universidad Católica Luis Amigó, Universidad Nacional Abierta y a Distancia, Universidad Autónoma de Manizales y Universidad de Caldas; y iii. Actores gremiales: Acopi, Fenalco, Fundacion Universidad Empresa, Red de Emprendimiento y ARCIS.

- **Respaldo y soporte profesional en Ciberseguridad**

El talento humano es uno de sus mayores activos de BIOS, contando con profesionales de la ingeniería, expertos en programación, ciencia de datos, y ciberseguridad, tanto en su equipo interno, como provenientes de las universidades públicas del Eje Cafetero que concurren al Centro. En el ámbito de la ciberseguridad, BIOS ostenta un relacionamiento que le permiten acceder a conocimiento especializado desde una visión crítica fundada en las diversas tecnologías disponibles en el mercado, otorgándole la capacidad de procurar soluciones agiles en beneficio de la Nación.

También es importante recalcar que el aporte de contrapartida que hará BIOS al Convenio, por $198.130.056 (ciento noventa y ocho millones ciento treinta mil cincuenta y seis pesos) en especie, están representados en recurso humano con experticia en metodologías de proyectos ágiles para los temas de TI, lo que brinda respaldo profesional especializado en favor del proyecto.

- **Experiencia en materia de proyectos de alto impacto**

BIOS ha demostrado su experiencia y capacidad para manejar proyectos de gran envergadura en el ámbito de la ciberseguridad, la bioinformática, la ciencia de datos y las tecnologías avanzadas. Sus proyectos en formación incluyen la creación de aulas virtuales para ofrecer cursos avanzados de tecnología propios y de las universidades vinculadas, la capacitación de empresarios en tecnología y la formación avanzada de investigadores en diversas tecnologías avanzadas. Además, ha sido ejecutor habitual y cumplido de los proyectos estratégicos de MinTIC desde 2011 y de regalías de ciencia y tecnología desde 2021.

Además, la propuesta técnica y económica presentada por el CENTRO DE BIOINFORMÁTICA Y BIOLOGÍA COMPUTACIONAL DE COLOMBIA – BIOS, por un valor total de MIL OCHOCIENTOS OCHENTA Y SEIS MILLONES NOVECIENTOS CINCUENTA Y DOS MIL NOVECIENTOS TRECE PESOS M/CTE. ($1.886.952.913) está no solo dentro del rango de análisis del estudio de mercado obtenido mediante la metodología de desviación estándar, sino que representa un valor de aproximadamente el 77% del valor promedio obtenido en el estudio que permite concluir que la propuesta plantea unos costos razonables con los valores de mercado consultados. El detalle de esta propuesta se presenta a continuación:

COMPONENTE	PROPUESTA BIOS
Componente 1. Identificación, clasificación y conformación de retos tecnológicos.	$242.526.251
Componente 2. Mapeo, selección y fortalecimiento de solucionadores tecnológicos.	$572.236.186

COMPONENTE	PROPUESTA BIOS
Componente 3. Diseño e implementación de soluciones innovadoras.	$757.404.830
Componente 4. Difusión tecnológica para el ecosistema de ciberseguridad.	$314.785.646
TOTAL GENERAL	**$1.886.952.913**

En adición de lo anterior, BIOS también propone un aporte en especie por un valor de CIENTO NOVENTA Y OCHO MILLONES CIENTO TREINTA MIL CINCUENTA Y SEIS PESOS ($198.130.056) en especie representados en recurso humano para el desarrollo de actividades técnicas y de administración del proyecto y que agrega valor al desarrollo de las actividades y permite fortalecer la decisión de ejecutar el proyecto de retos de innovación en materia de ciberseguridad mediante un convenio especial de cooperación con BIOS.

7. CONCLUSIONES

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

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

MATRIZ DE RIESGOS RECOMENDADA PARA EL PROCESO:		ÁREA SOLICITANTE:	DIRECCIÓN DE ECONOMÍA DIGITAL - SUBDIRECCIÓN DE INDUSTRIA TI		
129 CONVENIO ESPECIAL DE COOPERACIÓN - CIBERSEGURIDAD		TIPO DE CONTRATO:	Convenio Especial de Cooperación	Modalidad de Selección:	Contratación Directa

OBJETO CONTRACTUAL:

33200401811 - Aunar esfuerzos técnicos, administrativos, y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.

IDENTIFICACIÓN, CLASIFICACIÓN Y ASIGNACIÓN								CALIFICACIÓN CUALITATIVA Y VALORACIÓN						PLAN DE TRATAMIENTO						MONITOREO Y REVISIÓN		
										Valoración												
No.	Clase	Fuente	Etapa	Tipo	RIESGO (Descripción)	CONSECUENCIA (de la ocurrencia del evento)	ASIGNACIÓN (Entidad Estatal/ Ejecutor / Cooperante)	Probabilidad	Impacto	Probabilidad	Impacto	Total	Categoría Mapa de Riesgo	TRATAMIENTO - CONTROL	Persona responsable por implementar el tratamiento	EVITAR	TRANSFERIR	ACEPTAR	REDUCIR PROBABILIDAD	REDUCIR IMPACTO	FECHA ESTIMADA EN QUE SE COMPLETA EL TRATAMIENTO	CÓMO SE REALIZA EL MONITOREO	PERIODICIDAD
1	General	Interno	Planeación	Planeación	Efectos desfavorables por indebida escogencia de la modalidad de selección del Ejecutor / Cooperante.	La concreción de este riesgo puede traer consigo consecuencias en materia de responsabilidad penal y/o disciplinaria para los funcionarios y/o colaboradores del ministerio cuya competencia funcional verse en punto de la definición de la modalidad de selección.	MinTIC-FUTIC	BAJO	BAJO	2	2	4	Riesgo Bajo	La Entidad reduce la probabilidad de ocurrencia de este riesgo mediante la aplicación rigurosa de la normatividad vigente y de los procesos y procedimientos en materia de gestión contractual adoptados por la Entidad. Consecuentemente, es recomendable realizar una actualización permanente de dicho instrumento, de modo que el mismo responda a las novedades que presente el ordenamiento jurídico.	En virtud de las funciones y competencias asignadas a la Subdirección de Gestión Contractual, será ésta la dependencia encargada de impartir el tratamiento a que haya lugar.				X		El monitoreo se completa en la fecha en que la Subdirección de Gestión Contractual convoque al Comité Asesor de Contratación de la Entidad con el propósito de poner en su consideración el proceso de selección.	Mediante la realización de mesas de trabajo al interior de la Subdirección de Gestión Contractual, y el Comité Asesor de Contratación de la Entidad.	Por lo menos una vez, previo a la aprobación por parte del Comité Asesor de Contratación de la Entidad.
2	Específico	Interno	Planeación	Planeación	Efectos desfavorables por deficiencias en la planeación del proceso de contratación.	La concreción de este riesgo puede traer consigo la insatisfacción de la necesidad que originó el proceso de contratación.	MinTIC-FUTIC	BAJO	BAJO	2	2	4	Riesgo Bajo	El área originadora estructura todos los elementos del futuro negocio jurídico de modo que a través del mismo se logre la cabal satisfacción de la necesidad que pretende atender la entidad.	El área originadora es la responsable de implementar el tratamiento respectivo y designar el responsable de ejercer el mismo.				X		Con la fecha de aprobación del Comité asesor de Contratación y publicación de los documentos precontractuales	Mediante la realización de mesas de trabajo al interior de la Subdirección de Gestión Contractual, y el Comité Asesor de Contratación de la Entidad.	Por lo menos una vez, previo a la aprobación por parte del Comité Asesor de Contratación.
3	Específico	Interno	Selección	Selección	Efectos desfavorables por indebida escogencia de la tipología contractual del futuro negocio jurídico.	La concreción de este riesgo puede traer como consecuencia posibles reprocesos administrativos, así como los correlativos costos adicionales para la Entidad.	MinTIC-FUTIC	BAJO	BAJO	2	2	4	Riesgo Bajo	La dependencia solicitante, durante la etapa de estructuración desarrollará mesas de trabajo con la participación del equipo interdisciplinario (técnico y jurídico), con el apoyo de la Subdirección de Gestión Contractual, en la cual se plantearán los respectivos análisis de cara a la adecuada escogencia de la tipología contractual aplicable.	La dependencia originadora del proceso de selección será responsable de implementar el tratamiento respectivo, contando con el respaldo de la Subdirección de Gestión Contractual. Para lo cual las respectivas áreas define(n) el (o los) colaborador(es) a cargo del tratamiento.	X					El monitoreo se completa en la fecha en que la Subdirección de Gestión Contractual convoque al Comité de Contratación con el propósito de poner en su consideración el proceso de selección.	Mediante la realización de mesas de trabajo al interior de la Subdirección de Gestión Contractual, y el Comité Asesor de Contratación de la Entidad.	Por lo menos una vez, previo a la aprobación por parte del Comité Asesor de Contratación.

MATRIZ DE RIESGOS RECOMENDADA PARA EL PROCESO:		ÁREA SOLICITANTE:	DIRECCIÓN DE ECONOMÍA DIGITAL - SUBDIRECCIÓN DE INDUSTRIA TI		
129 CONVENIO ESPECIAL DE COOPERACIÓN - CIBERSEGURIDAD		TIPO DE CONTRATO:	Convenio Especial de Cooperación	Modalidad de Selección:	Contratación Directa

OBJETO CONTRACTUAL:

33200401811 - Aunar esfuerzos técnicos, administrativos, y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.

IDENTIFICACIÓN, CLASIFICACIÓN Y ASIGNACIÓN								CALIFICACIÓN CUALITATIVA Y VALORACIÓN						PLAN DE TRATAMIENTO						MONITOREO Y REVISIÓN		
										Valoración												
No.	Clase	Fuente	Etapa	Tipo	RIESGO (Descripción)	CONSECUENCIA (de la ocurrencia del evento)	ASIGNACIÓN (Entidad Estatal/ Ejecutor / Cooperante)	Probabilidad	Impacto	Probabilidad	Impacto	Total	Categoría Mapa de Riesgo	TRATAMIENTO - CONTROL	Persona responsable por implementar el tratamiento	EVITAR	TRANSFERIR	ACEPTAR	REDUCIR PROBABILIDAD	REDUCIR IMPACTO	FECHA ESTIMADA EN QUE SE COMPLETA EL TRATAMIENTO	CÓMO SE REALIZA EL MONITOREO	PERIODICIDAD
4	Específico	Interno	Selección	Selección	Efectos desfavorables por la indebida observancia de la cadena presupuestal que soporta el proceso de selección.	La concreción de este riesgo puede traer consigo consecuencias en materia de responsabilidad fiscal y/o disciplinaria para los funcionarios y/o colaboradores del Ministerio cuya competencia funcional se relacione con la definición presupuestal que soporta el proceso de selección. La concreción de este riesgo puede traer como consecuencia posibles reprocesos administrativos, así como los correlativos costos adicionales para la Entidad.	MinTIC-FUTIC	**BAJO**	**BAJO**	2	2	4	**Riesgo Bajo**	La dependencia solicitante, durante la etapa de estructuración desarrolla mesas de trabajo con la participación del equipo interdisciplinario (técnico y jurídico), en la cual se plantearán los respectivos análisis de cara a la observancia de la planeación presupuestal aplicable al proceso concursal que se depende adelantar.	La dependencia originadora será responsable de implementar el tratamiento respectivo.	X					El monitoreo se completa en la fecha en que la Subdirección de Gestión Contractual convoque al Comité Aseor de Contratación con el propósito de poner en su consideración el proceso bajo análisis.	Mediante la realización de mesas de trabajo entre el área originadora y las dependencias cuya función verse respecto del cumplimiento de la planeación y observancia de la cadena presupuestal del proceso concursal.	Por lo menos una vez, previo a la aprobación por parte del Comité Asesor de Contratación
5	General	Interno	Contratación	Contratación	Efectos desfavorables por retraso en el cumplimiento de los requisitos de ejecución del Convenio Especial de Cooperación, por causas atribuibles al Ejecutor / Cooperante.	Mayores costos y plazos asociados al proceso de contratación e imposibilidad de ejecutar el Convenio Especial de Cooperación.	MinTic FUTIC / Ejecutor / Cooperante	**BAJO**	**BAJO**	2	2	4	**Riesgo Bajo**	La Entidad reduce la probabilidad de este riesgo desde el establecimiento de procesos y procedimientos que permiten una gestión adecuada de los tiempos. Desde la etapa precontractual la entidad ha fijado los plazos para lograr los requisitos de ejecución. En caso de que se presenten retrasos en el cumplimiento de los requistos de ejecución del Convenio Especial de Cooperación y éstos sean atribuibles al Ejecutor / Cooperante, la Entidad estudiará la procedencia de ejercer la potestad sancionatoria contractual.	El área originadora será la encargada de implementar el tratamiento respectivo.				X		Hasta la fecha de inicio de la ejecución del negocio jurídico.	La supervisión y/o Comité Operativo del negocio jurídico verificará el cumplimiento de los requisitos de ejecución del mismo.	Diariamente, desde la adjudicación del Convenio Especial de Cooperación hasta el inicio efectivo de su ejecución.
6	Específico	Externo	Contratación	Económico	Efectos desfavorables o favorables por no estimar adecuadamente la oferta o los conceptos necesarios para el cumplimiento del objeto del Convenio Especial de Cooperación.	El proponente no estima adecuadamente la oferta o los conceptos necesarios para el cumplimiento del objeto solicitado, lo cual podría redundar en eventuales inconvenientes o incumplimiento durante el plazo de ejecución del Convenio Especial de Cooperación.	Ejecutor / Cooperante	**BAJO**	**BAJO**	2	2	4	**Riesgo Bajo**	En los estudios y documentos previos la Entidad debe dejar constancia del fundamento para considerar las condiciones de uno u otro Ejecutor / Cooperante como las más favorables. En virtud del principio de planeación, es responsabilidad del Ejecutor / Cooperante estimar adecuadamente su oferta y los flujos de recursos monetarios para ejecutar el alcance solicitado por la Entidad.	El responsable de la implementación del tratamiento es el Ejecutor / Cooperante.		X				Hasta el plazo de liquidación del Convenio Especial de Cooperación.	El Ejecutor / Cooperante deberá hacer la debida diligencia para estimar adecuadamente su oferta económica.	Permanente, desde la publicación del Convenio Especial de Cooperación, hasta la fecha de liquidación del Convenio Especial de Cooperación.

MATRIZ DE RIESGOS RECOMENDADA PARA EL PROCESO:		ÁREA SOLICITANTE:	DIRECCIÓN DE ECONOMÍA DIGITAL - SUBDIRECCIÓN DE INDUSTRIA TI		
129 CONVENIO ESPECIAL DE COOPERACIÓN - CIBERSEGURIDAD		TIPO DE CONTRATO:	Convenio Especial de Cooperación	Modalidad de Selección:	Contratación Directa

OBJETO CONTRACTUAL:

33200401811 - Aunar esfuerzos técnicos, administrativos, y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.

IDENTIFICACIÓN, CLASIFICACIÓN Y ASIGNACIÓN								CALIFICACIÓN CUALITATIVA Y VALORACIÓN						PLAN DE TRATAMIENTO							MONITOREO Y REVISIÓN		
										Valoración													
No.	Clase	Fuente	Etapa	Tipo	RIESGO (Descripción)	CONSECUENCIA (de la ocurrencia del evento)	ASIGNACIÓN (Entidad Estatal/ Ejecutor / Cooperante)	Probabilidad	Impacto	Probabilidad	Impacto	Total	Categoría Mapa de Riesgo	TRATAMIENTO - CONTROL	Persona responsable por implementar el tratamiento	EVITAR	TRANSFERIR	ACEPTAR	REDUCIR PROBABILIDAD	REDUCIR IMPACTO	FECHA ESTIMADA EN QUE SE COMPLETA EL TRATAMIENTO	CÓMO SE REALIZA EL MONITOREO	PERIODICIDAD
7	General	Externo	Ejecución	Operacional	Efectos desfavorables por alteración, modificación y/o divulgación indebida de la información, violación de seguridad de datos personales o confidenciales.	Sanciones, económicas y/o legales por el uso indebido de los datos o aquella información a que pueda tener acceso en virtud de la ejecución del Convenio Especial de Cooperación.	Ejecutor / Cooperante	BAJO	BAJO	2	2	4	Riesgo Bajo	El Ejecutor / Cooperante debe implementar protocolos, adoptar estrategias de seguridad y privacidad de la información que definan salvaguardias administrativas, técnicas y físicas adecuadas para proteger la seguridad de la información y los datos personales, así como tomar acciones para evitar el acceso o uso no autorizados de información o datos catalogados como clasificados o reservados. El Ejcutor/Ejecutor / Cooperante deberá contar con planes de contingencia, que permita el aseguramiento de los activos que hacen parte del Convenio Especial de Cooperación perminiento volver a condiciones de operación en caso de fallas y contar con niveles de seguridad que salvaguarden la información y su confidencialidad de ser el caso. Y conocer los protocolos dispuestos por la entidad para tal fin.	Corresponde al Ejecutor / Cooperante implementar el tratamiento respectivo.		X				Hasta el plazo de liquidación del Convenio Especial de Cooperación.	La supervisión y/o Comité Operativo del Convenio Especial de Cooperación deberá hacer seguimiento de la efectiva y eficiente implementación de las medidas adoptadas por parte del Ejecutor / Cooperante así como la aplicación de las medidas dispuestas por la Entidad para garantizar la seguridad de la información y la salvaguarda de la confidencialidad de los datos personales. El Ejecutor / Cooperante dispondrá de toda la información necesaria para documentar el cumplimiento del Convenio Especial de Cooperación a partir de reuniones, registros, actas, informes, y en general actividades que permitan realizar el seguimiento de esta.	Permanente
8	Específico	Externo	Ejecución	Operacional	Efectos desfavorables por la falta de aptitud técnica del personal dispuesto por el Ejecutor / Cooperante para la ejecución del Convenio Especial de Cooperación.	La falta de aptitud técnica por parte del personal del Ejecutor / Cooperante, puede traer como consecuencia retrasos en la ejecución de las actividades, así como reprocesos en las mismas, ocasionando costos adicionales a cargo del Ejecutor / Cooperante.	Ejecutor / Cooperante	BAJO	BAJO	2	2	4	Riesgo Bajo	De llegar a concretarse el riesgo, corresponderá al Ejecutor / Cooperante contar con un plan de contingencia que le permita disminuir el impacto generado por el acaeciminento del mismo. Se recomienda que el Ejecutor / Cooperante comparta dicho plan al Supervisor y/o Comité Operativo, a efectos de garantizar el efectivo seguimiento sobre la ejecución del Convenio Especial de Cooperación.	Corresponde al Ejecutor / Cooperante implementar el tratamiento respectivo.		X				Durante el plazo de ejecución del Convenio Especial de Cooperación.	Por su parte, La supervisión y/o Comité Operativo del conrato deberá hacer seguimiento de la efectiva y eficiente implementación de las medidas adoptadas por parte del Ejecutor / Cooperante. El Ejecutor / Cooperante dispondrá de toda la información necesaria para documentar las acciones pertinentes a partir de reuniones, registros, actas, informes, y en genera actividades que permitan realizar el seguimiento del Convenio Especial de Cooperación.	Desde la publicación del Convenio Especial de Cooperación, hasta la fecha de liquidación del Convenio Especial de Cooperación.
9	General	Externo	Ejecución	Operacional	Efectos desfavorables por inadecuados procesos, procedimientos y/o requisitos que impidan la adecuada ejecución del Convenio Especial de Cooperación por causas atribuibles al Ejecutor / Cooperante.	La concreción de este riesgo puede implicar la imposibilidad de ejecutar el Convenio Especial de Cooperación o en la satisfacción no oportuna de la necesidad que la entidad requiere atender.	Ejecutor / Cooperante	MEDIO	MEDIO	3	3	6	Riesgo Alto	El Ejecutor / Cooperante debe contar con las herramientas y condiciones que le permitan prevenir la ocurrencia del riesgo, contemplando los protocolos, los procedimientos y actividades que le permitan garantizar el pleno y oportuno cumplimiento de los requisitos necesarios para el cabal cumplimiento de sus obligaciones y dar continuidad a la ejecución contractual, teniendo en cuenta que los proyectos de creación digital y demás obligaciónes sean acordes con la oportunidad y pertinencia cultural y social realizados por los grupos étnicos y/o sociales en el marco del convenio.	El responsable de la implementación del tratamiento es el Ejecutor / Cooperante.		X				Hasta la finalización del plazo de ejecución del Convenio Especial de Cooperación.	El Ejecutor / Cooperante es el responsable de la implementación del tratamiento, por lo que dispondrá de toda la información necesaria para documentar el tratamiento del riesgo a partir de reuniones, registros, actas, informes, y en general actividades que permitan realizar el seguimiento de esta.	Permanente

MATRIZ DE RIESGOS RECOMENDADA PARA EL PROCESO:		ÁREA SOLICITANTE:	DIRECCIÓN DE ECONOMÍA DIGITAL - SUBDIRECCIÓN DE INDUSTRIA TI		
129 CONVENIO ESPECIAL DE COOPERACIÓN - CIBERSEGURIDAD		TIPO DE CONTRATO:	Convenio Especial de Cooperación	Modalidad de Selección:	Contratación Directa

OBJETO CONTRACTUAL:

33200401811 - Aunar esfuerzos técnicos, administrativos, y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.

IDENTIFICACIÓN, CLASIFICACIÓN Y ASIGNACIÓN								CALIFICACIÓN CUALITATIVA Y VALORACIÓN						PLAN DE TRATAMIENTO						MONITOREO Y REVISIÓN		
										Valoración												
No.	Clase	Fuente	Etapa	Tipo	RIESGO (Descripción)	CONSECUENCIA (de la ocurrencia del evento)	ASIGNACIÓN (Entidad Estatal/ Ejecutor / Cooperante)	Probabilidad	Impacto	Probabilidad	Impacto	Total	Categoría Mapa de Riesgo	TRATAMIENTO - CONTROL	Persona responsable por implementar el tratamiento	EVITAR	TRANSFERIR	ACEPTAR	REDUCIR PROBABILIDAD	REDUCIR IMPACTO	FECHA ESTIMADA EN QUE SE COMPLETA EL TRATAMIENTO	CÓMO SE REALIZA EL MONITOREO	PERIODICIDAD
10	Específico	Externo	Ejecución	Operacional	Efectos desfavorables ocasionados por la pérdida o el indebido tratamiento de la información, recursos físicos o moneratarios que generen inconvenientes en la ejecución de los compromisos u obligaciones por causas atribuibles al Ejecutor / Cooperante.	Eventual demora en las actividades durante la ejecución del Convenio Especial de Cooperación. Eventualmente se podrían presentar mayores plazos costos de ejecución.	Ejecutor / Cooperante	**MEDIO**	**BAJO**	3	2	5	**Riesgo Medio**	El Ejecutor / Cooperante deberá tomar todas las medidas que sean necesarias para dar continuidad a la ejecución del Convenio Especial de Cooperación, contemplando medios alternativos para atender las actividades afectadas de modo que pueda tomar aquellas medidas que resulten necesarias, pertinentes y oportunas para garantizar la realización de las actividades y manejo de la información en el marco del negocio jurídico.	Corresponde al Ejecutor / Cooperante la implementación del tratamiento respectivo.		X				Hasta el plazo de ejecución del Convenio Especial de Cooperación.	La supervisión y/o Comité Operativo del Convenio Especial de Cooperación verificará la correcta implementación del tratamiento. Por su parte, el Ejecutor / Cooperante realizará permanente revisión de la efectividad de las medidas tomadas en virtud del tratamiento descrito.	Permanente
11	General	Externo	Ejecución	Operacional	Efectos desfavorables por inadecuados procesos, procedimientos y/o parámetros, en el manejo de la información, equipos y/o de los activos / o de las actividades previstas en el marco de la ejecución del Convenio Especial de Cooperación por parte del Ejecutor / Cooperante.	La concreción de este riesgo puede implicar la imposibilidad de ejecutar el Convenio Especial de Cooperación en el plazo fijado o en la satisfacción no oportuna de la necesidad que la entidad requiere atender.	Ejecutor / Cooperante	**MEDIO**	**MEDIO**	3	3	6	**Riesgo Alto**	El Ejecutor / Cooperante deberá implementar protocolos y prácticas de seguridad de la información, equipos, procesos y procedimientos que se administren en virtud de la ejecución del Convenio Especial de Cooperación. El Ejecutor / Cooperante debe contar con las herramientas y condiciones que le permitan prevenir la ocurrencia del riesgo, contemple además de los protocolos los procedimientos y actividades que le permita garantizar la ejecucuión de las atividades y contar con planes de contingencia ante eventuales inconvenientes, garantizando la continuidad del negocio.	El responsable de la implementación del tratamiento es el Ejecutor / Cooperante.		X				Hasta la finalización del plazo de ejecución del Convenio Especial de Cooperación.	El Ejecutor / Cooperante es el responsable de la implementación del tratamiento, por lo que dispondrá de toda la información necesaria para documentar el tratamiento del riesgo a partir de reuniones, registros, actas, informes, y en general actividades que permitan realizar el seguimiento de esta.	Permanente
12	Específico	Externo	Ejecución	Operacional	Efectos favorables o desfavorables por la no observancia de los requisitos legales, normas presupuestales y de inversión de los recursos o restitución de excedentes a que haya lugar y/o de las obligaciones encomendadas acorde con el Objeto del Convenio Especial de Cooperación.	La concreción de este riesgo puede traer como consecuencia retrasos en el cumplimiento del objeto del Convenio Especial de Cooperación, o incluso poner en riesgo el cumplimiento cabal y oportuno de las obligaciones derivadas del mismo.	Ejecutor / Cooperante	**MEDIO**	**MEDIO**	3	3	6	**Riesgo Alto**	El Ejecutor / Cooperante deberá generar estrategias que permitan identificar la ocurrencia de situaciones que afecten el cumplimiento de las especificaciones y obligaciones que emanan del Convenio Especial de Cooperación, de modo que sea posible tomar las medidas necesarias para lograr la cabal ejecución del mismo. El Ejecutor / Cooperante, deberá dar aviso al MinTIC/ Fondo Único TIC de la ocurrencia de estos eventos, debidamente sustentados. Así mismo, las partes concertarán las medidas a tomar para evitar la paralización de la ejecución y logro de los objetivos propuestos independiente de los actos administrativos sanionatorios a que haya lugar.	El responsable de la implementación del tratamiento es el Ejecutor / Cooperante.					X	Hasta la finalización del plazo de ejecución del Convenio Especial de Cooperación.	Por su parte, la Supervisión / Junta Administradora del Convenio Especial de Cooperación, deberán hacer seguimiento de la efectiva y eficiente implementación de las medidas adoptadas por parte del Ejecutor / Cooperante. El Ejecutor / Cooperante dispondrá de toda la información necesaria para documentar las acciones pertinentes a partir de reuniones, registros, actas, informes, y en general de aquellas actividades que permitan realizar el seguimiento del obligaciones que emanan del Convenio Especial de Cooperación y demás documentos que lo integran.	Permanente

MATRIZ DE RIESGOS RECOMENDADA PARA EL PROCESO:		ÁREA SOLICITANTE:	DIRECCIÓN DE ECONOMÍA DIGITAL - SUBDIRECCIÓN DE INDUSTRIA TI		
129 CONVENIO ESPECIAL DE COOPERACIÓN - CIBERSEGURIDAD		TIPO DE CONTRATO:	Convenio Especial de Cooperación	Modalidad de Selección:	Contratación Directa

OBJETO CONTRACTUAL:

33200401811 - Aunar esfuerzos técnicos, administrativos, y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.

IDENTIFICACIÓN, CLASIFICACIÓN Y ASIGNACIÓN								CALIFICACIÓN CUALITATIVA Y VALORACIÓN						PLAN DE TRATAMIENTO						MONITOREO Y REVISIÓN		
										Valoración												
No.	Clase	Fuente	Etapa	Tipo	RIESGO (Descripción)	CONSECUENCIA (de la ocurrencia del evento)	ASIGNACIÓN (Entidad Estatal/ Ejecutor / Cooperante)	Probabilidad	Impacto	Probabilidad	Impacto	Total	Categoría Mapa de Riesgo	TRATAMIENTO - CONTROL	Persona responsable por implementar el tratamiento	EVITAR	TRANSFERIR	ACEPTAR	REDUCIR PROBABILIDAD	REDUCIR IMPACTO	FECHA ESTIMADA EN QUE SE COMPLETA EL TRATAMIENTO	CÓMO SE REALIZA EL MONITOREO	PERIODICIDAD
13	Específico	Interno	Ejecución	Operacional	Efectos desfavorables como consecuencia de errores o inconsistencias por causas atribuibles al Ejecutor / Cooperante en desarrollo de cualquiera de las actividades en cumplimiento de las obligaciones que emanan del Convenio Especial de Cooperación.	Las inconsistencias o errores asociados a la calidad de los desarrollos, material, herramientas, plataformas y/o diseño de dibulgación y de más actividades y entregables en virtud de las obligaciones a su cargo del Ejecutor / Cooperante, que puedan traer como consecuencia reprocesos, costos administrativos e insatisfacción de la necesidad que se pretende satisfacerse con el futuro Convenio Especial de Cooperación.	Ejecutor / Cooperante	**MEDIO**	**MEDIO**	3	3	6	**Riesgo Alto**	El Ejecutor / Cooperante deberá garantizar la calidad de los desarrollos, material, las herramientas, plataformas y diseño de material de divulgación y demás obligaciones contempladas durante la ejecución del Convenio Especial de Cooperación y que con ello no se vea afectada la imagen del Ministerio ni los objetivos que se pretenden con el desarrolo del mismo.	El responsable de la implementación del tratamiento es el Ejecutor / Cooperante.		X				Hasta la finalización del plazo de ejecución del Convenio Especial de Cooperación.	El Ejecutor / Cooperante dispondrá de toda la información necesaria para documentar el cumplimiento del Convenio Especial de Cooperación y la calidad de la información entregada por ejemplo, a partir de reuniones, registros, actas, informes, y en general actividades que permitan realizar el seguimiento respectivo. Se hará el monitoreo y seguimiento con los informes de las actividades realizadas durante el mes o periodo, al igual que con los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos en cada actividad encomendada, cuando así se requiera, así como con reuniones y mesas de trabajo	Permanente
14	Específico	Externo	Ejecución	Operacional	Efectos desfavorables por interrupciones en la ejecución del objeto del Convenio Especial de Cooperación por fallas atribuibles al Ejecutor / Cooperante por demoras en las actividades técnicas, operativas y de gestión, necesarias para implementar las obligaciones y actividades a desarrollar en el marco del Convenio Especial de Cooperación.	La concreción de este riesgo puede traer como consecuencia retrasos en el cumplimiento del plan de trabajo adoptado para la ejecución del Convenio Especial de Cooperación, o incluso poner en riesgo el cumplimiento cabal y oportuno de las obligaciones derivadas del mismo.	Ejecutor / Cooperante	**BAJO**	**MEDIO**	2	3	5	**Riesgo Medio**	Dado que el riesgo es transferido al Ejecutor / Cooperante, es su responsabilidad definir la forma en que mitigará el riesgo, garantizando además la continuidad del negocio. Así mismo, el Ejecutor / Cooperante, tiene a su cargo asumir a su costo y riesgo el cumplimiento de los procesos, procedimientos, sistemas de información y técnicos y cualquier efecto negativo derivado de fallas en estos.	El Ejecutor / Cooperante es el responsable por la implementación del tratamiento.		X				Durante el plazo de ejecución del Convenio Especial de Cooperación.	La supervisión y/o Comité Operativo del Convenio Especial de Cooperación deberá hacer seguimiento de la efectiva y eficiente implementación de las medidas adoptadas por parte del Ejecutor / Cooperante. El Ejecutor / Cooperante dispondrá de toda la información necesaria para documentar las acciones pertinentes a partir de reuniones, registros, actas, informes, y en general actividades que permitan realizar el seguimiento del Convenio Especial de Cooperación.	Permanente
15	Específico	Interno	Ejecución	Operacional	Efectos desfavorables por fallas en la seguridad, malware o vulnerabilidades que permita el uso o acceso indebido de terceros a la información o activos de información o equipos sin previa autorización, por errores u omisiones y/o falta de rigor y/o en general por razones atribuibles al Ejecutor / Cooperante.	Pérdida de equipos, información o acceso y uso malintencionado de a la que se pueda tener acceso.	Ejecutor / Cooperante	**MEDIO**	**MEDIO**	3	3	6	**Riesgo Alto**	El Ejecutor / Cooperante debe implementar protocolos, adoptar estrategias de seguridad y privacidad de la información que definan salvaguardias administrativas, técnicas y físicas adecuadas para proteger la seguridad de la información y los datos personales, así como tomar acciones para evitar el acceso o uso no autorizados de información o datos catalogados como clasificados o reservados. El Ejcutor/Ejecutor / Cooperante deberá contar con planes de contingencia, que permita el aseguramiento de los activos que hacen parte del Convenio Especial de Cooperación perminiento volver a condiciones de operación en caso de fallas y contar con niveles de seguridad que salvaguarden la información y su confidencialidad de ser el caso.	El responsable de la implementación del tratamiento es el Ejecutor / Cooperante.		X				Hasta la finalización del plazo de ejecución del Convenio Especial de Cooperación.	El Ejecutor / Cooperante como reponsable de la implementación del tratamiento, por lo que dispondrá de toda la información necesaria para documentar el cumplimiento del Convenio Especial de Cooperación a partir de reuniones, registros, actas, informes, y en general actividades que permitan realizar el seguimiento respectivo. Se hará el monitoreo y seguimiento con los informes de las actividades realizadas durante el mes o periodo, al igual que con los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos en cada actividad encomendada, cuando así se requiera, así como con reuniones y mesas de trabajo.	Permanente

MATRIZ DE RIESGOS RECOMENDADA PARA EL PROCESO:		ÁREA SOLICITANTE:	DIRECCIÓN DE ECONOMÍA DIGITAL - SUBDIRECCIÓN DE INDUSTRIA TI		
129 CONVENIO ESPECIAL DE COOPERACIÓN - CIBERSEGURIDAD		TIPO DE CONTRATO:	Convenio Especial de Cooperación	Modalidad de Selección:	Contratación Directa

OBJETO CONTRACTUAL:

33200401811 - Aunar esfuerzos técnicos, administrativos, y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.

IDENTIFICACIÓN, CLASIFICACIÓN Y ASIGNACIÓN								CALIFICACIÓN CUALITATIVA Y VALORACIÓN						PLAN DE TRATAMIENTO						MONITOREO Y REVISIÓN		
										Valoración												
No.	Clase	Fuente	Etapa	Tipo	RIESGO (Descripción)	CONSECUENCIA (de la ocurrencia del evento)	ASIGNACIÓN (Entidad Estatal/ Ejecutor / Cooperante)	Probabilidad	Impacto	Probabilidad	Impacto	Total	Categoría Mapa de Riesgo	TRATAMIENTO - CONTROL	Persona responsable por implementar el tratamiento	EVITAR	TRANSFERIR	ACEPTAR	REDUCIR PROBABILIDAD	REDUCIR IMPACTO	FECHA ESTIMADA EN QUE SE COMPLETA EL TRATAMIENTO	CÓMO SE REALIZA EL MONITOREO	PERIODICIDAD
16	Específico	Externo	Ejecución	Económico	Efectos favorables o desfavorables por cambios en las variables macroeconómicas, tales como, pero sin limitarse a tasa de cambio, inflación, commodities, entre otros.	Como consecuencia de la dinámica de dichas variables, es posible que se afecte negativamente la estructura financiera del negocio jurídico, impactando los determinantes necesarios para el cumplimiento del objeto contractual ocasionando posibles retrasos, reprocesos y costos adicionales para el Ejecutor / Cooperante.	Ejecutor / Cooperante	MEDIO	MEDIO	3	3	6	Riesgo Alto	Se reduce la probabilidad del riesgo desde el establecimiento de las condiciones técnicas, alcances y obligaciones que debe cumplir el Ejecutor / Cooperante, más aún cuando las obligaciones y alcance del Convenio Especial de Cooperación son de amplio debate, conocimiento y revisión durante el proceso precontractual.	El Ejecutor / Cooperante es el responsable de la implementación del tratamiento, por lo que dispondrá de toda la información necesaria para documentar el cumplimiento del Convenio Especial de Cooperación a partir de reuniones, registros, actas, informes, y en general actividades que permitan realizar el seguimiento de esta.		X				Hasta el plazo de ejecución del Convenio Especial de Cooperación.	Se hará el monitoreo y seguimiento con los informes de las actividades realizadas durante el mes o periodo, al igual que con los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos en cada actividad encomendada, cuando así se requiera, así como con reuniones y mesas de trabajo	Permanente
17	General	Externo	Ejecución	Financiación	Efectos desfavorables por falta de liquidez o capital de trabajo del Ejecutor / Cooperante.	El Ejecutor / Cooperante no estima adecuadamente los flujos de recursos monetarios (liquidez financiera) para la ejecución del Convenio Especial de Cooperación o para la provisión de los recursos o determinantes necesarios para el cumplimiento del objeto del Convenio Especial de Cooperación ocasionando posibles retrasos, reprocesos y costos adicionales para el Ejecutor / Cooperante.	Ejecutor / Cooperante	BAJO	MEDIO	2	3	5	Riesgo Medio	El Ejecutor / Cooperante deberá tomar todas las medidas que sean necesarias para dar continuidad a la ejecución del del Convenio Especial de Cooperación. Es responsabilidad del Ejecutor / Cooperante estimar adecuadamente los flujos de liquidez y capital de trabajo para la ejecución del proyecto acorde con los documentos que hacen parte integral del Convenio Especial de Cooperación. El Ejecutor / Cooperante deberá considerar en sus cuentas y flujos monetarios los efectos de las necesidades de liquidez y capital de trabajo para el cabal cumplimiento de sus obligaciones que emanan del Convenio Especial de Cooperación.	El Ejecutor / Cooperante es el responsable de la implementación del tratamiento, por lo que dispondrá de toda la información necesaria para documentar el cumplimiento del Convenio Especial de Cooperación a partir de reuniones, registros, actas, informes, y en genera actividades que permitan realizar el seguimiento de esta.		X				Hasta el plazo de ejecución del Convenio Especial de Cooperación.	Se hará el monitoreo y seguimiento con los informes de las actividades realizadas durante el mes o periodo, al igual que con los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos en cada actividad encomendada, cuando así se requiera, así como con reuniones y mesas de trabajo.	Permanente
18	General	Externo	Ejecución	Social - Político	Efectos desfavorables por eventos de fuerza mayor asegurables.	Se refiere a eventos no imputables a las partes, pero que son asegurables. La ocurrencia de este tipo de eventos puede implicar la necesidad de reprogramar la ejecución de las obligaciones contractualesque eventualmente se vean afectadas.	Ejecutor / Cooperante	BAJO	MEDIO	2	3	5	Riesgo Medio	El Ejecutor / Cooperante deberá contratar todas aquellas coberturas y amparos que lo cubran de eventualidades o afectaciones a terceros y mantener indemne al MinTic FUTIC, de conformidad con lo establecido en todos los documentos que son parte integral del Convenio Especial de Cooperación.	El Ejecutor / Cooperante como responsable de la implementación del tratamiento dispondrá de toda la información necesaria para documentar el cumplimiento del Convenio Especial de Cooperación a partir de reuniones, registros, actas, informes, y en general actividades que permitan realizar el seguimiento de esta.		X				Hasta el plazo de ejecución del Convenio Especial de Cooperación.	Se hará el monitoreo y seguimiento con los informes de las actividades realizadas durante el mes o periodo, al igual que con los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos en cada actividad encomendada, cuando así se requiera, así como con reuniones y mesas de trabajo	Permanente

MATRIZ DE RIESGOS RECOMENDADA PARA EL PROCESO:		ÁREA SOLICITANTE:	DIRECCIÓN DE ECONOMÍA DIGITAL - SUBDIRECCIÓN DE INDUSTRIA TI		
129 CONVENIO ESPECIAL DE COOPERACIÓN - CIBERSEGURIDAD		TIPO DE CONTRATO:	Convenio Especial de Cooperación	Modalidad de Selección:	Contratación Directa

OBJETO CONTRACTUAL:

33200401811 - Aunar esfuerzos técnicos, administrativos, y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.

IDENTIFICACIÓN, CLASIFICACIÓN Y ASIGNACIÓN								CALIFICACIÓN CUALITATIVA Y VALORACIÓN						PLAN DE TRATAMIENTO							MONITOREO Y REVISIÓN		
										Valoración													
No.	Clase	Fuente	Etapa	Tipo	RIESGO (Descripción)	CONSECUENCIA (de la ocurrencia del evento)	ASIGNACIÓN (Entidad Estatal/ Ejecutor / Cooperante)	Probabilidad	Impacto	Probabilidad	Impacto	Total	Categoría Mapa de Riesgo	TRATAMIENTO - CONTROL	Persona responsable por implementar el tratamiento	EVITAR	TRANSFERIR	ACEPTAR	REDUCIR PROBABILIDAD	REDUCIR IMPACTO	FECHA ESTIMADA EN QUE SE COMPLETA EL TRATAMIENTO	CÓMO SE REALIZA EL MONITOREO	PERIODICIDAD
19	General	Externo	Ejecución	Social - Político	Efectos desfavorables por eventos de fuerza mayor no asegurables.	Se refiere a eventos no imputables a las partes pero que no son asegurables. La ocurrencia de este tipo de eventos puede implicar la necesidad de reprogramar la ejecución de obligaciones contractuales, o la imposibilidad del cumplimiento de las mismas.	MinTicFUTIC	BAJO	MEDIO	2	3	5	Riesgo Medio	La supervisión y/o Comité Operativo del Convenio Especial de Cooperación y el Ejecutor / Cooperante deberán generar estrategias que permitan identificar la ocurrencia de situaciones de caso fortuito o fuerza mayor bajo las definiciones normativas y lineamientos de política, de modo que sea posible tomar las medidas necesarias para lograr la cabal ejecución del Convenio Especial de Cooperación, acorde con el Plan de Contingencia que el Ejecutor / Cooperante deberá preparar con las alternativas y soluciones ante el acaecimiento de dicho riesgo. El Ejecutor / Cooperante deberá dar aviso al Supervisor de la ocurrencia de eventos constitutivos de caso fortuito y/o fuerza mayor, debidamente sustentados. Así mismo, las partes concertarán las medidas a tomar para evitar la paralización de la ejecución del Convenio Especial de Cooperación.	El responsable de la implementación del tratamiento es el Ejecutor / Cooperante, debiendo realizar la respectiva coordinación con La supervisión y/o Comité Operativo del Convenio Especial de Cooperación.					X	Hasta el plazo de ejecución del Convenio Especial de Cooperación.	La supervisión y/o Comité Operativo del Convenio Especial de Cooperación deberá hacer seguimiento del cumplimiento de las obligaciones que emanan de la transferencia de este riesgo y tomar las demás acciones pertinentes para monitorear la efectividad del cumplimiento de la misma. El Ejecutor / Cooperante como responsable de la implementación del tratamiento dispondrá de toda la información necesaria para documentar el cumplimiento del Convenio Especial de Cooperación a partir de reuniones, registros, actas, informes, y en genera actividades que permitan realizar el seguimiento de esta.	Permanente

Nota 1: Cabe aclarar que no obstante que la Entidad realiza el ejercicio de tipificación, estimación y asignación de riesgos, es obligación del futuro Ejecutor / Cooperante analizar y realizar su propia estimación de riesgos, la cual debe entenderse reflejada en la propuesta de servicios presentada a la Entidad.

Nota 2: La suscripción de este documento por parte de la Entidad implica la aprobación de la identificación del contexto y del planteamiento del mapa de riesgos, los cuales hacen parte integral del ejercicio de identificación, estimación y asignación de los riesgos contenidos en la presente matriz.

Revisó:	Coral Delgado y Asociados - CDYA. - José Pablo Jaramillo		Javier Delgado - CDYA.		
Proyectó:	Luz Elena Paternina Mora - CDYA.				
Aprobó:	Funcionario responsable MinTIC.	Firma:	Colaboradores designados:		
		ANDRES ENRIQUE GALINDO BERNAL			DIRECCIÓN DE ECONOMÍA DIGITAL - SUBDIRECCIÓN DE IT
Adoptó:	Área Misional MinTic.	DIRECCIÓN DE ECONOMÍA DIGITAL - SUBDIRECCIÓN DE INDUSTRIA TI	DIRECCIÓN DE ECONOMÍA DIGITAL - SUBDIRECCIÓN DE INDUSTRIA TI		

CONTEXTO:

La metodología planteada por Colombia Compra Eficiente indica que es necesario como punto inicial identificar el contexto en el cual interactúa la Entidad Estatal, lo que permitirá la identificación de los riesgos previsibles para el proceso de contratación objeto de estructuración. En consecuencia, previo a la elaboración de la matriz de riesgos se procedió a analizar el documento de estudios previos, la necesidad en él identificada, la estimación del presupuesto oficial, entre otros aspectos señalados por el Decreto 1082 de 2015, la documentación e información histórica remitida por el área originadora en virtud de lo indicado en la circular 011 de 2022 emitida por la Secretaría General del Ministerio de Tecnologías de la Información y las Comunicaciones, por lo que a continuación se sintetizan las notas características del proceso.

De acuerdo con los documentos entregados por la **DIRECCIÓN DE ECONOMÍA DIGITAL SUBDIRECCIÓN DE INDUSTRIA TI**, las siguientes son las características más relevantes del proceso de contratación que nos ocupa, las cuales se abstraen del contexto fijado por la Entidad en el documento de estudios previos y demás documentos de la etapa precontractual.

El proceso de contratación que nos ocupa tiene por objeto: "33200401811 - Aunar esfuerzos técnicos, administrativos, y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.".

Según el estudio previo, en virtud de lo señalado en la Ley 1150 de 2007, que establece: las actividades de Ciencia, tecnología e innovación pueden ser contratadas a través de la causal de contratación directa las cuales están definidas en el literal (a), artículo 2 del Decreto-Ley 393 de 1991, literal (b) del artículo 2 del Decreto-Ley 591 de 1991, así mismo, Así mismo, la Circular Externa No. 6 del 27 de septiembre de 2013 emitida por Colombia Compra Eficiente.

Para los efectos legales y fiscales el valor del Convenio es:El Valor total del proyecto se estima en DOS MIL OCHENTA Y CINCO MILLONES OCHENTA Y DOS MIL NOVECIENTOS SESENTA Y NUEVE PESOS M/CTE ($2.085.082.969) aportados así:

- Aporte del MinTIC/FONDO ÚNICO El aporte del fondo será de MIL OCHOCIENTOS OCHENTA Y SEIS MILLONES NOVECIENTOS CINCUENTA Y DOS MIL NOVECIENTOS TRECE PESOS ($1.886.952.913).

- De acuerdo con la propuesta del día 13 de agosto de 2024 se agrega el aporte de la contrapartida de CIENTO NOVENTA Y OCHO MILLONES CIENTO TREINTA MIL CINCUENTA Y SEIS PESOS ($198.130.056) en especie representados en recurso humano para el desarrollo de actividades técnicas y de administración del proyecto.

Plazo: El plazo de ejecución del convenio será hasta el treinta y uno (31) de diciembre de 2024, contado a partir de la suscripción del acta de inicio, previo el cumplimiento de los requisitos de perfeccionamiento y ejecución del convenio.

Ahora bien, claro el contexto en que se desarrollaría el proceso de contratación, se procedió a la identificación, asignación y valoración de los respectivos riesgos, obteniendo el siguiente mapa de riesgos:

MAPA DE RIESGO ACORDE CON LA CATEGORÍA DEL RIESGO

Probabilidad		
	EXTREMO	5
	ALTO	4
	MEDIO	3
	BAJO	2
	REMOTO	1



1	2	3	4	5
REMOTO	BAJO	MEDIO	ALTO	EXTREMO
Impacto				

Probabilidad		
	EXTREMO	5
	ALTO	4
	MEDIO	3
	BAJO	2
	REMOTO	1

6	7	8	9	10
5	6	7	8	9
4	5	6	7	8
3	4	5	6	7
2	3	4	5	6

1	2	3	4	5
REMOTO	BAJO	MEDIO	ALTO	EXTREMO
Impacto				

INSTRUCCIONES DE DILIGENCIAMIENTO

Identificar y clasificar los Riesgos

Identificar e incluir en la matriz propuesta los Riesgos del Proceso de Contratación.

Fuentes: los planes estratégicos, planes de acción, reportes de desempeño, presupuestos, Riesgos identificados por otras Entidades Estatales, lluvia de ideas, paneles de expertos cuando la complejidad del Proceso de Contratación lo exige, análisis DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas), encuestas y cuestionarios.

Clase

General: es un Riesgo de todos los Procesos de Contratación adelantados por la Entidad Estatal, por lo cual está presente en toda su actividad contractual.

Específico: es un Riesgo propio del Proceso de Contratación objeto de análisis.

Fuente

Interno: es un Riesgo asociado a la operación, capacidad, o situación particular de la Entidad Estatal (reputacional, tecnológico).

Externo: es un Riesgo del sector del objeto del Proceso de Contratación, o asociado a asuntos no referidos a la Entidad Estatal (desastres económicos, existencia de monopolios, circunstancias electorales).

Etapa

Planeación: la etapa de planeación está comprendida entre la elaboración del Plan Anual de Adquisiciones y la fecha en la cual se decide continuar o no con el Proceso de Contratación. Durante esta etapa, la Entidad Estatal elabora los estudios previos y el proyecto de pliegos de condiciones o sus equivalentes. Dentro de las preguntas que la Entidad Estatal debe hacerse para identificar los Riesgos de la etapa de planeación se encuentran las siguientes:

(i) La modalidad de contratación es adecuada para el bien servicio u obra necesitado.

(ii) Los requisitos habilitantes son los apropiados para el Proceso de Contratación y es posible encontrar proponentes que los cumplan incluyendo los Riesgos relacionados con la habilidad para determinar requisitos habilitantes consistentes con el Proceso de Contratación y con el sector económico en el que actúan los posibles oferentes.

(iii) El valor del contrato corresponde a los precios del mercado.

(iv) La descripción del bien o servicio requerido es claro.

(v) El Proceso de Contratación cuenta con las condiciones que garanticen la transparencia, equidad y competencia entre los proponentes.

(vi) El estudio de mercado permite identificar los aspectos de oferta y demanda del mercado respectivo.

(vii) El diseño del Proceso de Contratación permite satisfacer las necesidades dela Entidad Estatal, cumplir su misión y si es coherente con el cumplimiento de sus objetivos y metas.

Selección: la etapa de selección está comprendida entre el acto de Apertura del Proceso de Contratación y la Adjudicación o la declaración de desierto del Proceso de Contratación. En la etapa de selección la Entidad Estatal selecciona al contratista. En esta etapa los Riesgos frecuentes son los siguientes:

(i) Falta de capacidad de la Entidad Estatal para promover y adelantar la selección del contratista, incluyendo el riesgo de seleccionar aquellos que no cumplan con la totalidad de los requisitos habilitantes o se encuentren incursos en alguna inhabilidad o incompatibilidad.

(ii) Riesgo de colusión.

(iii) Riesgo de ofertas artificialmente bajas.

Contratación: Una vez adjudicado el contrato objeto del Proceso de Contratación, inicia la etapa de contratación en la cual se debe cumplir con el cronograma previsto para la celebración del contrato, el registro presupuestal, la publicación en el SECOP y el cumplimiento de los requisitos para el perfeccionamiento, ejecución y pago. En esta etapa los Riesgos frecuentes son los siguientes:

(i) Riesgo de que no se firme el contrato.

(ii) Riesgo de que no se presenten las garantías requeridas en los Documentos del Proceso de Contratación o que su presentación sea tardía.

(iii) Riesgos asociados al incumplimiento de la publicación o el registro presupuestal del contrato.

(iv) Riesgos asociados a los reclamos de terceros sobre la selección del oferente que retrasen el perfeccionamiento del contrato.

Ejecución: la etapa de ejecución inicia una vez cumplidos los requisitos previstos para iniciar la ejecución del contrato respectivo y termina con el vencimiento del plazo del contrato o la fecha de liquidación si hay lugar a ella. Esta etapa puede extenderse cuando hay lugar a garantías de calidad, estabilidad y mantenimiento, o a condiciones de disposición final o recuperación ambiental de las obras o bienes. En esta etapa se cumplen con las obligaciones previstas en el contrato, permitiendo el logro del objeto del Proceso de Contratación; en consecuencia los Riesgos frecuentes son los asociados al cumplimiento del contrato y el logro del objeto propuesto, el rompimiento del equilibrio económico del contrato, los asociados a la liquidación y terminación del contrato y aquellos relacionados con el incumplimiento de la normativa posconsumo.

Tipo de Riesgo

Riesgos Económicos: son los derivados del comportamiento del mercado, tales como la fluctuación de los precios de los insumos, desabastecimiento y especulación de los mismos, entre otros.

Riesgos Sociales o Políticos: son los derivados de los cambios de las políticas gubernamentales y de cambios en las condiciones sociales que tengan impacto en la ejecución del contrato.

Riesgos Operacionales: son los asociados a la operatividad del contrato, tales como la suficiencia del presupuesto oficial, del plazo o los derivados de procesos, procedimientos, parámetros, sistemas de información y tecnológicos, equipos humanos o técnicos inadecuados o insuficientes.

Riesgos Financieros: son (i) el riesgo de consecución de financiación o riesgo de liquidez para obtener recursos para cumplir con el objeto del contrato, y (ii) el riesgo de las condiciones financieras establecidas para la obtención de los recursos, tales como plazos, tasas, garantías, contragarantías, y refinanciaciones, entre otros.

Riesgos Regulatorios: derivados de cambios regulatorios o reglamentarios que afecten la ecuación económica del contrato.

Riesgos de la Naturaleza: son los eventos naturales previsibles en los cuales no hay intervención humana que puedan tener impacto en la ejecución del contrato, por ejemplo los temblores, inundaciones, lluvias, sequías, entre otros.

Riesgos Ambientales: son los derivados de las obligaciones legales o reglamentarias de carácter ambiental, así como de las licencias, planes de manejo o de permisos y autorizaciones ambientales, incluyendo tasas retributivas y compensatorias, obligaciones de mitigación, tareas de monitoreo y control, entre otras.

Riesgos Tecnológicos: son los derivados de fallas en los sistemas de comunicación de voz y de datos, suspensión de servicios públicos, nuevos desarrollos tecnológicos o estándares que deben ser tenidos en cuenta para la ejecución del contrato, obsolescencia tecnológica.

Evaluar y calificar los Riesgos

Evaluar cada uno de los Riesgos identificados, estableciendo el impacto de los mismos frente al logro de los objetivos del Proceso de Contratación y su probabilidad de ocurrencia. Esta evaluación tiene como fin asignar a cada Riesgo una calificación en términos de impacto y de probabilidad, la cual permite establecer la valoración de los Riesgos identificados y las acciones que se deban efectuar. Para estimar el impacto y la probabilidad de ocurrencia de un evento que afecte de manera negativa el Proceso de Contratación, se sugiere considerar fuentes de información como:

a. Registros anteriores de la ocurrencia del evento en Proceso de Contratación propios y de otras Entidades Estatales.

b. Experiencia relevante propia y de otras Entidades Estatales.

c. Prácticas y experiencia de la industria o el sector en el manejo del Riesgo identificado.

d. Publicaciones o noticias sobre la ocurrencia del Riesgo identificado.

INSTRUCCIONES DE DILIGENCIAMIENTO

e. Opiniones y juicios de especialistas y expertos.

f. Estudios técnicos.

Se debe evaluar los Riesgos combinando la probabilidad de ocurrencia y el impacto del evento para:

(a) Asignar una categoría a cada Riesgo de acuerdo con la probabilidad de ocurrencia así: raro, improbable, posible, probable y casi cierto y valorarlos de 1 a 5 siendo raro el de valor más bajo y casi cierto el de valor más alto. Se puede utilizar las fuentes de información sugeridas anteriormente, métodos cuantitativos con diferentes metodologías que arrojen otros resultados y complementen los resultados de la matriz de evaluación de riesgos.

Tabla 1 - Probabilidad del Riesgo

(b) Determinar el impacto del Riesgo, utilizando la Tabla 2, analizando los siguientes criterios: (i) la calificación cualitativa del efecto del Riesgo, y (ii) la calificación monetaria del Riesgo, la cual corresponde a la estimación de los sobrecostos ocasionados por la ocurrencia del Riesgo como un porcentaje del valor total del presupuesto del contrato. Se debe escoger la mayor valoración resultante de los criterios (i) y (ii) para determinar el impacto del Riesgo.

Tabla 1 - Probabilidad del Riesgo:

	Categoría	Valoración
Probabilidad	Raro (puede ocurrir excepcionalmente)	1
	Improbable (puede ocurrir ocasionalmente)	2
	Posible (puede ocurrir en cualquier momento futuro)	3
	Probable (probablemente va a ocurrir)	4
	Casi cierto (ocurre en la mayoría de circunstancias)	5

Tabla 2 - Impacto de Riesgo

(c) Para cada Riesgo se deben sumar las valoraciones de probabilidad e impacto, para obtener la valoración total del Riesgo.

Tabla 2 - Impacto del Riesgo

Impacto						
Calificación Cualitativa		Obstruye la ejecución del contrato de manera intrascendente.	Dificulta la ejecución del contrato de manera baja, aplicando medidas mínimas se pueden lograr el objeto contractual.	Afecta la ejecución del contrato sin alterar el beneficio para las partes.	Obstruye la ejecución del contrato sustancialmente pero aun así permite la consecución del objeto contractual.	Perturba la ejecución del contrato de manera grave imposibilitando la consecución del objeto contractual.
Calificación Monetaria		Los sobrecostos no representan más del uno por ciento (1%) del valor del contrato.	Los sobrecostos no representan más del cinco por ciento (5%) del valor del contrato.	Genera un impacto sobre el valor del contrato entre el cinco (5%) y el quince por ciento (15%).	Incrementa el valor del contrato entre el quince (15%) y el treinta por ciento (30%).	Impacto sobre el valor del contrato en más del treinta por ciento (30%).
	Categoría / Valoración	Insignificante	Menor	Moderado	Mayor	Catastrófico
		1	2	3	4	5
Probabilidad	Raro (puede ocurrir excepcionalmente) 1	2	3	4	5	6
	Improbable (puede ocurrir ocasionalmente) 2	3	4	5	6	7
	Posible (puede ocurrir en cualquier momento futuro) 3	4	5	6	7	8
	Probable (probablemente va a ocurrir) 4	5	6	7	8	9
	Casi cierto (ocurre en la mayoría de circunstancias) 5	6	7	8	9	10

Tabla 3 - Valoración del Riesgo

(d) Finalmente, la valoración completa del Riesgo permite establecer una categoría a cada uno de ellos para su correcta gestión:

INSTRUCCIONES DE DILIGENCIAMIENTO

Tabla 3 - Categoría del Riesgo

Valoración del Riesgo	Categoría
8, 9 y 10	Riesgo extremo
6 y 7	Riesgo alto
5	Riesgo medio
2, 3 y 4	Riesgo bajo

Tabla - Categoría del Riesgo

Asignación y tratamiento de los Riesgos

Una vez realizada la evaluación y calificación de cada uno de los Riesgos asociados al Proceso de Contratación, se debe establecer un orden de prioridades para decidir:

(a) Evitar el Riesgo, para lo cual debe decidir no proceder con la actividad que causa el Riesgo o buscar alternativas para obtener el beneficio del Proceso de Contratación.

(b) Transferir el Riesgo haciendo responsable a otra entidad quien asume las consecuencias de la materialización del Riesgo, típicamente se transfiere el Riesgo a través de las garantías previstas en el Proceso de Contratación o en las condiciones del contrato estableciendo con claridad quien es el responsable. El principio general es que el Riesgo debe asumirlo la parte que pueda enfrentarlo en mejor forma, bien sea por su experiencia, conocimiento o papel dentro de la ecuación contractual, entre otras.

(c) Aceptar el Riesgo cuando no puede ser evitado ni ser transferido o el costo de evitarlo o transferirlo es muy alto. En este caso se recomiendan medidas para reducir el Riesgo o mitigar su impacto, así como el monitoreo.

(d) Reducir la probabilidad de la ocurrencia del evento, cuando el Riesgo debe ser aceptado. Para el efecto se sugieren medidas como: (i) aclarar los requisitos, requerimientos y especificaciones y productos del contrato; (ii) revisar procesos; (iii) establecer sistemas de aseguramiento de calidad en los contratos; (iv) especificar estándares de los bienes y servicios; (v) hacer pruebas e inspecciones de los bienes; (vi) establecer sistemas de acreditación profesional; (vii) incluir declaraciones y garantías del contratista; (viii) administrar la relación entre proveedores y compradores.

(e) Reducir las consecuencias o el impacto del Riesgo a través de planes de contingencia, en los términos y condiciones del contrato, inspecciones y revisiones para revisar el cumplimiento del contrato y programas de apremio para lograr el cumplimiento del contrato.

Se debe seleccionar la opción apropiada teniendo en cuenta el costo y el beneficio de cualquiera de las acciones identificadas para el tratamiento del Riesgo, enumeradas anteriormente. En la mayoría de los casos una combinación de opciones permite el mejor resultado.

Generalmente las medidas para tratar los Riesgos son acciones o actividades específicas para responder a los eventos, para lo cual se sugiere preparar un plan de tratamiento para documentar cómo se enfrenta cada uno de los Riesgos (ver matriz), incluyendo acciones, cronogramas, recursos (personal, información) y presupuesto, responsabilidades, necesidades de informes y reportes y de monitoreo.

La tarea más importante del manejo del Riesgo es la implementación del plan de tratamiento, lo cual requiere atención, asegurar los recursos que requiere y el cumplimiento oportuno de las tareas previstas en este plan. La matriz debe contener la información básica del tratamiento de los Riesgos.

Monitorear los Riesgos

Se debe realizar un monitoreo constante a los Riesgos del Proceso de Contratación pues las circunstancias cambian rápidamente y los Riesgos no son estáticos. La matriz y el plan de tratamiento deben ser revisadas constantemente y revisar si es necesario hacer ajustes al plan de tratamiento de acuerdo con las circunstancias.

Este monitoreo debe:

(a) Garantizar que los controles son eficaces y eficientes en el diseño y en la operación.

(b) Obtener información adicional para mejorar la valoración del Riesgo.

(c) Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.

(d) Detectar cambios en el contexto externo e interno que puedan exigir revisión de los tratamientos del Riesgo y establecer un orden de prioridades de acciones para el tratamiento del Riesgo.

(e) Identificar nuevos Riesgos que pueden surgir.

Finalmente, se debe monitorear los Riesgos y revisar la efectividad y el desempeño de las herramientas implementadas para su gestión. Para lo cual, debe: (i) asignar responsables; (ii) fijar fechas de inicio y terminación de las actividades requeridas; (iii) señalar la forma de seguimiento (encuestas, muestreos aleatorios de calidad, u otros); (iv) definir la periodicidad de revisión; y (v) documentar las actividades de monitoreo.

Los Documentos a incluir del Proceso de Contratación y en la audiencia de asignación de Riesgos

Se debe incluir en los Estudios Previos del Proceso de Contratación los Riesgos que afecten la ejecución del contrato y que identificó en la matriz de administración de Riesgos. Esta misma matriz debe incluirse en el proyecto de Pliego de Condiciones o su equivalente y la información contenida en ella debe utilizarse para analizar y tratar los riesgos del proceso de contratación. Aquellos tratamientos que correspondan a garantías, cláusulas penales o multas y sanciones, deben ser incluidos en el Pliego de Condiciones o su equivalente y en la minuta del contrato. En los procesos de licitación pública, se debe adelantar una audiencia de asignación de Riesgos en la cual debe presentar el análisis de Riesgos efectuado y presentar a los interesados la matriz incluida en los pliegos y revisar la asignación de los Riesgos.

INSTRUCCIONES DE DILIGENCIAMIENTO

METODOLOGÍA - CDYA

Para el presente proceso de contratación, se tomó en cuenta los lineamientos fijados por CCE, el documento Conpes 3714, y demás normatividad aplicable en materia de riesgos previsibles en la contratación estatal. Así las cosas, de manera conjunta con el área originadora se analizaron cada uno de los Riesgos identificados, estableciendo el impacto de los mismos frente al logro de los objetivos del Proceso de Contratación y su probabilidad de ocurrencia. Esta evaluación tuvo como fin asignar a cada Riesgo una calificación en términos de impacto y de probabilidad, de manera cualitativa. Para estimar el impacto y la probabilidad de ocurrencia se consideraron como fuentes de información las siguientes:

a. Experiencia relevante propia y de otras Entidades Estatales.

b. Opiniones y juicios de especialistas y expertos internos y externos a la Entidad contratante.

c. Estudios técnicos y documentos precontractuales suministrados por la Entidad.

d. El contexto se analizó teniendo en cuenta los siguientes aspectos que indica la guía de CCE, acorde con los items aplicables en línea con los documentos precontractuales, así:

(i) El objeto del Proceso de Contratación.

(ii) Los partícipes del Proceso de Contratación.

(iii) La ciudadanía que se beneficia del Proceso de Contratación.

(iv) La suficiencia del presupuesto oficial del Proceso de Contratación.

(v) Las condiciones geográficas y de acceso del lugar en el cual se debe cumplir el objeto del Proceso de Contratación.

(vi) La capacidad de la Entidad Estatal entendida como la disponibilidad de recursos y conocimientos para el Proceso de Contratación.

(vii) El entorno socio ambiental.

(viii) Las condiciones políticas.

(ix) Los factores ambientales.

(x) El sector del objeto del Proceso de Contratación y su mercado.

(xi) La normativa aplicable al objeto del Proceso de Contratación.

(xii) Experiencia propia y de otras Entidades Estatales en Procesos de Contratación del mismo tipo.

Adicionalmente se aplicaron los lineamientos de CCE con el fin de calcular el mapa de riesgos y establecer el tratamiento y mecanismos de seguimiento acorde con las políticas, procesos y procedimientos de MinTic - FU Tic.

CORAL DELGADO & ASOCIADOS | ABOGADOS	**FONDO ÚNICO DE TIC** **MINTIC** **FORMATO DE RECOMENDACIÓN ESQUEMA DE ASEGURAMIENTO DE PROCESOS DE SELECCIÓN, CONTRATOS Y CONVENIOS PARA LA VIGENCIA 2024**	TIC

CDYA-2024-673 v2

I. DATOS DEL ASESOR

REVISIÓN REALIZADA POR:	CORAL DELGADO & ASOCIADOS S.A.S.	**EN FECHA:**	16/09/2024	
SOPORTE CONTRACTUAL:	CONTRATO DE PRESTACIÓN DE SERVICIOS PROFESIONALES FONDO TIC No. 764 DE 2024.			
OBJETO:	"Prestación de servicios altamente calificados en la asesoría al MinTIC/Fondo Único de TIC en la identificación y valoración de riesgos previsibles en los procesos de contratación que deba adelantar la entidad, así como la forma de mitigarlos y en la estructuración de las garantías y seguros que deban requerirse en éstos y en los demás procesos institucionales que así lo requieran, así como en la revisión, verificación y confirmación del origen, características y elementos relevantes de las pólizas, garantías bancarias, los contratos de seguro de cumplimiento y los patrimonios autónomos otorgados en virtud de los procesos de contratación y/o actividad contractual y/o administrativa desarrollada por la entidad, previo a su probación, conforme la normatividad vigente y en articulación con el Modelo Integrado de Gestión".			

Se presenta el presente análisis de garantías requeridas, en cumplimiento del objeto y alcance contractual, para determinación de su inclusión por parte de la Dirección de Economía Digital y/o de la Subdirección de Gestión Contractual del Fondo Único de TIC / MINTIC en los documentos precontractuales del proceso de contratación conforme a las previsiones normativas aplicables, según la modalidad de selección, la tipología de contratación y, en todo caso, atendiendo las disposiciones del Estatuto General de Contratación de la Administración Pública, especialmente lo contenido en el Decreto 1082 de 2015.

1. CARACTERISTICAS DEL PROCESO.

De acuerdo con los documentos entregados por la Dirección de Economía Digital, las siguientes son las características fundamentales del proceso que nos ocupa:

- El objeto del contrato a celebrar es "Aunar esfuerzos técnicos, administrativos, y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.".

- El valor del convenio se fijó en el numeral 11 del estudio previo, el cual está determinado de la siguiente manera:

  "El Valor total del proyecto se estima en DOS MIL OCHENTA Y CINCO MILLONES OCHENTA Y DOS MIL NOVECIENTOS SESENTA Y NUEVE PESOS M/CTE ($2.085.082.969) aportados así:

A. Aporte del MinTIC/FONDO ÚNICO El aporte del fondo será de MIL OCHOCIENTOS OCHENTA Y SEIS MILLONES NOVECIENTOS CINCUENTA Y DOS MIL NOVECIENTOS TRECE PESOS ($1.886.952.913).

B. De acuerdo con la propuesta del día 13 de agosto de 2024 se agrega el aporte de la contrapartida de CIENTO NOVENTA Y OCHO MILLONES CIENTO TREINTA MIL CINCUENTA Y SEIS PESOS ($198.130.056) en especie representados en recurso humano para el desarrollo de actividades técnicas y de administración del proyecto."

- El plazo de ejecución del convenio será hasta el 31 de diciembre de 2024, contado a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del convenio.
- El negocio jurídico a celebrar corresponde a un convenio especial de cooperación.

2. GARANTIAS

2.1 GARANTÍA DE CUMPLIMIENTO

De conformidad lo establecido por el artículo "*2.2.1.2.3.1.7. Garantía de cumplimiento*" del decreto 1082 de 2015, y dado que se evidencia la necesidad, en términos de ejecución del futuro convenio especial de cooperación, de amparar a la entidad mediante garantías, se considera que se deberá exigir para cubrir cualquier hecho constitutivo de incumplimiento los amparos que a continuación se señalan, correspondiendo al asociado la obligación de presentar la garantía de cumplimiento en original al MINTIC, dentro de los tres (3) días hábiles siguientes contados a partir de la firma del convenio.

Esta garantía tendrá las siguientes características:

CARACTERISTICA	CONDICIÓN
TIPO DE GARANTÍA	Cualquiera de las clases permitidas por el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, a saber: (i) Contrato de seguro, contenido en una póliza para Entidades Estatales; (ii) Patrimonio autónomo; (iii) Garantía Bancaria.
TOMADOR	Asociado
BENEFICIARIO / ASEGURADO	Fondo Único de Tecnologías de la Información y las Comunicaciones (Nit. 800.131.648-6) y Ministerio de Tecnologías de la Información y las Comunicaciones (Nit. 899.999.053-1)
AMPAROS	

AMPARO	VIGENCIA	VALOR ASEGURADO
Cumplimiento general del convenio	Por el plazo de ejecución del convenio y seis (6) meses más. En todo caso, este amparo deberá mantenerse vigente hasta la liquidación del contrato.	Por el veinte por ciento (20%) del valor total del convenio
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales.	Por el plazo de ejecución del contrato y tres (3) años más.	Por el cinco por ciento (5%) del valor total del convenio.
Calidad del servicio	Por seis (6) meses contados a partir de la terminación del convenio.	Por el diez (10%) por ciento del valor total del conveni.

Nota 1: El asociado está obligado a restablecer el valor de la garantía cuando esta se vea reducida por razón de las reclamaciones que efectúe la Entidad, así como, a ampliar las garantías en los eventos de adición y/o prórroga del convenio.

Nota 2: El asociado deberá presentar el certificado de no expiración de la póliza por falta de pago de la prima, lo anterior bajo los términos del artículo 2.2.1.2.3.2.5 del Decreto 1082 de 2015.

2.2.2 PÓLIZA DE RESPONSABILIDAD CIVIL EXTRACONTRACTUAL -RCE.

De acuerdo con el Artículo 2.2.1.2.3.1.8 del decreto 1082 de 2015, cubrimiento de la responsabilidad civil extracontractual, "La Entidad Estatal debe exigir en los contratos de obra, y en aquellos en que por su objeto o naturaleza lo considere necesario con ocasión de los Riesgos del contrato, el otorgamiento de una póliza de responsabilidad civil extracontractual que la proteja de eventuales reclamaciones de terceros derivadas de la responsabilidad extracontractual que surja de las actuaciones, hechos u omisiones de su contratista.

La Entidad Estatal debe exigir que la póliza de responsabilidad extracontractual cubra también los perjuicios ocasionados por eventuales reclamaciones de terceros derivadas de la responsabilidad extracontractual que surjan de las actuaciones, hechos u omisiones de los subcontratistas autorizados o en su defecto, que acredite que el subcontratista cuenta con un seguro propio con el mismo objeto y que la Entidad Estatal sea el asegurado".

Así las cosas, y de acuerdo con el contenido de las obligaciones específicas a cargo del futuro asociado, se recomienda la exigencia de una garantía, con las siguientes características:

CORAL DELGADO & ASOCIADOS | ABOGADOS	**FONDO ÚNICO DE TIC** **MINTIC** **FORMATO DE RECOMENDACIÓN ESQUEMA DE ASEGURAMIENTO DE PROCESOS DE SELECCIÓN, CONTRATOS Y CONVENIOS PARA LA VIGENCIA 2024**	TIC

CDYA-2024-673 v2

<table>
<tr><th>CARACTERISTICA</th><th>CONDICIÓN</th></tr>
<tr><td>TIPO DE GARANTÍA</td><td>Contrato de seguro, el cual reúna los requisitos y términos establecidos en el Decreto 1082 de 2015.</td></tr>
<tr><td>TOMADOR</td><td>o Asociado</td></tr>
<tr><td>ASEGURADO</td><td>Fondo Único de Tecnologías de la Información y las Comunicaciones (Nit. 800.131.648-6), Ministerio de Tecnologías de la Información y las Comunicaciones (Nit. 899.999.053-1) y el asociado.</td></tr>
<tr><td>BENEFICIARIO</td><td>Fondo Único de Tecnologías de la Información y las Comunicaciones (Nit. 800.131.648-6), Ministerio de Tecnologías de la Información y las Comunicaciones (Nit. 899.999.053-1) y terceros afectados.</td></tr>
<tr><td>AMPAROS</td><td>
<table>
<tr><th>AMPARO</th><th>VIGENCIA</th><th>VALOR ASEGURADO</th></tr>
<tr><td>El amparo Responsabilidad Civil Extracontractual - RCE deberá constituirse de acuerdo con las coberturas y requisitos establecidos en el Decreto 1082 de 2015 sin sublimitarse.

El seguro deberá incluir los siguientes amparos:
o Predios, Laborales y Operaciones
o Cobertura expresa de perjuicios por daño emergente y lucro cesante.
o Cobertura expresa de perjuicios extrapatrimoniales.
o Cobertura expresa de la responsabilidad surgida por actos de contratistas y subcontratistas.
o Cobertura expresa de amparo patronal.
o Cobertura expresa de vehículos propios y no propios.</td><td>La vigencia de esta garantía deberá ser igual al periodo de ejecución del convenio.</td><td>El valor asegurado corresponderá a 300 SMLMV</td></tr>
</table>
</td></tr>
</table>

Nota 1: El asociado está obligado a restablecer el valor del seguro cuando esta se vea reducida por razón de las reclamaciones que efectúe la Entidad y/o terceros afectados, así como, a ampliar las garantías en los eventos de adición y/o prórroga del convenio.

Nota 2: El asociado deberá entregar a la Entidad el respectivo soporte de pago de la póliza.

Se presenta el presente análisis realizado por profesionales de Coral Delgado y Asociados S.A.S., en ejecución del contrato arriba identificado el 27 de agosto de 2024.

Cordialmente;

Jose Pablo Jaramillo Triana

JOSÉ PABLO JARAMILLO TRIANA
Abogado Asociado

JAVIER E. DELGADO CAMPUZANO
Abogado Líder Proyecto

	ANEXO TÉCNICO	TIC

Proyecto de retos de innovación tecnológica en ciberseguridad

AUNAR ESFUERZOS TÉCNICOS, ADMINISTRATIVOS Y FINANCIEROS PARA IMPLEMENTAR UNA ESTRATEGIA BASADA EN LA TRANSFERENCIA DE CONOCIMIENTO, DIFUSIÓN Y ADOPCIÓN TECNOLÓGICA QUE PERMITA IDENTIFICAR Y PLANTEAR SOLUCIONES INNOVADORAS A RETOS TECNOLÓGICOS EN MATERIA DE CIBERSEGURIDAD PARA SER RESUELTOS POR EMPRESAS DEL SECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN

SEPTIEMBRE DE 2024

Ministerio de Tecnologías de la Información y las Comunicaciones
Edificio Murillo Toro, Carrera 8a, entre calles 12A y 12B
Código Postal: 111711. Bogotá, Colombia
T: +57 (1) 3443460 Fax: 57 (1) 344 2248
www.mintic.gov.co

TABLA DE CONTENIDO

1 JUSTIFICACIÓN 3
2 NECESIDAD Y PERTINENCIA DEL PROYECTO 3
3 GENERALIDADES 9
4 ALCANCE TÉCNICO DEL PROYECTO 10
4.1 Objetivos del proyecto 10
4.2 Fases del proyecto 10
5 EQUIPO DE TRABAJO 18
5.1 Conformación mínima del equipo 18
5.2 Consideraciones sobre los requisitos de experiencia 20
6 INFORMES DE EJECUCIÓN 21
7 PLAZO DE EJECUCIÓN 22
8 ENTIDAD EJECUTORA: IDONEIDAD Y CAPACIDADES 22
8.1 Especialidad, unicidad y vínculo especial con el Ministerio de Tecnologías de la Información y las Comunicaciones 23
8.2 Liderazgo en Ciberseguridad 23
8.3 Respaldo y soporte profesional en Ciberseguridad 24
8.4 Experiencia en materia de proyectos de alto impacto 24
9 GLOSARIO 24

ANEXO TÉCNICO PARA EL PROYECTO "PROYECTO RETOS DE INNOVACIÓN TECNOLOGICA EN CIBERSEGURIDAD"

1 JUSTIFICACIÓN

El presente anexo contempla la totalidad de requerimientos técnicos, listado de entregables, alcances de ejecución y programación de actividades previstas en el marco del proyecto denominado "RETOS DE INNOVACION TECNOLOGICA EN CIBERSEGURIDAD" estructurado por la Subdirección de Industria de Tecnologías de la Información en cumplimiento de las funciones establecidas por el artículo 31 del decreto 1064 de 2020: "*1. Apoyar la formulación de políticas y estrategias, y poner en marcha programas, planes y proyectos que promuevan y generen emprendimiento digital en el Estado y la comunidad, e incrementen la productividad económica del país. 2. Fomentar el desarrollo de emprendimientos de base tecnológica, en sus diferentes fases de desarrollo, promover su visibilización y difusión del ecosistema emprendedor colombiano. 4. Diseñar e implementar modelos de conocimiento prácticos y competitivos, que se puedan adoptar en el sector público y privado y que fomenten el emprendimiento y la creatividad en la industria TI. 5. Diseñar y proponer nuevas formas de negocio digital de vanguardia y competitivos, acorde con el entorno económico, social, cultural y tecnológico del País. 6. Diseñar y proponer nuevas formas de financiamiento de negocios para la industria y la comunidad del emprendimiento digital.* ***8. Diseñar e implementar estrategias especializadas para la industria de tecnologías de información que dinamicen la creación de nuevas empresas innovadoras en el sector, y el fortalecimiento de las existentes. 10. Apoyar la formulación y ejecutar políticas, estrategias, programas planes y proyectos de Investigación, Desarrollo e Innovación, buscando que se genere verdadero valor a la oferta de la Industria TI.*** *11. Elaborar estudios de viabilidad para la implementación de infraestructura apta y pertinente a las tendencias, para fomentar la industria TI. 12. Proponer modelos de calidad de información tecnológica globalmente reconocidos por parte de las empresas que hacen parte de la Industria TI que permitan fortalecer el sector público y privado del país. 13. Las demás que le sean asignadas, inherentes a la naturaleza de la dependencia."* En negrilla y subrayado fuera del texto.

Las especificaciones mínimas para la ejecución del citado proyecto, plasmadas en el presente documento harán parte integral de la relación jurídica por suscribir, por tanto, los ejercicios de evaluación y aprobación de las actividades previstas tendrán como único referente admisible la descripción desarrollada en el presente anexo.

Todo lo anterior, en articulación con las obligaciones establecidas en el manual de supervisión y facultades otorgadas a las instancias de acompañamiento, seguimiento y control.

En lo relacionado con el establecimiento del presupuesto asignado al proyecto, y la identificación de los posibles ejecutores, debe destacarse que estos aspectos se consolidarán según los elementos identificados en el estudio de sector y de mercado adelantados en el ejercicio de estructuración.

2 NECESIDAD Y PERTINENCIA DEL PROYECTO

La ciberseguridad se ha convertido en una prioridad estratégica para Colombia en esta era digital, donde la protección de datos y la infraestructura tecnológica son esenciales para el desarrollo económico y social del país.

Con el auge de la digitalización, también se han incrementado las amenazas cibernéticas, por eso el gobierno ha implementado políticas y normativas para salvaguardar la información y los sistemas críticos, alineada con el Plan Nacional de Desarrollo 2022–2026, la estrategia de seguridad busca proteger los activos digitales y fomentar una cultura de seguridad y confianza en el uso de tecnologías de la información. Desde la Ley 1273 de 2009, que tipifica los delitos informáticos, hasta los documentos CONPES de Política Nacional enfocados hacia la Ciberseguridad y Ciberdefensa, Colombia está fortaleciendo su capacidad de respuesta y de adaptación ante posibles ataques cibernéticos, garantizando así un entorno digital seguro y confiable para todos sus ciudadanos y organizaciones.

En el marco del Plan Nacional de Desarrollo (PND) 2022-2026 “Colombia, Potencia Mundial de la Vida”, se establece la “Transformación productiva, internacionalización y acción climática”, enfocada en generar una transición hacia actividades productivas diversificadas, incentivando el desarrollo sostenible y la competitividad y teniendo en cuenta un componente de inclusión social que debe ir a la par con la inclusión productiva. Esto requiere desarrollar una producción industrial sostenible, cerrar brechas tecnológicas, impulsar cadenas de valor para la integración regional, fortalecer las capacidades humanas y generar empleos de calidad. En el ámbito de la transformación digital, el PND 2022-2026 destaca la importancia de la ciberseguridad como un elemento crítico para la modernización del Estado y la competitividad del sector privado. El plan propone la implementación de políticas robustas de ciberseguridad para proteger las infraestructuras críticas, fortalecer la resiliencia cibernética y garantizar la privacidad y protección de datos personales. Entre las metas específicas se incluyen la creación de capacidades técnicas y operativas en ciberseguridad, el fomento de la cooperación público-privada en la gestión de riesgos cibernéticos, y el impulso a la educación y la formación en competencias digitales. Además, el PND enfatiza la necesidad de una regulación dinámica y adaptable que permita enfrentar las nuevas amenazas cibernéticas, asegurando así un entorno digital seguro que propicie la innovación y el desarrollo económico sostenible del país.

En ese sentido, con el catalizador “Economía productiva a través de la reindustrialización y la bioeconomía”, se establece como objetivo generar un impulso a la industria digital del país mediante el desarrollo de una estrategia que involucre aspectos técnicos, de financiamiento, cultura empresarial, emprendimiento e innovación. Esto puede lograrse mediante el fortalecimiento de los productos y servicios de las industrias de TI, a partir de la generación de conocimiento y el fomento a la innovación para el desarrollo de modelos de negocio de base tecnológica que habilite el acceso a mercados de alto valor agregado, como el de la industria de la ciberseguridad.

El CONPES 3854 del 11 de abril de 2016, establece la Política Nacional de Seguridad Digital, que crea las condiciones para que las partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, siendo uno de los principales aportes el desarrollo de estrategias que establecieron un marco institucional para la seguridad digital con un enfoque de gestión de riesgos, con una visión preventiva antes que reactiva ante las posibles amenazas.

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.

Bajo el documento CONPES 3854 de 2016, titulado "Política Nacional de Seguridad Digital", establece una serie de lineamientos estratégicos para fortalecer la seguridad digital en Colombia. Este reconoce la importancia de crear un entorno seguro y confiable para el uso de tecnologías de la información y la comunicación (TIC), esencial para el desarrollo económico y social del país. Entre sus objetivos principales se encuentran la protección de las infraestructuras críticas, la promoción de la colaboración entre el sector público y privado, y el fomento de una cultura de seguridad digital entre los ciudadanos. El CONPES 3854 de 2016 también destaca la necesidad de mejorar las capacidades técnicas y operativas del país en materia de ciberseguridad, así como la importancia de la cooperación internacional para enfrentar amenazas cibernéticas globales. Además, el CONPES 3854 establece acciones concretas para prevenir, detectar y responder a incidentes de seguridad digital, para garantizar la integridad, disponibilidad y confidencialidad de la información en Colombia.

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.

Además, dando continuidad a lo relacionado con Ciberseguridad, el documento CONPES 3995 de 01 julio de 2020, titulado "Política Nacional de Confianza y Seguridad Digital", dicha política pública busca fortalecer la seguridad digital y fomentar la confianza en el entorno digital del país. Que tiene como objetivo general, fortalecer la confianza digital y la seguridad en Colombia para garantizar que el país sea una sociedad inclusiva y competitiva en el entorno digital. Unas de las metas principales es preparar a Colombia para los desafíos de la cuarta revolución industrial (4RI) mediante la implementación de tecnologías avanzadas, maximizar la generación de valor socioeconómico a través del uso seguro y eficiente del internet y el ciberespacio e impulsar la confianza digital entre los ciudadanos y las organizaciones, asegurando la protección de datos y la privacidad. Este CONPES 3995, se espera que contribuya significativamente al desarrollo económico y social de Colombia, al proporcionar un entorno digital seguro y confiable que fomente la innovación y el crecimiento económico. Además, busca que Colombia avance hacia una mayor inclusión digital y competitividad en el ámbito internacional.

El Ministerio de Tecnologías de la Información y las Comunicaciones estableció, mediante 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, que lleva a preservar la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, aplicando un proceso de gestión del riesgo, brindando confianza a los interesados sobre 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 síntesis, la normativa colombiana ha establecido un marco robusto para la protección y la seguridad digital, resaltando la importancia de la ciberseguridad para el desarrollo económico y social del país. Esta serie de leyes y políticas, incluyendo los documentos CONPES y diversas resoluciones, proporcionan las bases sobre las cuales se deben desarrollar y ejecutar las estrategias de ciberseguridad. En este contexto, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) juega un papel crucial.

En este sentido, el Ministerio de Tecnologías de la Información y las Comunicaciones, en conformidad con lo dispuesto en el artículo 18 de la Ley 1341 de 2009 modificado por el artículo 14 de la Ley 1978 de 2019, conocida como Ley de modernización del sector TIC, es la entidad responsable de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

Así mismo, el artículo 18 de la Ley 1341 de 2009, modificado parcialmente por el artículo 14 de la Ley 1978 de 2019, establece como funciones del MinTIC, entre otras, las siguientes: *"1. Diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. 2. Definir, adoptar y promover las políticas, planes y programas tendientes a incrementar y facilitar el acceso de todos los habitantes del territorio nacional, a las tecnologías de la información y las comunicaciones y a sus beneficios para lo cual debe: a) Diseñar, formular y proponer políticas, planes y programas que garanticen el acceso y la implantación de las Tecnologías de la Información y las Comunicaciones, con el fin de fomentar su uso como soporte del crecimiento y aumento de la competitividad del país en los distintos sectores; b) Formular políticas, planes y programas que garanticen a través del uso de Tecnologías de la Información y las Comunicaciones: el mejoramiento de la calidad de vida de la comunidad, el acceso a mercados para el sector productivo, y el acceso equitativo a oportunidades de educación, trabajo, salud, justicia, cultura y recreación, entre otras. (…); 14. Propender por la utilización de las TIC para mejorar la competitividad del país. (…)"*

Por otra parte, 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, el cual tiene como objeto: *"financiar los planes, programas y proyectos para facilitar prioritariamente el acceso universal y del servicio universal a 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 productivo de las TIC, así como apoyar las actividades del Ministerio y la Agencia Nacional del Espectro, y el mejoramiento de su capacidad administrativa, técnica y operativa para el cumplimiento de sus funciones".*

En línea con lo anterior y de conformidad con lo dispuesto en el artículo 35 de la Ley 1341 de 2009, modificado por el artículo 22 de la Ley 1978 de 2019, el Fondo Único de Tecnologías de la Información y las Comunicaciones – Fondo Único de TIC, cuenta, entre otras, con las siguientes funciones: *"(…) 4. Financiar proyectos para promover el desarrollo de contenidos multiplataforma de interés público que promuevan la preservación de la cultura e identidad nacional y regional, mediante el desarrollo de esquemas concursables para la promoción de contenidos*

digitales multiplataforma por parte de los operadores del servicio de televisión regional. 5. Financiar planes, programas y proyectos para promover el desarrollo de contenidos, aplicaciones digitales y emprendimientos para la masificación de la provisión de trámites y servicios del estado, que permitan implementar las políticas de gobierno digital y de transformación digital pública. 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****. (…)"* (Negrita y subrayado fuera de texto), por lo que a través de dicho Fondo se financian las planes, programas y proyectos del MinTIC, así como las actividades administrativas, técnicas y operativas para el cumplimiento de las funciones asignadas a este Ministerio.

Igualmente, el artículo 2º del Decreto 1064 de 2020[3], establece como funciones del MinTIC, entre otras las siguientes: *"(…) 1. Diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. 2. Definir, adoptar y promover las políticas, planes y programas tendientes a incrementar y facilitar el acceso de todos los habitantes del territorio nacional, a las tecnologías de la información y las comunicaciones y a sus beneficios, para lo cual debe: a) "Diseñar, formular y proponer políticas, planes y programas que garanticen el acceso y la implantación de las Tecnologías de la Información y las Comunicaciones, con el fin de fomentar su uso como soporte del crecimiento y aumento de la competitividad del país en los distintos sectores. b) Formular políticas, planes y programas que garanticen a través del uso de Tecnologías de la Información y las Comunicaciones: el mejoramiento de la calidad de vida de la comunidad, el acceso a mercados para el sector productivo, y el acceso equitativo a oportunidades de educación, trabajo, salud, justicia, cultura y recreación, entre otras. c) Apoyar a las entidades del Estado en el acceso y uso de las Tecnologías de la Información y las Comunicaciones para facilitar y optimizar la gestión de los organismos gubernamentales y la contratación administrativa transparente y eficiente, y prestar mejores servicios a los ciudadanos. d) Apoyar a las entidades del Estado en la formulación de los lineamientos generales para la difusión de la información que generen los Ministerios, Departamentos Administrativos y Establecimientos Públicos y efectuar las recomendaciones que considere indicadas para lograr que esta sea en forma ágil y oportuna. e) Planear, formular, estructurar, dirigir, controlar y hacer el seguimiento a los programas y proyectos del Ministerio. f) Diseñar y desarrollar estrategias masivas que expliquen a los ciudadanos las utilidades y potencialidades de las TIC. 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. 4. Coordinar con los actores involucrados, el avance de los ejes verticales y transversales de las TIC, y el plan nacional correspondiente, brindando apoyo y asesoría a nivel territorial. (…)"*

De igual forma el artículo 29 del Decreto 1064 de 2020, establece como funciones de la Dirección de Economía Digital, las siguientes: *"(…) 1. Dirigir el diseño, la formulación, la implementación y el seguimiento de políticas para la industria de Tecnologías de la Información y las Comunicaciones. 2. Promocionar e incentivar en el país la innovación en materia de Tecnologías de la Información y las Comunicaciones. 3. Apoyar la formulación y ejecutar en coordinación con las entidades competentes, organismos y grupos interesados, la visión estratégica en materia de Tecnologías de la Información y las Comunicaciones, que permita posicionar esta industria en el País como una industria de talla mundial. 4. Liderar procesos de investigación que permitan identificar Tecnologías de la*

Información y Comunicaciones innovadoras a nivel mundial y evaluar la viabilidad de su adopción en la industria nacional de Tecnologías de la Información y las Comunicaciones. 5. Formular, coordinar y hacer seguimiento a la implementación de políticas públicas y programas orientados al aprovechamiento de Tecnologías de la Información y las Comunicaciones para el desarrollo y promoción del comercio electrónico de bienes y servicios. 6. En coordinación con el Ministerio del Trabajo y el Departamento Administrativo de la Función Pública, adelantar evaluaciones del capital humano del País en materia de Tecnologías de la Información y las Comunicaciones, y promover y articular acciones para mejorar la cantidad y la calidad del talento humano en Tecnologías de la Información, tanto a nivel estatal como en el sector privado. 7. Coordinar las acciones que promuevan la industria de Tecnologías de la Información y las Comunicaciones con las entidades del gobierno que tengan competencia en la materia. 8. Estudiar, evaluar y preparar los procesos y los actos administrativos relacionados con la industria de las Tecnologías de la Información y las Comunicaciones, en el marco de sus funciones. 9. Definir, diseñar y promover políticas y acciones relacionadas con la adopción de buenas prácticas para la industria de Tecnologías de la Información y las Comunicaciones. 10. Definir, diseñar y promover la creación de mecanismos de fomento para la industria de Tecnologías de la Información y las Comunicaciones. 11. Apoyar la formulación, articular e impulsar programas para el aprovechamiento de Tecnologías de la Información y las Comunicaciones, para desarrollar el comercio electrónico de bienes y servicios. 12. Las demás que le sean asignadas, inherentes a la naturaleza de la dependencia."

A su vez, el artículo 31 del Decreto 1064 de 2020, establece que la Subdirección de Industria de Tecnologías de la Información y las Comunicaciones tiene entre otras, asignadas las siguientes funciones: "*1. Apoyar la formulación de políticas y estrategias, y poner en marcha programas, planes y proyectos que promuevan y generen emprendimiento digital en el Estado y la comunidad, e incrementen la productividad económica del país. 2. Fomentar el desarrollo de emprendimientos de base tecnológica, en sus diferentes fases de desarrollo, promover su visibilización y difusión del ecosistema emprendedor colombiano. 3. Apoyar el desarrollo de soluciones tecnológicas que beneficien a los sectores sociales y económicos del país. 4. Diseñar e implementar modelos de conocimiento prácticos y competitivos, que se puedan adoptar en el sector público y privado y que fomenten el emprendimiento y la creatividad en la industria TI. 5. Diseñar y proponer nuevas formas de negocio digital de vanguardia y competitivos, acorde con el entorno económico, social, cultural y tecnológico del País. 6. Diseñar y proponer nuevas formas de financiamiento de negocios para la industria y la comunidad del emprendimiento digital. 7. Administrar las plataformas de APPS.co buscando promover el uso por parte de los ciudadanos y los sectores público; privado, en el marco del emprendimiento digital del país.* ***8. Diseñar e implementar estrategias especializadas para la industria de tecnologías de información que dinamicen la creación de nuevas empresas innovadoras en el sector, y el fortalecimiento de las existentes.*** *9. Diseñar y poner en marcha estrategias y programas para el desarrollo de la industria de contenidos digitales en el País.* ***10. Apoyar la formulación y ejecutar políticas, estrategias, programas planes y proyectos de Investigación, Desarrollo e Innovación, buscando que se genere verdadero valor a la oferta de la Industria TI.*** *11. Elaborar estudios de viabilidad para la implementación de infraestructura apta y pertinente a las tendencias, para fomentar la industria TI. 12. Proponer modelos de calidad de información tecnológica globalmente reconocidos por parte de las empresas que hacen parte de la Industria TI que permitan fortalecer el sector público y privado del país. 13. Las demás que le sean asignadas, inherentes a la naturaleza de la dependencia."* En negrilla y subrayado fuera del texto.

Igualmente, la Ley 1978 de 2019 en su artículo 22 estableció entre las funciones del Fondo: i. "(...) 13. Cofinanciar planes, programas y proyectos para el fomento de la industria de software y de computación en la nube" y "(...) 22.

Financiar planes, programas y proyectos para apoyar emprendimientos de contenidos y aplicaciones digitales y fomentar el capital humano en Tecnologías de la Información y las Comunicaciones". Atendiendo las disposiciones de la Ley la Dirección de Economía Digital busca adelantar una estrategia que permita potenciar el uso de las tecnologías asociadas a la cuarta revolución industrial.

Es de anotar también que el Ministerio TIC tiene como antecedes el Convenio Especial de Cooperación de Proyectos de Ciencia, Tecnología e Innovación No. 1257 de 2023 suscrito entre Fondo Único de Tecnologías de la Información y las Comunicaciones y el Centro de Bioinformática y Biología Computacional de Colombia.

3 GENERALIDADES

Este proyecto se fundamenta en la necesidad de comprender los retos tecnológicos que enfrentan las MIPYMES del país en materia de ciberseguridad y las capacidades del sector de las industrias de tecnologías de la información para atender de manera innovadora estos retos, contribuyendo de este modo al fortalecimiento de un ecosistema que aproveche el conocimiento y las tendencias tecnológicas para estimular las dinámicas de oferta y demanda en torno al negocio de la ciberseguridad.

El objetivo general se encuentra enfocado como un proyecto en Ciencia, Tecnológica e Innovación, estando alineado con el Decreto 393 de 1991 *"Por el cual se dictan normas sobre asociación para actividades científicas y tecnológicas, proyectos de investigación y creación de tecnologías"*, que en su artículo 2, literal h) el cual menciona, lo siguiente: *"Asesorar la negociación, aplicación y adaptación de tecnologías nacionales y extranjeras",* apartado según el cual resulta valida de la celebración de convenios de cooperación entre una entidad gestora (Aliado) y el Ministerio. Este Decreto establece incentivos y estímulos para la inversión en proyectos de ciencia y tecnología en Colombia.

Al promover el desarrollo tecnológico, se incrementa la creación y uso de sistemas informáticos y redes de comunicación, los cuales requieren una sólida infraestructura de ciberseguridad para garantizar su operación segura y eficiente. La ciberseguridad asegura que las innovaciones y los avances tecnológicos no sean vulnerables a ataques cibernéticos, protegiendo tanto la propiedad intelectual como la integridad de los datos y sistemas que son fundamentales para el progreso científico y tecnológico. En este sentido, este proyecto de ciberseguridad aprovecha las tendencias tecnológicas para validar soluciones innovadoras que contribuyen a fortalecer y consolidar el ecosistema de empresas de tecnologías de la información como referente en soluciones de ciberseguridad, en coherencia con el Decreto 391 de 1991.

Adicionalmente, también se hace constar que los objetivos específicos responden a su vez al catálogo de actividades científicas y tecnológicas contenido en el artículo 2 del Decreto 591 de 1991 *"Por el cual se regulan las modalidades específicas de contratos de fomento de actividades científicas y tecnológicas"*, así:

No. 1: Conformación de redes de investigación e información (numeral 1 del artículo ibidem).
No. 2: Transferencia tecnológica que comprende la negociación, apropiación, desagregación, asimilación, adaptación y aplicación de nuevas tecnologías nacionales o extranjeras (numeral 5 del artículo ibidem).
No. 3: Proyectos de innovación que incorporen tecnología, creación, generación, apropiación y adaptación de esta (numeral 4 del artículo ibidem).
No. 4: Cooperación científica y tecnológica nacional (numeral 6 del artículo ibidem).

Este Decreto 591 de 1991 reglamenta el funcionamiento del Sistema Nacional de Ciencia y Tecnología (SNCyT) y establece lineamientos para la coordinación de actividades relacionadas con la investigación y desarrollo tecnológico. La Ciberseguridad se relaciona con este marco al proporcionar las salvaguardas necesarias para proteger la información y los resultados de investigaciones científicas. Además, garantiza la continuidad operativa de las infraestructuras tecnológicas y de información, promoviendo un entorno seguro.

4 ALCANCE TÉCNICO DEL PROYECTO

Este proyecto se fundamenta en la necesidad de comprender los retos tecnológicos que enfrentan las MIPYMES del país en materia de ciberseguridad y las capacidades del sector de las industrias de tecnologías de la información para atender de manera innovadora estos retos, contribuyendo de este modo al fortalecimiento de un ecosistema que aproveche el conocimiento y las tendencias tecnológicas para estimular las dinámicas de oferta y demanda en torno al negocio de la ciberseguridad.

Por tanto, el proyecto se llevará a cabo para lograr los siguientes objetivos:

5 Objetivos del proyecto

Implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.

Para este fin, se plantean los siguientes objetivos específicos:

1. Identificar, clasificar y definir retos tecnológicos en materia de ciberseguridad, tomando como grupo focal un conjunto de MIPYMES colombianas en las que se identifiquen necesidades de seguridad de la información.

2. Mapear y seleccionar empresas del sector de tecnologías de la información con potencial para desarrollar soluciones en materia de ciberseguridad y fortalecer sus capacidades mediante actividades de transferencia de conocimiento para atender los retos tecnológicos identificados.

3. Plantear e implementar soluciones innovadoras a los retos identificados, mediante procesos de transferencia tecnológica entre las MIPYMES y las empresas del sector de tecnologías de la información.

4. Generar espacios de difusión tecnológica para fortalecer las capacidades del país en materia aplicación y adaptación de tecnologías de ciberseguridad.

5.1 Fases del proyecto

Para el desarrollo del proyecto se plantean las siguientes fases con sus actividades, resultados esperados y entregables. Los plazos de presentación de los entregables, para aprobación del supervisor designado por parte del Ministerio, corresponden a los plazos límite contados a partir de la fecha de suscripción del convenio.

Fase 1. Planeación y alistamiento

En esta fase se definirá el plan detallado de trabajo, las herramientas y plataformas que se utilizarán para soportar la ejecución y seguimiento de las actividades del proyecto. Así mismo, se conformará el equipo de trabajo que ejecutará el proyecto.

	Actividades	Resultados	Entregables
Fase 1. Planeación y alistamiento	**Actividad 1.1** Elaborar el plan de trabajo de detallado para ejecutar las actividades del proyecto hasta el 31 de diciembre del 2024.	**Resultado 1.1** El plan de trabajo detallado para la ejecución técnica y financiera del proyecto.	**Entregable 1.1** Plan de trabajo detallado que incluya todas las fases del proyecto y con un cronograma que considere los momentos de los entregables, los hitos, entregas de informes, desembolsos y demás aspectos del proyecto.
	Actividad 1.2 Definir el equipo de trabajo mediante la selección de las personas que lo integrarán y presentar sus perfiles al Ministerio de Tecnologías de la Información y las Comunicaciones para validación.	**Resultado 1.2** Equipo de trabajo del proyecto definido.	**Entregable 1.2** Matriz que recopile cada uno de los perfiles seleccionados junto con las hojas de vida de cada perfil.

Fase 2. Definición de retos tecnológicos

En esta fase se identificarán, clasificarán y definirán los retos tecnológicos en materia de ciberseguridad de un grupo de 100 MIPYMES colombianas en las que se identifiquen necesidades de seguridad de la información, seleccionadas mediante una convocatoria.

Objetivo Específico 1: Identificar, clasificar y definir retos tecnológicos en materia de ciberseguridad, tomando como grupo focal un conjunto de MIPYMES colombianas en las que se identifiquen necesidades de seguridad de la información.

	Actividades	Resultados	Entregables
Fase 2. Definición de retos tecnológicos	**Actividad 2.1** Realizar una convocatoria dirigida a MIPYMES constituidas en Colombia, de cualquier sector económico, que requieran soluciones de ciberseguridad.	**Resultado 2.1** Una (1) convocatoria realizada a nivel nacional que vincule al menos cien (100) empresas que tengan una necesidad	**Entregable 2.1** Plan operativo de la convocatoria que incluya, entre otros elementos, la estrategia de comunicación y divulgación, los mecanismos para la identificación y vinculación de empresas, la metodología e instrumentos para la inscripción y validación de empresas y el cronograma del proceso.

		tecnológica en ciberseguridad.	**Entregable 2.2** Términos de referencia de la convocatoria dirigida a las MYPES que desean participar en el proyecto.
			Entregable 2.3 Informe de implementación de la convocatoria en las que se incluya tanto las empresas inscritas, como las que participan en el proceso de las 100 empresas vinculadas. (empresas seleccionadas).
	Actividad 2.2 Identificar y clasificar los retos tecnológicos de ciberseguridad de cada MIPYME, realizando la clasificación según las categorías de ciberseguridad y tipo de innovación	**Resultado 2.2** Al menos cien (100) retos con sus respectivas fichas de caracterización estructuradas, una para cada empresa vinculado en la convocatoria.	**Entregable 2.4** Un banco de al menos cien (100) retos con sus respectivas fichas de caracterización estructuradas, una para cada empresa, que incluya un planteamiento de las temáticas necesarias a desarrollar en los procesos de transferencia de conocimiento de la Fase 3
	Actividad 2.3 Conformar un banco de retos a solucionar con la caracterización detallada de cada reto que incluya, entre otros, el alcance, el problema, los recursos científicos, técnicos y tecnológicos mínimos necesarios para resolver el problema y los resultados esperados.		

Fase 3. Fortalecimiento de solucionadores tecnológicos

En esta fase se seleccionarán hasta 45 empresas del sector de tecnologías de la información que tengan potencial para desarrollar soluciones en materia de ciberseguridad, con el fin de fortalecer sus capacidades mediante actividades de transferencia de conocimiento para atender los retos tecnológicos identificados en la Fase 2.

Objetivo Específico 2: Mapear y seleccionar empresas del sector de tecnologías de la información con potencial para desarrollar soluciones en materia de ciberseguridad y fortalecer sus capacidades mediante actividades de transferencia de conocimiento para atender los retos tecnológicos identificados.			
	Actividades	**Resultados**	**Entregables**

Fase 3. Fortalecimiento de solucionadores tecnológicos	**Actividad 3.1** Realizar una convocatoria dirigida a empresas del sector de tecnologías de la información en ciberseguridad en Colombia para fortalecerlas en tendencias de ciberseguridad, y seleccionar hasta cuarenta y cinco (45) empresas con potencial para desarrollar soluciones en ciberseguridad mediante un análisis de su portafolio, capacidades y experiencia.	**Resultado 3.1** Una (1) convocatoria realizada a nivel nacional que vincule hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información en ciberseguridad.	**Entregable 3.1** Plan operativo de la convocatoria que incluya, entre otros elementos, la estrategia de comunicación y divulgación, los mecanismos para la identificación y vinculación de empresas, la metodología e instrumentos para la inscripción y validación de empresas y el cronograma del proceso.
			Entregable 3.2 Términos de referencia de la convocatoria con los criterios de selección de las empresas de tecnologías de la información.
			Entregable 3.3 Informe de implementación de la convocatoria que dé cuenta del proceso de selección y vinculación de las 45 empresas de tecnologías de la información vinculadas.
	Actividad 3.2 Realizar un mapeo sobre las tecnologías e innovaciones de punta en ciberseguridad (vigilancia tecnológica), que permita identificar herramientas, prácticas, modelos de negocio innovadores y tendencias para facilitar los procesos de transferencia de conocimiento en las soluciones de los retos.	**Resultado 3.2** Un (1) mapeo sobre las tecnologías e innovaciones de punta en ciberseguridad (vigilancia tecnológica).	**Entregable 3.4** Documento con el resultado del mapeo sobre las tecnologías e innovaciones de punta en ciberseguridad (vigilancia tecnológica), que incluya la identificación de herramientas, prácticas, modelos de negocio innovadores y tendencias para tener en cuenta en los procesos de transferencia de conocimiento.

	Actividad 3.3 Diseñar e implementar un plan de transferencia de conocimiento para el fortalecimiento de las empresas de tecnologías de la información, que incluya cursos cortos (micro acreditaciones), la realización de un *bootcamp* y sesiones de mentoría especializada dirigidas a las empresas solucionadoras seleccionadas.	**Resultado 3.3** Cinco (5) micro cursos (micro acreditaciones) de ciberseguridad desarrollados, de diez (10) horas cada uno, dirigidos a las hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información seleccionadas, con la participación de una persona por empresa, en temáticas basadas en el estudio de vigilancia tecnológica sobre tendencias actuales en ciberseguridad.	**Entregable 3.5** Plan de transferencia de conocimiento para las 45 empresas de tecnologías de la información vinculadas, sobre los micro cursos, el bootcamp y las mentorías especializadas, que incluya, entre otros elementos, los contenidos a desarrollar, las metodologías a implementar, las herramientas tecnológicas a utilizar, el cronograma y la intensidad horaria de las actividades, los mecanismos de control, evaluación y validación de la efectividad de la transferencia.
		Resultado 3.4 Un (1) *bootcamp* de 20 horas sobre seguridad digital desarrollado para las hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información seleccionadas, con la participación de una persona por empresa.	**Entregable 3.6** Informe de implementación del plan de transferencia de conocimiento para las 45 empresas de tecnologías de la información vinculadas, que incluya, entre otros elementos, las listas de asistencia, las memorias de los cursos, el bootcamp y las mentorías especializadas (* un apartado por cada actividad), grabaciones, las certificaciones o reconocimientos otorgados a las empresas participantes, encuestas de satisfacción y evaluación realizadas por las empresas beneficiarias, y lecciones aprendidas u oportunidades de

		Resultado 3.5 Cuatro (4) horas de mentoría especializada e individualizada para cada una de las hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información en ciberseguridad seleccionadas, enfocadas en metodologías de innovación para la solución de los retos tecnológicos planteados.	mejora para un eventual escalamiento del proyecto.

Fase 4. Implementación de retos tecnológicos

En esta fase se implementarán soluciones innovadoras a los retos de ciberseguridad de al menos diez (10) MIPYMES seleccionadas del banco conformado en la Fase 1 del proyecto, mediante procesos de transferencia tecnológica desarrollados por las empresas del sector de tecnologías de la información fortalecidas en la Fase 2.

Objetivo Específico 3: Plantear e implementar soluciones innovadoras a los retos identificados, mediante procesos de transferencia tecnológica entre las MIPYMES y las empresas del sector de tecnologías de la información.			
	Actividades	**Resultados**	**Entregables**
Fase 4. Implementación de retos tecnológicos	**Actividad 4.1** Diseñar soluciones para los retos tecnológicos, con al menos una solución propuesta por cada empresa del sector de tecnologías de la información fortalecida en la Fase 2.	**Resultado 4.1** Al menos cuarenta y cinco (45) propuestas de soluciones para retos tecnológicos de MIPYMES del banco conformado en la Fase 2, planteadas por las empresas del sector de tecnologías de la información fortalecidas en la Fase 3.	**Entregable 4.1** Modelo o formato de ficha para la presentación de propuesta de solución de retos. **Entregable 4.2** Un banco de al menos cuarenta y cinco (45) propuestas de soluciones, conformado con las soluciones propuestas por las empresas del sector de tecnologías de la información fortalecidas, con las respectivas fichas de solución que incluya, entre otros aspectos, la metodología de solución, recursos

			científicos, técnicos y tecnológicos a utilizar y el componente innovador de la solución diseñada por las empresas.
	Actividad 4.2 Implementar las soluciones para los retos de al menos diez (10) MIPYMES seleccionadas (retadoras) del banco conformado en la Fase 2.	**Resultado 4.2** Al menos diez (10) retos de ciberseguridad solucionados para las MIPYMES seleccionadas (retadoras), por parte de empresas del sector de tecnologías de la información.	**Entregable 4.3** Documento de lineamientos operativos para la selección de las diez (10) MIPYMES y sus retos, los criterios para los emparejamientos de solucionador-retador, las condiciones contractuales, técnicas y jurídicas para estos emparejamientos, el mecanismo de operación del desarrollo de las soluciones, entre otros.
			Entregable 4.4 Diez (10) fichas de ejecución de las soluciones tecnológicas implementadas, que describan las metodologías utilizadas, los servicios tecnológicos y las capacidades transferidas a las empresas, los resultados e impactos de la solución, oportunidades, etc.
			Entregable 4.5 Informe general de todo el proceso desarrollado en la Fase 4, que incluya como mínimo los resultados generales, las lecciones aprendidas y las oportunidades de mejora para una eventual replicación o escalamiento del proyecto.

Fase 5. Difusión y cierre

En esta fase se llevará a cabo un evento de divulgación tecnológica para el ecosistema de ciberseguridad, con el fin de fortalecer las capacidades del país en materia de aplicación y adaptación de tecnologías de ciberseguridad.

Objetivo Específico 4: Generar espacios de difusión tecnológica para fortalecer las capacidades del país en materia aplicación y adaptación de tecnologías de ciberseguridad.			
	Actividades	**Resultados**	**Entregables**
Fase 5. Difusión y cierre	**Actividad 5.1** Organizar y desarrollar un evento académico y colaborativo en temas de ciberseguridad para un aforo de 80 personas, con una duración de hasta tres días	**Resultado 5.1** Un evento académico y colaborativo en temas de ciberseguridad para un aforo de 80 personas, con una duración de tres días y participación de expertos nacionales e internacionales para	**Entregable 5.1** Plan de organización y desarrollo del evento que incluya, entre otros aspectos, la planeación logística,

	y participación de expertos nacionales e internacionales para abordar las últimas tendencias tecnológicas, desafíos y estrategias en ciberseguridad. Con una agenda compuesta de conferencias, conversatorios y sesiones de networking que apunte a fortalecer las capacidades en ciberseguridad de profesionales, académicos y estudiantes, fomente la cooperación y el intercambio de conocimientos. Además, con stands empresariales y académicos, promoviendo la innovación y el desarrollo en el campo de la seguridad informática.	abordar las últimas tendencias tecnológicas, desafíos y estrategias en ciberseguridad.	cotizaciones y proveedores, las listas de invitados y conferencistas, los temas y actividades a desarrollar y la agenda académica. **Entregable 5.2** Informe de realización del evento que incluya las memorias, listas de asistencia y registros audiovisuales.
	Actividad 5.2 Desarrollar una herramienta tecnológica para hacer seguimiento y control del proyecto.	**Resultado 5.2** Herramienta virtual en la nube desarrollada para seguimiento y gestión del proyecto y visibilización de las innovaciones en ciberseguridad, que incluya los siguientes módulos: Módulos Backend (5) 1. Gestión de Usuarios y Autenticación: 2. Gestión de Proyectos 3. Base de Datos de Empresas y MIPYMES 4. Gestión de Retos Tecnológicos Transferencia de Conocimiento 5. Gestión de propuestas de soluciones innovadoras. Módulos Frontend (6) 1. Dashboard Principal 2. Gestión de Usuarios	**Entregable 5.3** Herramienta virtual en la nube desarrollada para seguimiento y gestión del proyecto y visibilización de las innovaciones en ciberseguridad.

		3. Visualización de Proyectos 4. Empresas y MIPYMES: 5. Retos Tecnológicos 6. Eventos y Difusión	

6 EQUIPO DE TRABAJO

El ejecutor deberá conformar el equipo de trabajo para la ejecución del proyecto y presentar sus perfiles y hojas de vida para validación del Ministerio. El ejecutor seleccionará y vinculará a los integrantes del equipo, garantizando la idoneidad y experiencia requerida de las personas a fin de velar por la oportuna y eficiente ejecución del proyecto.

6.1 Conformación mínima del equipo

El equipo se conformará con al menos los siguientes integrantes cuyos contratos con cargo a recursos del Ministerio deberán tener dedicación exclusiva al proyecto:

ROL	1. **Gerente del Proyecto (1)**
Perfil	**Profesional en un programa según clasificación SNIES del núcleo básico de conocimiento de:** Economía, mercadeo o afines, Administración o afines, Derecho o afines, Ciencia política o afines, Relaciones internacionales o afines, Ciencias sociales y humanas o afines, Ingeniería administrativa o afines, Ingeniería de sistemas o afines, Ingeniería en Telemática o afines, Ingeniería electrónica o afines, Ingeniería en telecomunicaciones o afines, Ingeniería civil o afines Ingeniería industrial, o afines. Título de postgrado en la modalidad de postgrado y/o doctorado en un programa según la clasificación del SNIES de los mismos núcleos básicos de conocimiento enunciados. **Experiencia:** Mínimo Cinco (5) años de experiencia profesional en calidad de Gestor, Gerente y/o director de proyecto, y/o Project mánager y/o coordinador de proyectos en el sector de comercio electrónico y/o sector Ciencia, Tecnología e Innovación y/o sector TIC.
Dedicación	**100%**
ROL	2. **Líder Administrativo y Financiero (1)**
Perfil	**Profesional en un programa según clasificación SNIES del núcleo básico de conocimiento de:** Economía o afines, Administración o afines, Contaduría Pública o afines, Finanzas y afines. **Experiencia:** Tres (3) años de experiencia profesional en alguno de los siguientes temas: administración de recursos, o gestión de contratos y/o convenios, o seguimiento de presupuestos públicos y/o privados, Asesor Financiero, Supervisor financiero, Líder administrativo y financiero, Coordinador administrativo y financiero, Coordinador financiero.
Dedicación	**100%**
ROL	3. **Asesor Legal (1)**

Perfil	**Profesional en un programa según clasificación SNIES del núcleo básico de conocimiento de:** Derecho o afines. **Experiencia:** Tres (3) años de experiencia profesional, de los cuales uno (1) años debe corresponder a experiencia en contratación estatal en sus diferentes etapas (Precontractual, Contractual y Poscontractual) y relacionadas con proyectos TI
Dedicación	**100%**
ROL	4. **Líder de Tecnología (1)**
Perfil	**Profesional en cualquiera de los siguientes programas según la clasificación del SNIES del núcleo básico de conocimiento:** Ingeniería de Sistemas y afines o Ingeniería Electrónica y afines o Ingeniería Telemática y afines. Título de posgrado en cualquiera de los siguientes programas según la clasificación del SNIES del núcleo básico de conocimiento: tecnologías de la información y afines o ingeniería y afines o arquitectura empresarial y afines. **Experiencia:** Cinco (5) años en la formulación y ejecución de proyectos de CTEI
Dedicación	**100%**
ROL	5. **Profesionales Expertos en ciberseguridad (5)**
Perfil	**Profesional en cualquiera de los siguientes programas según la clasificación del SNIES del núcleo básico de conocimiento:** Ingeniería en Sistemas, Telecomunicaciones, Ciberseguridad o afines. **Experiencia:** Tres (3) a cinco (5) años de experiencia en la implementación de soluciones de seguridad y gestión de proyectos en MIPYMES En desarrollo de herramientas para la clasificación de retos y capacidades de proveedores, la creación de informes detallados sobre resultados y potencial de las empresas, y en liderar la implementación y evaluación de proyectos de ciberseguridad, con habilidades administrativas para coordinar equipos y gestionar recursos de manera efectiva.
Dedicación	**100%**
ROL	6. **Líder Comunicaciones Divulgación Tecnológica (1)**
Perfil	**Profesional en cualquiera de los siguientes programas según la clasificación del SNIES del núcleo básico de conocimiento:** Profesional en mercadeo y afines o negocios internacionales y afines o publicidad y afines, o comunicaciones y afines o administración y afines Título de posgrado en cualquiera de los siguientes programas según la clasificación del SNIES del núcleo básico de conocimiento: ventas o marketing y afines o innovación y afines o gerencia de mercadeo y afines. **Experiencia:** Cinco (5) años
Dedicación	**100%**
ROL	7. **Profesional Líder transferencia de conocimiento (1)**

Perfil	**Profesional en cualquiera de los siguientes programas según la clasificación del SNIES del núcleo básico de conocimiento:** Ingeniería Industrial y afines o; Ingeniería Administrativa y afines o administración y afines, o; economía y afines u otras ingenierías. **Experiencia:** Cinco (5) años
Dedicación	**100%**

Este equipo mínimo de trabajo será propuesto por el ejecutor del proyecto, sin perjuicio de que este disponga de personal adicional que considere necesario para el cumplimento del objeto contractual, sin que esto suponga un costo adicional para el Ministerio.

El ejecutor deberá mantener el equipo que presente y que sea aprobado por el supervisor durante la ejecución del proyecto. Si por razones justificadas se hace necesario realizar una modificación o cambio de algún integrante del equipo de trabajo durante la ejecución del proyecto, esta deberá ser aprobado por el Ministerio, a través del supervisor, previa verificación del cumplimiento de los requisitos de cada perfil definido en el presente documento.

El personal debe ser idóneo y calificado en concordancia con las condiciones requeridas para llevar a cabo de buena forma el proyecto. Cualquiera que sea el tipo de contratación, actividades relacionadas a contratos laborales o fijación de salarios u honorarios, se deberán regir y estar enmarcados dentro de las leyes colombianas. En todo caso el supervisor del contrato del Ministerio podrá requerir aclaración conforme a sus funciones de los pagos u honorarios que se efectúan al personal contratado. Las remuneraciones u honorarios que se asignen al personal deberán ser concordantes con sus funciones y afines con posiciones o cargos similares en organizaciones de la misma categoría. Para la definición de los honorarios, se deberá tener en cuenta lo estipulado en la Resolución 00016 del 2023 modificada por la Resolución 04981 del 2023 expedida por el Ministerio TIC, mediante la cual se establece los honorarios de los contratistas del Ministerio/Fondo de TIC.

6.2 Consideraciones sobre los requisitos de experiencia

Para la presentación y aprobación del equipo de trabajo, el ejecutor deberá presentar los siguientes documentos que acrediten el cumplimiento de los requisitos establecidos:

- Copia del documento de identificación: cédula de ciudadanía, cédula de extranjería o pasaporte.
- Hoja de vida.
- Fotocopia copia del título de técnico, tecnólogo o profesional o del acta de grado.
- Certificaciones académicas (actas o diplomas de grado) o certificación expedida por la institución de educación superior en la que se indique la fecha de terminación y aprobación de materias correspondientes al pensum académico de educación superior, cuando haya lugar a ello.
- Copia de la tarjeta o matrícula profesional para los profesionales que la ley les establezca este requisito para ejercer su profesión.
- Certificado de vigencia de la tarjeta o matrícula profesional, para los profesionales que la ley establezca este requisito para ejercer su profesión.
- Certificaciones de la experiencia profesional.

Las certificaciones, constancias o cualquier otro documento que acredite la experiencia profesional del equipo de trabajo requerido deberán ser expedidas por quienes directamente los contrataron o por la entidad para la que se realizaron los trabajos y en los que éstos participaron. La documentación presentada para la acreditación de la experiencia del equipo de trabajo deberá permitir en conjunto la verificación de la siguiente información:

- Empresa o entidad contratante con sus respectivos datos de contacto.
- Nombre del candidato que acredita la experiencia.
- Cargos, roles o perfiles nominales y/o funcionales desempeñados.
- Actividades, obligaciones o funciones por cada uno de los cargos, roles o perfiles desempeñados.
- Objeto del contrato, obligaciones, entregables u actividades que permita verificar de manera explícita la experiencia requerida.
- Periodo de vinculación, con fecha inicial y fecha final expresadas en día, mes y año). En caso de que en las certificaciones solamente se evidencia el mes y el año, para efectos de verificar y calificar la experiencia se procederá así: para fecha (mes, año) de suscripción y/o inicio del contrato, se tendrá en cuenta el último día del mes que se encuentre señalado en la certificación; para fecha (mes, año) de terminación del contrato, se tendrá en cuenta el primer día del mes que se encuentre señalado en la certificación.
- Las experiencias reportadas podrán estar vigentes, caso en el cual se contabilizarán hasta la fecha de expedición de la certificación.
- En el evento que las certificaciones no contengan la información que permita la verificación de estos datos, el ejecutor deberá anexar copia del contrato o documentos soporte que sean del caso, que permita tomar la información que falte en la certificación y permita validar la experiencia específica solicitada.

La contabilización de la experiencia profesional se considerará de acuerdo con lo señalado en el Decreto Ley 019 de 2012 y con la Sentencia del Consejo de Estado del 12 de diciembre de 2022.

El Ministerio realizará la verificación de la documentación que el ejecutor presente y podrá solicitar aclaraciones a los documentos que acreditan la experiencia y formación de los profesionales propuestos.

7 INFORMES DE EJECUCIÓN

El ejecutor presentará informes mensuales de ejecución con corte el último día de cada mes, dentro de los cinco (5) días calendario siguientes a la fecha de corte. Los informes se deberán presentar desde el primer mes de inicio y hasta la finalización del convenio.

Los informes deberán presentar información de forma clara y completa y deberán permitir realizar seguimiento detallado de la ejecución del proyecto. El ejecutor deberá seguir las recomendaciones de presentación de informes establecidas por el Fondo Único de TIC.

Los informes deberán incluir como mínimo:

- Tablero de control que dé cuenta del avance general del proyecto en los componentes técnico, financiero y administrativo.

- Reporte de cumplimiento de metas, alertas de incumplimiento y planes de choque si aplica.
- Informe financiero que dé cuenta del compromiso, ejecución presupuestal y financiera de los recursos.

La supervisión adelantará la revisión, verificación de cumplimiento y contenido de cada informe en un plazo máximo de cinco (5) días hábiles tras la presentación de estos, para solicitar la información necesaria. La supervisión podrá dar concepto parcial al informe y solicitar aclaraciones y complemento de este. En todo caso, el supervisor del Ministerio podrá implementar diversos mecanismos de seguimiento y control al proyecto, para constatar el correcto avance, implementación, operación y ejecución de este.

8 PLAZO DE EJECUCIÓN

El plazo de ejecución del convenio será hasta el treinta y uno (31) de diciembre de 2024, contado a partir de la suscripción del acta de inicio, previo el cumplimiento de los requisitos de perfeccionamiento y ejecución del convenio.

9 ENTIDAD EJECUTORA: IDONEIDAD Y CAPACIDADES

La entidad ejecutora será el Centro de Bioinformática y Biología Computacional de Colombia - BIOS, conforme las siguientes consideraciones:

BIOS posee experiencia probada en materia de ejecución de proyectos de alto impacto que impliquen procesos de innovación, desarrollo tecnológico y el estudio de escenarios que promuevan gestión del conocimiento. En dichas materias: aunó esfuerzos para el favorecimiento del análisis de los determinantes sociales para la toma de decisiones en el marco de la ciencia, la biotecnología e innovación con la Alcaldía de Bogotá (2017); aunó esfuerzos técnicos, administrativos y financieros para el desarrollo de proyectos de ciencia tecnología e innovación con énfasis en los sectores estratégicos de las Direcciones del Gobierno en Línea, Políticas y Desarrollo de TI, I+D+I, que permitan el desarrollo de los objetivos planteados en el plan estratégico con MinTIC (2017); Aunó esfuerzos para fortalecer el ecosistema de ciencia, tecnología, innovación y transferencia de conocimiento a través de la implementación de la iniciativa estratégica denominada: Uso de IoT en la Gestión del Riesgo Ambiental con MinTIC (2018); Desarrolló un "sistema de inteligencia epidemiológica para el apoyo en la toma de decisiones en el control del Covid-19 en Latinoamérica para la Universidad de Caldas (2020); aunó esfuerzos técnicos, administrativos y financieros para realizar las acciones y estrategias correspondientes para la creación y articulación de la Red Nacional de Servicios de Computación de Alto Rendimiento con MinTIC (2021); implementó y puso en marcha el Centro de Servicios Compartidos para la Transformación Digital CSCTD para la Fundación Tecnalia (2021), financiado con concursos MinTIC; aunó esfuerzos administrativos, técnicos, operativos, financieros y científicos para el desarrollo, investigación e implementación de una herramienta web para el mejoramiento de los sistemas de información del IDEAM mediante la estrategia de fábrica de software y solución HPC, que permite llevar a cabo metodologías convencionales y ágiles, así como la atención de los servicios complementarios que se deriven del desarrollo de la herramienta con IDEAM (20121); prestó servicios para operar el Centro de Servicios Compartidos para la Transformación Digital – Tecdigital; realizó el acompañamiento a empresas en su camino de transformación digital bajo la adopción de Tecnologías Avanzadas y Emergentes (TAES); y aplicó el Modelo de Madurez Digital Avanzada-MMDA, garantizando el cumplimiento de

las metas, y el diseño e implementación de la estrategia en su conjunto para la Fundación TECNALIA (2022) financiado con concursos MinTIC.

Adicionalmente, BIOS está equipado con tecnología de vanguardia, incluyendo potentes sistemas informáticos, redes de alta velocidad y acceso a recursos especializados en ciberseguridad, capacidades que le permiten simulaciones complejas y tareas intensivas de analítica de datos que resultan fundamentales para soportar planes de capacitación en materia de ciberseguridad. Desde dicha óptica, poseer infraestructura de supercomputación disponible le permite abordar problemas complejos de ciberseguridad mediante el uso de técnicas de paralelismo, acelerando el tiempo de entrenamiento y de análisis de datos, condiciones especialmente útiles cuando se trata de grandes volúmenes de información y análisis de malware, condiciones objetivas que permiten a BIOS simular entornos de red y sistemas informáticos reales para que los beneficiarios del convenio practiquen sus habilidades en escenarios más cercanos a situaciones del mundo real, contribuyendo a mejorar la preparación para enfrentar amenazas reales y desarrollar habilidades prácticas.

BIOS es un reconocido actor del ecosistema de ciencia y tecnología de la nación, capaz de articular actores públicos y privados para la gestión de conocimiento y el impulso de procesos de alto impacto, sumando dentro sus aliados para la estructuración de planes, mejoramiento de capacidades y formación del recurso humano, con la Universidad Nacional de Colombia, la Universidad de Caldas y la Universidad Tecnológica de Pereira, contando además con acceso a recursos especializados en materia de ciberseguridad al amparo de acuerdos con actores de mercado reconocidos tales como IBM, Bulkware, Td Synnex y Lenovo, entre otros, relacionamiento que confieren a dicho Centro la capacidad para satisfacer la necesidad del Ministerio. Sin perjuicio de lo anterior, BIOS posee además otras potencialidades:

9.1 Especialidad, unicidad y vínculo especial con el Ministerio de Tecnologías de la Información y las Comunicaciones

BIOS es una entidad única en Colombia que combina una amplia gama de especialidades, incluyendo bioinformática, ciencia de datos, ciberseguridad, computación de alto rendimiento (HPC) e infraestructura tecnológica. Su misión, centrada en la generación de valor a través de la incorporación efectiva de tecnologías avanzadas en el ecosistema de tecnología del país, hace que BIOS sea un actor fundamental en el sector tecnológico y de ciberseguridad. Aquí cabe resaltar que BIOS fue creada por iniciativa de la Nación como corporación sin ánimo de lucro de carácter privado, contando con participación de MinTic en su Junta Directiva, siendo históricamente el principal aportante del Centro.

9.2 Liderazgo en Ciberseguridad

BIOS es el líder promotor del HUB de Ciberseguridad (ubicado en el municipio de Villamaría) en concurso con la Gobernación del Departamento de Caldas. Para tal efecto, BIOS cuenta con la manifestación de un número importante de actores, tanto de la academia como del sector real, interesadas en ofrecer coordinadamente sus productos y servicios a través del HUB para fortalecer las capacidades técnicas y humanas del país en materia de ciberseguridad, así: **i.** Actores empresariales: Dragonjar, Kavantic, Data & Service, IBM, TD Synnex, Global AST, People Contact, Bulwark, IT Forensic, Fygp, Innerconsulting, Lenovo, Hispasec; **ii.** Actores académicos: Universidad de Manizales, Universidad Católica de Manizales, Universidad Católica Luis Amigó, Universidad

Nacional Abierta y a Distancia, Universidad Autónoma de Manizales y Universidad de Caldas; y **iii.** Actores gremiales: Acopi, Fenalco, Fundacion Universidad Empresa, Red de Emprendimiento y ARCIS.

9.3 Respaldo y soporte profesional en Ciberseguridad

El talento humano es uno de sus mayores activos de BIOS, contando con profesionales de la ingeniería, expertos en programación, ciencia de datos, y ciberseguridad, tanto en su equipo interno, como provenientes de las universidades públicas del Eje Cafetero que concurren al Centro. En el ámbito de la ciberseguridad, BIOS ostenta un relacionamiento que le permiten acceder a conocimiento especializado desde una visión crítica fundada en las diversas tecnologías disponibles en el mercado, otorgándole la capacidad de procurar soluciones agiles en beneficio de la Nación.

9.4 Experiencia en materia de proyectos de alto impacto

BIOS ha demostrado su experiencia y capacidad para manejar proyectos de gran envergadura en el ámbito de la ciberseguridad, la bioinformática, la ciencia de datos y las tecnologías avanzadas. Sus proyectos en formación incluyen la creación de aulas virtuales para ofrecer cursos avanzados de tecnología propios y de las universidades vinculadas, la capacitación de empresarios en tecnología y la formación avanzada de investigadores en diversas tecnologías avanzadas. Además, ha sido ejecutor habitual y cumplido de los proyectos estratégicos de MinTIC desde 2011 y de regalías de ciencia y tecnología desde 2021.

10 GLOSARIO

i. Activo: Cualquier recurso o componente de valor para una organización, equipos o servicios, que debe ser protegido.
ii. Amenaza: Potencial ocurrencia de un evento no deseado que puede causar daño a un sistema o a la información que maneja.
iii. Autenticación: Proceso de verificación de la identidad de un usuario o sistema antes de permitirle el acceso a los recursos protegidos.
iv. Backup (Copia de Seguridad): Copia de datos importante almacenada en un lugar seguro para su recuperación en caso de pérdida o daño.
v. Ciberespacio: Entorno complejo resultante de la interacción de personas, software y servicios en Internet, mediante dispositivos y redes de tecnología.
vi. Ciberdelito: Actividad criminal realizada a través de computadoras y redes, generalmente con la intención de robar información o causar daño.
vii. Ciberseguridad: Conjunto de medidas, controles y procesos destinados a proteger la información y los sistemas informáticos de ataques, daños o accesos no autorizados.
viii. Cifrado (Encriptación): Proceso de conversión de información legible en un formato codificado para evitar el acceso no autorizado.
ix. Confidencialidad: Propiedad de la información que asegura que ésta no es divulgada a personas, entidades o procesos no autorizados.
x. Denegación de Servicio (DoS): Ataque que busca hacer que un servicio en línea no esté disponible para sus usuarios legítimos.
xi. Firewall (Cortafuegos): Dispositivo o software que controla el acceso entre redes, bloqueando el tráfico no autorizado y permitiendo el tráfico autorizado.
xii. Gestión de Identidades*: Conjunto de procesos y tecnologías utilizadas para gestionar y proteger la identidad digital de los usuarios dentro de una organización.

xiii. Gateway: Dispositivo que conecta redes diferentes, actuando como punto de entrada o salida de la información.
xiv. Herramientas de seguridad: Instrumento hardware y/o software de protección para equipos informáticos, redes y de telecomunicaciones para combatir y prevenir amenazas virtuales externas.
xv. Incidente de Seguridad*: Evento que compromete la confidencialidad, integridad o disponibilidad de la información o sistemas informáticos.
xvi. Integridad: Propiedad de la información que asegura que ésta no ha sido alterada o destruida de manera no autorizada.
xvii. Intrusión: Acceso no autorizado a sistemas informáticos o redes.
xviii. ISP (Internet Service Provider): el proveedor de servicios de internet se refiere a una empresa o compañía que proporciona acceso a Internet, tanto a personas como organizaciones, permitiendo que sus clientes puedan navegar en la web.
xix. Lista de Control de Acceso: Conjunto de reglas que determinan quien puede acceder a determinados recursos en una red.
xx. Malware (Software Malicioso): Programa o código dañino diseñado para infiltrarse y causar daño en un sistema informático sin el conocimiento del usuario.
xxi. Mediana empresa: Aquella cuyos ingresos por actividades ordinarias anuales sean superiores a cuatrocientos treinta un mil ciento noventa y seis Unidades de Valor Tributario (431.196 UVT) e inferiores o iguales a dos millones ciento sesenta mil seiscientos noventa y dos Unidades de Valor Tributario (2'160.692 UVT).
xxii. Microempresa: Aquella cuyos ingresos por actividades ordinarias anuales sean inferiores o a cuarenta y cuatro mil setecientos y nueve Unidades de Valor Tributario (44.769 UVT).
xxiii. Mitigación: Acciones tomadas para reducir la severidad o impacto de un incidente de seguridad.
xxiv. Nube (Cloud): Modelo de computación que permite acceder a recursos y servicios a través de internet.
xxv. Pequeña empresa: Aquella cuyos ingresos por actividades ordinarias sean superiores a y cuatro mil setecientos y nueve Unidades de Valor Tributario (44.769 UVT) e inferiores o iguales a cuatrocientos y un mil ciento noventa y seis Unidades de Valor Tributario (431.196 UVT).
xxvi. Phishing: Técnica de ingeniería social utilizada para engañar a las personas y obtener información confidencial, como contraseñas y detalles de tarjetas de crédito.
xxvii. Política de Seguridad: Conjunto de reglas y prácticas que regulan cómo se maneja, protege y distribuye la información dentro de una organización.
xxviii. Ransomware: Tipo de malware que cifra los datos de una víctima y exige un pago para restaurar el acceso a la información.
xxix. Red Privada Virtual (VPN): Tecnología que crea una conexión segura y cifrada sobre una red pública, como Internet, permitiendo el acceso seguro a recursos de red remotos.
xxx. SIEM (Gestión de Información y Eventos de Seguridad): Herramientas y servicios que proporcionan una visión en tiempo real de las actividades y eventos de seguridad en una organización.
xxxi. Tecnologías de la Información y las Comunicaciones (TIC): Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación,

procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Art. 6 Ley 1341 de 2009).

xxxii. Troyano: Tipo de malware que se disfraza de software legitimo para engañar a los usuarios y obtener acceso no autorizado a los sistemas.

xxxiii. Vulnerabilidad: Debilidad en un sistema que puede ser explotada para causar daño o ganar acceso no autorizado.

xxxiv. Virus: Programa malicioso que se replica a sí mismo y se propaga a otros archivos y sistemas.

xxxv. Worm (Gusano): Tipo de malware que se replica y se propaga automáticamente a través de redes sin intervención humana.

REGISTRO DE FIRMAS ELECTRONICAS

Anexo tecnico Ciberseguridad

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

Id Acuerdo: 20240909-113609-05c5b8-24123781
Creación: 2024-09-09 11:36:09
Estado: Finalizado
Finalización: 2024-09-09 15:56:34

Escanee el código para verificación

Revisión: Carlos Felipe Gomez Pelaez Contratista Subdireccion de Industria de TI



Carlos Felipe Gomez Pelaez
CC94472127
cgomezp@mintic.gov.co

Elaboración: Andrés Ricardo García Soto Contratista SITI



ANDRES RICARDO GARCIA SOTO
86083502
agarcias@mintic.gov.co
CONTRATISTA
SUBDIRECCIÓN DE INDUSTRIA TI - MINTIC

Elaboración: César Mauricio Cortés Alarcón Contratista SITI



Cesar Mauricio Cortes Alarcon
80221518
ccortes@mintic.gov.co
Contratista DED SITI
Ministerio TIC

Elaboración: Carlos Andrés Londoño Zuluaga Contratista SITI



Carlos Andrés Londoño Zuluaga
16079899
clondono@mintic.gov.co
Contratista
Subdirección de Industria de Tecnologías de la Información

REGISTRO DE FIRMAS ELECTRONICAS

Anexo tecnico Ciberseguridad

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

Id Acuerdo: 20240909-113609-05c5b8-24123781

Creación: 2024-09-09 11:36:09

Estado: Finalizado

Finalización: 2024-09-09 15:56:34

Escanee el código para verificación

Firma: Maria Lucía Flórez Jiménez- Directora de Economía Digital



María Lucía Flórez Jiménez
1010198800
mlflorez@mintic.gov.co
Directora de Economía Digital
MinTIC

Revisión: Lyda Marcela Tiria Medina Contratista Subdireccion de Industria de TI



LYDA MARCELA TIRIA MEDINA
1052385544
ltiria@mintic.gov.co
CPS- Abogada
Subdirección de Industria de TI

REPORTE DE TRAZABILIDAD

Anexo tecnico Ciberseguridad

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

Id Acuerdo: 20240909-113609-05c5b8-24123781
Creación: 2024-09-09 11:36:09
Estado: Finalizado
Finalización: 2024-09-09 15:56:34

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	Carlos Andrés Londoño Zuluaga clondono@mintic.gov.co Contratista Subdirección de Industria de Tecnologías	Aprobado	Env.: 2024-09-09 11:36:16 Lec.: 2024-09-09 11:37:05 Res.: 2024-09-09 11:37:34 IP Res.: 186.81.88.13
Elaboración	Cesar Mauricio Cortes Alarcon ccortes@mintic.gov.co Contratista DED SITI Ministerio TIC	Aprobado	Env.: 2024-09-09 11:37:34 Lec.: 2024-09-09 11:37:54 Res.: 2024-09-09 11:39:12 IP Res.: 152.201.103.202
Elaboración	ANDRES RICARDO GARCIA SOTO agarcias@mintic.gov.co CONTRATISTA SUBDIRECCIÓN DE INDUSTRIA TI - MINTIC	Aprobado	Env.: 2024-09-09 11:39:12 Lec.: 2024-09-09 11:42:31 Res.: 2024-09-09 11:42:47 IP Res.: 190.26.160.37
Revisión	Carlos Felipe Gomez Pelaez cgomezp@mintic.gov.co	Aprobado	Env.: 2024-09-09 11:42:47 Lec.: 2024-09-09 11:58:39 Res.: 2024-09-09 12:19:38 IP Res.: 190.71.137.3
Revisión	LYDA MARCELA TIRIA MEDINA ltiria@mintic.gov.co CPS- Abogada Subdirección de Industria de TI	Aprobado	Env.: 2024-09-09 12:19:38 Lec.: 2024-09-09 12:30:16 Res.: 2024-09-09 12:30:51 IP Res.: 181.51.34.76
Firma	María Lucía Flórez Jiménez mlflorez@mintic.gov.co Directora de Economía Digital MinTIC	Aprobado	Env.: 2024-09-09 12:30:51 Lec.: 2024-09-09 15:56:28 Res.: 2024-09-09 15:56:34 IP Res.: 181.78.78.237