Datos del área gestora:	Dependencia solicitante:	Viceministerio De Transformación Digital
	Nombre del viceministro o Jefe o Director o Subdirector de la Dependencia solicitante	Viceministra Sindey Carolina Bernal Villamarín

2. DESCRIPCIÓN DE LA NECESIDAD QUE LA ENTIDAD PRETENDE SATISFACER

2.1 ANÁLISIS SOBRE LA PERTINENCIA Y NECESIDAD.

2.1.1 INTRODUCCIÓN.

La Ley 1341 de 2009, modificada por la Ley 1978 de 2019, tiene principios orientadores como la investigación, el fomento, la promoción y el desarrollo de las tecnologías de la información y las comunicaciones como una política de Estado que involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto a los derechos humanos inherentes y la inclusión social.

En el numeral 8 del artículo 2 de la Ley 1341 de 2009 se establece el principio orientador de Masificación del Gobierno en Línea, hoy Gobierno Digital, el cual dispone: *"Con el fin de lograr la prestación de servicios eficientes a los ciudadanos, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones en el desarrollo de sus funciones. El Gobierno Nacional fijará los mecanismos y condiciones para garantizar el desarrollo de este principio. Y en la reglamentación correspondiente establecerá los plazos, términos y prescripciones, no solamente para la instalación de las infraestructuras indicadas y necesarias, sino también para mantener actualizadas y con la información completa los medios y los instrumentos tecnológicos".*

De acuerdo con el numeral 2 del artículo 17 de la misma Ley (1341 de 2009) el Ministerio de Tecnologías de la Información y las Comunicaciones tiene dentro de sus objetivos 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.

Por otra parte, el CONPES 3854 del 11 de abril de 2016, establece la Política Nacional de Seguridad Digital, mediante la cual crea las condiciones para que las múltiples 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 de esta política el desarrollo de estrategias que establecieron un marco institucional para la seguridad digital con un enfoque de gestión de riesgos, es decir, con una visión preventiva antes que reactiva ante las posibles amenazas en seguridad digital.

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

"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"

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

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

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

Mediante el Decreto 338 de 2022 se adicionó el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones. Con la expedición de este Decreto se: (i) actualizó el marco para la Gobernanza nacional de la seguridad digital, (ii) se fortaleció los equipos nacionales de respuesta a incidentes de seguridad digital y (iii) se definieron instrumentos para la identificación de infraestructuras críticas del sector público.

2.1.2 EQUIPO DE RESPUESTA A EMERGENCIAS CIBERNÉTICAS DE COLOMBIA (COLCERT).

Por medio del Decreto 338 de 2022, se dispuso un marco para la gobernanza de la seguridad digital del país, así como implementación y aplicación de Modelos de Gestión de Riesgos de Seguridad y un Modelo Nacional de Atención a incidentes y la creación de un Equipo de Respuesta a Incidentes de seguridad Informática (CSIRT GOBIERNO) por sus siglas en inglés (Computer Security Incident & Response Team), con el fin de prevenir y mitigar los riesgos de seguridad y generar confianza.

En el artículo 2.2.21.1.5.2 del Decreto 338 de 2022, se establece que el Ministerio de Tecnologías de la Información y las Comunicaciones coordinará el Equipo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT), cuya finalidad es asesorar, apoyar y coordinar a las múltiples partes interesadas para la adecuada gestión de los riesgos e incidentes digitales. Así mismo, el COLCERT es el punto único de contacto y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los incidentes de seguridad digital y a gestionar de forma activa las amenazas de seguridad digital, incluyendo la coordinación a nivel nacional e internacional de las distintas capacidades de respuesta a incidentes o Centros de Operaciones de Seguridad Digital existentes. Dentro de las actividades que debe cumplir COLCERT se encuentran:

- El desarrollo y divulgación de procedimientos, protocolos, guías y recomendaciones para la gestión

"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"

de riesgos e incidentes de Seguridad Digital.

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

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

Con la transformación digital global cada vez nos hacemos más dependientes de las capacidades de TI en la prestación de servicios esenciales, lo cual nos hace potencialmente vulnerables a los incidentes cibernéticos.

A nivel nacional, la encuesta de Convivencia y Seguridad Ciudadana realizada por el Departamento Nacional de Estadística -DANE evidencia que el 2.1% de los colombianos ha sufrido un incidente de Seguridad Digital. El hackeo de redes sociales y plataformas de email, así como el fraude bancario, se ubican en las primeras modalidades de ciberdelitos y son los que tienen más prevalencia en el territorio nacional.

Además, otras encuestas realizadas por el DANE evidencian que cerca del 11% de las empresas en Colombia han tenido incidentes cibernéticos. Tanto empresas como ciudadanos sufren efectos negativos, bien sea en pérdidas económicas, tiempos de indisponibilidad o afectaciones a la reputación, por esta razón, para este Gobierno ha sido una prioridad contar con instrumentos y herramientas para crear un entorno digital seguro.

En línea con lo expuesto, la necesidad de aumentar estrategias de respuesta y solución en ciberseguridad, surge de varias causas que al ser analizadas, generan la pertinencia de estructurar un proyecto que permita aunar esfuerzos institucionales de todos los sectores para construir un ecosistema de seguridad digital.

A continuación, se relacionan algunas causas que se tratan en la estructuración del ecosistema digital:

1. Amenazas cibernéticas en aumento: Con el aumento de la digitalización y la conectividad, también han aumentado las amenazas cibernéticas. Los ciberdelincuentes utilizan técnicas cada vez más sofisticadas para acceder a la información confidencial y causar daños a los sistemas informáticos. Esta creciente amenaza requiere que las empresas y los individuos tengan un mayor conocimiento de ciberseguridad para protegerse adecuadamente.
2. Falta de conocimiento de ciberamenazas: Muchas personas y empresas no están al tanto de las amenazas cibernéticas y cómo protegerse contra ellas. A menudo, la falta de conocimiento es el

"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"

resultado de la falta de formación en ciberseguridad. Por lo tanto, aumentar los niveles de formación en ciberseguridad es esencial para mejorar la conciencia sobre los riesgos y la manera de protegerse.

3. Falta de habilidades especializadas en ciberseguridad: Los profesionales que trabajan en ciberseguridad deben tener destrezas especializadas en áreas como la detección de vulnerabilidades, la gestión de incidentes, la evaluación de riesgos y la implementación de políticas de seguridad. Sin embargo, a menudo se carece de este conocimiento debido a la escasez en la oferta de capacitación en temas relacionados con ciberseguridad. Aumentar los niveles de formación en seguridad informática, ayudará a adquirir estas habilidades especializadas en los profesionales que trabajan en este campo.
4. Cambios tecnológicos rápidos de prevención: Los avances tecnológicos están en constante cambio y evolución, lo que significa que las amenazas cibernéticas también evolucionan constantemente. Esto hace que sea importante estar actualizado en cuanto a las últimas tecnologías y los riesgos asociados con ellas. La formación continua en ciberseguridad es necesaria para mantenerse al día con las últimas amenazas y tecnologías.

Por esta razón, el Gobierno Colombiano, en la Ley del Plan Nacional de Desarrollo 2022 -2026 “Colombia Potencia Mundial de la Vida” en su artículo 116 “Transformación Digital como motor de oportunidades e igualdad” señala que el Ministerio de Tecnologías de la Información y las Comunicaciones, diseñará e implementará una estrategia integral para democratizar las TIC y desarrollar la sociedad del conocimiento y la tecnología en la población, mediante las siguientes medidas, entre otras:

1. Promover un entorno digital seguro para generar confianza en el uso y apropiación de las TIC.
2. En las bases del Plan Nacional de Desarrollo, se encuentra que el Gobierno nacional fortalecerá las capacidades de ciberseguridad y ciberdefensa, para garantizar los intereses nacionales.
3. En el impulso de la transformación digital territorial, se promoverá la ciberseguridad en los territorios.

De esta manera el MinTIC gestiona a través del Grupo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT que es el punto único de contacto para coordinar la prevención, mitigación y respuesta (gestión), los incidentes de Seguridad Digital Nacional de manera rápida y eficiente, a través de:

- El desarrollo y divulgación de procedimientos, protocolos, guías y recomendaciones para la gestión de riesgos e incidentes de Seguridad Digital.
- La Generación de acciones efectivas para la recuperación y puesta en operación de las entidades u organizaciones que así lo soliciten, una vez se presenta y un incidente, tales como:
- Direccionamiento para el plan de acción frente a la recuperación de la operación del incidente.
- Coordinar: (i) apoyos con industria, (ii) capacidades de otras instancias del Estado (iii) Capacidades con homólogos locales, regionales y globales.
- Iniciar las gestiones pertinentes con las autoridades (DIJIN, FGN y SIC, etc.), haciendo seguimiento al cumplimiento del marco jurídico frente a la notificación del caso ante las autoridades.
- La ejecución de acciones para promover el desarrollo de capacidades locales y sectoriales, mediante la implementación del modelo de Gobernanza de Seguridad Digital (determinación de roles y responsabilidades a nivel, nacional, regional, local e individual, frente a la gestión de los riesgos e incidentes de seguridad digital).
- La definición de la metodología para la identificación de las infraestructuras críticas cibernéticas y

“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”

servicios esenciales, así como levantar el inventario de infraestructuras críticas públicas cibernéticas nacionales y de servicios esenciales en el ciberespacio.

- Identificar, que con la trasformación digital global cada vez nos hacemos más dependientes de las capacidades de TI en la prestación de servicios esenciales, lo cual nos hace potencialmente vulnerables a los incidentes cibernéticos.

2.1.3 JUSTIFICACIÓN DE LA NECESIDAD.

El Ministerio de las Tecnologías de la Información y Comunicaciones (MinTIC) en el cumplimiento de sus funciones relativas a la transformación digital y en especial, aquellas relacionadas con la seguridad digital impulsa la creación de un Hub de ciberseguridad, como parte del ecosistema de seguridad digital del País, toda vez que a través de esta iniciativa permitirá la protección de las instituciones, las personas, de las infraestructuras digitales, fortalecimiento de las entidades del Estado, fortalecimiento en la gestión de capacidades y brindará las garantía en la prestación de sus servicios en el entorno digital, proponiendo diseñar e implementar una estrategia para adelantar las medidas enfocadas a salvaguardar la infraestructura crítica cibernética del país.

Con ello, se busca proteger la información de las entidades gubernamentales y de las personas de posibles ataques cibernéticos y delitos informáticos, bajo principios de resiliencia y rápida recuperación.

Adicionalmente, se promoverá definir una estrategia para impulsar hitos de seguridad digital para garantizar la continua prestación de los servicios ofrecidos por las entidades públicas, así como establecer los lineamientos técnicos para adoptar los estándares y buenas prácticas en el tema.

Muchas instituciones públicas o privadas tienen ante sí el reto de la transformación digital. La llamada Industria 4.0 requiere la conjunción de las tecnologías de operación (OT) e Internet de las Cosas (IoT), reconociendo que hay nuevos riesgos y ciberamenazas y por ello, se requieren nuevas herramientas de gestión. A través del presente proyecto, se busca elaborar un ecosistema que pretende ser el aliado de las organizaciones porque atiende a las nuevas necesidades de ciberseguridad y privacidad y, ello, se materializará a través del hub.

En ese orden, el ecosistema que se necesita implementar deberá ser completamente compatible e integrable con el Modelo de Gobierno y Gestión de las TIC y abarcará las siguientes líneas:

a. Seguridad de la información
b. Esquema Nacional de Seguridad
c. Prestadores de Servicios cualificados de Confianza
d. Ley de Protección de Datos
e. Ciberseguridad del Dato
f. Ciberseguridad Industrial

1.1.3.1. Establecimiento de un Ecosistema de seguridad digital a través de un Hub de Ciberseguridad.

Para abordar estrategias y soluciones que permita potencializar las capacidades de respuesta a los ciberataques, se requiere construir un ecosistema de seguridad digital que integre estado, empresas, universidades, sociedad civil y organizaciones internacionales, para promover el desarrollo de capacidades nacionales en ciberseguridad a través de la creación de un HUB de ciberseguridad, un SOC especializado

"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"

para el sector público y el desarrollo de un plan maestro de capacitación, formación y entrenamiento.

Para ello se definen tres líneas de desarrollo del ecosistema:

1. Estructuración de un HUB de Ciberseguridad: Definido como un ecosistema abierto que impulsará la investigación, innovación y desarrollo de soluciones tecnológicas para la seguridad digital de las instituciones.

2. Estructuración de un Centro de Operaciones de Seguridad - SOC (Security Operations Center): Estará definido a través de profesionales de seguridad de TI quienes supervisarán la infraestructura tecnológica de las organizaciones aliadas para detectar eventos de ciberseguridad en tiempo real y abordarlos de la forma más rápida y eficaz posible.

3. Desarrollo de un Plan Maestro de Formación, Capacitación y Entrenamiento en Ciberseguridad: El plan de ciberseguridad será la hoja de ruta, en la que se definirán y planificarán una serie de acciones y proyectos con el objetivo de reducir los riesgos a los que están expuestas las empresas y desarrollar su actividad con seguridad mediante formación en dicha materia.

2.1.4 ESTADÍSTICAS SOBRE SEGURIDAD INFORMÁTICA:

Teniendo en cuenta la publicación realizada de *"30 Estadísticas Importantes de Seguridad Informática (2022) | Prey Blog (preyproject.com)"*[1], para el año 2022 se presentaron las siguientes estadísticas sobre seguridad informática:

- El 78% de líderes de seguridad TI creen que sus organizaciones no tienen suficiente protección contra ciberataques a pesar de las inversiones en ciberseguridad realizadas en 2020. (Insight Enterprises)
- Más del 90 por ciento de todas las organizaciones de salud han reportado al menos una brecha de ciberseguridad en los últimos tres años. (Frost & Sullivan)
- 62,7% de las empresas creen que los ciberataques han aumentado desde el año 2020 debido a la pandemia de COVID-19. (Prey)
- 43% de los ciberataques afectan a pequeños negocios. (Small Business Trends)
- Las detecciones de malware y ransomware de endpoint superaron el volumen total observado en 2020 a fines del tercer trimestre de 2021, según los investigadores de WatchGuard Threat Lab. (HelpNet Security)
- 93% del malware observado el año 2019 es polimórfico, es decir que es capaz de modificar su programación para evitar ser detectado. (Webroot)
- A una compañía le toma aproximadamente seis (6) meses detectar una brecha de seguridad. (ZD Net)
- Windows es el sistema operativo más atacado por hackers, Android viene en segundo lugar. (Computer World)

1 Publicación realizada en la página web https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

"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"



Por otra parte, la comunicadora social y periodista Gloria Helena Rey de la Casa Editorial El Tiempo,[i] realizó una investigación donde determinó que entre enero y octubre del 2022 se reportaron 54.121 denuncias por ciberataques y 10 empresas fueron hackeadas, según estadísticas del Centro Cibernético de la Policía Nacional y según expertos, Colombia es el tercer país con mayor número de ciberataques en América Latina, después de México y Brasil.

Eso prendió las alarmas para priorizar la adopción de una gestión corporativa e individual para establecer un sistema de seguridad informática y mitigar los innumerables riesgos que enfrentamos.

"*La información que tienen las empresas es uno de los activos más valiosos, sólo comparable con el recurso humano. Protegerla es inherente a cualquier negocio*", dice Efraín Soleringeniero industrial con maestría en finanzas de la Universidad de los Andes y experto en el tema. Así mismo señaló que *"(…) Las empresas que invierten en ciberseguridad son más efectivas a la hora de prevenir ciberataques y sostiene que, entre otras cosas, se benefician a nivel corporativo en "integridad y privacidad de los datos al minimizar las probabilidades de que la información se vea comprometida".*[ii] (…) Además, el profesional resalta que cuando se cuentan con procedimientos adecuados "*se puede actuar de manera rápida y conjunta, minimizando los tiempos de contención. La ciberseguridad es un valor diferencial que crea una relación de mayor confianza con los clientes, que exigen una interacción segura y sin riesgos*". A lo anterior se suma la mitigación de riesgos y la minimización de eventuales pérdidas económicas, por lo que conocidos los riesgos a los que está expuesta una organización es preciso "diseñar una estrategia para recuperar el negocio de manera rápida".

Por eso, desde el punto de vista empresarial, la ciberseguridad es necesaria *"para defender y anticipar las amenazas digitales propias del ecosistema donde opera una organización con el fin de proteger y asegurar la resiliencia de las operaciones, la reputación de la empresa y su promesa de valor*", explica a Portafolio en otra entrevista Jeimy J. Cano M, Ph.D,[2] profesor universitario y consultor internacional independiente en

2 Seguridad-informática.pdf (3ciencias.com)

seguridad/ciberseguridad.

Adicionalmente sostiene que no se trata de un reto técnico *"sino de un riesgo de negocio estratégico frente a un entorno cada vez más digital y tecnológicamente modificado".*

Las razones de peso para que una empresa invierta en Ciberseguridad son, entre otras, proteger su reputación y promesa de valor; defenderse de ataques que demoran, disuaden o confunden; anticipar amenazas latentes o emergentes y responder a eventos inesperados.

Además de vulnerabilidades cibernéticas como: Ransomware, Malware, y Phishing, se suman el robo de los datos confidenciales de un sistema y la identificación de sus vulnerabilidades tales como contraseñas poco seguras, que facilitan el ingreso de los ciberdelincuentes. Por lo tanto, es importante partir de la premisa de que todos estamos expuestos a los ciberataques por lo que es necesario aplicar diferentes estrategias para proteger los bienes y patrimonios con los que cuenta cada una de las partes que conforman el ecosistema digital, señalan los expertos.

Existen varios tipos de ciberseguridad como lo son: La industrial, asociada con el tema de automatización y operación de plantas o equipos industriales (particularmente asociado con infraestructuras críticas cibernéticas); la de las empresas y la de las naciones, las cuales protegen la seguridad de un país; la sus ciudadanos e infraestructuras críticas cibernéticas y de información.

Así mismo señala el ingeniero Efraín Soler[3] que los sectores más afectados por ciberataques han sido el comercio minorista y mayorista. Las finanzas y seguros fueron el segundo sector más atacado en 2022 con el 24 por ciento de los casos, seguidos por energía y manufactura, ambos con un 20 por ciento. Esto demuestra que en Colombia están aumentando los ataques cibernéticos y, por esa razón, las empresas locales necesitan más y mejores estrategias, donde no se trate solamente de saber cómo reaccionar a un ciberataque sino cómo prevenirlo y recuperarse rápidamente.

Conforme lo anterior, se considera necesario estimular un proyecto que borde las causas que afectan la seguridad digital de las instituciones y a la vez, proporcione habilidades adecuadas a ciudadanos y empresas para mejorar estrategias, conocimiento y destrezas sobre temas que cada día hacen parte del entorno laboral y personal.

En línea con lo expuesto, la necesidad de aumentar los niveles de prevención, solución y defensa en ciberseguridad surge de varias causas que pueden ser consideradas para construir un proyecto eficaz. Algunas de estas causas, son:

1. Amenazas cibernéticas en aumento: Con el aumento de la digitalización y la conectividad, también han aumentado las amenazas cibernéticas. Los ciberdelincuentes utilizan técnicas cada vez más sofisticadas para acceder a la información confidencial y causar daños a los sistemas informáticos. Esta creciente amenaza requiere que las empresas y los individuos tengan un mayor conocimiento de ciberseguridad para protegerse adecuadamente.
2. Falta de conocimiento de amenazas cibernéticas: Muchas personas y empresas no están al tanto de las amenazas cibernéticas y cómo protegerse contra ellas. A menudo, la falta de conocimiento es el resultado de la falta de formación en ciberseguridad. Por lo tanto, aumentar los niveles de formación

3 ::Evaluamos - Periodismo de Código Abierto

"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"

en ciberseguridad es esencial para mejorar la conciencia sobre los riesgos y la manera de protegerse.

3. Falta de habilidades especializadas: Los profesionales que trabajan en ciberseguridad deben tener destrezas especializadas en áreas como la detección de vulnerabilidades, la gestión de incidentes, la evaluación de riesgos y la implementación de políticas de seguridad. Sin embargo, a menudo se carece de este conocimiento debido a la escasez en la oferta de capacitación en temas relacionados con ciberseguridad. Aumentar los niveles de formación en seguridad informática, ayudará a adquirir estas habilidades especializadas en los profesionales que trabajan en este campo.
4. Cambios tecnológicos rápidos: Los avances tecnológicos están en constante cambio y evolución, lo que significa que las amenazas cibernéticas también evolucionan constantemente. Esto hace que sea importante estar actualizado en cuanto a las últimas tecnologías y los riesgos asociados con ellas. La formación continua en ciberseguridad es necesaria para mantenerse al día con las últimas amenazas y tecnologías.

Finalmente, en concordancia con la necesidad previamente descrita y con la normativa correspondiente a: el numeral 1 del artículo 2 del Decreto Ley 591 de 1991, el literal e) del numeral 4º del artículo 2º de la Ley 1150 de 2007, el artículo 18 de la Ley 1286 de 2009 el cual modificó la Ley 29 de 1990, el Decreto 393 de 1991, el documento CONPES 4069 de 2022 y la sentencia radicado número 11001-03-06-000-2010-00058-00(2007) del ocho (8) de julio de dos mil diez (2010) del Consejo de Estado, la presente contratación se considera como una actividad de Ciencia, Tecnología e Innovación (ACTI), toda vez que comprenden actividades sistemáticas que están estrechamente relacionadas con la producción, promoción, difusión y aplicación de conocimientos tecnológicos, científicos y técnicos en los campos de la ciencia, la tecnología y la innovación, por lo que es procedente adelantar la contratación directa de la misma.

El artículo 2° del Decreto 393 de 1991 estableció los propósitos de la asociación, la cual, bajo cualquiera de las modalidades previstas en el artículo 1º, la asociación podrá tener entre otros, los siguientes propósitos, entre otros.

c) Organizar centros científicos y tecnológicos, parques tecnológicos, e incubadoras de empresas.
d) Formar y capacitar recursos humanos para el avance y la gestión de la ciencia y la tecnología.
e) Establecer redes de información científica y tecnológica.
k) Realizar seminarios, cursos y eventos nacionales o internacionales de ciencia y tecnología

Adicionalmente es importante precisar que, con el fin de desarrollar en forma conjunta las actividades de ciencia y tecnología que le son asignadas a la entidad, como lo es el "*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",* se analizó la experiencia y trayectoria del CENTRO DE BIOINFORMATICA Y BIOLOGIA COMPUTACIONAL DE COLOMBIA y este cuenta con la capacidad de promover el desarrollo de capacidades en ciberseguridad a través de la creación de un HUB de ciberseguridad, un SOC especializado para el sector público y el desarrollo de un plan maestro de capacitación, formación y entrenamiento, cumpliendo con ello las necesidades de la entidad previamente descritas.

Así, con el presente convenio se busca impulsar y fortalecer al CENTRO DE BIOINFORMATICA Y BIOLOGIA COMPUTACIONAL DE COLOMBIA para que de manera conjunta se desarrolle los cometidos de la entidad.

"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"

Por lo que en estos términos no le es aplicable lo dispuesto en la Directiva Presidencial 06 de 14 noviembre de 2023, toda vez que las actividades técnico científica serán realizadas directamente por la empresa cooperante.

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

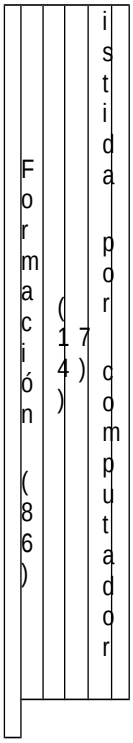
2.1. Descripción del Objeto a contratar	Aunar esfuerzos para desarrollar un ecosistema de seguridad digital que impulse procesos de innovación y desarrollo tecnológico, mediante el estudio de escenarios que promuevan la gestión del conocimiento de los riesgos cibernéticos y las afectaciones de los incidentes de seguridad digital entre los diferentes grupos poblacionales del territorio colombiano. Código TIC 3020001.
2.1.1 Códigos de clasificación UNSPSC:	El objeto antes señalado se encuentra enmarcado en los siguientes códigos de clasificación UNSPSC:

Segmento	Familia	Clase	Producto	Código
Servicios (Fabricación de ingeniería)	Servicios de tecnología de la información	Servicios de administración de sistemas	Servicios de administración de sistemas de información	81161501

		Servicios de tecnología (81)	Servicios de ingeniería de sistemas e industria de tecnología de la información (16)	Servicios de acceso de software (15)	Servicios de aplicaciones de software (01)	86111502

		Educativos y de Formación (86)	Educativos alternativos (110)	de apredizaje a distancia (15)	de enseñanza a distancia (02)
		Servicios Educati	Instalaciones	Servicios de	Servicios de	86141501

		Servicios Educativos y de Formación (86)	Instalaciones educativas (14)	Tecnología educacional (15)	Instituciones educativas (01)	86141703



2.2. Especificaciones del Objeto:

2.2.1. Alcance.

Construir un ecosistema de seguridad digital que integre estado, empresas, universidades, sociedad civil y organizaciones internacionales, para promover el desarrollo de capacidades nacionales en ciberseguridad a través de la creación de un HUB de ciberseguridad, un SOC especializado para el sector público y el desarrollo de un plan maestro de capacitación, formación y entrenamiento.

2.2.1.1. HUB de Ciberseguridad.

Objetivos específicos:

a. Estructuración técnica, legal, financiera y organizacional del proyecto.
b. Análisis de Requerimientos: Identificar y documentar los requerimientos necesarios para la implementación del HUB en el PCTC en los componentes físicos y tecnológicos, incluyendo un presupuesto estimado para las adecuaciones.
c. Identificación de Aliados Potenciales: Establecer espacios para realizar ruedas de negocios y definir contactos con empresas e instituciones que estén interesadas en participar en el HUB, en los distintos roles definidos.

"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"

Entregables:

a. Proyecto para la creación del HUB de Ciberseguridad.
b. Plan de adecuación física y tecnológica de las instalaciones del PTC para albergar al HUB.
c. Informe final de avance en gestiones de presentación y promoción del HUB con diversos aliados potenciales
d. Ficha Bpin proyecto HUB de Ciberseguridad

2.2.1.2. Centro de Operaciones de Seguridad - SOC (Security Operations Center).

Objetivos específicos:

a. Definir los requerimientos técnicos específicos para el SOC.
b. Diseñar la arquitectura tecnológica adecuada para el SOC.
c. Establecer la estructura organizacional y definir roles dentro del SOC.
d. Realizar un análisis financiero y proyección de costos de implementación y operación del SOC.
e. Formular un plan detallado para la contratación y puesta en marcha del SOC.

Entregables:

a. Requerimientos técnicos del SOC
b. Propuesta detallada de arquitectura tecnológica.
c. Documento de estructura organizacional y roles del SOC.
d. Plan financiero detallado para la implementación y sostenimiento del SOC.
e. Plan para la implementación y puesta en marcha del SOC.
f. Ficha Bpin Proyecto SOC

Nota: La entidad realiza el proceso de contratación FTIC-LP-008-2023 cuyo objeto es Prestar servicios especializados de monitoreo de seguridad, infraestructura y red (SOC/NOC), mediante una herramienta que se integre con las plataformas tecnológicas y sistemas de información del MINTIC / Fondo Único de Tecnologías de la Información y las Comunicaciones, cuya actividad principal consiste en implementar una herramienta de monitoreo y prestar solución a los reportes sobre cada incidente atendido y solucionado, cuya diferencia con el presente proyecto se da en que, mediante el diseño técnico, tecnológico, financiero y organizacional a través de un centro de operaciones de seguridad que prestará el servicio de detección de incidentes mediante la observación de eventos técnicos en redes, infraestructura, sistemas de información en plataforma on premise y nube de las entidades públicas y privadas a nivel nacional y territorial de manera permanente, como mecanismos de alerta temprana para la prevención de incidentes de seguridad digital. Es decir, se diseñará más no se ejecutará en esta vigencia.

2.2.1.3. Plan Maestro de Formación, Capacitación y Entrenamiento en Ciberseguridad.

Objetivos específicos:

- Diseñar el plan maestro para la vigencia del presente gobierno, incluyendo metas y presupuesto.
- Diseñar la estrategia de comunicación ciudadana sobre ciberseguridad
- Diseñar el modelo de alianzas para el logro de las metas de formación en ciberseguridad
- Diseñar un programa de educación formal en técnico en ciberseguridad que pueda ser implantado en

"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"

diversas instituciones de educación superior.

Alcance: El plan para desarrollar debe estar enfocado al desarrollo de las capacidades técnicas del recurso humano del país en los diferentes segmentos definidos, a saber:

a. Ciber Expertos: Profesionales en áreas de tecnología de la información, ingeniería de sistemas o carreras afines con formación básica en ciberseguridad y que desean dedicarse a la ciberseguridad de manera profesional.
b. Ciber Líderes TI: directores o jefes de tecnología de empresas y entidades públicas y privadas y requieren capacidades avanzadas en ciberseguridad para incorporar la tecnología adecuada en sus organizaciones y responder adecuadamente ante posibles ataques.
c. Ciber Profesionales TI: Profesionales de trabajan en áreas de tecnología de empresas y entidades del país que requieren desarrollar competencias para atender necesidades y riesgos de ciberseguridad de sus organizaciones.
d. Ciber Profesores: Docentes en tecnología interesados en profundizar sus conocimientos y dedicarse a la enseñanza de la ciberseguridad en la educación superior.
e. Ciber Estudiantes: Estudiantes en los niveles técnico, tecnológico y profesional que van a requerir conocimientos en ciberseguridad para desempeñarse en su vida profesional.
f. Ciudadanos: Ciudadanos y habitantes del territorio nacional que hacen uso de servicios digitales y requieren sensibilización y conocimientos básicos sobre ciberseguridad.

Entregables:

a. Plan Maestro de capacitación, formación, entrenamiento del recurso humano del país en ciberseguridad: Este plan debe contener como mínimo un análisis de sector y definición de necesidades de recurso humano en ciberseguridad, una definición de segmentos y subsegmentos, una propuesta de estrategia de formación para cada uno y una cuantificación de las metas por segmento para el período 2023-II a 2026-II.
b. Análisis de sector y definición de necesidades de recurso humano en ciberseguridad, una definición de segmentos y subsegmentos, una propuesta de estrategia de formación para cada uno y una cuantificación de las metas por segmento para el período 2023-II a 2026-II.
c. Modelo de asociación y alianzas para el logro de alcance del plan maestro: Identificación y gestión de convenios con los aliados potenciales de la industria que están en capacidad y disposición de ofrecer formación pagada, gratuita o subsidiada adicional a la entregada por el ministerio, para alcanzar las metas propuestas. Se deben definir los segmentos a los que estará dirigida esta formación y como se incorporan estos esfuerzos en el plan general.
d. Programa académico formal para formación de Técnico profesional en ciberseguridad: Definición de Syllabus propuesto para el programa, identificación de IES potencialmente capaces de implantar estos programas.
e. Estrategia de comunicación integral para sensibilización ciudadana sobre ciberseguridad para el período 2023-II a 2026-II que defina las audiencias, conocimientos y mensajes clave y que pueda ser ejecutada desde el ministerio en el período definido.

2.2.1.4. **Formación en ciberseguridad en el período 2023**

En el componente de formación, el Ciclo inicial para alcanzar las metas propuestas en el periodo 2023-II por el Ministerio, estarán dadas, así: Capacitar 1800 personas en ciberseguridad de acuerdo con las metas definidas

"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"

en cada segmento:

Segmento	Meta (No. de Personas)	Mínimo de Horas x Persona
Ciber Líderes TI	400	20 capacitación /10 horas practicas
Ciber Profesionales TI	350	20 capacitación/ 10 horas prácticas
Ciber Profesores	50	20 capacitación /10 horas practicas
Ciber Estudiantes	1000	20 capacitación
Total	**1.800**	**Personas**

Metodología de enseñanza
Se podrán usar una o varias de las modalidades definidas a continuación:

- Clases en línea: Se podrán impartir clases teóricas en modalidad síncrona o asíncrona, según el diseño de la formación presentado por el aliado, utilizando la plataforma propuesta dispuesta para ello.
- Seminarios web: Se podrán llevar a cabo seminarios web para profundizar en temas específicos de ciberseguridad.

Laboratorios virtuales: Se podrán realizar prácticas en entornos virtuales, para que los participantes puedan aplicar los conocimientos teóricos adquiridos, según el contenido previsto en cada nivel

2.3 Obligaciones generales del contratista:	1. Cumplir con lo establecido en las políticas de tratamiento de Datos personales, Seguridad y Privacidad de la información, seguridad digital y continuidad de la operación de los servicios y tratamiento de la Información de la entidad. 2. Salvaguardar los activos de información del Ministerio/Fondo Único de TIC. 3. Suscribir el documento de compromiso de confidencialidad. 4. Reportar a la Mesa de Servicio o a quien haga sus veces, los incidentes que afecten o puedan afectar la Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad del servicio de la entidad. 5. Cumplir a cabalidad con lo establecido en el objeto descrito en el presente documento en los términos y condiciones aquí pactadas y lo señalado en su propuesta, observando en todo momento la constitución política, las leyes colombianas y el régimen de contratación pública. Por ningún motivo suspenderá o abandonará el cumplimiento del contrato, sin previa justificación aceptada por la Entidad contratante. 6. Ejercer la dirección y el control propio de todas las actividades encomendadas, en forma oportuna y dentro del término establecido, con el fin de obtener la correcta realización del objeto contratado. 7. Responder, sin perjuicio de la respectiva garantía, por el cumplimiento y calidad de los servicios prestados, por el término previsto en el presente proyecto. 8. Responder ante terceros por los daños que se ocasionen y que provengan de causas que le sean imputables, cuando dé lugar a ello. 9. Salvaguardar la información confidencial que obtenga o conozca en el desarrollo de sus actividades salvo requerimiento expreso de Autoridad competente. Toda 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"

	información y/o documentos que se produzcan en desarrollo del presente convenio serán de uso exclusivo del Fondo, obligándose desde ya el cooperante a no utilizarlos para fines distintos a los previstos en este contrato / convenio, ni a divulgar la información que se le suministre ni los resultados de su trabajo conservando la confidencialidad de estos, de conformidad con la Ley, so pena de las acciones civiles, administrativas o penales a que haya lugar. 10. Entregar al supervisor del control de ejecución del convenio, el informe de las actividades realizadas durante el mes o periodo, al igual que los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos en cada actividad encomendada cuando así se requiera. 11. Atender 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. 12. Reportar, de manera inmediata al supervisor, la ocurrencia de cualquier novedad o anomalía durante la ejecución del convenio. 13. Informar sobre peticiones o amenazas de que sea objeto por quienes actúen por fuera de la ley, con el propósito de obligarlo a hacer o a omitir algún acto o hecho, al Fondo Único de Tecnologías de la Información y las Comunicaciones a través del funcionario responsable de la supervisión y control de ejecución, y a las demás autoridades competentes para que se adopten las medidas y correctivos que fueren necesarios. 14. Realizar las actividades asignadas conforme lo estipulado contractualmente. 15. Responder dentro de los términos establecidos por la ley a todas las peticiones, quejas, reclamos, sugerencias y denuncias -PQRSD- que le hayan sido asignadas a través del sistema de información documental INTEGRATIC, o del que disponga la Entidad, sin ninguna tarea pendiente a su cargo, cuyo trámite será tenido en cuenta por parte del supervisor del contrato para la autorización de cobro y expedición de paz y salvos. 16. "Cumplir con lo establecido en las políticas de tratamiento de Datos Personales, Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios y Tratamiento de la Información de la Entidad, de conformidad a la Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 1074 de 2015 Resolución No. 448 de 2022 y demás normas que apliquen". 17. Presentar la solicitud de desembolso como requisito necesario para el pago de los servicios contratados.
2.4 Obligaciones específicas del contratista:	1. Presentar dentro de los primeros 5 días hábiles el plan de trabajo para el inicio de ejecución de las actividades 2. Desarrollar y presentar todos y cada uno de los entregables señalados en el Anexo Técnico que dio lugar a la suscripción del convenio, documento que hará parte integral de mismo. 3. Llevar contabilidad independiente para la ejecución del Convenio. 4. Disponer los recursos del convenio únicamente para el cumplimiento del objeto y las obligaciones derivadas del mismo. 5. Presentar y entregar al Supervisor los informes necesarios para dar cuenta del cumplimiento de las metas.

"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"

	6. Ceder la propiedad intelectual y patrimonial a la Entidad de la producción que se obtenga de los estudios y publicación de resultados de actividades de capacitación. 7. Designar un representante para integrar el Comité Técnico del Convenio, órgano encargado del seguimiento técnico, administrativo y financiero durante la ejecución. 8. Realizar la estructuración legal, financiera, tecnológica, organizacional de un HUB de Ciberseguridad que fomente la innovación y colabore en la protección de la infraestructura y los datos del Estado Colombiano mediante la prestación de servicios especializados y la formación de talento humano en ciberseguridad. 9. Realizar el diseño técnico, tecnológico, financiero y organizacional de un SOC que preste que preste servicio de detección de incidentes mediante la observación de eventos técnicos en redes, infraestructura, sistemas de información en plataforma On Premise y nube de las entidades públicas y privadas a nivel nacional y territorial de manera permanente. 10. Desarrollar la oferta del Plan Maestro de Capacitación con los componentes descritos en el anexo técnico. 11. Atender las sugerencias hechas por la supervisión a los cursos de formación, sin que ello afecte el contenido de estos, considerando además las recomendaciones que realice el área de Comunicaciones o el Cooperante para un mayor incentivo de participantes. 12. Garantizar que el personal requerido cuente con la formación académica, experiencia e idoneidad necesaria, los cuales han sido descritos en el anexo técnico. 13. Mantener de forma permanente, durante toda la ejecución del convenio, el equipo de trabajo mínimo requerido, garantizando en todo caso, los requisitos mínimos de los perfiles propuestos, con el fin de desarrollar las actividades que permitan el cumplimiento del objeto contractual. 14. Las demás establecidas en el anexo técnico.
2.4.1 Obligaciones particulares del Ministerio o del Fondo Único de Tic	1. Pagar oportunamente el valor total del convenio, de conformidad con lo estipulado en la forma de pago descrito en este mismo documento. 2. Designar al funcionario que ejercerá la supervisión y el control de ejecución del convenio, quien estará en permanente contacto con el Aliado / cooperante, para la coordinación de cualquier asunto que así se requiera. 3. Suscribir, a través del supervisor del control de ejecución del convenio, los documentos y actas que sean necesarias durante el desarrollo del proyecto. 4. Suministrar la información necesaria sobre los diferentes aspectos que sean requeridos para el logro de los objetivos propuestos, siempre y cuando no sea obligación del cooperante. 5. Informar de manera inmediata, acerca de cualquier circunstancia que amenace vulnerar los derechos del cooperante, al igual que cualquier perturbación que afecte el desarrollo normal del proyecto. 6. Guardar la confidencialidad y velar por la protección de los productos y/o servicios propuestos por el cooperante cuando a ello hubiere lugar. 7. Exigir a través del supervisor, el cumplimiento de aportes de la contrapartida ofrecida por el cooperante.
2.5 Plazo de ejecución del	El plazo de ejecución para el contrato resultante del proceso de selección **será hasta el 31 de diciembre de 2023,** contado a partir de la suscripción del acta de inicio, previo al

"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><td>contrato</td><td>cumplimiento de los requisitos de perfeccionamiento y ejecución.</td></tr>
<tr><td>2.6 Lugar de ejecución del contrato:</td><td>El contrato será ejecutado en la ciudad de Bogotá D.C.
Las actividades que no ameriten desplazamientos ni traslados podrán llevarse a cabo a través de los canales virtuales consensuados por las partes.</td></tr>
<tr><td>2.7. Valor del convenio / presupuesto oficial:</td><td>El presupuesto del presente convenio es hasta la suma de:

CINCO MIL CIEN MILLONES DE PESOS (5.100.000.000)

Aportes de MINTIC: CUATRO MIL OCHOCIENTOS MILLONES DE PESOS (4.800.000.000) MCTE, incluido, costos y gastos financieros y tributarios, costos directos e indirectos y demás impuestos que se causen por el hecho de su celebración, ejecución y liquidación, el cual se pagará conforme la forma de pago establecida.

Aportes del Aliado / Cooperante en Especie: TRESCIENTOS MILLONES DE PESOS (300.000.000),

Los aportes del Cooperante serán por la suma de: Trescientos millones de pesos (300’000.000) en especie, descritos así:

<table>
<tr><th>Descripción del aporte</th><th>Cant</th><th>Valor Unitario</th><th>Valor Total</th></tr>
<tr><td>Logos y manual de imagen del Hub De Ciberseguridad</td><td>1</td><td>50.000.000</td><td>50.000.000</td></tr>
<tr><td>Desarrollo de cortos y/o videos animados sobre ciberseguridad dirigidos a los ciudadanos, con logos e imagen institucional del MINTIC.</td><td>10</td><td>25.000.000</td><td>250.000.000</td></tr>
<tr><td colspan="3">TOTAL</td><td>300.000.000</td></tr>
</table>
Este valor incluye IVA SI ☐ NO ☐ No es sujeto de IVA ☒</td></tr>
<tr><td>2.7.1 Forma de pago y requisitos:</td><td>El Fondo Único TIC pagará el valor del presente convenio así:

Aportes del Ministerio y materialización de las metas:

Los aportes del Ministerio serán de: Cuatro mil ochocientos millones de pesos (4.800.000.000), desembolsados conforme los siguientes flujos de recursos en armonía con los entregables que implica la ejecución del proyecto:

La Forma de pago se establece así:

<table>
<tr><th>CONCEPTO</th><th>ENTREGABLE</th><th>%</th><th>VALOR</th></tr>
<tr><td>Primer desembolso
Noviembre/17/2023</td><td>a. Diseño Plan de trabajo
b. Cronograma de actividades.</td><td>31%</td><td>1.500.000.000</td></tr>
</table></td></tr>
</table>

“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”

CONCEPTO	ENTREGABLE	%	VALOR
	c. Diseño Metodología de desarrollo del proyecto.		
Segundo desembolso Nov/24/2023	a. Diseño de la estrategia de comunicación ciudadana sobre ciberseguridad. b. Diseño del modelo de alianzas para el logro de las metas de formación en ciberseguridad. c. Diseño de un programa de educación formal en técnico en ciberseguridad que pueda ser implantado en diversas instituciones de educación superior. d. Estructuración técnica, legal, financiera y organizacional del Hub de Ciberseguridad. e. Diagnóstico y definición de requerimientos técnicos específicos para el SOC. f. Diseño arquitectura tecnológica para el SOC.	48%	2.300.000.000
Tercer desembolso Dic/15/2023	a. Desarrollo Ciclo de formación mediante la capacitación de 1800 personas en ciberseguridad de acuerdo con las metas definidas en cada segmento definido en el anexo técnico. b. Informe de identificación y documentación de requisitos necesarios para la implementación del HUB en el Parque tecnológico de Villamaría en los componentes físicos y tecnológicos, incluyendo presupuesto estimado para las adecuaciones. c. Informe de identificación de Aliados Potenciales:	21%	1.000.000.000

"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"

CONCEPTO	ENTREGABLE	%	VALOR
	d. Informe de establecimiento de espacios para realizar ruedas de negocios y definir contactos con empresas e instituciones que estén interesadas en participar en el HUB, en los distintos roles definidos. e. Estructura organizacional y roles del SOC. f. Plan financiero para implementación y sostenimiento del SOC. g. Plan operativo y de gestión del SOC		
		TOTAL	**$4.800.000.000**

Para cada desembolso, el ALIADO deberá presentar:

1. Constancia suscrita por el supervisor del convenio, en la que se señale que el cooperante cumplió a satisfacción de la entidad, con el objeto y las obligaciones pactadas en el contrato.
2. Informe de ejecución del convenio GCC-TIC-FM- 055 durante el periodo objeto de desembolso. (o el formato que lo modifique).
3. Copia del comprobante de pago de las contribuciones al Sistema Integral de Seguridad Social en Salud, Pensiones y ARL, contribuciones parafiscales si a ello hubiere lugar, de acuerdo con lo establecido en la normatividad vigente y en el porcentaje establecido por el Gobierno Nacional.
4. Cada desembolso corresponderá a la real y efectiva prestación del servicio conforme los entregables cumplidos y aprobados ´por la supervisión. Los saldos sin ejecutar que hubieren sido asignados para el mismo, serán liberados por el GIT de Presupuesto de la Subdirección Financiera, con el fin de garantizar la adecuada gestión de los recursos durante la presente vigencia, previa validación con el supervisor del contrato.
5. Para el periodo de pago correspondiente al mes de diciembre se realizará entre el veintiuno (21) y el treinta (30) de diciembre.

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

Los recursos indicados, están asociados a las fichas de los proyectos de inversión señalados a continuación:

"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><td></td><td>• Ficha BPIN: 2018011000460: Nombre del proyecto: Fortalecimiento y Apropiación del Modelo de Gestión Institucional del Ministerio TIC.

• Ficha BPIN: 2018011000347: Nombre del proyecto: Aprovechamiento y uso de las tecnologías de la información y las comunicaciones en el sector público nacional.

Los desembolsos se harán con cargo al presupuesto asignado para la presente vigencia fiscal de conformidad con los Certificados de Disponibilidad Presupuestal No. 180423 expedido el 30 de octubre de 2023 (“Fortalecimiento y apropiación del modelo de gestión institucional del Ministerio TIC, Bogotá”)</td></tr>
<tr><td>2.7.2. Aportes en especie del Aliado / Cooperante</td><td>Aportes del Cooperante / Aliado del proyecto y materialización de las metas:

Los aportes del Cooperante serán por la suma de: Trescientos millones de pesos (300’000.000) en especie, tasados así:
<table>
<tr><th>Descripción del aporte</th><th>Cant</th><th>Valor Unitario</th><th>Valor Total</th></tr>
<tr><td>Logos y manual de imagen del Hub De Ciberseguridad</td><td>1</td><td>50.000.000</td><td>50.000.000</td></tr>
<tr><td>Desarrollo de cortos y/o videos animados sobre ciberseguridad dirigidos a los ciudadanos, con logos e imagen institucional del MINTIC.</td><td>10</td><td>25.000.000</td><td>250.000.000</td></tr>
<tr><td colspan="3">TOTAL</td><td>300.000.000</td></tr>
</table></td></tr>
<tr><td>2.2.8 Justificación del anticipo. Si aplica</td><td>No Aplica</td></tr>
<tr><td>2.2.9 Supervisión (indicar nombre y cargo del funcionario que se recomienda al ordenador del gasto)</td><td>La supervisión del contrato será ejercida por el Coordinador GIT COLCERT, o quien haga sus veces o por quien sea designado mediante oficio por el ordenador del gasto del FONDO ÚNICO DE TIC.

Entre sus funciones tendrán:

1. Realizar el seguimiento y control técnico, administrativo, financiero, contable y jurídico a la ejecución del contrato.
2. Verificar que el CONTRATISTA cumpla con el objeto, el alcance y calidad del servicio contratado conforme lo estipulado en el presente documento.
3. Requerir al CONTRATISTA sobre el cumplimiento de las obligaciones estipuladas en el presente documento y en la propuesta presentada al Fondo Único de TIC.
4. Suscribir los documentos y actas a que haya lugar durante la ejecución del contrato.
5. Informar al Fondo Único de TIC, así como al Ordenador del gasto con respecto a las demoras e incumplimiento de las obligaciones del aliado.
6. Recibir la información del aliado y hacer las observaciones que estime convenientes.
7. Solicitar la suscripción de contratos adicionales, prórrogas o modificaciones, previa la debida y detallada sustentación.</td></tr>
</table>

“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”

	8. Solicitar aclaraciones, adiciones, modificaciones o complementos al contenido de los informes presentados por el aliado, o de aquellos que específicamente requiera la entidad, siempre y cuando se estime su conveniencia y necesidad, propendiendo por el cumplimiento a cabalidad del objeto contratado. 9. Estudiar las situaciones particulares e imprevistas que se presenten en desarrollo del contrato, conceptualizando sobre su desarrollo general y los requerimientos para su mejor ejecución, manteniendo siempre el equilibrio contractual. 10. Certificar el cumplimiento de las actividades a cargo del aliado. Dicha certificación será requisito previo para cada uno de los pagos que deba realizar el Fondo Único de TIC. 11. Remitir a la Subdirección de Gestión Contractual para revisión y ajustes el proyecto de acta de liquidación del convenio una vez este se termine, adjuntando el balance económico y los soportes correspondientes, de ser necesario. 12. Remitir al Grupo Interno de Trabajo de Grupos de Interés y Gestión Documental del MINTIC o a la dependencia que haga sus veces, en forma permanente y a medida que avance la ejecución del convenio, toda la información y documentos que surjan en desarrollo del mismo, para efectos de mantener actualizada la respectiva carpeta contractual. 13. Verificar el cumplimiento de las obligaciones para con el sistema de seguridad social integral y parafiscales, de conformidad con el artículo 23 de la Ley 1150 de 2007, cuando ello de a lugar. 14. Las demás actividades inherentes a la función desempeñada, conforme a la Ley. En ningún caso el supervisor goza de la facultad de modificar el contenido y alcance del contrato suscrito entre el interventor y El Fondo Único de TIC, ni de eximir, a ninguno de ellos, de sus obligaciones y responsabilidades. Las atribuciones, responsabilidades y obligaciones serán las establecidas en el manual de contratación vigente, así como las indicadas en el manual de supervisión e interventoría del Ministerio de Tecnologías de Información y las Comunicaciones y aquellas dispuestas en los artículos 82 y 83 de la Ley 1474 de 2011. Por último, es de mencionar que el convenio a suscribir será un convenio especial de cooperación y estará sometido a la legislación y jurisdicción colombiana y se rige por las normas de la Ley 80 de 1993, la Ley 1150 de 2007, La Ley 498 de 1998 y el Decreto 1082 de 2015 y las demás normas que las complementen, modifiquen o reglamenten.
2.2.10 Comité de Seguimiento	Se conformará un Comité técnico de seguimiento a la ejecución del convenio, el cual deberá estar integrado por dos (2) representantes del MinTIC, uno de ellos será el supervisor del convenio (1) y un (1) delegado del Viceministerio de Transformación Digital y, por parte del aliado máximo dos (2) delegados del representante legal con capacidad para hacer recomendaciones específicas. El comité se reunirá periódicamente con el objeto principal de verificar que se cumpla lo acordado por las partes del convenio y tendrá, entre otras, las siguientes funciones:

"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"

	1. Revisar y analizar los informes técnicos, administrativos y financieros sobre la ejecución del convenio cuando haya lugar a ello. 2. Evaluar periódicamente el plan de trabajo e impartir las recomendaciones que considere sobre el mismo. 3. Hacer recomendaciones técnicas sobre la adecuada gestión y seguimiento del convenio. 4. Servir como espacio de discusión y debate de los asuntos relacionados con el desarrollo del convenio, así como ser el escenario donde se revisen las consultas o inquietudes que puedan presentarse durante la ejecución de éste. 5. Realizar seguimiento a los compromisos adquiridos en el marco del comité de seguimiento. 6. Aprobar los cambios presupuestales que se presenten al interior del comité y que conlleven a la correcta ejecución del convenio. El comité de seguimiento del convenio se reunirá por convocatoria del supervisor del MinTIC/Fondo Único de TIC con una periodicidad quincenal; de forma extraordinaria, se reunirá por convocatoria de cualquiera de las partes. La Secretaría del comité estará a cargo del supervisor del convenio por parte del MinTIC/Fondo Único de TIC y de cada una de las reuniones se dejará constancia frente a los compromisos adquiridos y recomendaciones efectuadas mediante actas que serán elaboradas por el aliado y entregadas al supervisor del convenio en un plazo máximo de tres (3) días hábiles después de realizada la reunión. Por último, al comité podrán asistir en calidad de invitados las personas naturales o jurídicas que puedan aportar al óptimo desarrollo del convenio.
2.3. Tipo del contrato a celebrar	Convenio Especial de Cooperación

3. **Fundamentos jurídicos de la modalidad de contratación:**

Para la celebración de este convenio especial de cooperación, se tuvo en cuenta las condiciones legales así como las obligaciones derivadas del mismo las cuales tienen relación directa con el objeto de la entidad ejecutora conforme lo señalado en la Ley y sus reglamentos.

La celebración de este convenio especial de cooperación es el resultado de una planeación adecuada del Proceso de Contratación por la Entidad, de manera que los estudios previos permitieron concluir que este negocio jurídico es la mejor alternativa para satisfacer la necesidad requerida y generar mayor valor por dinero, tiempo, calidad en el servicio y resultados esperados.

En conclusión, la Entidad pretende celebrar el presente convenio, toda vez que si su finalidad es cooperar en el cumplimiento de funciones administrativas y de prestar conjuntamente servicios que se hallen a su cargo, considerando que las obligaciones derivadas del mismo tienen relación directa con el objeto de la entidad ejecutora señalada en la Ley y en sus reglamentos.

"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"

La ley 1150 de 2007 estableció a través del artículo 2, dentro de las modalidades de selección, la contratación directa, la cual procede entre otras para los contratos para el desarrollo de actividades científicas y tecnológicas.

El artículo 2° del decreto 393 de 1991 estableció los propósitos de la asociación, la cual, bajo cualquiera de las modalidades previstas en el artículo 1º, la asociación podrá tener entre otros, los siguientes propósitos, entre otros.

c) Organizar centros científicos y tecnológicos, parques tecnológicos, e incubadoras de empresas.
d) Formar y capacitar recursos humanos para el avance y la gestión de la ciencia y la tecnología.
e) Establecer redes de información científica y tecnológica.
k) Realizar seminarios, cursos y eventos nacionales o internacionales de ciencia y tecnología.

El artículo 3° del decreto antes mencionado, determina que la autorización especial y aportes, corresponde a la Nación y a sus entidades descentralizadas, con el fin de crear y organizar con los particulares sociedades civiles y comerciales y personas jurídicas sin ánimo de lucro como corporaciones y fundaciones, con el objeto de adelantar las actividades científicas y tecnológicas, proyectos de investigación y creación de tecnologías para los propósitos señalados en el artículo anterior 2º.

Determina además que los aportes podrán ser en dinero, en especie o de industria, entendiéndose por aportes en especie o de industria, entre otros, conocimiento, patentes, material bibliográfico, instalaciones, equipos, y trabajo de científicos, investigadores, técnicos y demás personas que el objeto requiera.

De esta forma, en concordancia con la necesidad descrita en el numeral 1 del presente estudio previo y con la normativa del artículo 2 del Decreto Ley 591 de 1991, el literal e) del numeral 4º del artículo 2º de la Ley 1150 de 2007, el artículo 18 de la Ley 1286 de 2009 el cual modificó la Ley 29 de 1990, Decreto 393 de 1991, el documento CONPES 4069 de 2022 y la sentencia radicado número 11001-03-06-000-2010-00058-00(2007) del ocho (8) de julio de dos mil diez (2010) del Consejo de Estado, para adelantar actividades científicas y tecnológicas, proyectos de investigación y creación de tecnologías, la Nación y sus entidades descentralizadas podrán celebrar con los particulares convenios especiales de cooperación, que no darán lugar al nacimiento de una nueva persona jurídica.

El artículo 2° del decreto 393 de 1991 estableció los propósitos de la asociación, la cual, bajo cualquiera de las modalidades previstas en el artículo 1º, la asociación podrá tener entre otros, los siguientes propósitos, entre otros.

c) Organizar centros científicos y tecnológicos, parques tecnológicos, e incubadoras de empresas.
d) Formar y capacitar recursos humanos para el avance y la gestión de la ciencia y la tecnología.
e) Establecer redes de información científica y tecnológica.
k) Realizar seminarios, cursos y eventos nacionales o internacionales de ciencia y tecnología.

"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"

4. Análisis que soporta el valor estimado del contrato:

Anexo obligatorio ☐
(si hay estudio de mercado)
Número de Folios:

De conformidad con el artículo 2.2.1.1.1.6.1 del Decreto Reglamentario 1082 del 26 de mayo 2015 "Por medio del cual se expide el Decreto único Reglamentario del Sector Administrativo de Planeación Nacional", durante la etapa de planeación, la entidad elaboró los respectivos análisis del sector económico y de proveedores de servicios similares al del objeto del presente proyecto, desde la perspectiva legal, comercial, financiera, organizacional, técnica, y de análisis de riesgos, los cuales se encuentran contemplados en el anexo denominado estudios del sector.

En este estudio, la entidad pudo establecer el presupuesto oficial estimado del presente proceso de selección.

Análisis de las cotizaciones recibidas:

Mediante correo electrónico se enviaron solicitud de cotizaciones a tres (3) empresas del sector de las tecnologías y las comunicaciones, incluyendo al Centro de Desarrollo Tecnológico - BIOS.

El cronograma de las cotizaciones se realizó así:

Octubre 02 de 2023: Envío solicitud de cotizaciones.
Octubre 04 de 2023: (Desde octubre 03) Recibo respuestas de cotizaciones.

Análisis estadístico descriptivo:

Para el presente análisis, se utilizó el promedio cuyo procedimiento se basó en sumar todos los valores del grupo de datos, divido por el número de datos sumados. El valor obtenido sirvió para **representar** adecuadamente que pasa en el conjunto de datos y su análisis dependió del escenario en el que se aplicó.

Enfoque del análisis descriptivo:

Para el presente análisis, se realizó uno de los enfoques para el estudio y análisis de precios, extrayendo de métodos estadísticos, como es el del análisis descriptivo.

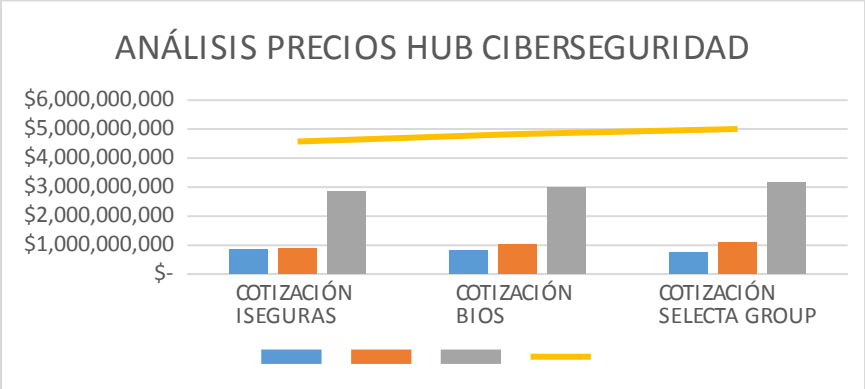
Con la aplicación del método, se definió el tipo de aproximación con el que se analizaron los datos procediendo a su descripción.

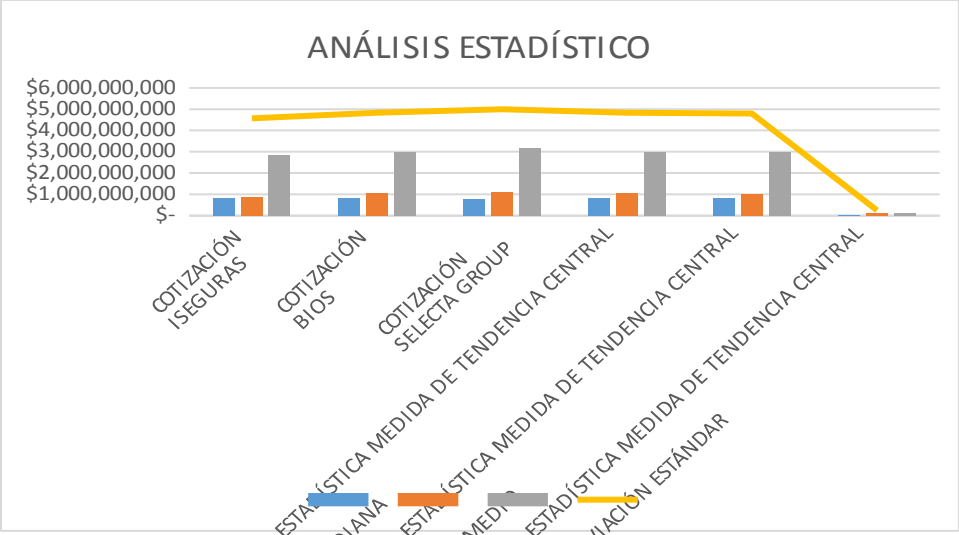
Mediante el análisis se recolectó y ordenó la información por medio de gráficas y medios visuales y se extrajo las características más representativas de la colección de datos para poder describir las tendencias.

El promedio aritmético calculado está dado así:

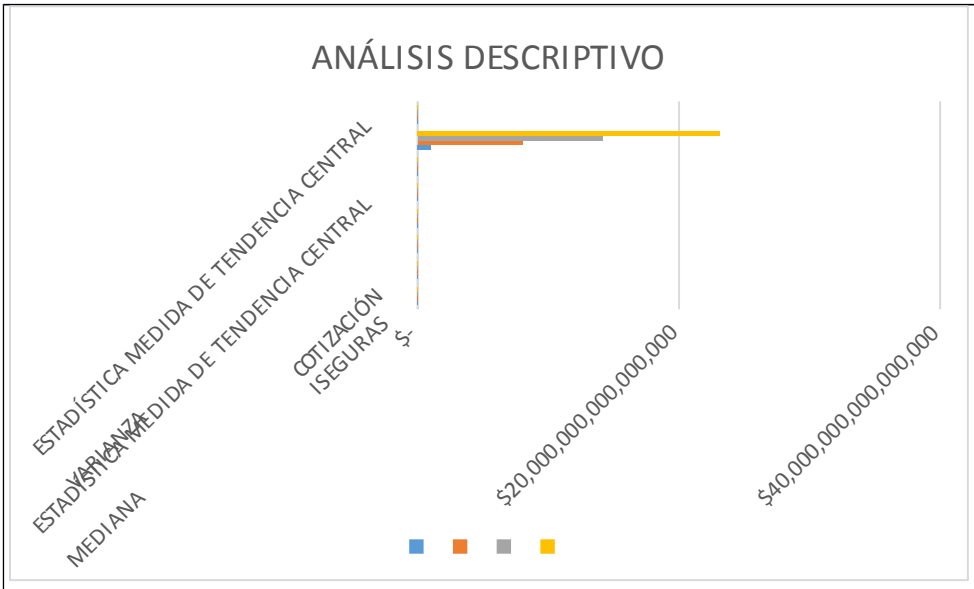
"Los datos proporcionados serán tratados de acuerdo a la política de tratamiento de datos personales del MinTIC (www.mintic.gov.co), la ley 1581 de 2012 y sus decretos reglamentarios"

COTIZACIÓN ISEGURAS	COTIZACIÓN BIOS	COTIZACIÓN SELECTA GROUP	ESTADÍSTICA MEDIDA DE TENDENCIA CENTRAL MEDIANA	ESTADÍSTICA MEDIDA DE TENDENCIA CENTRAL PROMEDIO	ESTADÍSTICA MEDIDA DE TENDENCIA CENTRAL DESVIACIÓN ESTÁNDAR
836.500.000	797.300.000	759.000.000	797.300.000	797.600.000	31.639.954
879.000.000	1.023.416.000	1.092.000.000	1.023.416.000	998.138.667	88.774.838
509.700.000	499.324.000	489.000.000	499.324.000	499.341.333	8.450.749
2.349.000.000	2.479.960.000	2.660.500.000	2.479.960.000	2.496.486.667	127.705.157
4.574.200.000	**4.800.000.000**	**5.000.500.000**	**4.800.000.000**	**4.791.566.667**	**256.570.696**





"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"



Conforme el anterior análisis estadístico, el valor estimado se realizó conforme el aporte del Mintic para el presente proyecto, estimándose en la suma de 4.800.000.000, considerando el valor asignado presupuestalmente en el Plan Anualizado de Adquisiciones.

De acuerdo con el estudio de mercado realizado, se tuvo en cuenta la capacidad tecnológica de BIOS para desarrollar los componentes del proyecto, entre ello, considerar que la entidad seleccionada es un centro de desarrollo tecnológico enfocado en la investigación aplicada. Por lo anterior, se evaluó cada actividad próxima a realizar en función de los objetivos trazados.

5. INDIVIDUALIZACIÓN DEL ALIADO:

Por ser un convenio especial de cooperación, la selección se realizó en consideración del artículo 2° del decreto 393 de 1991 el cual establece los propósitos de la asociación, la cual, bajo cualquiera de las modalidades previstas en el artículo 1º, la asociación podrá tener entre otros, actividades tales como formar y capacitar recursos humanos para el avance y la gestión de la ciencia y la tecnología y/o realizar seminarios, cursos y eventos nacionales o internacionales de ciencia y tecnología.

BIOS es un centro de desarrollo tecnológico enfocado en la investigación aplicada, constituido desde el 12 de noviembre de 2010 cuyo objeto es “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 el cual ofrece servicios en las áreas de biotecnología y ciencia de da tos para la empresa, academia y Estado. Cuenta además con infraestructura de supercomputación provista por el Gobierno Nacional (representado por Mintic y Minciencias) en alianza con universidades del país y aliados tecnológicos como Microsoft y Hewlett Packard Enterprise.

Así mismo, BIOS ha desarrollado Clúster HPC, definido también como clúster de computación de alto

“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”

rendimiento, el cual combina hardware especializado, que incluye un grupo de grandes y potentes PC, y un marco de software de procesamiento distribuido y configurado para gestionar cantidades masivas de datos a altas velocidades con rendimiento paralelo y alta disponibilidad.

En el aspecto de información robusta, BIOS desarrolla computación de alto desempeño, como respuesta a altos volúmenes de información que se encuentran disponible para resolver problemas complejos a los que se enfrentan las organizaciones e instituciones de hoy.

BIOS, posee computadores de alto desempeño, los cuales combinan altas capacidades y prestaciones, con el talento humano altamente especializado, permitiendo que el Big Data sea indispensable al contar con gran infraestructura de procesamiento de datos, que lo convierte en un aliado de la investigación en Colombia; así como un activo estratégico de interés nacional, por ello, el Gobierno Nacional reconoce las capacidades de supercomputación de BIOS, que fueron instaladas buscando apalancar proyectos que impulsen el progreso del país (CONPES 3920).

Adicionalmente, la capacidad tecnológica le ha permitido a BIOS desplegar proyectos de investigación e innovación enfocados en analítica de datos avanzada abarcando tres dimensiones: económica, social y ambiental, aplicadas en empresas y organizaciones alineadas con la cuarta revolución industrial. Para esto se usan tecnologías emergentes como: Bigdata, Ciencia de Datos, Blockchain, Machine Learning, Ia, Iot, que permiten extraer valor de los datos en 3 enfoques: **Descriptivo**: Cómo se comportan los datos; **Predictivo:** Cómo se comportarán los datos según histórico y **Prescriptivo:** Cómo puedo influenciar el comportamiento de los datos. Los análisis prescriptivos determinan las formas en que los procesos de negocios deben evolucionar o ser modificados.

Experiencia especializada de BIOS:

La línea especializada de la experiencia de Bios se ha desarrollado en los siguientes:

- Gestión de la Innovación:
- Bioinformática
- Bionegocios
- Bioingeniería
- Computación científica
- Bioinformática básica
- Transferencia tecnológica
- Utilización del programa R.
- Protección de desarrollos y productos biotecnológicos a través de los mecanismos de propiedad intelectual.
- Biotecnología: principios para entender el futuro.
- Fundamentos metodológicos para el análisis computacional de datos biológicos.
- Análisis e interpretación de datos bioinformáticos en agro.
- Análisis e interpretación de datos bioinformáticos en salud.

Por lo anterior, se considera técnica y científicamente que BIOS posee la capacidad para desarrollar 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"

estructuración de un ecosistema de seguridad digital que integrará instituciones del estado, empresas, universidades, sociedad civil y organizaciones internacionales, con el fin de promover el desarrollo de capacidades en ciberseguridad a través de la creación de un HUB de ciberseguridad, un SOC especializado para el sector público y el desarrollo de un plan maestro de capacitación, formación y entrenamiento.

6. 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 proceso de contratación o en la ejecución del contrato)

Se adjunta matriz de riesgo:

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

La Garantía de Seriedad debe estar vigente desde la presentación de la oferta y hasta la aprobación de la garantía de cumplimiento del contrato. Su valor depende del tipo de proceso de selección y de la cuantía del presupuesto oficial estimado, de conformidad con lo dispuesto en el artículo 2.2.1.2.3.1.9 del Decreto 1082 de 2015.

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	El cooperante/aliado		
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	Po plazo de ejecución del convenio y seis (6) meses más, y en todo caso hasta la liquidación del convenio.	Por el veinte por ciento (20%) del valor del aporte del Fondo Único TIC.
	Pago de salarios, prestaciones sociales legales e indemnizaciones laborales.	Por el plazo de ejecución del convenio y tres (3) años más.	Por el cinco por ciento (5%) del valor del aporte del Fondo Único TIC.

	Calidad del servicio	Por el plazo de ejecución del convenio y seis (6) meses más.	Por el veinte por ciento (20%) del valor del aporte del Fondo Único TIC.

Nota 1. El Cooperante /aliado 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 Cooperante /aliado 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.

Nota 3. INDENNIDAD: El ejecutor del proyecto mantendrá indemne al MinTIC de los reclamos, demandas, acciones legales y costas que surjan con ocasión de la ejecución del convenio e imputables a ejecutor

8. Indicar si la contratación esta cobijada por un Acuerdo Internacional o un tratado de Libre comercio vigente para el Estado Colombiano bajo los parámetros establecidos por el *Manual para el Manejo de Acuerdos Comerciales en Procesos de Contratación* emitido por Colombia Compra Eficiente, en desarrollo del artículo 2.2.1.2.5.2 del Decreto 1082 de 2015

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 le aplican los siguientes tratados de libre comercio y acuerdos internacionales, así:

Acuerdo comercial		Vigente	Entidad Estatal cubierta	Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
Alianza Pacífico	Chile	SI	SI	(i) adquirir bienes y servicios a partir de 50.000 DEG (275.195.500 COP) y (ii) para servicios de construcción desde 5.000.000 DEG (25.706.187.670 COP)	NO	SI
	México	SI	SI	(i) adquirir bienes y servicios a partir de 50.000 DEG (275.195.500 COP) y (ii) para servicios de construcción desde 12.001.460 USD**	NO	SI
	Perú	SI	SI	(i) adquirir bienes y servicios a partir de 95.000 DEG (522.871.450 COP) y (ii) para servicios de construcción desde 5.000.000 DEG (25.706.187.670 COP)	NO	SI
Canadá		SI	SI	(i) adquirir bienes y servicios a partir de US 83.099 (342.854.009) y (ii) para servicios de construcción desde 5.000.000 DEG	NO	SI

"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"

			(25.344.513.162)		
Chile		SI	SI	(i) adquirir bienes y servicios a partir de 50.000 DEG (275.195.500) y (ii) para servicios de construcción desde 5.000.000 DEG (25.545.923.858)	NO	SI
Corea		SI	SI	: (i) adquirir bienes y servicios a partir de 70.000 DEG (385.273.700) y (ii) para servicios de construcción desde 5.000.000 DEG (25.700.000.000)	NO	SI
Costa Rica		SI	SI	(i) adquirir bienes y servicios a partir de US 83.099 (342.854.009) y (ii) para servicios de construcción desde US 7.008.000 (25.725.714.885)	NO	SI
Estados Unidos		SI	SI	(i) adquirir bienes y servicios a partir de US 83.099 (342.854.009) y (ii) para servicios de construcción desde US 7.008.000 (25.725.714.885)	NO	SI
Estados AELC		SI	SI	(i) adquirir bienes y servicios a partir de 130.000 DEG (715.508.300) y (ii) para servicios de construcción desde 5.000.000 DEG (23.680.884.850)	NO	SI
México		SI	SI	(i) adquirir bienes y servicios a partir de US 84.918 (350.358.930)y (ii) para servicios de construcción desde US 11.039.387.	NO	SI
Triángulo Norte	El Salvador	SI	SI	Aplicable a los Procesos de Contratación a partir del valor de la menor cuantía de la Entidad Estatal.	NO	SI
	Guatemala	SI	SI		NO	SI
	Honduras	SI	NO		NO	NO
Unión Europea		SI	SI	(i) adquirir bienes y servicios a partir de 130.000 DEG (715.508.300) y (ii) para servicios de construcción desde 5.000.000 DEG (23.466.405.900)	NO	SI
Israel		SI	SI	(i) 130.000 DEG para bienes y servicios (715.508.300), (ii) Umbral: 8,500,000 DEG (30.948.976.544); iniciando el sexto año una vez entre en vigor el ACP revisado para Israel: 5,000,000 DEG.	NO	NO
Reino Unido e Irlanda del Norte		SI	SI	(i) adquirir bienes y servicios a partir de 130.000 DEG (715.508.300) y (ii) para servicios de construcción desde 5.000.000 DEG (18.205.280.320)	NO	SI
Comunidad Andina		SI	SI	La Decisión 439 de 1998 de la Comisión de la CAN es aplicable a todos los Procesos de Contratación de las Entidades Estatales del nivel nacional, independientemente del valor del Proceso de Contratación.	NO	SI

9. Certificado de disponibilidad presupuestal (CDP):	No. 180423		Fecha: (dd/mm/aaaa)	30-10-2023

"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"

10. Vigencias futuras:	No. Oficio		Año	Cuantía por año
	No. de aprobación			
(Incluir cuadro adicional con la programación de valores por vigencia específicamente del contrato a realizar)				

CONTRATACIÓN DIRECTA DECRETO 1082 DE 2015						
11. Nombre o Razón Social de la(s) persona(s) natural(es) o jurídica(s) a contratar:						
	Contacto		Dirección		Teléfono	
11.1. Perfil de la persona a contratar:						
12. Firmas autorizadas:						

Firma responsable: **Viceministro/Jefe/ Director /Subdirector/ de la Dependencia Solicitante** Nombre: SINDEY CAROLINA BERNAL VILLAMARIN Cargo: VICEMINISTRA Fecha: OCT-13-2023	**Firma responsable** **Subdirector o coordinador del GIT (si aplica)** **Nombre**: Cargo: Fecha:

ANEXOS

Listado de documentos anexos al formato general de estudios previos

Documentos Anexos
Documentos:
• Estudios del sector o Análisis de sector y/o Estudio mercado
• Matriz de riesgos
• Análisis de garantías (si aplica)
• Anexo técnico en procesos de selección
• Memorias de cálculo

"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"

i Rey, Gloria Helena, Ciberataques, Casa editorial El Tiempo, 2022
ii Soler, Efraín, Por qué ha crecido la importancia de la ciberseguridad, Portafolio, octubre 2022.

REGISTRO DE FIRMAS ELECTRONICAS

Estudio Previo HUB Ciberseguridad - Nov-14-2023

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

Id Acuerdo: 20231114-230259-46aa71-25620380 Creación: 2023-11-14 23:02:59

Estado: Finalizado Finalización: 2023-11-14 23:13:58

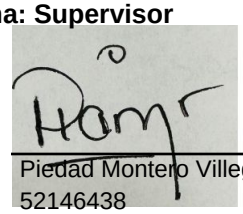
Escanee el código para verificación

Aprobación: Aprobación



Sindey Carolina Bernal
53040506
sbernal@mintic.gov.co
Viceministra de Transformación Digital
Ministerio de Tecnología de la Información y las Comunicaciones

Firma: Supervisor



Piedad Montero Villegas
52146438
pmontero@mintic.gov.co
Coordinadora GIT COLCERT

REPORTE DE TRAZABILIDAD

Estudio Previo HUB Ciberseguridad - Nov-14-2023

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

Id Acuerdo: 20231114-230259-46aa71-25620380 Creación: 2023-11-14 23:02:59

Estado: Finalizado Finalización: 2023-11-14 23:13:58

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Firma	Piedad Montero Villegas pmontero@mintic.gov.co Coordinadora GIT COLCERT	Aprobado	Env.: 2023-11-14 23:03:10 Lec.: 2023-11-14 23:03:19 Res.: 2023-11-14 23:04:20 IP Res.: 186.30.62.159
Aprobación	Sindey Carolina Bernal sbernal@mintic.gov.co Viceministra de Transformación Digital Ministerio de Tecnología de la Informaci	Aprobado	Env.: 2023-11-14 23:04:20 Lec.: 2023-11-14 23:04:28 Res.: 2023-11-14 23:13:58 IP Res.: 181.53.13.29