PROYECTO 3020001 - HUB de Ciberseguridad.

OBJETO: 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.

NOVIEMBRE DE 2023

Proyecto: Hub de Ciberseguridad.

Objeto: 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.

Nota: El Hub de Ciberseguridad es considerado 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.

Duración estimada del proyecto: Desde la suscripción del acta de inicio y hasta el 31 de diciembre de 2023.

Presupuesto estimado: Cinco mil cien millones de pesos (5.100.000.000), incluido impuestos directos, costos y gastos financieros.

1. INFORMACIÓN GENERAL

En los Catalizadores del Plan Nacional de Desarrollo 2022-2026 (Colombia, Potencia Mundial de la Vida), se estableció la seguridad digital confiable para la garantía de las libertades, la protección de la dignidad y el desarrollo integral de las personas, propósito que comporta el fortalecimiento de las entidades del Estado y la garantía en la prestación de sus servicios en el entornos digitales a través del diseño e implementación de estrategias orientadas a la adopción de medidas para la salvaguarda de la infraestructura crítica cibernética del país, como expresión de protección de las personas y de las instituciones. Lo anterior, redundaría en el mejoramiento de capacidades y el fortalecimiento de la cultura de la ciberseguridad como contribución a la protección de la información de las entidades gubernamentales y de las personas ante posibles ataques cibernéticos y la comisión de delitos informáticos.

Adicionalmente promueve definir una estrategia para impulsar el concepto de seguridad digital por defecto para garantizar la continua prestación de los servicios ofrecidos por las entidades públicas establecer los lineamientos técnicos para adoptar los estándares y buenas prácticas en el tema. En consonancia con lo anterior, el ejecutivo ha desarrollado instrumentos de política pública e iniciativas para crear una cultura de la seguridad digital (ciberseguridad) que permita proteger las actividades, las personas y la sociedad, sin inhibir los beneficios y oportunidades de las TIC.

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

a. Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado.
b. Actualizar el marco de gobernanza en materia de seguridad digital.

c. Adoptar modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

Por otro lado, en el marco de la implementación de la Política de Confianza y Seguridad Digital se expidió el Decreto 338 de 2022 mediante el cual:

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

De acuerdo con el mismo Decreto 338 de 2022 en su artículo 2.2.21.1.1.3, se definen las infraestructuras críticas cibernéticas de la siguiente manera: “Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía”. Estas infraestructuras deben ser, por lo tanto, protegidas como una prioridad de la nación.

Estos elementos normativos, también determinan los roles y compromisos de los diferentes entes responsables de la ciberseguridad en el país y la forma en que se deben coordinar; además, formaliza el Comité Nacional de Seguridad Digital que tiene como propósito adoptar un esquema de múltiples partes interesadas y brindar confianza a la ciudadanía. De esta forma, define sus participantes y la manera en que operará, así mismo, se formalizan e impulsan las estructuras de los equipos y/o grupos de respuesta a emergencias cibernéticas de Colombia tales como: El Grupo de Respuesta a Emergencias Cibernéticas de Colombia -ColCERT, Csirt del Gobierno de Colombia y Csirt de defensa, entre otros. De esta manera el Ministerio TIC recibe las responsabilidades de gestionar el Grupo de Respuesta a Emergencias Cibernéticas de Colombia-COLCERT, punto único de contacto para coordinar la prevención, mitigación y respuesta (gestión) ante incidentes de Seguridad Digital Nacional de manera rápida y eficiente, a través de:

a) El desarrollo y divulgación de procedimientos, protocolos, guías y recomendaciones para la gestión de riesgos e incidentes de Seguridad Digital.
b) La Generación de acciones para la recuperación y puesta en operación de las entidades u organizaciones que así lo soliciten, una vez se presenta 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 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.
    - 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).

Conforme las acciones que realiza COLCERT, para promover el desarrollo de capacidades locales y sectoriales, se plantea la creación de un HUB DE CIBERSEGURIDAD que integre diversos actores del ecosistema de ciberseguridad, incluyendo empresas, academia y entidades del estado. Así mismo, dentro del propio HUB, se hace necesaria la creación de un SOC para prestar servicios de monitoreo de ciberseguridad a las entidades que hacen parte del activo estratégico de la nación principalmente y por último, el desarrollo de un PLAN MAESTRO de capacitación, formación, entrenamiento y sensibilización del recurso humano del país en ciberseguridad.

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.

Para poder construir y desarrollar estas actividades, se requiere contar con un aliado con capacidades técnicas avanzadas en tecnología, así como capacidad de convocatoria y liderazgo nacional para desarrollar este ecosistema de ciberseguridad, para lo cual se ha identificado a BIOS, centro de desarrollo tecnológico del MINTIC, como el actor más adecuado para asumir este liderazgo, en particular por su estrecha relación con el ministerio, por sus capacidades técnicas y tecnológicas en computación avanzada.

Se tiene como referencia, que la gobernación ha encargado a BIOS del acompañamiento en la apertura y puesta en marcha del Parque Científico y Tecnológico de Caldas (PCTC), y su configuración tecnológica para dar cabida a las necesidades del HUB con el objeto de desarrollar de actividades de innovación y desarrollo tecnológico para fortalecimiento y gestión de estrategias de sostenibilidad y funcionalidad del Parque Tecnológico y de Innovación de Caldas. En este proyecto BIOS estará desarrollando actividades que resultan complementarias y necesarias para el desarrollo del HUB, entre las cuales se encuentran:

1. Proyectar estrategias orientadas a lograr un modelo de sostenibilidad y gobernanza del PCTC que puedan articularse con entidades del orden regional, departamental y nacional.
2. Diseñar la metodología de intervención regional en Ciencia, Tecnología e Innovación, garantizando metas que puedan ser desarrollados desde el PCTC.
3. Llevar a cabo la implementación de procesos de desarrollo tecnológico e innovación, que sirvan como estrategia de apertura y activación del PCTC.
4. Estructurar una base de datos de cada uno de los actores subregionales involucrados dentro de las iniciativas.
5. Realizar una estrategia de articulación e integración con interesados en participar como actores vinculados al Parque Tecnológico.
6. Diseñar y ejecutar las actividades necesarias para atracción y relacionamiento de actores del ecosistema de ciencia, tecnología e innovación de caldas.

7. Definir e implementar una metodología de articulación subregional para la identificación, de proyectos que integren componentes de CTeI, para el departamento de caldas que puedan ser operados a través del PCTC
8. Realizar el acompañamiento documental, técnico, presupuestal y de ejecución requerido al Departamento de Caldas, para permitir la viabilización de recursos en desarrollo y progreso del Parque Tecnológico.

Por lo tanto, se requiere avanzar en la formulación del proyecto para la creación y puesta en marcha de un HUB de Ciberseguridad en Villamaría, Caldas, como un centro de innovación y excelencia en ciberseguridad, donde se establecerán diversas empresas, tanto nacionales como multinacionales, que contribuirán al desarrollo de productos y servicios de ciberseguridad. Este HUB se enfocará en atender inicialmente a las entidades que hacen parte del activo estratégico de la nación y eventualmente expandirse a servir a otras entidades públicas y privadas en Colombia y Latinoamérica.

La Creación del Hub de ciberseguridad en el centro BIOS, ubicado en Villamaría, Caldas, contempla la puesta en marcha de un programa de ciberseguridad basado en la descentralización, debido a que se necesita que todas las regiones tengan oportunidades de desarrollo. Por lo que todos los esfuerzos se concentrarán para que este centro público se apropie y se fortalezca.

Se espera que este actúe como centro de seguridad digital de investigación, desarrollo e innovación, involucrando a diversos actores para fortalecer la seguridad a nivel local y nacional. Así aumentará la capacidad de respuesta del país frente a los ataques cibernéticos.

Dentro de las líneas estratégicas de desarrollo po se identifican:

- Desarrollar servicios de ciberseguridad basados en la nube utilizando la infraestructura de supercomputación con que cuenta el centro.
- Incrementar la cantidad de profesionales entrenados en seguridad digital.
- Desarrollar herramientas y servicios de protección a los activos del Estado frente a las crecientes amenazas cibernéticas, dando prioridad de acceso para el sector público, pero también con objetivos de expansión al privado que requiera servicios y no tenga acceso a soluciones de alto costo.
- Atraer empresas nacionales e internacionales para que establezcan sus sedes en el HUB y desde allí desarrollen productos y presten servicios de ciberseguridad a todo el país, generando una oferta complementaria a la que será ofrecida por el estado desde el mismo HUB.
- La implementación de infraestructura de seguridad y continuidad de operaciones a las capacidades de supercomputación de BIOS, para que se protejan las actividades de análisis de datos de las empresas, las instituciones académicas y gubernamentales de todo el país que hacen uso de ella.

2. ALCANCE

2.1. OBJETIVOS

- ✓ 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.
- ✓ 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.
- ✓ Diseñar un Plan Maestro de capacitación, formación, entrenamiento y sensibilización del recurso humano del país en ciberseguridad.
- ✓ Formar por lo menos 1800 personas en ciberseguridad en los segmentos definidos.

2.2. HUB DE CIBERSEGURIDAD.

Considerando el Hub de Ciberseguridad como una actividad de Ciencia, Tecnología e Innovación (ACTI), toda vez que comprende 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, se definen los componentes de desarrollo del proyecto, así:

2.2.1. Objetivo de la línea estratégica:

Realizar la estructuración legal, financiera, tecnológica, organizacional de un HUB de Ciberseguridad que fomente la innovación y colabore en la protección de infraestructuras críticas y datos sensibles mediante la prestación de servicios especializados y la formación de talento humano en ciberseguridad

2.2.2. Objetivos específicos:

- Estructuración técnica, legal, financiera y organizacional del proyecto.
- 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.
- 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.

2.2.3. Entregables:

- Proyecto para la creación del HUB DE CIBERSEGURIDAD.
- Plan de adecuación física y tecnológica de las instalaciones del PCTC para albergar al HUB y su presupuesto
- Informe final de avance en gestiones de presentación y promoción del HUB con diversos aliados potenciales.
- Ficha Bpin proyecto HUB de Ciberseguridad

2.2.4. Aspectos metodológicos.

Se establecen las líneas de trabajo base iniciales para el desarrollo del Hub de Ciberseguridad.

Nota: Las categorías pueden ajustarse a condiciones específicas de modo, tiempo y lugar acorde con el estudio que realice el aliado contemplando la definición de los actores identificados en el desarrollo del estudio.

Categoría	¿Para qué?	¿Cómo?
1. Espacio de encuentro	Punto de encuentro para el intercambio de conocimiento y gestión de incidentes de seguridad digital. Realizar evento para el encuentro	Información de fuentes institucionales mediante herramientas de reporte automático. Espacio físico o virtual para intercambiar información de todos los actores.
2. Capacitación	Identificar cuáles son las tendencias educativas en ciberseguridad, adaptar espacios de formación mediante alianzas con centros educativos. Después del encuentro, definir un programa periódico de capacitaciones a través de las instituciones vinculadas al HUB Definir que instituciones se vinculan al HUB cofinanciado por el MINTIC	Capacitación propia del hub. Alianzas institucionales mediante programas acreditados de formación Capacitación al ciudadano sobre cuidados básicos
3. Innovación	Espacio de investigación y desarrollo que permita crear herramientas de seguridad digital. Después del encuentro, definir que instituciones se vinculan al HUB a través de investigación en Ciberseguridad	Investigación formal de áreas de interés
4. Conciencia	Creación y participación de eventos de difusión para generar conciencia en temas de ciberseguridad. Definir de qué modo se van a crear eventos de difusión Establecer periodicidad de realización de eventos. Establecer modalidades de los encuentros y convocatorias	Información educativa, innovación, eventos conferencias, etc
5. Coordinación y respuesta (SOC)	Identificar cuáles son los sectores con requerimiento de coordinación para dar respuesta a incidentes. Se definiría con instituciones que se vinculan al HUB cofinanciado por el MINTIC	Monitoreo de incidentes (herramienta digital para la detección y respuesta) Análisis de incidentes Difusión de información actores de interés

2.3. CENTRO DE OPERACIONES DE SEGURIDAD - SOC (SECURITY OPERATIONS CENTER)

2.3.1. Objetivo de la línea estratégica:

Realizar el diseño técnico, tecnológico, financiero y organizacional de un centro de operaciones de seguridad SOC Nacional 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, como mecanismos de alerta temprana para la prevención de incidentes de seguridad digital.

2.3.2. Objetivos específicos:

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

2.3.3. Entregables:

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

Los cuales se detallan a continuación:

2.3.3.1. Requerimientos técnicos del SOC.

- Definición de portafolio de servicios del SOC para entidades públicas y privadas nacionales y territoriales, entre los cuales se deben tener en cuenta los siguientes:
  - Evaluación Estado de la Seguridad
  - Alerta Preventiva
  - Gestión de Vulnerabilidades web y on premise
  - Vigilancia Digital
  - Cyber Threat Intelligence - CTI
  - Auditorias Técnicas de Seguridad
  - Monitorización de Eventos
  - Respuesta a Incidentes de Seguridad
  - Monitoreo de disponibilidad sedes electrónicas, páginas y portales web
  - Gestión de Crisis

- Threat Hunting
- Alerta Temprana
- Análisis de Descubrimiento de Ataques - Zero Day
- El aliado debe incluir en su propuesta una oferta de servicio DFIR.

- Definición de las herramientas, soluciones y plataformas de seguridad que soportaran los servicios y gestión de incidencias del SOC.
- Definir y establecer herramientas de Inteligencia artificial IA, machine learning para la automatización tareas como es entre otra la revisión de eventos de seguridad entre las herramientas de seguridad, monitorización y realización análisis predictivo.
- Diseñar el plan de interoperabilidad entre las plataformas de gestión de incidentes y herramientas de seguridad para la generación de ticket de manera automatizada.
- Definir y establecer mecanismos de respuesta a eventos de seguridad en los equipos de seguridad de las infraestructuras tecnológicas de las entidades públicas y privadas (SOAR)
- Entrega de planos de las zonas de trabajo para el SOC, sus componentes de seguridad física y lógica, inmobiliarios, materiales utilizados, sistemas CCTV, controles biometricos, equipos de ofimática, impresoras, aires acondicionados, pantallas para los operadores y zonas sociales entre otras.
- Diseño y definición del Plan de Recuperación ante Desastres DRP.
- Diseño y definición del plan de continuidad del Negocio BCP.

2.3.3.2. **Diseñar la arquitectura tecnológica adecuada para el SOC**

- Definir y entregar la arquitectura física y lógica de los componentes del data center e infraestructura tecnológica.
- Definir las características técnicas de la matriz de video y pantallas, teniendo en cuenta el servicios y herramientas de seguridad instaladas.
- Definición y entrega de la arquitectura de conexión de las entidades públicas y privadas.
- Definición de componentes de monitoreo para la recolección de eventos de seguridad para las entidades públicas y privadas.
- Definición de los mecanismos y protocolos para el intercambio de log´s entre las sedes a nivel nacional y territorial con el SOC, para los servicios de monitorización.
- Definición de fuentes de información que serán monitoreas para las entidades públicas y privadas a nacional y territoriales.
- Definición de las capacidades técnicas, (almacenamiento, procesamiento y memoria) de los equipos y dispositivos que soportan las herramientas de seguridad del SOC.
- Definición de las políticas de almacenamiento de Log´s y la infraestructura tecnológica que soportaría este almacenamiento.
- Definir el plan de certificación SOC 2 e ISO/IEC 27001 para el Centro de Operaciones de Seguridad - SOC
- Definir las características técnicas de data center que cumpla como mínimo un nivel de disponibilidad de 99,98

- La solución de correlación debe ser compatible con los métodos de recopilación de logs de la industria como por ejemplo (syslog, WMI, JDBC, SNMP, Checkpoint LEA, OPSEC, ALE, registros de FTP, SCP, SFTP, entre otros).

2.3.3.3. **Estandarización y normatividad aplicable al diseño de infraestructura y consideraciones**

El Sistema de Cableado Estructurado de voz y datos debe cumplir con las especificaciones de la categoría y las recomendaciones consignadas en los siguientes estándares:

- ANSI/TIA-942-B Infraestructura de Telecomunicaciones para Centros de Datos. Provee las guías y los requerimientos para el diseño e instalación de un Centro de Datos o cuarto de cómputo.
- ANSI/TIA 568-D conjunto de normas para instalaciones de cableado on premise del cliente
- ANSI/TIA 568-0-D
- ANSI/TIA 568-1-D
- ANSI/TIA 568-2-D
- ANSI/TIA 568-3-D
- ANSI/TIA-569-D Commercial Building Standard for Telecomunications Pathways and Spaces, que estandariza prácticas de diseño y construcción dentro y entre edificios, que son hechas en soporte de medios y/o equipos de telecomunicaciones tales como canaletas y guías, facilidades de entrada al edificio, armarios y/o closet de comunicaciones y cuarto de equipos.
- ANSI/TIA-606-C Administration Standard for the Telecomunications Commercial Building of Comercial Buildings, que da las guías para marcar y administrar los componentes de un sistema de Cableado Estructurado.
- ANSI/TIA-607-C Commercial Building Grounding and Bonding Requeriments for Telecomunications, que describe los métodos estándares para distribuir las señales de tierra a través de un edificio.
- NTC 6064 Tecnología de la Información Cableado Genérico para Instalaciones de Clientes.
- ISO-IEC TS 22237-1-2018 Tecnología de la información - Instalaciones e infraestructuras del centro de datos - Parte 1: Conceptos generales.
- ISO/IEC TS 22237-2:2018 Tecnología de la información. Instalaciones e infraestructuras del centro de datos. Parte 2: Construcción de edificios.
- ISO/IEC TS 22237-3:2018 Tecnología de la información. Instalaciones e infraestructuras del centro de datos. Parte 3: Distribución de energía.
- ISO/IEC 22301:2019 Security and resilience — Business continuity management systems — Requirements. En este documento especifica los requisitos para implementar, mantener y mejorar un sistema de gestión para proteger, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de las interrupciones cuando surjan.
- Entrega del diseño del cableado estructurado vertical y horizontal, categoría 6A para usuarios finales y en categoría 8 para el caso de Data Center (Diseño Área Blanca) en el caso que aplique. de cableado a la fecha del estudio.
- Certificación de puntos de cableado y enlaces de Fibra Óptica.

- Entregar una garantía mínima de 25 años con el fabricante del sistema de cableado estructurado (debe ser considerarse la garantía de fábrica para lo que se establezca en este apartado).
- Definición del sistema de voz IP para el SOC.

2.3.3.4. Establecer la estructura organizacional y definir roles dentro del SOC.

- Definir el direccionamiento estratégico del SOC alienado a las metas y objeticos de MinTIC.
- Definición y proyección de la estructura organiza del SOC según los servicios ofrecidos y los procesos estratégicos, misionales, de soporte y mejora.
- Entrega de las políticas, procedimientos, protocolos del SOC alienados al sistema de gestión de calidad.
- Establecer los procedimientos para cada uno de los servicios incluidos en el portafolio de servicios del SOC
- Definición de roles y competencias para las personas que harán parte de los equipos de operaciones, tácticos y estratégicos del SOC.
- Establecer los indicadores de cumplimiento, eficacia, eficiencia y efectividad para el SOC.

2.3.3.5. Realizar un análisis financiero y proyección de costos de implementación y operación del SOC

- Establecer el plan de costos para los mantenimientos preventivos y correctivos de los equipos, dispositivos y en general para cada elemento de configuración de la infraestructura tecnológica del SOC.
- Establecer los costos de operación de los equipos técnicos de los niveles estratégico, táctico y operativo.
- Establecer los costos de suministros para la operación del SOC.
- Establecer el modelo financiero para el sostenimiento en el tiempo de los servicios ofrecidos por el SOC.
- Establecer el mecanismo de vinculación de las entidades públicas y privadas a nivel nacional y territorial
- Establecer el modelo de negocio del SOC alineados a las directrices de MinTIC.

2.3.3.6. Formular un plan detallado para la contratación y puesta en marcha del SOC

El aliado deberá definir un plan para la contratación y puesta en marcha del SOC, incluyendo.

- Definir el anexo técnico para la contratación de la infraestructura física, técnica y tecnológica del SOC
- Definir el anexo técnico para la contratación de los servicios técnicos para la selección, entrenamiento y seguimiento del personal del SOC, la elaboración de los documentos técnicos, el montaje del modelo de operaciones, y todas las actividades necesarias para la puesta en marcha del SOC.
- Definir el cronograma de actividades para la puesta en marcha
- Definir el presupuesto integral del proyecto.

2.4. PLAN MAESTRO DE FORMACIÓN CAPACITACIÓN Y ENTRENAMIENTO EN CIBERSEGURIDAD

Objetivo:

Diseñar un Plan Maestro de capacitación, formación, entrenamiento y sensibilización del recurso humano del país 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 diversas instituciones de educación superior.

Alcance:

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

- 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.
- 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.
- 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.
- Ciber Profesores: Docentes en tecnología interesados en profundizar sus conocimientos y dedicarse a la enseñanza de la ciberseguridad en la educación superior.
- Ciber Estudiantes: Estudiantes en los niveles técnico, tecnológico y profesional que van a requerir conocimientos en ciberseguridad para desempeñarse en su vida profesional.
- Ciudadanos: Ciudadanos y habitantes del territorio nacional que hacen uso de servicios digitales y requieren sensibilización y conocimientos básicos sobre ciberseguridad.

Nota: Deberá contener los requisitos mínimos de capacitación y entrenamiento para un profesional en las áreas técnicas, Resultados de Aprendizaje, competencias y capacidades adquiribles una vez culmine su capacitación.

Entregables:

- 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.

- 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.
- 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.
- 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.
- 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.

2.4.1 FORMACIÓN EN CIBERSEGURIDAD

2.5. Dentro del plan maestro de formación capacitación y entrenamiento en ciberseguridad, se desarrollará el componente de Formación en ciberseguridad, el cual contendrá, lo siguiente:

Objetivo:

Capacitar 1800 personas en ciberseguridad de acuerdo con las metas definidas en cada segmento:

Segmento	**Meta (Personas)**	**Mínimo de Horas x Persona**
Ciber Líderes	400	20 capacitación /10 horas practicas
Ciber Profesionales	350	20 capacitación /10 horas practicas
Ciber Profesores	50	20 capacitación /10 horas practicas
Ciber Estudiantes	1000	20 capacitación
Total	**1.800**	**Personas formadas**

2.4.1.1 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.

2.4.1.2 **Diseño del programa de formación**

El diseño curricular de los programas especializados será responsabilidad del aliado en los cuales se traten mínimo los siguientes temas:

- Introducción a la ciberseguridad
- Seguridad de redes
- Seguridad en aplicaciones
- Seguridad en la nube
- Análisis de Malware
- Hacking ético
- Gestión de riesgos y cumplimiento normativo

2.4.1.3 **Otros requerimientos del diseño de los programas de formación:**

- La duración de cada nivel será de 30 horas mínimas, con distribución entre teórica y práctica de acuerdo con el perfil y programa.
- Cada nivel de formación entregará un certificado a aquellas personas que lo terminen exitosamente.
- Las clases podrán tener actividades prácticas o laboratorios, según el programa por nivel y perfil.
- La plataforma para el desarrollo de talleres prácticos debe contar con las capacidades para desarrollar laboratorios específicos de simulación para hacer las practicas cyber-range. o herramientas en un entorno de juego competitivo y totalmente rastreable.

2.4.2 **Requisitos del aliado ejecutor del proyecto:**

- El aliado deberá diseñar el contenido curricular acorde a la metodología de formación, de los cursos especializados que se ofrecerán en los distintos segmentos.
- El aliado debe evaluar que los inscritos cumplan con los criterios para acceder a la formación.
- El aliado debe poner a disposición una plataforma Web de formación virtual o Sistema de Gestión de Aprendizaje (LMS), con capacidad de registro de usuarios, herramienta que permita realizar seguimiento o monitoreo del proyecto en tiempo real y los módulos de formación virtual estipulados en el presente anexo técnico. Esta herramienta web deberá ser parametrizable y escalable.

Para tal fin la herramienta o plataforma Web debe contener como mínimo las siguientes características:

Características generales de la plataforma:

1. Administración de Usuarios
    - Creación de cuentas de usuario
    - Autenticación de usuarios

- Restablecimiento de contraseñas
- Modificación de cuentas de usuario
- Gestión de usuarios
- Administración de perfiles de usuario

2. Registro de auditoría. Este registro podrá ser consultado y exportado por los perfiles asignados a los usuarios del Ministerio TIC para seguimiento y control. Este informe debe contener como mínimo la siguiente información:
   - ID de usuario
   - Dirección IP de origen
   - Hora y fecha del registro de inscripción
   - Hora y fecha de registro por cada evento
   - Hora y fecha de último acceso

3. Prueba de compatibilidad de dispositivos
   - Verificación de aplicación móvil
   - Revisión de acceso a navegadores
   - Revisión de accesos a sistemas operativos

- El aliado deberá disponer de un único formulario de inscripción a nivel nacional de los funcionarios de las empresas. Los campos del formulario deberán ser acorde con las exigencias de MINTIC y deberá entregar un reporte de inscritos semanales.
- El aliado deberá garantizar las gestiones que conlleven a que el público objetivo adelante de manera efectiva el proceso de inscripción a las convocatorias.
- El aliado deberá realizar el seguimiento a los beneficiarios para que obtengan la certificación de aprobación del curso.
- El aliado debe garantizar un canal para la recepción y trámite de las PQRS relacionadas con los cursos, o la plataforma, y deberá reportar a MINTIC la gestión de las respuestas y atención adecuada a las mismas al final del proyecto.
- El aliado se compromete a que toda la publicidad realizada para el proyecto debe incluir el logo oficial de MINTIC, incluyendo en la plataforma utilizada para la formación

3 INFORMES DE AVANCE Y EVALUACIÓN DEL PROCESO.

El Aliado del proyecto deberá presentar informes semanales de avance del proyecto, en la fecha definida por la supervisión, indicando los resultados de los procesos de ejecución de cada componente frente al plan establecido por el aliado en términos de cumplimiento de metas.

4 EQUIPO DE TRABAJO MÍNIMO.

El aliado deberá informar el equipo de proyecto que designará, el cual desarrollará el objeto de esta invitación, así como el nivel profesional, perfil de cada persona asignada y el tiempo de experiencia.

El aliado debe demostrar que el equipo asignado al proyecto cuenta con las credenciales tanto en conocimiento, como en experiencia desarrollando este tipo de proyectos.

El ejecutor del proyecto es independiente para establecer el número de personas a emplear para la implementación y desarrollo del programa de acuerdo con el enfoque y organización que proponga del mismo, siempre y cuando mantenga el equipo de trabajo mínimo requerido con los perfiles mínimos requeridos, los cuales deberán ser aportados por el aliado / cooperante, con la dedicación necesaria a la firma del acta de inicio, así:

Cargo	Perfil mínimo	Responsabilidades
Director de Proyecto	Profesional en un programa según clasificación SNIES del núcleo básico de conocimiento de: Ingeniería industrial y afines, Ingeniería de sistemas, telemática y afines, Ingeniería electrónica, telecomunicaciones y afines. Postgrado en un programa según clasificación SNIES del núcleo básico de conocimiento de: Ingeniería industrial y afines, Ingeniería de sistemas, telemática y afines, Ingeniería electrónica, telecomunicaciones y afines. Cinco (5) años de experiencia profesional relacionada (Gerente o Director de proyectos en tecnología, innovación, formación ó transformación digital). Nota: Se podrá homologar el título de postgrado con dos (2) años de experiencia profesional adicional a la mínima requerida.	Responsable de la planeación, ejecución y cierre del proyecto. Adicionalmente, tiene a cargo la responsabilidad de presentar los reportes e informes y será el responsable de atender los requerimientos del MinTIC. Será el responsable de liderar el equipo operativo para facilitar la administración del proyecto desde los aspectos científicos, pedagógicos, operativos, logísticos y de comunicaciones, así como el equipo que desarrollará todas las actividades asociadas en el Hub.
Coordinador Científico del Proyecto	Profesional en un programa según clasificación SNIES del núcleo básico de conocimiento de: Ingeniería industrial y afines, Ingeniería de sistemas, telemática y afines, Ingeniería electrónica, telecomunicaciones y afines. Postgrado en un programa según clasificación SNIES del núcleo básico de conocimiento de: Ingeniería industrial y afines, Ingeniería de sistemas, telemática y afines, Ingeniería electrónica, telecomunicaciones y afines. Cinco (5) años de experiencia profesional relacionada (Desarrollo tecnológico, innovación, tecnología). Nota: Se podrá homologar el título de postgrado con dos (2) años de experiencia profesional adicional a la mínima requerida	Coordinar las acciones relacionados con la implementación del proyecto, verificar el cumplimento de los aspectos operativos y administrativos del proceso de creación del Hub de ciberseguridad, desarrollo de los niveles en la fase de formación, inclusive selección de instructores, velar por la calidad de las evidencias y productos presentados, realizar la realimentación a los agentes promotores y balance de actividades e información al director del proyecto y al grupo de seguimiento y coordinación.
Gerente de Proyectos SOC	Formación Académica Ingeniería electrónica o telemática o de sistemas o	▪ Liderar todas las actividades descritas en el capítulo de Centro de Operaciones de Seguridad

Cargo	Perfil mínimo	Responsabilidades
	telecomunicaciones o afines, entendidas como aquellas que comparten núcleo básico de conocimiento, de acuerdo con el Sistema de Información SNIES del Ministerio de Educación Nacional. El profesional debe contar con la tarjeta profesional respectiva. • Postgrado en Gerencia de Proyectos Informáticos o Gerencia de Proyectos de Ingeniería o Gestión de Proyectos de Ingeniería o Gerencia de sistemas de información o Maestría en Administración de Empresas • Implementador Líder ISO27001:2013 • Risk manager ISO 31000:2018 • Auditor interno ISO 22301:2019 • Scrum Master • Project Management Profesional (PMP) Diez (10) años de experiencia profesional en donde mínimo cinco (5) años de experiencia específica en dirección o gerencia de proyectos relacionados con seguridad de la información, debe tener experiencia con mínimo dos (2) sistemas de seguridad que haya implementado en otros proyectos	SOC. ▪ Establecer los entregables para cada uno de los componentes del SOC ▪ Hacer seguimiento al desarrollo de las actividades para el cumplimiento ante el MinTIC.
Profesional Senior en desarrollo operaciones de SOC	Formación Académica Ingeniero con título profesional en ingeniería de sistemas, telemática, ingeniería electrónica, telecomunicaciones o afines. El profesional debe contar con la tarjeta profesional respectiva. • Especialista en Auditoría de sistemas de información. • CEH • Implementador en ISO 27001 • Certificación ISO 31000 Risk Manager • Certificación en CISM. Experiencia: Mínimo cuatro (4) años de experiencia laboral desarrollando actividades en seguridad informática. Conocimientos en gestión de incidentes, networking,	▪ Diseñar el modelo de negocio y de operación del SOC. ▪ Desarrollar las especificaciones en el frente de operaciones del SOC, coordinando con el gerente de proyectos la definición de cada uno de los servicios del portafolio. ▪ Hacer seguimientos a las actividades definidas para el desarrollo de los entregables de cada línea estratégica en especial del SOC. ▪ Revisar los informes técnicos que generen los diferentes entregables. ▪ Establecer los servicios del SOC, así como los perfiles del equipo del SOC.

Cargo	Perfil mínimo	Responsabilidades
	herramientas de seguridad, sistemas operativos, bases de datos, servidores y conectividad.	
Profesional Senior en Seguridad de la Información.	Formación Académica Ingeniero con título profesional en ingeniería de sistemas, telemática, ingeniería electrónica, telecomunicaciones o afines. • Especialista en Seguridad informática o de la información • Certificación en CBCP (Certified Business Continuity Professional) • Certificación CISA (Certified Information systems auditor) • Certificación Risk Manager ISO 31000:2018 • Implementador Lider ISO 27001:2013 • Implementador lider ISO 22301. • Certificación COBIT2019 CISA • Certificación CISM Experiencia de por lo menos Diez (10) años como líder y/o consultor de proyectos relacionados con seguridad informática o de la información Conocimientos en gestión de incidentes, networking, herramientas de seguridad, sistemas operativos, bases de datos, servidores y conectividad.	• Desarrollar políticas procesos y procedimientos orientados a generar todo el componente de gobernanza del Hub de Ciberseguridad, atendiendo de manera especial la orientación de requerimientos definidos para el cumplimiento normativo y de certificación para proyectar los documentos correspondientes.
Especialista de Inteligencia de Amenazas y CSIRT	Profesional Ingenieros en ingeniería electrónica o informática o sistemas o telemática o telecomunicaciones o análisis y desarrollo de sistemas de información o soporte de telecomunicaciones o afines. El profesional debe contar con Tarjeta profesional. • Certified Threat Intelligence Analyst (CTIA) Experiencia: Tres (3) años de experiencia en seguridad digital y equipos de respuesta a incidentes de seguridad – CSIRT, inteligencia de amenazas, Gestión de Crisis, CTI, análisis situacional	▪ Diseño de estrategia en inteligencia de amenazas ▪ Diseño para el análisis de riesgos situacionales cibernéticos ▪ Diseño de metodología en investigación de amenazas y establecimiento de perfiles de actores de amenaza.
Asesor de formación	Profesional en un programa según clasificación SNIES del núcleo básico de conocimiento de ingeniería y afines. Posgrado en un programa según clasificación SNIES de nucleo básico de conocimiento de Ingeniería, Administración, Educación, Afines. Cinco (5) años de experiencia profesional relacionada en	▪ Administrar plataformas de formación y realizar la gestión virtual o presencial de los componentes de formación y sensibilización, verificar el cumplimento de los aspectos operativos del proceso de formación, velar por la calidad de

Cargo	Perfil mínimo	Responsabilidades
	Coordinación, enseñanza, formación, capacitación, tecnologías y/o Ciberseguridad.	las evidencias y productos presentados, realizar la realimentación a los formadores y balance de actividades e información al director del proyecto y al grupo de seguimiento y coordinación.
Coordinador Administrativo	Profesional universitario en áreas del conocimiento tales como: economía, administración, contaduría, ingeniería administrativa y afines ó ingeniería industrial y afines. Con título de postgrado en la modalidad de especialización o maestría en según clasificación SNIES del núcleo básico de conocimiento de: Economía, Administración, Contaduría, Ingeniería Administrativa y Afines, Ingeniería Industrial y Afines. Cuatro (4) años de experiencia profesional relacionada en una o varias de las siguientes opciones: - Coordinación administrativa y/o financiera de proyectos - Planeación financiera. - Gestión contable. Nota: Se podrá homologar el título de postgrado con dos (2) años de experiencia profesional adicional a la mínima requerida.	▪ Coordinar la gestión administrativa del proyecto, asegurando que se cumplan los requisitos de perfeccionamiento y ejecución del contrato; y que se gestionen informes, oficios, logística, y demás documentos relacionados con la gestión administrativa del mismo.
Asesor de comunicaciones	Profesional universitario en áreas del conocimiento de Comunicación Social, Periodismo y Afines, o profesional en otras disciplinas con título de postgrado en la modalidad de especialización o maestría. Cuatro (4) años de experiencia profesional relacionada en comunicación comunitaria o comunicación para el desarrollo, comunicación sobre ciencia y tecnología.	▪ Apoyar la estrategia de comunicaciones adoptada para el desarrollo del proyecto en armonía con los lineamientos de imagen y constreñido concertados con MinTic.

Todo el equipo de trabajo deberá estar disponible para cumplir con sus responsabilidades del proyecto, con los requerimientos del supervisor y participar en forma presencial o virtual en las reuniones que se estime necesario, previa convocatoria por parte del supervisor. En todo caso, el cooperante deberá contar con los profesionales requeridos, para cumplir con el objeto, así como la disponibilidad de tiempo[1] para atender los requerimientos de la supervisión del convenio.

Nota: Este equipo de trabajo deberá ser propuesto por el ejecutor del proyecto, sin perjuicio de que este disponga de personal adicional que considere suficiente y/o necesario para el cumplimento del objeto contractual, sin que el mismo genere un valor adicional para el Mintic.

1 Se entiende por disponibilidad el tiempo en el que el equipo de trabajo debe atender las necesidades del programa para la correcta ejecución del contrato, de acuerdo con la programación del proyecto.

4.4 Requisitos del equipo de trabajo mínimo obligatorio:

El ejecutor del proyecto deberá entregar los siguientes documentos para el equipo de trabajo:

Experiencia específica y formación académica del personal propuesto con sus respectivos soportes, así:

- Fotocopia legible del título de técnico, tecnólogo o profesional o del acta de grado.
- 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).
- Fotocopia legible del diploma de posgrado, o del acta de grado del posgrado.
- Fotocopia legible de la tarjeta o matrícula profesional. Sólo se deberá anexar 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.
- Fotocopia legible del documento de identificación: cédula de ciudadanía, cédula de extranjería o pasaporte.
- Fotocopia legible de los documentos soporte de experiencia.

El Ministerio realizará la verificación de la documentación que el Cooperante presente, y podrá solicitar aclaraciones a los documentos que acreditan la experiencia y formación de los profesionales propuestos.
El ejecutor del proyecto deberá mantener el equipo que presentó y que fue aprobado por el supervisor durante la ejecución del contrato / convenio. Si por causas excepcionales no atribuibles al Cooperante, caso fortuito o fuerza mayor, se hace necesario realizar una modificación o cambio de algún integrante del equipo de trabajo durante la ejecución del contrato / convenio, deberá ser aprobado por MINTIC, a través del supervisor, previa verificación del cumplimiento de los requisitos de cada perfil definido en el presente documento.

El ejecutor del proyecto debe garantizar que durante el transcurso del proyecto se cuente con todo el Equipo de Trabajo, por esta razón, al solicitar un cambio de profesional para determinado Cargo, el Cooperante deberá entregar la solicitud de cambio, la hoja de vida de candidato que cumpla el perfil requerido debidamente soportada, dando cumplimiento a las mismas o mejores calidades del profesional acreditado a reemplazar, para que la supervisión adelante la evaluación y con una antelación de diez (10) días hábiles de la fecha en la que se vincularía el nuevo profesional.

NOTA: Los documentos del equipo de trabajo, deberán ser presentados a la firma del acta de inicio.

4.1.1 Consideraciones sobre el equipo de trabajo:

4.1.1.1 Inhabilidad y Compatibilidad

No podrán formar parte del equipo de trabajo del ejecutor del proyecto quienes hayan suscrito directamente con el Ministerio de Tecnologías de la Información y las Comunicaciones o el FONDO ÚNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES contratos como asesores o quienes se hayan desempeñado como

funcionarios dentro de los últimos dos años contados a partir de la firma del acta de inicio, siempre y cuando el objeto que desarrollan tenga relación con el sector al cual prestaron sus servicios.

Lo anterior se constituye como una incompatibilidad o inhabilidad sin que ellos signifiquen una vulneración a la igualdad
laboral dado que corresponde a la garantía de participación y generación de empleo en el sector abriendo el espectro sistémico.

Las obligaciones relacionadas con el personal requerido para la ejecución del objeto contractual serán objeto de especial verificación por la supervisión.

Los profesionales en ciberseguridad deben partir de un área de experiencia orientada a la gestión de incidentes cibernéticos, protección de los datos, protección de la infraestructura crítica digital y algunos aspectos orientados al mejoramiento de las capacidades del SOC operacional que debe contener algunas de las siguientes líneas orientativas:

- Análisis de Malware
    - Scaninng de vulnerabilidades
    - Análisis de Vulnerabilidades
    - Administración de Dispositivos
    - Recertificación de identidad
    - Testing de penetración

- Tipos de amenaza contra instituciones financieras y redes (SCADA) traducido del inglés como:
    - Supervisory Control And Data Acquisition

- Con base en las anteriores líneas los profesionales y el personal experto deberá contener como mínimo 3 certificaciones de herramientas de análisis de vulnerabilidades, denominadas SIEM, SOC o SOAR.

- Certificación mínima de una o dos metodologías o procedimientos para recolectar, analizar y/o presentar evidencia digital que oriente de manera reactiva o preventiva los eventos procesados en el SOC.

- Certificación mínima de dos herramientas o metodologías para poder realizar análisis a dispositivos de almacenamiento o de sistemas convencionales de información, ejemplo. Windows o Linux

- Conocimiento en hardening y pruebas de pentesting preventivo, y acreditar cursos de actividades de escaneo de vulnerabilidades orientadas a infraestructuras SCADA.

- Analistas que realicen aseguramiento de canales de datos para la recolección y prevención de actividades originadas desde la recolección, monitoreo y análisis de eventos e incidentes.

4.1.2 Consideraciones frente a la formación académica:

- Todos los programas profesionales, incluidos los de posgrados, que se presenten como parte de la formación académica de algún integrante del personal propuesto, deberán contar con su correspondiente aprobación del ICFES o de la Secretaría de Educación correspondiente (si fueron obtenidos con anterioridad a la entrada en vigencia de la Ley 30 de 1992) o del Ministerio de Educación de conformidad con el Decreto 2230 de 2003.
- Para definir si un determinado título académico se adecúa al requerimiento académico establecido en el pliego de condiciones, se verificará que el área básica de conocimiento del título acreditado por el profesional propuesto corresponda al requerido, de acuerdo con la información que arroje el SNIES en su página https://snies.mineducacion.gov.co/consultasnies/programa.
- Si se trata de estudios obtenidos en el exterior, se deberá presentar la convalidación del título expedida por el Ministerio de Educación – Sistema Nacional de Información de la Educación Superior SNIES, de acuerdo con lo señalado en la Ley 30 de 1992, la Resolución 5547 de 2005, la Resolución 20797 de 2017 o aquellas que las modifiquen o adicionen o de acuerdo con la Circula Externa Única expedida por Colombia Compra Eficiente y sus modificaciones, el proponente podrá acreditar la formación académica en el exterior con copia del diploma expedido por el centro educativo y la descripción del programa correspondiente que permita conocer el nivel de los estudios y su clasificación en la Clasificación Internacional Normalizada de Educación Nivel CINE 6 (pregrado), 7 (especialización o maestría). En este caso, deberá tener en cuenta las siguientes recomendaciones:
  - Si la certificación se encuentra en idioma distinto al de la República de Colombia, deberá adjuntarse además del documento en idioma extranjero, la traducción oficial del documento.
  - Si el programa académico que se pretende acreditar no se encuentra en el SNIES por no estar vigente al momento de firma del contrato, el proponente deberá anexar el documento emitido por la institución educativa que ofreció el programa, en el cual se especifique el pensum respectivo, sin perjuicio de las verificaciones que para el efecto realice la Entidad.
- En cualquier programa, cada diploma o acta de grado será reconocido para una sola clase de formación, otorgada por el SNIES – Ministerio de Educación, independiente de los calificativos que incorpore el diploma y/o acta de grado; Para este efecto, no se considera el orden cronológico de la realización de las diversas formaciones presentadas.
- No deberán ser incluidos ni serán tenidos en cuenta para efectos de la revisión del equipo de trabajo: (i) programas de formación académica que no hayan conducido a la obtención de títulos permitidos para este proceso o que no cuenten con la debida aprobación; (ii) Cursos seminarios que no hayan conducido a la obtención de títulos profesionales o títulos de posgrado.

4.1.3 Consideraciones frente a la experiencia del equipo de trabajo:

Las certificaciones, constancias o cualquier otro documento que acredite la experiencia del equipo de trabajo mínimo 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.

- Cargo(s), rol(es) o perfil(es) nominales y/o funcionales desempeñado(s)
- Actividades y/u obligaciones y/o funciones por cada uno del (los) cargo(s), rol(es) o perfil(es) desempeñado(s).
- Objeto del contrato, obligaciones, entregables u actividades que permita verificar de manera explícita la experiencia requerida.
- Periodo de vinculación (Fecha inicial y Fecha Final expresadas en día, mes y año). En caso de que el proponente aporte en las certificaciones fechas en las que no se indique el día, sino solamente el mes y el año, para efectos de verificar y calificar la experiencia, se procederá así:
- 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.
- 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 Cooperante 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.

Para acreditar la experiencia del equipo de trabajo deberá tenerse en cuenta lo siguiente:

- Los trabajos deben haber sido realizados por la persona para la cual el proponente está aportando la acreditación de la experiencia y que dicha experiencia es la requerida para este convenio. De igual modo, en los documentos aportados debe establecerse el tiempo en el cual se realizó la ejecución de las actividades.
- Las certificaciones que acrediten la experiencia del personal propuesto se considerarán expedidas bajo gravedad de juramento.
- Para que sean consideradas válidas, las certificaciones deben acreditar la experiencia específica requerida, señalando de manera clara las actividades u obligaciones o funciones realizadas por el profesional propuesto.

Nota. Se entenderá que un (1) año corresponde a 360 días y un (1) mes a 30 días.

- De conformidad a lo establecido en el artículo 229 del Decreto-Ley 019 de 2012, la experiencia profesional será computada a partir de la terminación y la aprobación de materias correspondientes al respectivo pensum académico de educación superior, excepto en los casos de profesiones relacionadas con el sistema de seguridad social en salud, en los que dicha experiencia se computará a partir de la inscripción o registro profesional. Lo anterior de conformidad con la Circular Externa Única expedida por Colombia Compra Eficiente.
- Para el caso de las profesiones relacionadas con la ingeniería o de alguna de sus profesiones afines o auxiliares, la experiencia profesional será computada a partir de la terminación y aprobación del pensum académico. Lo anterior, sin perjuicio de lo dispuesto en el artículo 192 de la Ley 1955 de 2019, que dispone que «la práctica laboral que el estudiante realice para optar a su título de profesional, tecnológico o técnico

cuenta como experiencia laboral». Lo anterior de conformidad con el concepto de Colombia Compra Eficiente del 14/04/2020 No. de radicado 2202013000002648.

- Para el caso de la contabilización de la experiencia de los ingenieros graduados y con ejercicio en el exterior, la experiencia que ha de ser tenida en cuenta en Colombia será aquella obtenida en el extranjero, siempre y cuando, de conformidad con la normatividad del respectivo país, la haya adquirido legalmente; circunstancia que le corresponde probar al profesional que solicita la validez de la misma. El documento que acredite la validez de la experiencia obtenida en el extranjero deberá cumplir con lo preceptuado en la Ley 455 de 1998 y en el Decreto 106 de 2001 y en la resolución 10547 del 14 de diciembre de 2018 del Ministerio de Relaciones Exteriores y demás normas que la adicionen, modifiquen o deroguen, en lo relacionado con el apostille.
- En todo caso y para efectos de la ejecución del convenio, el ingeniero domiciliado en el exterior deberá ostentar el Permiso Temporal expedido por el COPNIA (http://www.copnia.gov.co/).
- El Cooperante adquiere la obligación de que todos sus profesionales en ingeniería cuenten con permisos temporales o licencias y si su vigencia expira durante la ejecución del contrato, se lleve a cabo la renovación del permiso temporal de manera sucesiva hasta la terminación del contrato.
- Para efectos de contabilizar los tiempos requeridos, sólo se contarán una vez aquellos períodos “traslapados”, es decir, aquellos que se sobrepongan o que se hayan desarrollado en un mismo lapso por la misma persona.
- Si el Cooperante es el mismo que certifica la experiencia del profesional propuesto, además de esta certificación, deberá presentar fotocopia legible del contrato suscrito entre el Cooperante y la persona, a través del cual se evidencie el vínculo contractual.
- En caso de no existir contrato suscrito, deberá allegar certificación de la junta directiva o junta de socios (la que corresponda), con el visto bueno del revisor fiscal o contador (en caso de no existir revisor fiscal) para acreditar la experiencia el profesional propuesto.

5 OBLIGACIONES ESPECIALES DEL COOPERANTE COMO EJECUTOR DEL PROYECTO:

- Disponer la capacidad de técnica y humana necesaria materializar el alcance.
- Presentar el plan de trabajo necesario para ejecutar el proyecto.
- Entregar cronograma de hitos, actividades y entregables de manera detallada para el seguimiento y presentar sus avances en la reuniones de seguimiento con la supervisión y el equipo de apoyo a la supervisión del proyecto.
- Llevar contabilidad independiente para la ejecución del proyecto.
- Celebrar los actos necesarios para la ejecución del proyecto conforme su manual interno de contratación.
- Disponer los recursos del proyecto únicamente para el cumplimiento del objeto y las obligaciones del mismo.
- Realizar los aportes ofrecidos para la ejecución del proyecto, representados en capacidad técnica y humana.
- Presentar mensualmente al Supervisor informe de ejecución financiera y cumplimiento de metas.
- Disponer y hacer uso eficiente de los recursos afectados a la ejecución del proyecto.
- Designar un representante en el grupo de seguimiento y coordinación del proyecto, quien será el encargado del seguimiento técnico, administrativo y financiero durante el término de duración de este.

- Cumplir con los requisitos establecidos en el proyecto para efectuar los desembolsos.
- Desarrollar los entregables definidos en el Alcance del anexo técnico.

6 MODALIDAD DE CONTRATACIÓN:

El Hub de Ciberseguridad es considerado 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.

Conforme lo anterior, la modalidad de contratación para la ejecución del proyecto es convenio especial de cooperación. Conforme el articulo 1 Decreto 393 de 1991 *"Por el cual se dictan normas sobre asociación para actividades científicas y tecnológicas, proyectos de investigación y creación de tecnologías"*, la Nación y sus entidades descentralizadas podrán asociarse con los particulares para adelantar actividades científicas y tecnológicas, proyectos de investigación y creación de tecnologías, "Mediante la celebración de convenios especiales de cooperación" (numeral 2).

El artículo 1° del decreto 393 de 1991, las Modalidades de asociación 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.

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.

Por lo anterior descrito, según el Artículo 6 del decreto 393/1991, 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.

Por ello, en virtud de estos convenios, las personas que los celebren aportan recursos de distinto tipo para facilitar fomentar, desarrollar y alcanzar en común algunos de los propósitos contemplados en el artículo segundo.

6.1 Códigos de clasificación UNSPSC:

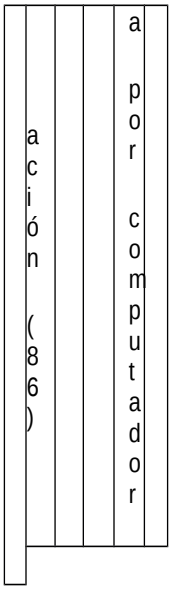
El objeto del proyecto antes señalado se encuentra enmarcado en los siguientes códigos de clasificación UNSPSC:

A	Segmento	Familia	Clases	Producto	Código
Servicios (F)	Servicios basados en ingeniería, in	Entrega de servicios de tecnología	Servicios de administración de acce	Servicios de administración de apli	81161501

	vestigación, y tecnología (81)	de información (16)	so (15)	caciones de software (01)	
	Servicios Educati	Sistemas educativ	Servicios de apre	Servicios de ense	86111502

vos y de Formación (86)	os alternativos (11)	ndizaje a distancia (15)	ñanza a distancia (02)		
Servicios Educativos y	Instalaciones educativa	Servicios de guía infor	Servicios de asesorías	86141501	

	de Formación (86)	s (14)	mativa (15)	educativas (01)	
	Servicios Educativos y de Form	Instalaciones educativas (14)	Tecnología educacional (17)	Institución programada asistid	86141703



7 ENTIDAD ALIADA

Para lo anterior, la entidad ejecutora seleccionada es el Centro de Bioinformática y Biología Computacional de Colombia - BIOS, conforme las siguientes consideraciones:

7.4 Idoneidad y capacidad de BIOS para el desarrollo del Convenio.

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), Desarrollo 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 del 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 permita 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 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.

Cabe señalar que 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:

7.1.1. Especialidad, unicidad y vínculo especial con MinTic. 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.

7.1.2. Liderazgo en Ciberseguridad. BIOS es el líder promotor del HUB de Ciberseguridad (que será 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.

7.1.3. 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.

7.1.4. 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. Así mismo ha sido ejecutor habitual y cumplido de los diversos proyectos estratégicos de Mintic desde el año 2011 y de proyectos de regalías de ciencia y tecnología desde el año 2021.

8 VALOR DEL CONVENIO.

El valor del convenio, incluyendo aportes del aliado, se estima en la suma de $5.100’000.000.

8.1 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:

CONCEPTO	ENTREGABLE	%	VALOR
Primer desembolso Noviembre/17/2023	a. Diseño Plan de trabajo b. Cronograma de actividades. c. Diseño Metodología de desarrollo del proyecto.	31 %	1.500.000.000
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

CONCEPTO	ENTREGABLE	%	VALOR
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: 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	21 %	1.000.000.000
		TOTAL	**$4.800.000.000**

Nota: Los entregables sujetos a los desembolsos, se detallan en el anexo técnico del presente proyecto.

Para cada desembolso, el aliado / cooperante 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 durante el periodo objeto de desembolso. (o el formato que lo modifique).
3. Certificación de pago de las contribuciones al Sistema Integral de Seguridad Social en Salud, Pensiones y ARL, contribuciones parafiscales si a ello hubiere lugar, expedido por el revisor fiscal de la entidad.
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 15 y el 30 de diciembre.

8.2 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, descritos así:

Descripción del aporte	Cant	Valor Unitario	Valor Total
Logos y manual de imagen del Hub De Ciberseguridad	1	50.000.000	50.000.000
Desarrollo de cortos y/o videos animados sobre ciberseguridad dirigidos a los ciudadanos, con logos e imagen institucional del MINTIC.	10	25.000.000	250.000.000
		TOTAL	**300.000.000**

Firmado en Original

PIEDAD CECILIA MONTERO VILLEGAS
GIT. Equipo de Respuesta a Emergencias Cibernética de Colombia - COLCERT
CSIRT GOBIERNO

REGISTRO DE FIRMAS ELECTRONICAS

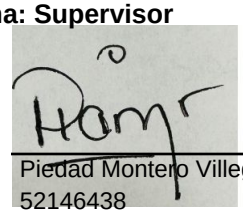
Anexo Técnico HUB Ciberseguridad - Nov -14-2023 (1)

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

Id Acuerdo: 20231114-230853-f310b5-04791567
Creación: 2023-11-14 23:08:53
Estado: Finalizado
Finalización: 2023-11-14 23:09:54

Escanee el código para verificación

Firma: Supervisor



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

REPORTE DE TRAZABILIDAD

Anexo Técnico HUB Ciberseguridad - Nov -14-2023 (1)

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

Id Acuerdo: 20231114-230853-f310b5-04791567 Creación: 2023-11-14 23:08:53

Estado: Finalizado Finalización: 2023-11-14 23:09:54

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 23:08:59 Lec.: 2023-11-14 23:09:45 Res.: 2023-11-14 23:09:54 IP Res.: 186.30.62.159