PROYECTO PARA EL FORTALECIMIENTO INTEGRAL DE LA SEGURIDAD DIGITAL Y EL DESARROLLO DE CAPACIDADES EN CIBERSEGURIDAD

ColCERT – Viceministerio de Transformación Digital
Ministerio de Tecnologías de la Información y las Comunicaciones

1 Contenido

1 OBJETO DE CONTRATACIÓN

Prestar servicios especializados orientados al fortalecimiento de la seguridad digital en Colombia, mediante el desarrollo de competencias prácticas, la automatización de herramientas especializadas y la integración de acciones alineadas con la Estrategia Nacional de Seguridad Digital, con el propósito de reducir brechas sectoriales y apoyar la transparencia electoral.

2 INTRODUCCIÓN Y JUSTIFICACIÓN

En el marco de la transformación digital en Colombia, la ciberseguridad se consolida como un pilar estratégico y prioritario tanto para el sector público como para el privado. El incremento sostenido de los servicios digitales, el auge del comercio electrónico y la masificación del uso de tecnologías de la información han ampliado de manera significativa la superficie de exposición de ciudadanos, empresas e instituciones a riesgos cada vez más sofisticados. Esta realidad ha puesto de manifiesto brechas relevantes en las competencias digitales orientadas a la prevención, detección y mitigación de ciberataques, lo que genera vulnerabilidades críticas en el ecosistema digital nacional.

La limitada cultura y conciencia en materia de seguridad digital ha propiciado un aumento de los delitos informáticos, impactando la privacidad de los usuarios y comprometiendo la integridad de la infraestructura tecnológica. Esta situación se traduce en que tanto personas naturales como organizaciones no identifiquen ni implementen controles básicos de protección, incrementando la exposición a incidentes como robo de información, fraudes electrónicos o sabotaje de sistemas críticos. Por ello, la capacitación permanente y especializada de ciudadanos, profesionales y servidores públicos emerge como un imperativo para robustecer la defensa ante amenazas cibernéticas avanzadas.

Frente a este escenario, el Ministerio TIC, a través del ColCERT, asume un rol estratégico en la formulación, despliegue y seguimiento de la Estrategia Nacional de Seguridad Digital. Esta función implica no solo la articulación de esfuerzos interinstitucionales y el fortalecimiento de la gobernanza, sino también la anticipación y respuesta efectiva ante desafíos derivados de la expansión de servicios digitales, la sofisticación de los actores maliciosos y la protección integral de la infraestructura crítica y la privacidad ciudadana.

Es así como entre 2022 y 2025 el ColCERT ha implementado un programa de transferencia de conocimiento que ha fortalecido a más de 8.000 funcionarios, contratistas y colaboradores. La adquisición prevista de recursos y mecanismos permitirá la continuidad y expansión de estos procesos, alineándose con la macrometa institucional de formación en seguridad digital y preparando a los equipos nacionales y territoriales para responder con eficacia ante incidentes de seguridad.

De la misma forma y en cumplimiento de los lineamientos constitucionales, legales y regulatorios en materia de gestión del riesgo, respuesta a incidentes y gobernanza de la

seguridad digital, el ColCERT requiere consolidar un portafolio robusto de herramientas tecnológicas, capacidades especializadas y servicios estratégicos que soporten la continuidad, disponibilidad y resiliencia del ecosistema de seguridad digital estatal. Esta necesidad adquiere especial relevancia durante el ciclo electoral 2026, dado el rol del ColCERT como Secretaría Técnica del PMU Cyber Electoral, liderando la articulación nacional para la protección de la infraestructura electoral, en coordinación con la Registraduría Nacional del Estado Civil (RNEC), el Consejo Nacional Electoral (CNE) y demás entidades.

El aumento significativo de incidentes de seguridad digital en el país, sumado a los riesgos asociados a los procesos electorales recientes, evidencia que la capacidad actual del Estado debe ampliarse y modernizarse. La tendencia ascendente de ataques de denegación de servicio, campañas de desinformación, explotación de vulnerabilidades y la sofisticación de actores maliciosos —tanto locales como internacionales— obliga a adoptar tecnologías robustas, actualizadas y alineadas con mejores prácticas globales. Adicionalmente, la experiencia acumulada en acompañamientos a entidades públicas, así como la creciente demanda de asesorías, monitoreo, validaciones de infraestructura y apoyo en incidentes, exige herramientas de mayor alcance, automatización y precisión analítica.

El contexto actual evidencia una presión creciente sobre infraestructuras públicas y privadas, marcada por la sofisticación de ataques y la necesidad crítica de talento especializado, soluciones de defensa avanzadas y políticas nacionales sólidas.

Como respuesta, el Ministerio TIC define la iniciativa “Ciberseguridad 360”, diseñada para abordar de manera sistemática los desafíos históricos en materia de protección digital. Este programa se fundamenta en una estrategia multidimensional que contempla el fortalecimiento de capacidades técnicas mediante capacitación especializada del talento humano, así como la actualización e integración de infraestructuras tecnológicas avanzadas. Estas acciones estratégicas están dirigidas a optimizar la resiliencia y asegurar la protección eficiente de los activos críticos nacionales frente a amenazas cibernéticas emergentes.

Como componentes fundamentales de la iniciativa se tienen:

1. Un componente técnico que permite cubrir no solamente la infraestructura tecnológica que soporta los servicios propuestos en el marco de la iniciativa garantizando no solo la continuidad del portafolio del ColCERT, sino que amplía su capacidad operativa y estratégica, permitiendo anticipar riesgos, reaccionar con mayor eficiencia y acompañar al país en periodos de alta sensibilidad, como los procesos electorales legislativos y presidenciales.
2. La formación de talento humano especializado es un componente central de esta estrategia. Se busca genera formación práctica y certificable, orientada a fortalecer competencias digitales y consolidar una cultura resiliente y sostenible en

ciberseguridad. Esta estrategia responde a la demanda creciente de protección digital y contribuye a la formación de una fuerza laboral capacitada para enfrentar los desafíos emergentes en la materia.

Las acciones de capacitación están diseñadas bajo un enfoque práctico, orientado a la toma de decisiones informadas, la reducción de errores operativos y el fortalecimiento de la resiliencia institucional, aspectos especialmente relevantes para entidades con funciones críticas durante periodos electorales. La adquisición de herramientas, licenciamientos y capacidades tecnológicas constituye, por tanto, una necesidad estratégica para asegurar la defensa digital del Estado y la confianza en los procesos democráticos.

El portafolio tecnológico propuesto cubre de forma integral las fases de prevención, detección temprana, respuesta, análisis forense y comunicación institucional. Su implementación potencia la capacidad preventiva y reactiva del ColCERT, posicionando a la entidad como referente nacional durante el ciclo electoral 2026 y en la operación continua del ecosistema de seguridad digital del país.

En conclusión, la iniciativa “Ciberseguridad 360” se alinea plenamente con los lineamientos de la Estrategia Nacional de Seguridad Digital, enfocándose en el fortalecimiento de capacidades, la promoción de una cultura de ciberseguridad, la modernización de herramientas y el impulso de la cooperación interinstitucional. Su despliegue permitirá reducir brechas, optimizar la gestión pública y garantizar un entorno digital seguro y confiable para Colombia.

3 DEFINICIÓN DEL ALCANCE DEL PROYECTO

Este proyecto surge con el propósito de reforzar la seguridad digital en el Estado, tomando como base las mejores prácticas tanto nacionales como internacionales y siguiendo los lineamientos de la Estrategia Nacional de Seguridad Digital. El desarrollo del mismo resulta especialmente relevante en el contexto electoral, donde es fundamental salvaguardar la información, mantener la continuidad operativa y generar confianza en la ciudadanía.

De esta forma, el objetivo principal consiste en diseñar e implementar acciones que fortalezcan de manera integral la seguridad digital en de los diferentes sectores, abarcando tanto la modernización de infraestructuras tecnológicas como la capacitación especializada. El alcance del proyecto contempla la identificación de posibles riesgos, la reducción de vulnerabilidades y el desarrollo de capacidades, asegurando así la sostenibilidad y la mejora continua de los servicios digitales institucionales y de los procesos democráticos.

Para el desarrollo de las iniciativas descritas se contemplan dos líneas estratégicas a través de las cuales se desarrollará el proyecto:

3.1 Fortalecimiento de la Infraestructura Tecnológica

La protección de infraestructuras críticas será una prioridad, aplicando metodologías avanzadas para gestionar riesgos y aumentar la resiliencia ante nuevas amenazas digitales.

Las medidas a implementar abarcan la mejora y actualización de la infraestructura tecnológica con que cuenta el ColCERT teniendo en cuenta:

- **Gestión temprana de vulnerabilidades (Tenable One):** Permite visibilidad integral de activos, configuraciones inseguras y puntos críticos; su renovación fortalece la postura de seguridad del Estado y reduce brechas explotables.
- **Detección y respuesta ante amenazas (Trellix):** Plataforma que identifica comportamientos anómalos, bloquea malware avanzado y contiene ataques; clave para mantener la continuidad operativa y apoyar entidades sin tecnología propia.
- **Protección DNS (Cisco Umbrella):** Actúa como defensa temprana bloqueando conexiones maliciosas, reduciendo phishing y exfiltración de datos; esencial en contextos de alto tráfico como procesos electorales.
- **Mitigación de ataques DDoS (Cloudflare):** Proporciona protección contra denegación de servicio y mejora la estabilidad y rendimiento de servicios críticos durante picos de consultas.
- **Plataforma de comunicaciones (Mailchimp):** Facilita envío masivo y segmentado de alertas, boletines y mensajes institucionales confiables; crucial para contrarrestar desinformación.
- **Laboratorio de simulación y pruebas (VMware ESXi/vCenter):** Permite ejecutar análisis, ejercicios y pruebas sin comprometer producción; su renovación garantiza continuidad y preparación técnica.
- **Capacidad forense digital (MAGNET AXIOM Cyber + Torre Forense):** Habilita adquisición remota de evidencia, análisis profundo y generación de reportes con cadena de custodia; fundamental en incidentes durante procesos electorales.
- **Videowall del Centro de Operaciones:** Es vital para la visualización situacional y coordinación con el PMU Cyber Electoral; requiere soporte y mantenimiento para garantizar operación continua.
- **Servicio MDR con CrowdStrike:** Proporciona monitoreo continuo 24/7, caza de amenazas y contención inmediata; reduce significativamente los tiempos de detección (MTTD) y respuesta (MTTR), fortaleciendo la defensa estatal.

3.2 Formación Especializada

La formación permanente del personal es esencial para asegurar la protección y eficiencia de las operaciones. Por ello, el proyecto prevé:

- Programas de capacitación y actualización en seguridad digital.

- Desarrollo de habilidades básicos y/o especializadas para prevenir y responder a incidentes.
- Impulso al aprendizaje organizativo como medio para fortalecer la democracia.
- Plataforma de formación avanzada basada en **IA y algoritmos propietarios**, para personalizar el aprendizaje y predecir tendencias formativas.
- Solución **parametrizable, escalable y 100% web**, accesible sin instalación desde cualquier navegador.
- Incluye **retos técnicos** en áreas como criptografía, forense, explotación web, pentesting y reversing.
- Ofrece **formatos de competencia**: individual, por equipos, por niveles, tiempo limitado o ranking abierto.
- Posee **gamificación completa**: puntuación automática, rankings, insignias y progresión por niveles.
- Puede integrarse con procesos formativos previos y funcionar como herramienta de **evaluación post-entrenamiento**.
- Genera **métricas detalladas**: análisis por participante, tipo de reto y tiempos de resolución.
- Incluye **administración integral de usuarios**, con autenticación segura y mecanismos de recuperación de credenciales.
- Provee **registro de auditoría exportable**, con datos como ID, IP, fechas, horas y eventos.
- Garantiza compatibilidad con múltiples **dispositivos, sistemas operativos y navegadores**.
- Gestión centralizada de inscripciones mediante **formulario único nacional**, con reportes quincenales y apoyo en certificación.
- Permite **talleres prácticos** durante el proyecto.
- Programas de formación de **mínimo 40 horas**, con docentes especializados y al menos una clase sincrónica grabada.
- Enfoque **práctico y aplicado**, evitando contenidos puramente teóricos mediante ejercicios, laboratorios y competencias simuladas.
- Estrategia de formación alineada con los **objetivos del plan sectorial TIC**.
- Actividades clave: talleres, clases sincrónicas, difusión segmentada, integración institucional, monitoreo y retroalimentación continua.
- **Meta de formación:** capacitar a *5.000 usuarios* en competencias básicas y especializadas (curso especialista en ciberseguridad, CTF, ciudadanía, profesionales y funcionarios).
- Toda comunicación cumple lineamientos de **imagen institucional del MinTIC y ColCERT**.
- Mecanismos rigurosos de **seguimiento y mejora continua**, con informes periódicos e indicadores de impacto.

Gracias a esta estructura, se promueve una ejecución global que fortalece la sostenibilidad, genera confianza y contribuye al cumplimiento de los objetivos nacionales en materia de seguridad digital, integrando claramente ambas líneas estratégicas principales.

4 OBJETIVOS ESPECÍFICOS

- Implementar prácticas avanzadas para la protección, prevención y respuesta ante incidentes de ciberseguridad, garantizando el cumplimiento de políticas y lineamientos nacionales.
- Optimizar el monitoreo y la administración de sistemas de información, incorporando tecnologías de predicción de demanda que faciliten la toma de decisiones y la resiliencia institucional.
- Fortalecer las competencias técnicas y operativas de entidades frente a los riegos durante los procesos electorales en materia de seguridad digital.
- Desarrollar y consolidar capacidades técnicas básicas y/o avanzadas en las entidades beneficiarias, mediante programas de formación certificados y actividades prácticas que eleven la preparación frente a riesgos y amenazas digitales, especialmente en el contexto de procesos electorales.
- Garantizar la trazabilidad, seguimiento y certificación de los procesos de formación y simulación, mediante la generación de informes estructurados y la retroalimentación continua de los participantes y aliados estratégicos.

5 ENTREGABLES

El proyecto consolida cinco entregables estratégicos diseñados para fortalecer la seguridad digital del Estado, asegurar la continuidad operativa del ColCERT y soportar los servicios de monitoreo, respuesta, análisis, formación y comunicación. Cada entregable integra actividades de licenciamiento, soporte, despliegue, transferencia de conocimiento y producción de informes, alineadas con los lineamientos del Ministerio TIC.

5.1 Licenciamiento, despliegue y operación de soluciones tecnológicas

- Garantizar que todas las herramientas, plataformas y soluciones de ciberseguridad estén **debidamente licenciadas, activas y documentadas** durante un mínimo de 12 meses.
- Asegurar la **entrega oportuna de licencias** antes del vencimiento de las existentes, sin generar interrupciones de operación.
- Incluir tecnologías esenciales como Tenable One, Trellix, Cisco Umbrella, Cloudflare, VMware ESXi/vCenter, MDR, Magnet AXIOM Cyber, Mailchimp, Kiteworks y otras soluciones complementarias.
- Activar la **membresía FIRST** como mecanismo de cooperación internacional en ciberseguridad.

- Desarrollar y entregar un **plan completo de soporte**, mantenimiento, actualizaciones, escalamiento y evidencia documental.
- Ejecutar **transferencia de conocimiento especializada** para cada herramienta, impartida por personal certificado, con materiales, prácticas guiadas y evidencias formativas.

5.2 Plataforma de vigilancia y monitoreo continuo (MDR)

- Implementar una plataforma integral de **detección y respuesta 24/7**, capaz de cubrir entre **mínimo 2000 activos de TI**.
- Integrar múltiples fuentes de telemetría: EDR/XDR, DNS seguro, análisis de vulnerabilidades, infraestructura crítica, flujos de red e indicadores de compromiso.
- Desplegar completamente la solución MDR: instalación de agentes, reglas, tableros de monitoreo y afinamiento inicial en máximo 30 días.
- Garantizar soporte 24/7, **gestión de escalamiento**, coordinación con SOC y servicios expertos de cacería de amenazas.
- Documentar cada incidente desde la detección hasta el cierre y asegurar que **toda la información pertenezca al Ministerio TIC**.
- Entregar informes por entidad, incluyendo análisis, resultados, recomendaciones y reportes forenses cuando corresponda.
- Definir y activar **estrategias de contingencia y continuidad operativa**.

5.3 Programas de formación y certificación

- Diseñar y ejecutar programas de formación alineados con la **Estrategia Nacional de Seguridad Digital**, con módulos prácticos y certificación verificable.
- Garantizar disponibilidad en una **plataforma web interactiva**, funcional durante toda la vigencia contractual.
- Realizar actividades de difusión y publicidad respetando el manual de identidad del MinTIC.
- Entregar certificados digitales y mantener actualizados los registros de beneficiarios conforme a las políticas de datos personales.
- Incluir entrenamientos especializados para el personal del Centro de Operaciones del ColCERT.
- Alertar al Ministerio sobre **amenazas emergentes** que puedan afectar la continuidad del servicio formativo.

5.4 Producción de piezas comunicativas e institucionales

- Diseñar piezas de comunicación alineadas con los lineamientos de imagen y accesibilidad del MinTIC y el ColCERT.
- Apoyar las actividades del proyecto: formación, campañas de ciberseguridad, notificaciones y mensajes institucionales.
- Validar contenido técnico y narrativo en coordinación con el área de comunicaciones.
- Incorporar estas piezas en la plataforma de formación y en las estrategias de comunicación para situaciones de riesgo o eventos críticos.

5.5 Informes estratégicos, métricas y evaluación

- Elaborar informes mensuales, trimestrales y de cierre que integren:
  - Métricas de desempeño.
  - Indicadores estratégicos.
  - Análisis de vulnerabilidades e incidentes.
  - Uso del MDR.
  - Avances de formación y resultados del cyber-range.
- Incluir retroalimentación estructurada, análisis de impacto, riesgos y acciones adelantadas con el ColCERT.
- Entregar la totalidad de la información generada y recolectada, asegurando que permanezca bajo propiedad exclusiva del Ministerio TIC.

6 DESCRIPCIÓN DE LAS LÍNEAS DE DESARROLLO

6.1 Línea de servicios para herramientas de Apoyo y Fortalecimiento de la Gestión del ColCERT

El éxito de la operación depende de herramientas tecnológicas actualizadas y ajustadas a las necesidades cambiantes del entorno.

6.1.1 Actualización de licenciamientos

El proyecto contempla la renovación y gestión de licencias de las soluciones identificadas por ColCERT por un periodo no menor a 12 meses, así como la integración de nuevas funcionalidades que optimicen la prestación del servicio y la infraestructura disponible. Se fortalecerá la colaboración a través de la afiliación al FIRST, fomentando el intercambio de información, la participación en ejercicios globales de ciberseguridad y el acceso a alertas y mejores prácticas internacionales. Se prevé un proceso

sistemático para la actualización de configuraciones, capacitación del personal en el uso de herramientas y mantenimiento preventivo y correctivo, tales como:

- **Cloudflare DNS**

  El servicio de gestión y administración del Sistema de Nombres de Dominio (DNS) para colcert.gov.co reviste una importancia crítica para la correcta publicación y accesibilidad de los servicios del ColCERT en internet. Un DNS gestionado eficientemente garantiza que los usuarios puedan acceder sin problemas a la información, herramientas y recursos que el ColCERT ofrece. Esto implica la configuración precisa de los registros DNS, la monitorización constante para asegurar la resolución adecuada de nombres de dominio y la implementación de medidas de seguridad para proteger contra ataques como el DNS spoofing. En esencia, una administración robusta del DNS es fundamental para la presencia en línea confiable y la operatividad continua de los servicios del ColCERT.

Services:

Services Description	Unit of Measure per Month	Quantity
CDN - Total Data Transfer	TB	2
Foundation DNS - Queries	MM DNS Queries	400
Advanced Certificates Manager - Domains	Zones	35
Foundation DNS - Records	10K DNS Records	100
CDN - Requests	MM Requests	400
Advanced DDoS	TB	Included

Services Description	Unit of Measure per Month	Quantity
Enterprise - Primary - Domains	Zones	5
Enterprise - Secondary - Domains	Zones	35
WAF	TB	Included
Standard Success Offering		Included

- **Sistema Sandbox Trellix Intelligent Sandbox (DoD)**

  La actualización del sistema Sandbox DoD a la última versión de Trellix Intelligent Sandbox (Grant Number: 17971347-NAI) representa un avance significativo para la capacidad del ColCERT de ofrecer servicios de análisis automatizado de malware. Esta modernización optimizará la detección y el análisis de amenazas sofisticadas, proporcionando información crucial a entidades públicas, privadas y a la ciudadanía en general. La continuidad de este servicio automatizado es fundamental para la respuesta proactiva ante incidentes de seguridad y para la mejora continua de la postura defensiva del país.

  Requisitos: Licenciamiento para una base mínima de 250 usuarios donde cada usuario dispone de una capacidad de 20 envíos mensuales para análisis en

Sandbox, garantizando un volumen total de 60,000 procesamientos anuales como requerimiento mínimo.

- **Mailchip (Standard) – Hasta 10.000 Correos electrónicos**

  Una plataforma de automatización de marketing digital, enfocada en el envío masivo de correos electrónicos y campañas de email marketing directamente desde los buzones del CSIRT Gobierno y ColCERT, se constituye como un canal estratégico para la difusión de comunicaciones esenciales. Esta herramienta permitirá la distribución eficiente de piezas informativas cruciales, tales como alertas tempranas, advertencias sobre amenazas, informes técnicos detallados y boletines informativos, emanados principalmente de la línea de análisis situacional. Al utilizar los canales de correo electrónico oficiales del CSIRT Gobierno y ColCERT, se asegura una mayor credibilidad y alcance de la información, facilitando que las entidades públicas y privadas en Colombia estén oportunamente informadas sobre el panorama de ciberseguridad y puedan tomar las acciones preventivas necesarias.

- **Tenable ONE (Web y On-premise):** Es una solución integral que escanea y gestiona vulnerabilidades en los activos tecnológicos, Ayuda a medir de forma continua la ciberpostura, identificando debilidades tanto en la nube, web, DA como en servidores locales, con mínimo 10.000 Unidades.

Category	Qty	Item	Description
New	1	TONE	Tenable One Tenable Vulnerability Management, Tenable Security Center Plus, Tenable Security Center Director, Tenable Identity Exposure, Tenable Cloud Security Standard and Enterprise, Tenable CIEM, Tenable Web App Scanning, OT Security, Attack Surface Management, Lumin Exposure View and Attack Path Analysis. Number of Tenable Web App Scanning has limits based on the actual asset count purchased. Annual Subscription based on number of Assets.
New	1	TOME	Tenable One OT Security Companion License for both Tenable One Standard and Tenable One Enterprise

- **Cisco Umbrella DNS Security Advantage**

Solución de seguridad de capa de red que protege la infraestructura mediante el bloqueo preventivo de dominios maliciosos antes de que se establezca una conexión IP. Su arquitectura permite realizar una investigación profunda de consultas DNS para identificar patrones de tráfico sospechosos, proporcionando visibilidad total sobre las solicitudes de internet realizadas por usuarios locales y remotos. Esta herramienta facilita la revisión exhaustiva del tráfico saliente para detectar exfiltración de datos o comunicaciones con centros de comando y control, garantizando una cobertura ininterrumpida por un periodo mínimo de doce meses bajo un modelo de protección nativa en la nube.

- **VMware (ESXi, vCenter, vSphere):**

Software que permite crear y administrar servidores virtuales, optimizando el uso del hardware físico disponible. Su objetivo es dar flexibilidad y estabilidad a la infraestructura del ColCERT, facilitando el despliegue rápido de nuevos servicios.

- **Solución DFIR – Torre Forense:**

Es un conjunto de herramientas especializadas para la respuesta a incidentes y el análisis forense digital directamente en el lugar de los hechos. Permite recolectar evidencias técnicas de ataques de forma segura y profesional para apoyar procesos judiciales o de investigación.

Torre Forense - Características

Procesador:

- Intel Core i9 (14ª Generación) i9-14900KS Procesador Tetracosa-core (24 núcleos) a 3.20 GHz - 36MB de caché L3 - 32MB de caché L2 Velocidad de overclocking de 6.20 GHz - Socket LGA-1700 - Intel UHD Graphics 770 (Sí, gráficos integrados) - 150 W - 32 hilos

Memoria:

- 192GB (4x48GB) DDR5-6000/PC5-48000 DDR5 SDRAM - Memoria de doble rango - CL32 - 1.35 V - No ECC – No registrada - 288 pines – DIMM

Video:

- Tarjeta gráfica NVIDIA GeForce RTX 4070 SUPER - 12 GB GDDR6X - Resolución de 7680 x 4320 - 1.98 GHz de velocidad base - 2.49 GHz de velocidad de impulso - Ancho de bus de 192 bits - PCI Express 4.0 x16 - 3 x DisplayPort – HDMI

Audio:

- Realtek S1220A 7.1 Surround Sound, Códec de audio de alta definición, 5 jacks de audio

Unidad del Sistema/APP:

- 1TB SSD - M.2 2280 Interna - PCI Express NVMe 4.0 x4 - Velocidad máxima de lectura de 7450MB/s - Cifrado AES de 256 bits

Unidad de caché/temporal:

- 2TB SSD - M.2 2280 Interna - PCI Express NVMe 4.0 x4 - Velocidad máxima de lectura de 7450MB/s - Cifrado AES de 256 bits

Unidad PG/DB:

- 4TB SSD - M.2 2280 Interna - PCI Express NVMe 4.0 x4 - Velocidad máxima de lectura de 7450MB/s - Cifrado AES de 256 bits

RAID:

- Controlador SAS 8i - 12Gb/s SAS, RAID soportado - Niveles RAID 0, 1, 5, 6, 10, 50, 60, JBOD - 1 x SFF-8654 – 8 puertos SAS en total

- **Dispositivos externos de evidencia forense y almacenamiento adicional:**
  - 1x Caja para discos 5.25" - Interfaz de host Serial ATA/600 interna - Bahías intercambiables en caliente - 5 x bahías para discos de 2.5"/3.5"
  - 5x 18TB (RAID-5) HHD - 3.5" Interno - SAS (12Gb/s SAS) - Dispositivo de almacenamiento en arreglo -7200rpm
  - 1x Rack miniSAS de 5.25" a 4x 2.5" SATA SAS 12 Gb/s con intercambio en caliente
  - 1x SSD QVO de 8TB - 2.5" Interno - SATA (SATA/600)
  - 1x SSD EVO de 2TB - 2.5" SATA (SATA/600)
  - 2x Bahías abiertas
  - 1x Cajón de disco duro SATA (vacío) - Bahía de 5.25” - Rack móvil SATA de 3.5” - Rack - Bahía de disco duro extraíble

- **HARDWARE FORENSE:**
  - Óptico: Grabadora triple 16X (DVD/CD/Blu-Ray)
  - Logicube WriteProtect-BAY, bloqueador forense de escritura SAS/SATA/USB3/FW. Conexión host USB 3.0
  - Ace Exclusive Extendable Cooling Bay con Hub USB 3.X integrado y lector de tarjetas micro forense
  - Tarjeta de expansión USB PCIe – Puertos traseros adicionales
  - **Monitor:**
  - 1x Monitor de 34"

Teclado/raton:

- Combo de teclado y ratón inalámbrico, ratón inalámbrico USB RF - Óptico - 3 botones - Rueda de desplazamiento

Sistema operativo:

- Windows 11 Pro de alta gama (Español)

Capacitación:

- Capacitación certificada de 4 horas por el canal o Fabricante

Soporte:

- Soporte y mantenimiento por 12 meses.

- **Licenciamiento MAGNET AXIOM CYBER**

Solución de respuesta a incidentes y análisis forense digital para adquirir y analizar de forma remota evidencia de computadoras, junto con la nube, IoT y dispositivos móviles.

- MÓVIL: Procesamiento y análisis de extracciones de iOS y Android, con integración directa de GrayKey y soporte para herramientas de terceros como UFED, Oxygen y más.
- COMPUTADORA: Recuperación de evidencia de dispositivos Windows, Mac, Chrome y Linux. para análisis de RAM, historial del navegador, los archivos eliminados entre otros.
- NUBE: Adquirir y analizar información depositada en sitios de Internet, a través de las credenciales y claves de acceso encontradas en dispositivos móviles y que están sincronizados con sitios de servicios web de los usuarios propietarios.
- Transferencia de conocimiento: Transferencia de conocimiento por parte del canal o distribuidor por 4 horas.
- **Soporte:**

Soporte y mantenimiento por 12 meses.

6.1.2 Soporte y mantenimiento sistema de videwall RGBlink - Ref: Q16PRO GEN2-8U matriz de 3X6 (Pantalla industrial de 55 pulgadas LG Ref 55VSH7J)

Garantizar la operatividad continua del sistema videowall de 3x6 mediante revisiones técnicas periódicas para prevenir fallos y la corrección inmediata de averías en sus paneles o controladores. Incluye el soporte técnico especializado para la calibración de imagen y la actualización de software y firmware de los procesadores de video para asegurar la compatibilidad con nuevas fuentes de señal. El objetivo es mantener una visualización óptima y sin interrupciones para el monitoreo situacional, optimizando la vida útil de los componentes electrónicos del sistema.

6.1.3 *Monitoreo Continuo, Detección Avanzada y Respuesta Eficiente ante Incidentes de Seguridad*

Para garantizar un esquema de defensa robusto y permanente en las entidades beneficiarias, el proyecto implementará un servicio de monitoreo continuo 24/7 basado en la solución CrowdStrike Falcon® Enterprise. Esta plataforma nativa en la nube unifica en un único agente funciones de antivirus de nueva generación, detección y respuesta extendida, inteligencia de amenazas y cacería gestionada, permitiendo identificar y neutralizar ataques conocidos y desconocidos en tiempo real. Su arquitectura ligera y su capacidad de reconstrucción detallada de incidentes, combinada con análisis contextual e investigación humana especializada, aseguran una respuesta oportuna y una reducción significativa de los tiempos de detección y remediación. Con estas capacidades, el ColCERT podrá centralizar la supervisión de miles de activos territoriales, ejecutando acciones de contención guiada, fortaleciendo la resiliencia institucional y compensando las brechas tecnológicas que actualmente afectan a las entidades públicas, especialmente a aquellas sin infraestructura de seguridad moderna.

- Características técnicas

- Plataforma nativa en la nube que unifica NGAV, EDR, inteligencia de amenazas y cacería gestionada en un único agente ligero, facilitando despliegues rápidos y operación centralizada.
- Antivirus de nueva generación alimentado por IA y machine learning que bloquea malware conocido, desconocido, ransomware, ataques sin archivos y amenazas de Estado-nación en tiempo real.
- Capacidades avanzadas XDR/EDR con captura de eventos sin procesar, visibilidad histórica y reconstrucción detallada de incidentes mediante CrowdScore™ e Incident Workbench.
- Servicio de cacería gestionada 24/7 (Falcon OverWatch) ejecutado por expertos que investigan actividades sigilosas, priorizan amenazas críticas y reducen falsos positivos.
- Control granular de dispositivos USB con políticas avanzadas para evitar fugas de información y refuerzo adicional mediante un firewall de host administrado centralmente.
- Inteligencia integrada que analiza tácticas, técnicas y procedimientos (TTP) de adversarios, apoyada en Threat Graph para correlación histórica y análisis contextual del entorno.
- Agente multiplataforma de mínimo impacto compatible con Windows, macOS, Linux, ChromeOS, iOS y Android, ofreciendo protección online y offline bajo un modelo de actualización continua.
- Capacidades de respuesta remota que permiten contener, investigar y remediar endpoints comprometidos con acciones guiadas desde la plataforma Falcon.

- Visibilidad unificada del entorno con análisis en tiempo real y datos contextualizados que aceleran la toma de decisiones y reducen significativamente MTTD/MTTR.
- Soporte técnico especializado 24/7 provisto por expertos de CrowdStrike, con recursos educativos avanzados para despliegue, operación y optimización continua de la solución.

6.2 Línea de servicios para el proceso de Formación y Generación de Capacidades

La adquisición de licenciamiento de una plataforma tecnológica de formación que será el eje articulador de esta línea. Se optará por una solución avanzada, basada en inteligencia artificial y algoritmos propietarios, que favorezca la predicción de tendencias de formación y la personalización del aprendizaje. La plataforma será parametrizable y escalable, adaptable a los requerimientos inmediatos y futuros del MinTIC, y deberá contemplar como mínimo:

- Retos por áreas técnicas que incluyan: criptografía, forense, explotación web, pentesting, reversing, etc.
- Formatos de competencia Individual, por equipos, por niveles, tiempo limitado o ranking abierto.
- Plataforma 100% web Accesible desde navegador sin instalación.
- Gamificación completa Puntuación automática, rankings, badges y progresión por niveles.
- Integración con formación previa Se puede usar como evaluación después de procesos de entrenamiento.
- Métricas y reportes Análisis detallado por participante, tipo de reto, tiempo de resolución.
- Administración integral de usuarios y perfiles, con autenticación segura y mecanismos eficientes de recuperación y modificación de credenciales.
- Registro de auditoría exportable, detallando ID de usuario, dirección IP de origen, fechas y horas de inscripción, eventos y accesos, permitiendo un seguimiento transparente y sistemático.
- Compatibilidad con dispositivos, navegadores y sistemas operativos diversos, garantizando el acceso equitativo para la totalidad de los beneficiarios.
- Gestión integral de solicitudes y seguimiento personalizado de procesos, a través de un único formulario nacional de inscripción, reportes de inscritos cada 15 días y asistencia activa en la certificación de cada participante.
- Provisión de herramientas de gamificación durante el desarrollo del proyecto, asegurando la realización de retos prácticos.

- Programas de formación con una duración mínima de 40 horas asincrónicas, impartidos por personal docente especializado, para workshop y webinars entregando certificados a quienes culminen cada nivel y garantizando al menos una clase sincrónica obligatoria, grabada y disponible para consulta posterior.
- Enfoque curricular en la práctica, incorporando retos y competencias en entornos simulados y rastreables, evitando contenidos puramente teóricos.

La estrategia de formación y promoción responderá a los objetivos estratégicos del plan sectorial TIC, alcanzando una amplia difusión y adhesión de los públicos objetivo.

6.2.1 Actividades Claves para la ruta de formación

- Diseño e implementación de talleres prácticos, con evaluación de competencias en ciberseguridad, alineados al marco de referencia nacional.
- Desarrollo de talleres asincrónicos obligatorios, grabadas y disponibles para consulta, que contribuyan a la consolidación de capacidades técnicas especializadas.
- Ejecución de estrategias de difusión segmentada, garantizando el acceso y adhesión de públicos objetivo y favoreciendo la apropiación de la cultura de seguridad digital.
- Integración sistemática de elementos institucionales y visuales en todas las plataformas y materiales, asegurando coherencia y reconocimiento público del proyecto y sus objetivos.
- Establecimiento de mecanismos rigurosos para el monitoreo y seguimiento, con generación de informes basados en indicadores de impacto y canales de comunicación eficaces entre aliados, ColCERT y personas beneficiarias.
- Implementación de procesos de retroalimentación y mejora continua, adaptando las intervenciones a las lecciones aprendidas y a los objetivos específicos del documento de Estrategia Nacional de Seguridad Digital.

6.2.2 Meta de formación:

Formar a 5.000 usuarios en competencias tanto básicas de ciberseguridad como especializadas a través de las siguientes líneas:

- Formación Profesionales (Curso de especialista en Ciberseguridad)
- Competencias CTF Ciudadanía, Profesionales y funcionarios

La iniciativa está dirigida a:

Ciudadanos colombianos mayores de edad interesados en desarrollar competencias digitales en ciberseguridad con formación y experiencia básica en infraestructura tecnológica, riesgo y seguridad digital que quieran ampliar sus conocimientos y servidores públicos de entidades nacionales y territoriales, con funciones relacionadas con infraestructura tecnológica y gestión del riesgo digital.

Para la selección de los beneficiarios se tendrá en cuenta, además de lo anteriormente señalado, la fecha y hora de registro para verificación del cumplimiento de los requisitos para su inscripción a la formación hasta llegar al cupo disponible de este contrato.

Los criterios para seleccionar los beneficiarios son: mayor edad; Técnico, tecnólogo u profesional relacionadas con el sector de las TICs. En síntesis, este proyecto impactará de manera integral el ecosistema digital colombiano, incrementando el nivel de preparación y habilidades de líderes de seguridad, profesionales TIC y servidores públicos, fortaleciendo la capacidad de las organizaciones para enfrentar los desafíos del panorama de amenazas cibernéticas en el país.

Lo anterior es de conformidad al cumplimiento a la macrometa institucional en lo relacionado a la formación de personas en seguridad digital.

6.3 Estrategia de Comunicación e Imagen Institucional

Toda acción de comunicación y difusión cumplirá a cabalidad los lineamientos de imagen institucional del MinTIC y ColCERT. El logotipo oficial se integrará en la plataforma de formación y en todas las piezas publicitarias, garantizando la coherencia visual y la adecuada representación del proyecto ante la ciudadanía. La aprobación y ajuste de materiales se concertarán con las autoridades responsables, asegurando la transparencia y alineación a la política institucional.

7 SEGUIMIENTO, EVALUACIÓN Y MEJORAMIENTO CONTINUO

Se establecerán mecanismos rigurosos para el control de calidad y el monitoreo del avance, mediante la generación de informes periódicos, el seguimiento de indicadores clave y la implementación de canales de comunicación efectivos entre aliados, ColCERT y beneficiarios. Se fomentará la retroalimentación constante para la mejora continua, adaptando los procesos a las lecciones aprendidas y evolucionando conforme a los objetivos estratégicos definidos en el plan sectorial TIC.

8 PERFILES PROFESIONALES REQUERIDOS

- *Gerente General del Proyecto – Experiencia mínima: 5 años*

El Gerente General del Proyecto será el responsable de liderar integralmente la ejecución del contrato, garantizando el cumplimiento de los objetivos, hitos, entregables técnicos y administrativos establecidos por el Ministerio TIC y el ColCERT. Este profesional deberá ser ingeniero de sistemas, telecomunicaciones, electrónico o de carreras afines, con estudios complementarios o certificaciones en gestión de proyectos y conocimientos en ciberseguridad. Su trayectoria deberá demostrar al menos cinco años de experiencia en la dirección, implementación y supervisión de proyectos tecnológicos o de seguridad digital, preferiblemente en el sector público.

Dentro de sus funciones se encuentra asegurar la coordinación continua entre el proveedor y el equipo técnico del ColCERT, supervisar la entrega oportuna de licenciamientos, plataformas y servicios asociados al MDR, validar informes técnicos y operativos, y garantizar la correcta ejecución de las actividades previstas en el Anexo Técnico. Será el enlace principal para el seguimiento contractual, la interlocución interinstitucional y la resolución de riesgos o contingencias que puedan afectar el cronograma. Además, deberá velar por la calidad de la documentación entregada, la trazabilidad de los procesos y la estricta adherencia a las políticas de seguridad de la información y tratamiento de datos personales del Ministerio TIC. Con un tiempo de dedicación del 50 %, para el seguimiento de las actividades según las responsabilidades.

- *Líder de Despliegue Tecnológico y Operación de Soluciones – Experiencia mínima: 3 años*

El Líder de Despliegue Tecnológico será el profesional encargado de coordinar y ejecutar las actividades técnicas relacionadas con la instalación, configuración, afinamiento, operación y soporte de los licenciamientos y herramientas adquiridas o renovadas en el marco del proyecto. Este perfil deberá ser ingeniero de sistemas, telecomunicaciones, electrónico o de áreas relacionadas, con conocimientos demostrables en ciberseguridad y experiencia mínima de tres años en la implementación y operación de plataformas de seguridad digital, gestión de vulnerabilidades, infraestructura virtualizada y servicios de monitoreo. Es indispensable que cuente con experiencia específica en la puesta en marcha y seguimiento de soluciones MDR, EDR/XDR o SOC, incluyendo el despliegue de agentes, integración de fuentes de telemetría, creación de tableros y afinamiento de reglas de detección.

El profesional será responsable de asegurar que todas las soluciones entregadas estén correctamente instaladas y operativas dentro de los plazos definidos, incluyendo la

configuración de línea base, la integración con el equipo técnico del ColCERT, el aseguramiento de compatibilidades, la gestión de actualizaciones y la documentación técnica correspondiente. Asimismo, deberá atender requerimientos de soporte especializado, garantizar la correcta recolección de información para análisis, mantener operativos los dashboards de monitoreo, y acompañar la transferencia de conocimiento al equipo del ColCERT, facilitando sesiones prácticas basadas en estándares del fabricante. Con un tiempo de dedicación del 50 %, para el seguimiento de las actividades según las responsabilidades.

- *Líder de Formación, Capacitación y Transferencia de Conocimiento – Experiencia mínima: 3 años*

El Líder de Formación y Transferencia de Conocimiento será el responsable del diseño, adecuación, coordinación y ejecución de los programas de capacitación y certificación previstos en el proyecto, incluyendo cursos virtuales, talleres prácticos, CTF y sesiones especializadas para el personal del ColCERT y las entidades beneficiarias. Este profesional deberá ser ingeniero de sistemas, telemático, informático o de áreas afines, con conocimientos en seguridad digital, pedagogía aplicada a TI o experiencia comprobada en procesos de formación técnica. Se requiere una experiencia mínima de tres años en el diseño, impartición o gestión de proyectos de capacitación relacionados con ciberseguridad, tecnologías de la información o despliegue de herramientas tecnológicas. Con un tiempo de dedicación del 50 %, para el seguimiento de las actividades según las responsabilidades.

9 TRANSFERENCIA DE CONOCIMIENTO DE LICENCIAMIENTOS, HERRAMIENTAS Y SOLUCIONES TECNOLÓGICAS

La transferencia de conocimiento constituye un componente esencial para garantizar la apropiación, sostenibilidad y correcta operación de los licenciamientos, soluciones tecnológicas y herramientas adquiridas en el marco del proyecto. Este proceso deberá ser coordinado directamente con la supervisión designada por el Ministerio TIC/ColCERT, asegurando que los contenidos formativos respondan a las necesidades operativas de la entidad y a las capacidades requeridas para la administración técnica de las plataformas durante toda la vigencia contractual.

El proveedor deberá garantizar que la transferencia de conocimiento sea impartida por personal certificado por el fabricante de cada herramienta o solución, asegurando el cumplimiento de los estándares oficiales y la calidad formativa. Cada paquete de licenciamiento deberá incluir un mínimo de 16 horas de capacitación especializada, distribuidas en sesiones teóricas y prácticas que aborden la instalación, configuración, operación, afinamiento, monitoreo y mejores prácticas del fabricante. Las capacitaciones deberán incluir la entrega de material técnico en español, documentación actualizada,

manuales operativos, guías de referencia rápida y acceso a plataformas de entrenamiento cuando el fabricante así lo permita.

En el desarrollo de la transferencia de conocimiento deberán contemplarse componentes básicos e imprescindibles tales como:

- Arquitectura técnica de la solución y sus principios de funcionamiento.
- Despliegue, configuración inicial y validación de compatibilidad con la infraestructura del Ministerio y las entidades beneficiarias.
- Gestión diaria de la herramienta, interpretación de alertas, buenas prácticas operacionales y lineamientos de administración segura.
- Integración con otros sistemas de monitoreo o gestión de seguridad, cuando aplique.
- Procedimientos para actualización, fortalecimiento, resolución inicial de incidencias y uso adecuado del soporte del fabricante.
- Lineamientos de seguridad, privacidad, tratamiento de información y manejo de registros técnicos derivados del uso de la solución.

La transferencia deberá incluir espacios de demostración funcional, simulación de escenarios de uso real y resolución de dudas técnicas, permitiendo que los equipos técnicos del ColCERT cuenten con capacidades adecuadas para operar las herramientas de manera independiente.

10 SOPORTE TÉCNICO, MANTENIMIENTO Y ACTUALIZACIÓN DE LICENCIAMIENTOS

El servicio de soporte técnico constituye un componente transversal que garantiza la continuidad operativa, estabilidad funcional y aprovechamiento pleno de las soluciones tecnológicas desplegadas durante los doce (12) meses de vigencia del contrato. El proveedor será responsable de proporcionar soporte técnico especializado de primer, segundo y tercer nivel, articulado con el fabricante de cada solución y sujeto a los acuerdos de niveles de servicio establecidos en el Anexo Técnico.

El soporte incluirá actividades de mantenimiento preventivo y correctivo, atención de incidentes, gestión de actualizaciones, aplicación de parches, acompañamiento en ajustes de configuración, análisis de fallas y validación de funcionamiento posterior a cada intervención. Cada licenciamiento entregado deberá acompañarse del servicio de soporte oficial del fabricante, garantizando acceso directo a documentación especializada, bases de conocimiento, actualizaciones, matrices de compatibilidad y gestión de casos técnicos que requieran intervención experta.

El proveedor deberá establecer un plan de escalamiento formal, que contemple los tiempos máximos de respuesta y resolución, los flujos de comunicación entre niveles técnicos y los responsables de cada instancia. Este plan incluirá la interacción directa con el fabricante para la resolución de casos complejos, asegurando que los problemas críticos se escalen

sin demoras y que la supervisión del proyecto disponga de visibilidad total sobre el estado de cada requerimiento.

Asimismo, el proyecto contará con una mesa de servicios dedicada para la recepción, registro, clasificación y seguimiento de incidentes o solicitudes técnicas derivadas del uso de las soluciones adquiridas. Esta mesa deberá operar con disponibilidad acorde al nivel de criticidad de las herramientas (incluyendo atención 24/7 cuando la herramienta lo requiera), registrar cada caso en un sistema de atención con trazabilidad completa y garantizar la generación de reportes periódicos para la supervisión.

Durante la vigencia del contrato, el provvedor deberá asegurar que todas las soluciones, plataformas y licencias se mantengan actualizadas a sus versiones más recientes, incluyendo parches de seguridad, mejoras funcionales y actualizaciones críticas del fabricante. Cualquier actualización deberá ser previamente validada en coordinación con el equipo técnico del ColCERT, confirmando su compatibilidad y evitando interrupciones operacionales.

Finalmente, al término del proyecto, el contratista deberá entregar a la supervisión toda la documentación relacionada con el soporte prestado, los reportes de incidentes atendidos, las actualizaciones aplicadas, los certificados de soporte del fabricante y las recomendaciones para asegurar la continuidad operativa posterior a la finalización del contrato.

11 ACUERDO DE NIVELES DE SERVICIO ANS

11.1 Entrega y activación de licenciamientos

Objetivo. Garantizar continuidad operativa sin brechas de cobertura, entregando licencias a tiempo, con soporte de fabricante y trazabilidad documental.

11.2 Compromisos.

- Entrega y activación de cada licencia hasta 15 días calendario antes del vencimiento previo o dentro del plazo acordado para nuevas adquisiciones; documentación en orden (derecho de uso, versión y soporte vigente). Buenas prácticas exigen plazos claros y remedios ante demoras.
- Soporte del fabricante incluido en cada licencia (nivel estándar o superior) y acceso a actualizaciones durante los 12 meses de vigencia. [crowdstrike.com]

11.3 Métricas.

- Tasa de activación a tiempo ≥ 98% (licencias activas dentro de la ventana comprometida). Basado en prácticas de gestión contractual y control de SLAs (entrega y performance).
- Cumplimiento documental (100% licencias con evidencia de soporte vigente).

Objetivo. Asegurar cobertura ininterrumpida 24/7/365, con detección, análisis y contención guiada.

11.4 Disponibilidad del servicio.

- Uptime de la plataforma ≥ 99,9% mensual para los componentes cloud, excluyendo mantenimientos programados y causas de fuerza mayor, con esquema de créditos por indisponibilidad por debajo del umbral (cuando aplique). Este umbral es consistente con SLAs de SaaS de referencia y compromisos típicos de disponibilidad. [unlimited.humio.com], [odoo.com], [dev.to]

11.5 Métricas operativas MDR/SOC.

- MTTD (Mean Time To Detect): objetivo en minutos para incidentes P1/P2 en horas críticas (p. ej., ≤15 min); la literatura de MDR y operación SOC prioriza MTTD/MTTR como KPI centrales y sitúa expectativas de respuesta en “minutos”, no horas.
- MTTR (Mean Time To Respond/Recover): objetivo ≤4 horas para P1 con acciones de contención guiada y medidas de erradicación inicial; benchmarks de respuesta y resolución se alinean con prácticas ITSM y marcos de incidentes.
- Cacería gestionada 24/7 (Falcon OverWatch) activa con alertamiento y guía de remediación; OverWatch está diseñado para priorizar amenazas críticas y apoyar la contención en coordinación con el equipo del cliente.

11.6 Soporte y atención de casos (prioridades).

- P1 – Crítico (brecha activa, indisponibilidad mayor o propagación rápida): ack 5–15 min, acción inicial ≤60 min, actualizaciones cada 15–30 min.
- P2 – Alto (degradación relevante sin paro total): ack ≤30 min, acción inicial ≤4 h, actualizaciones cada 30–60 min.
- P3 – Medio y P4 – Bajo: respuesta y resolución conforme a matriz ITIL (p. ej., P3 en 1–3 días hábiles; P4 en 3–5 días hábiles), con frecuencia de actualización acorde a impacto/urgencia.

11.7 Mesa de servicios y escalamiento.

- Service Desk 24/7 para registro, clasificación y seguimiento; matriz de escalamiento técnico y jerárquico con tiempos máximos por prioridad (incluye escalamiento al fabricante cuando aplique).

12 CUMPLIMIENTO NORMATIVO Y ALINEACIÓN CON POLÍTICAS DE SEGURIDAD

El proveedor debe alinear sus procesos y procedimientos con las políticas de seguridad y protección de datos del Ministerio TIC, garantizando la confidencialidad, integridad y disponibilidad de la información. El cumplimiento de la normativa vigente y la firma de acuerdos de confidencialidad por parte del personal técnico son actividades críticas para la protección de los datos y la confianza institucional.

(firmado digitalmente)
ANGELA JANETH CORTÉS HÉRNANDEZ
Coordinadora del Git De COLCERT

REGISTRO DE FIRMAS ELECTRONICAS

Anexo Técnico_Ciberseguridad 360

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

Id Acuerdo: 20260128-145531-1de112-71690329

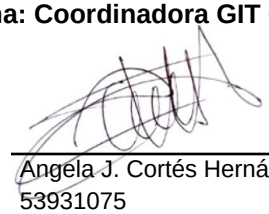
Estado: Finalizado

Creación: 2026-01-28 14:55:31

Finalización: 2026-01-28 15:08:42

Escanee el código para verificación

Firma: Coordinadora GIT ColCERT



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

Ministerio TIC

Elaboración: Abogado GIT ColCERT

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

REPORTE DE TRAZABILIDAD

Anexo Técnico_Ciberseguridad 360

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

Id Acuerdo: 20260128-145531-1de112-71690329
Creación: 2026-01-28 14:55:31
Estado: Finalizado
Finalización: 2026-01-28 15:08:42

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	JAIRO ALEXANDER MARTINEZ MARTINEZ jmartinezm@mintic.gov.co	Aprobado	Env.: 2026-01-28 14:55:37 Lec.: 2026-01-28 14:58:25 Res.: 2026-01-28 14:58:36 IP Res.: 191.95.55.234 Canal: Email
Firma	Angela J. Cortés Hernández acortes@mintic.gov.co Ministerio TIC	Aprobado	Env.: 2026-01-28 14:58:37 Lec.: 2026-01-28 15:08:36 Res.: 2026-01-28 15:08:42 IP Res.: 191.156.234.16 Canal: Email