



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

Contenido

Introducción y Justificación	2
Justificación	¡Error! Marcador no definido.
Objetivos Específicos	3
Entregables	4
1. Línea de servicios para herramientas de Apoyo y Fortalecimiento de la Gestión del ColCERT	4
1.1. Actualización de licenciamientos	4
1.2. Soporte y mantenimiento sistema de videwall matriz de 3X6	11
1.3. Monitoreo Continuo, Detección Avanzada y Respuesta Eficiente ante Incidentes de Seguridad	11
• Implementación de monitoreo continuo y detección avanzada	12
• Gestión proactiva de incidentes y remediación	12
• Soporte técnico y mantenimiento 24/7	13
2. Línea de servicios para el proceso de Formación y Generación de Capacidades	13
2.1. Actividades Claves para la ruta de formación	14
2.2. Meta de formación:	15
3. Estrategia de Comunicación e Imagen Institucional	15
4. Seguimiento, Evaluación y Mejoramiento Continuo	15
5. Cumplimiento normativo y alineación con políticas de seguridad	16



Objeto de contratación: Brindar servicios profesionales para fortalecer la seguridad digital en Colombia, mediante el desarrollo de competencias prácticas, automatización de herramientas especializadas e integración de acciones de la Estrategia Nacional de Seguridad Digital, con el fin de reducir brechas sectoriales y respaldar la transparencia electoral.

Introducción y Justificación

El vertiginoso avance de la transformación digital en instituciones públicas y privadas ha provocado un incremento significativo en la exposición a riesgos cibernéticos. Esta realidad demanda respuestas integrales y coordinadas capaces de garantizar la protección de activos críticos y el desarrollo de talento especializado en seguridad digital. En este contexto, el presente proyecto se plantea como una respuesta estratégica cuyo propósito es elevar los estándares de seguridad digital de las entidades beneficiarias.

Para lograr dicho propósito, la iniciativa promueve la consolidación de servicios de monitoreo, una gestión eficaz de incidentes, la optimización de herramientas tecnológicas y el fortalecimiento de capacidades técnicas avanzadas en el recurso humano. De esta manera, se busca impactar positivamente los activos digitales de las organizaciones, asegurando una adaptabilidad efectiva frente a la diversidad tecnológica presente en los diferentes territorios.

Enfoque Metodológico y Alineación Estratégica

La estructura formal y profesional del proyecto, sustentada en la definición de objetivos específicos, entregables concretos y actividades clave, garantiza una ejecución integral que se encuentra alineada a las mejores prácticas internacionales y nacionales en materia de seguridad digital. La estrategia diseñada responde de forma directa y eficiente a los lineamientos y prioridades de la Estrategia Nacional de Seguridad Digital, lo cual contribuye a asegurar la sostenibilidad de las acciones, el desarrollo continuo de talento especializado y el fortalecimiento institucional, aspectos especialmente relevantes en el marco de los procesos electorales.



Alineación con la Estrategia Nacional y Enfoque en Procesos Electorales

El proyecto mantiene una rigurosa alineación con las directrices establecidas en la Estrategia Nacional de Seguridad Digital, priorizando la protección integral de infraestructuras críticas a través de la implementación de metodologías avanzadas para la gestión de riesgos y la mejora continua de la resiliencia institucional ante amenazas digitales emergentes. En particular, en el contexto de los procesos electorales, la iniciativa incorpora prácticas robustas orientadas a propender por altos estándares de seguridad, transparencia operativa y fortalecimiento de la confianza ciudadana, contribuyendo así al cumplimiento directo de los objetivos definidos por la Estrategia Nacional.

Evaluación, Capacitación y Sostenibilidad

El proyecto contempla la realización de evaluaciones periódicas, la impartición de capacitación especializada y la adopción de tecnologías innovadoras. Estas acciones permiten anticipar y mitigar posibles vulnerabilidades, consolidando un entorno digital seguro y confiable tanto para las instituciones públicas como para el ejercicio democrático. De esta manera, se promueve la sostenibilidad, el desarrollo continuo de capacidades y el fortalecimiento de la confianza en los procesos institucionales y electorales.

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 riesgos durante los procesos electorales en materia de seguridad digital.
- Desarrollar y consolidar capacidades técnicas 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.

Entregables

- Licencias gestionadas y activas para soluciones tecnológicas y herramientas de simulación, con documentación validada conforme a las directrices nacionales. (incluyendo la membresía FIRST)
- Plataforma de vigilancia constante para la detección de amenazas realizando un monitoreo continuo en la modalidad 24/7, por el término de doce (12) meses para por lo menos 800 activos TI.
- Programas de formación certificados, con contenido curricular alineado a competencias prioritarias definidas en la Estrategia Nacional de Seguridad Digital, y registro de participantes graduados por nivel.
- Laboratorios y talleres prácticos en entornos simulados (cyber-range), con informes de resultados y trazabilidad de habilidades desarrolladas.
- Piezas comunicativas y materiales institucionales aprobados bajo los lineamientos del MinTIC y ColCERT, con integración visual y conceptual de la imagen oficial.
- Informes periódicos de seguimiento y resultados, incluyendo análisis de indicadores estratégicos descritos en la Estrategia Nacional, y retroalimentación estructurada de personas beneficiarias y aliados.

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.

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: [REDACTED]) 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.

Category	Qty	# Units	Item	Description
New		1	36,200	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	4,500	TONE-OT
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) HDD - 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 distribuidor

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.

1.2. Soporte y mantenimiento sistema de videowall 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.

1.3. Monitoreo Continuo, Detección Avanzada y Respuesta Eficiente ante Incidentes de Seguridad

Se implementará un servicio robusto de monitoreo continuo (24/7) sobre los activos digitales de las entidades beneficiarias. Este monitoreo no solo detectará amenazas de manera proactiva, sino que habilitará mecanismos de respuesta guiada y remediación integral ante incidentes de seguridad. El sistema abarcará ambientes tecnológicos heterogéneos, garantizando una cobertura total y manteniendo la trazabilidad de eventos. Las capacidades incluirán generación de informes de incidentes, seguimiento de acciones correctivas y actualización constante de procesos frente a nuevas amenazas, promoviendo así una cultura de prevención y resiliencia ante ataques informáticos.

- Implementación de monitoreo continuo y detección avanzada

El proyecto exige la vigilancia constante de los activos digitales de las entidades beneficiarias, utilizando tecnologías como MDR para detectar y responder a amenazas en tiempo real. Esta actividad es esencial para anticipar y contener incidentes de seguridad antes de que generen daños significativos.

Actualmente, las entidades territoriales no solo carecen de soluciones como firewalls, antivirus o procedimientos para parcheo y copias de seguridad, sino que también se encuentran en un punto crítico donde su limitada infraestructura no puede mitigar los riesgos de ciberseguridad por sí sola. Por ello, la implementación de una solución MONITOREO CONTINUO, DETECCIÓN AVANZADA Y RESPUESTA ante incidentes de seguridad digital MDR (Managed Detection and Response) se vuelve indispensable. Este servicio garantiza el monitoreo, la detección y la respuesta oportuna ante incidentes, lo que les permite asegurar la continuidad de sus operaciones y mitigar de manera efectiva las deficiencias que no pueden ser resueltas con la infraestructura actual.

El servicio de MONITOREO CONTINUO, DETECCIÓN AVANZADA Y RESPUESTA A INCIDENTES DE SEGURIDAD DIGITAL – MDR estará destinado a fortalecer la postura de seguridad de las entidades del orden territorial de Colombia, priorizando aquellas que enfrentan mayores desafíos en infraestructura tecnológica. El proyecto se enfocará en las alcaldías clasificadas en las categorías 2 a 6, así como en las entidades que prestan servicios esenciales a nivel territorial, tales como hospitales, empresas de energía, y acueductos, desplegando como mínimo 2000 agentes de MDR, con gestión centralizada en el centro de monitoreo del ColCERT y de manera específica para las entidades vinculadas a la iniciativa de escudo digital.

- Gestión proactiva de incidentes y remediación

Se debe establecer un procedimiento de gestión de incidentes alineado al estándar NIST 800-61 R3, garantizando la contención, erradicación y recuperación de los sistemas comprometidos. La gestión eficiente y oportuna de los incidentes, incluyendo la entrega de informes preliminares y finales, es clave para minimizar el impacto y fortalecer la resiliencia operativa.

- Soporte técnico y mantenimiento 24/7

La continuidad operativa depende de la provisión de soporte técnico y mantenimiento directo por parte del fabricante, bajo la modalidad 24/7. Esto incluye la entrega de protocolos de escalamiento, manuales técnicos y legales, y la actualización constante de las herramientas y plataformas utilizadas.

2. Línea de servicios para el proceso de Formación y Generación de Capacidades

La adquisición e implementación de una plataforma tecnológica de formación 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 simulación durante el desarrollo del proyecto, asegurando la realización de talleres prácticos y laboratorios de simulación (cyber-range).
- Programas de formación con una duración mínima de 40 horas, impartidos por personal docente especializado, 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 ejercicios, laboratorios 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.

2.1. Actividades Claves para la ruta de formación

- Diseño e implementación de talleres prácticos y laboratorios de simulación, con evaluación de competencias en ciberseguridad, alineados al marco de referencia nacional.
- Desarrollo de clases sincrónicas obligatorias, 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.

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 AWARENESS Profesionales
- Competencias CTF Ciudadanía, Profesionales Y Funcionarios

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.

4. 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.



5. 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.