

ANEXO TÉCNICO

1. OBJETO DE CONTRATACIÓN

Prestar servicios tecnológicos especializados para el fortalecimiento de la infraestructura tecnológica del ColCERT, mediante la actualización de licenciamiento especializado en seguridad digital, así como la prestación de servicios técnicos asociados a dicho licenciamiento, incluyendo el monitoreo, detección y respuesta ante incidentes de seguridad digital (MDR), y el soporte y mantenimiento del sistema de videowall, de conformidad con las condiciones y alcances definidos en el Anexo Técnico, en el marco de la ejecución del Componente 1 del contrato interadministrativo suscrito entre la Corporación Agencia Nacional de Gobierno Digital – AND y el Fondo Único de Tecnologías de la Información y las Comunicaciones – FUTIC.

2. INTRODUCCIÓN Y JUSTIFICACIÓN

En el marco de la iniciativa Ciberseguridad 360 y en cumplimiento del Contrato Interadministrativo 1217-2026 suscrito entre la AND y el FUTIC, el presente Anexo Técnico define el alcance del Componente 1, orientado exclusivamente al fortalecimiento de la infraestructura tecnológica del ColCERT, mediante la renovación de licenciamiento especializado, la operación de servicios avanzados de monitoreo y respuesta (MDR) y el soporte de plataformas críticas.

El contexto electoral 2026, así como el incremento sostenido de amenazas cibernéticas dirigidas contra infraestructura estatal, exige la actualización y ampliación de las capacidades tecnológicas del ColCERT, garantizando continuidad operativa, resiliencia y protección efectiva de activos estratégicos.

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 a través de entre otros aspectos 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 tiene el 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.

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 la modernización de infraestructuras tecnológicas. El alcance del proyecto contempla la identificación de posibles riesgos, la reducción de vulnerabilidades.

Fortalecimiento de la Infraestructura Tecnológica

La protección de infraestructuras críticas es 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.

4. OBJETIVOS ESPECIFICOS

- 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.

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. Cada entregable integra actividades de licenciamiento, soporte, despliegue 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. 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 DEL ALCANCE DE LA CONTRATACIÓN

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.

C.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 Tetracore (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 pVO 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.

C.1.2 *Soporte y mantenimiento sistema de videowall RGBlink - Ref: Q1CPRO GEN2-8U matriz de 3XC (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.

C.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.

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 proveedor 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

Entrega y activación de licenciamientos

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

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]

Métricas.

- Tasa de activación a tiempo $\geq 98\%$ (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.

Disponibilidad del servicio.

- Uptime de la plataforma $\geq 99,9\%$ 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]

Métricas operativas MDR/SOC.

- MTDD (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 MTDD/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.

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.

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.



JULIO ERNESTO ECHAVARRÍA POVEDA

**Subdirector de Desarrollo y Servicios Ciudadanos Digitales AGENCIA
NACIONAL DIGITAL**

Elaboró: David Leonardo Medina. – Contratista – Subdirección de Desarrollo Y SCD

Revisó componente Jurídico: Christian Santiago Guzmán López. Contratista
Subdirección Jurídica.