Contenido

OBJETO

Adquirir la renovación de la suscripción y el servicio gestionado de administración de una herramienta de seguridad cibernética de última generación, basada en Inteligencia Artificial (IA), que permita al MINTIC/FONTIC detectar, administrar y responder a amenazas en tiempo real.

ABREVIATURAS Y DEFINICIONES

A continuación, se enuncian algunas abreviaturas y definiciones, las cuales se utilizarán en los anexos técnicos y son la representación escrita de una palabra con una o varias de sus letras:

ABREVIATURAS

- MINTIC: Ministerios de Tecnologías de la Información y las Comunicaciones
- OTI: Oficina de Tecnología de la Información.
- GD: Gobierno Digital.
- PEI: Plan Estratégico Institucional
- PETI: Plan Estratégico de Tecnologías de la Información y las Comunicaciones.
- TI: Tecnologías de la Información.
- TIC: Tecnologías de la Información y Comunicación.
- SI: Sistemas de Información
- DDos: (Distributed Denial of Service): es un tipo de ataque cibernético en el que múltiples dispositivos comprometidos se utilizan para inundar un servidor o una red con tráfico malintencionado, lo que resulta en la interrupción o la denegación de servicio para los usuarios legítimos.
- SOC (Security Operations Center): Security Operations Center es una instalación que centraliza la monitorización y gestión de la seguridad de la información de una organización.
- NOC (Network Operations Center): Centro de Operaciones de Red. Un NOC es una instalación que centraliza la monitorización, gestión y mantenimiento de la red de una organización.
- SIEM: Security Information and Event Manager:es una solución de seguridad que combina la funcionalidad de dos tipos de herramientas de seguridad: la gestión de eventos de seguridad (SEM) y la gestión de información de seguridad (SIM).
- VPN: significa "Virtual Private Network" (Red Privada Virtual, en español) y se refiere a una tecnología de red que permite crear una conexión segura y privada a través de una red pública como Internet.
- DMZ significa "zona desmilitarizada" (del inglés "demilitarized zone"). Se refiere a una red intermedia que se encuentra entre la red interna de una organización y la red externa (generalmente Internet),

y que se utiliza para alojar servicios y recursos que deben estar disponibles para el público en general, pero que deben estar protegidos de los posibles ataques externos.

DEFINICIONES

Activo: Cualquier cosa que tiene valor para la organización (datos, servidores, dispositivos).

Evento: Cualquier suceso que se produce en un sistema o red informática y que puede ser registrado o monitoreado.

Incidente de Seguridad: Evento no planificado que involucra la pérdida, alteración o destrucción de información o sistemas.

Vulnerabilidad: Debilidad o defecto en un sistema que puede ser explotado por un atacante.

Blue Team: Grupo de profesionales que trabajan en la defensa, prevención y detección de ataques

Red Team: Profesionales que simulan ataques para evaluar la efectividad de las defensas

Seguridad de la Información: Prácticas para proteger la Confidencialidad, Integridad y Disponibilidad de los datos.

Virtual Appliance: Solución de software preconfigurada que se ejecuta en un entorno de virtualización (forma común de entrega de Darktrace).

On-Premise / Nube: Define si la infraestructura está en las instalaciones físicas de la entidad o en un proveedor externo.

Plataforma SIEM: Tecnología para gestionar eventos de seguridad donde Darktrace suele enviar sus alertas.

Seguridad Perimetral: Medidas para proteger la red desde el exterior (donde Darktrace actúa como sensor).

Inteligencia Artificial (IA) y Aprendizaje Automático (ML): Capacidad de la herramienta para aprender el comportamiento normal de la red y detectar anomalías sin reglas previas.

Análisis de Riesgo: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Medidas Preventivas y Correctivas: Acciones para evitar incidentes o remediar problemas ya identificados.

2. OBJETIVOS GENERALES Y ESPECÍFICOS

2.1 OBJETIVOS GENERALES

El MINTIC/FONTIC requiere contratar una solución integral de seguridad cibernética que combine una herramienta de última generación con un modelo de servicio gestionado. Lo anterior, bajo las condiciones técnicas, económicas y financieras definidas por la entidad en el presente documento. En este contexto, los objetivos son:

- **Fortalecimiento de la Postura de Seguridad**: Actualizar la herramienta basada en Inteligencia Artificial (IA) y Aprendizaje Automático (ML) que permita proteger la infraestructura y los activos críticos de la entidad contra amenazas avanzadas como malware, ransomware, phishing, ataques de denegación de servicio (DDoS) y amenazas internas.

- **Gestión y Administración Delegada**: Garantizar que la plataforma sea administrada técnica y operativamente por el proveedor, quien será responsable del afinamiento constante de la solución, el monitoreo proactivo y la respuesta ante incidentes detectados.

- **Visibilidad y Alertamiento en Tiempo Real**: Lograr una visibilidad total del tráfico de red y el comportamiento de los usuarios, asegurando que el proveedor suministre alertamientos inmediatos y precisos que permitan minimizar el impacto de cualquier anomalía en las operaciones de la entidad.

- **Inteligencia de Datos y Reportes**: Asegurar la entrega periódica de informes de gestión, análisis de amenazas y reportes bajo demanda que faciliten la toma de decisiones estratégicas por parte de la OTI y la supervisión del contrato.

- **Cumplimiento y Confianza Institucional**: Alinear la operación tecnológica con los marcos de seguridad digital vigentes, garantizando la confidencialidad, integridad y disponibilidad de la información de los ciudadanos y las partes interesadas, apoyando así la transformación digital segura del país.

- **Mitigación de Impacto Operativo**: Reducir el riesgo de interrupciones del servicio y pérdidas reputacionales mediante una detección temprana y una capacidad de respuesta técnica coordinada entre el proveedor y la entidad.

2.2 OBJETIVOS ESPECÍFICOS

2.2.1. Detección y protección avanzada mediante Inteligencia Artificial (IA):

- Asegurar que el proveedor realice el afinamiento constante de los modelos de IA para minimizar falsos positivos y maximizar la detección de anomalías críticas.

2.2.2. Visibilidad 360° y análisis proactivo de la red:

- Proporcionar visibilidad completa de la actividad en la red institucional, incluyendo tráfico interno (este-oeste), perímetros, entornos de nube y aplicaciones críticas.

- El proveedor deberá realizar un análisis continuo de los patrones detectados para identificar vectores de ataque antes de que se materialicen, suministrando inteligencia accionable a la OTI.

2.2.3. Respuesta autónoma y contención administrada:

- Habilitar capacidades de respuesta autónoma que permitan neutralizar ataques de forma quirúrgica y en tiempo real, sin interrumpir las operaciones normales del negocio.

- El proveedor será responsable de configurar y supervisar los umbrales de respuesta automatizada (ej. cuarentena de dispositivos o bloqueo de conexiones maliciosas), informando de inmediato a la supervisión o a quien este designe sobre las acciones tomadas.

2.2.4. Gestión integral, alertamiento y reportes:

- Establecer un esquema de administración delegado donde el proveedor gestione la plataforma de monitoreo 7x24x365 y suministre alertas tempranas ante cualquier incidente.

- Garantizar la entrega de reportes mensuales de gestión y reportes técnicos bajo demanda que incluyan el estado de la postura de seguridad, hallazgos relevantes y recomendaciones de mejora.

2.2.5. Cumplimiento normativo y estándares de seguridad:

- Asegurar que la operación de la herramienta apoye el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, la Ley 1581 de 2012 (Protección de Datos Personales) y los controles de la norma ISO/IEC 27001:2022.

- Proporcionar las evidencias técnicas necesarias para los procesos de auditoría y cumplimiento normativo que adelante la entidad.

2.2.6. Transferencia de conocimiento y soporte especializado:

- El proveedor deberá ejecutar sesiones de transferencia de conocimiento para el personal técnico del MINTIC/FONTIC sobre las capacidades de la herramienta y los hallazgos en la infraestructura.

- Garantizar soporte técnico de nivel superior con tiempos de respuesta definidos (SLA), acceso a portales de soporte y asistencia directa de ingenieros certificados.

2.3 OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

2.3.1. Suministro, Instalación y Puesta en Marcha:

- El contratista deberá suministrar las suscripciones y/o licencias de la actualización de la herramienta de seguridad cibernética solicitada, junto con los componentes lógicos (Virtual Appliances) necesarios para su correcto funcionamiento en los entornos de red, nube o centros de datos del MINTIC/FONTIC.

- Entregar la documentación técnica actualizada, que incluya manuales de configuración, diagramas de arquitectura lógica de la solución implementada y protocolos de administración.

2.3.3. Servicio Gestionado de Administración y Operación:

- Administración Integral: El contratista será el responsable directo de la gestión técnica de la plataforma, incluyendo el afinamiento continuo de algoritmos de detección, creación de políticas de exclusión y mantenimiento preventivo.

- Monitoreo y Alertamiento 7x24x365: Garantizar un esquema de monitoreo constante (24 horas al día, 7 días a la semana). Ante cualquier anomalía crítica, el contratista deberá notificar de forma inmediata a través de los canales oficiales establecidos (correo, ticket o mensajería institucional).

- Análisis Táctico de Incidentes: Suministrar un análisis preliminar por cada incidente de alta criticidad, detallando el vector de ataque, dispositivos afectados, impacto potencial y la ruta sugerida de remediación.

2.3.4. Mantenimiento, Actualización y Soporte Técnico:

- Realizar el mantenimiento correctivo y preventivo de los componentes lógicos y firmas de la solución, asegurando que la herramienta opere siempre en su versión más estable y segura.

- Proporcionar soporte técnico especializado de nivel superior, garantizando tiempos de respuesta (SLA) para la resolución de fallos técnicos o dudas en la operación de la herramienta.

2.3.5. Respuesta Coordinada a Incidentes de Seguridad:

- Colaborar activamente con el Equipo o personal de la OTI en la investigación de la causa raíz de eventos de seguridad detectados por la herramienta.

- Asistir técnicamente en la ejecución de medidas de contención (aislamiento de dispositivos, bloqueo de conexiones) y en la implementación de acciones correctivas para evitar la recurrencia de incidentes.

2.3.6. Entregables de Gestión y Reportes:

- Generar y sustentar informes mensuales de gestión que resuman el estado de la postura de seguridad, las amenazas neutralizadas y las recomendaciones de robustecimiento.

- Entregar informes técnicos específicos bajo demanda cuando el supervisor del contrato o quien este designe lo requiera, en los plazos estipulados.

2.3.7. Cumplimiento Normativo y Estándares de Ciberseguridad:

- Garantizar que la operación de la herramienta y el tratamiento de los datos recolectados cumplan con la Ley 1581 de 2012 (Protección de Datos Personales), el Modelo de Seguridad y Privacidad de la Información (MSPI) y los controles aplicables de la norma ISO/IEC 27001:2022.

- Suministrar las evidencias y logs necesarios para soportar procesos de auditoría interna o externa que se realicen sobre la infraestructura del MINTIC/FONTIC.

2.3.8. Confidencialidad y Protección de la Información:

- Suscribir y dar cumplimiento estricto a los acuerdos de confidencialidad de la entidad, manteniendo reserva total sobre la arquitectura de red, vulnerabilidades halladas y cualquier dato sensible procesado por la herramienta durante la ejecución del contrato.

3. DESCRIPCIÓN DE LAS CAPACIDADES DE LA HERRAMIENTA Y DEL SERVICIO

3.1. Análisis de Comportamiento (Self-Learning):

- La herramienta debe realizar un análisis profundo y continuo del comportamiento de usuarios, aplicaciones y dispositivos en la red del MINTIC/FONTIC para establecer perfiles de base (Línea base de comportamiento).
- Debe ser capaz de detectar desviaciones sutiles en estos perfiles (anomalías) que puedan indicar amenazas desconocidas, movimientos laterales o ataques de día cero, sin depender exclusivamente de firmas o reglas predefinidas.

3.2. Visibilidad en Tráfico Cifrado y Ofuscado:

- La herramienta debe analizar tráfico cifrado para detectar patrones maliciosos sin necesidad de realizar procesos de ruptura de cifrado (decryption) que afecten la privacidad, utilizando análisis de metadatos y patrones de tráfico.
- Debe identificar amenazas que utilicen técnicas de ofuscación o canales de comunicación no convencionales para evadir controles perimetrales.

3.3. Respuesta Autónoma y Contención en Tiempo Real:

- La herramienta ejecutará actividades de respuesta autónoma (Antigena) para neutralizar ataques en su fase inicial, como ransomware o exfiltración de datos, operando de manera quirúrgica para no afectar la disponibilidad del negocio.
- Debe generar el aislamiento de endpoints comprometidos, bloqueo de conexiones maliciosas y contención de movimientos laterales de manera automática o bajo aprobación del administrador.

3.4. Investigación Forense y Análisis de Causa Raíz:

- Proporcionar una línea de tiempo detallada (Forensic Loop) de los eventos antes, durante y después de un incidente, permitiendo reconstruir la actividad de la red para determinar la causa raíz.

3.5. Integración y Visibilidad Unificada:

- Integración bidireccional con la infraestructura actual de la entidad (Firewalls, SIEM, EDR, Directorio Activo) para enriquecer el contexto de las alertas y coordinar acciones de respuesta.
- Envío de logs en formatos estándar (Syslog, JSON, etc.) para su correlación en el centro de monitoreo principal SOC.

3.6. Cumplimiento con el Marco de Seguridad Digital:

- Generación de reportes técnicos de cumplimiento que sirvan como evidencia ante auditorías sobre la efectividad de los controles de detección y respuesta implementados.

3.8. Seguridad de los Datos y Privacidad:

- Generación del cifrado de los datos recolectados tanto en tránsito como en reposo.

- El proveedor debe asegurar que la recolección de metadatos para el análisis de IA se realice bajo los principios de la Ley 1581 de 2012 de Protección de Datos Personales.

4. SISTEMA DE CORRELACIÓN E INTEROPERABILIDAD TÉCNICA

Para maximizar la efectividad de la detección y respuesta, la herramienta deberá mantener la integración y correlación de eventos de manera bidireccional con el ecosistema tecnológico actual de la entidad. El contratista será responsable de asegurar las siguientes integraciones:

4.1. Con el Centro de Operaciones de Seguridad (SOC):

- Ingesta de Eventos: Envío de alertas y logs enriquecidos al SIEM institucional o a la plataforma que disponga el SOC, utilizando formatos estándar (Syslog, JSON, API).

- Notificación Inmediata: Configuración de flujos de notificación automática para que el equipo del SOC reciba alertas de criticidad alta o media en tiempo real.

- Contexto para Investigación Forense: Incluir los metadatos detallados de red que permitan a los analistas del SOC reconstruir ataques y determinar el "Paciente Cero" de un incidente.

4.2. Con el Centro de Operaciones de Red (NOC):

- Visibilidad del Tráfico: Proporcionar al NOC una vista granular del consumo de ancho de banda y flujos de red anómalos que puedan afectar la disponibilidad de los servicios.

- Correlación de Fallas vs. Ataques: Ayudar al NOC a diferenciar entre un problema de rendimiento de red y un incidente de seguridad (como un ataque DDoS o exfiltración masiva).

4.3. Con la Seguridad Perimetral (Firewalls / IPS):

- Bloqueo Coordinado: Exportación de indicadores de compromiso (IoC), como direcciones IP maliciosas, para que puedan ser bloqueadas de forma manual o automática en los Firewalls perimetrales.
- Análisis de Tráfico Norte-Sur: Correlacionar los intentos de intrusión detectados en el perímetro con los movimientos internos (Este-Oeste) identificados por la IA.

4.4. Con el Ecosistema Microsoft Azure y Office 365:

- Protección de Cargas de Trabajo en la Nube: Integración con los entornos de Azure para monitorear el tráfico de máquinas virtuales, contenedores y servicios PaaS.
- Sincronización con Microsoft Defender: Capacidad de compartir alertas con Microsoft Defender for Cloud y Microsoft Defender for Endpoint para tener una visión unificada de la seguridad entre la red y los dispositivos finales.
- Monitoreo de Identidad: Correlación de anomalías de red con eventos de inicio de sesión sospechosos en Azure Active Directory (Entra ID).

4.5. Con Soluciones de Antivirus / EDR:

- Complementariedad en Detección: detección con comportamientos maliciosos que el antivirus tradicional pueda omitir (como ataques "fileless" o uso de herramientas legítimas con fines maliciosos).
- Confirmación de Amenazas: Correlacionar una detección de red (ej. conexión a un servidor C2) con una alerta en el endpoint para priorizar la respuesta.

5. REQUERIMIENTOS OPERATIVOS DEL SERVICIO

5.1. Desempeño y Disponibilidad:

- Procesamiento en Tiempo Real: procesar y analizar grandes volúmenes de datos y metadatos de red en tiempo real, sin introducir latencia ni afectar el rendimiento de la red troncal o las aplicaciones críticas de la entidad.

- Alta Disponibilidad (HA): La solución (tanto sensores como consola de gestión) debe garantizar una disponibilidad del 99.9%, asegurando que el monitoreo sea ininterrumpido.

- Escalabilidad Elástica: La arquitectura debe permitir el crecimiento en el número de dispositivos monitoreados y el aumento del ancho de banda (throughput) mediante licencias o nodos adicionales, según las necesidades del MINTIC/FONTIC.

5.2. Interfaz y Experiencia de Usuario (UX):

- Visualización Avanzada: Consola centralizada de administración basada en web, con dashboards intuitivos que permitan visualizar en tiempo real las amenazas y el mapa de relaciones de la red.

- Accesibilidad: Compatible con los navegadores web modernos y permitir el acceso seguro mediante protocolos cifrados y autenticación multifactor (MFA).

5.3. Interoperabilidad y Estándares:

- Conectividad API: Expocisión de APIs (RESTful o similares) para permitir la automatización de tareas y la integración con el ecosistema de seguridad del MINTIC (SOC, NOC, Azure, Antivirus).

- Adopción de Estándares: Compatibilidad con estándares de la industria para el intercambio de inteligencia de amenazas, tales como formato STIX/TAXII, Syslog, JSON y capacidad de integración con soluciones SIEM.

5.4. Soporte Técnico y Garantía del Servicio:

- Soporte Especializado 7x24x365: El proveedor debe garantizar soporte técnico de nivel superior con disponibilidad total (24/7/365). Se deben definir niveles de servicio (SLA) para la atención de incidentes técnicos según su severidad (Crítica, Alta, Media, Baja).

- Actualización Continua: El contratista es responsable de mantener la herramienta actualizada con las últimas versiones de software, firmware y modelos de aprendizaje de IA, sin costo adicional para la entidad durante la vigencia del contrato.

- Consultoría de Valor: El proveedor debe incluir sesiones trimestrales de revisión técnica para optimizar las políticas de detección y respuesta basadas en el comportamiento real de la red.

5.5. Seguridad y Privacidad de la Información:

- Cifrado de Datos: Todos los datos recolectados deben ser cifrados en tránsito (TLS 1.2 o superior) y en reposo (AES-256 o superior).

- Soberanía de Datos: El proveedor debe garantizar que el tratamiento de la información se realice bajo los lineamientos de la Ley 1581 de 2012, asegurando que los datos de la entidad no sean utilizados para fines distintos a los del objeto contractual.

5.6. Modelo de Suscripción y Licenciamiento:

- Licenciamiento Integral: El modelo de suscripción debe cubrir la totalidad de las capacidades técnicas solicitadas (IA, Respuesta Autónoma, Visibilidad de Nube) durante la vigencia estipulada.

- Transparencia: El oferente debe detallar claramente los límites de su licencia (por ejemplo, número de dispositivos, ancho de banda o usuarios) para evitar sobrecostos por crecimiento orgánico de la red durante la ejecución del contrato.

5.7 Acuerdos de Niveles de Servicio (SLA):

El contratista deberá garantizar el cumplimiento de los siguientes niveles de servicio para la atención de incidentes técnicos y de seguridad asociados a la operación de la solución:

Severidad	Descripción	Tiempo de Respuesta	Tiempo de Solución
Crítica	Incidentes que comprometan la disponibilidad o seguridad de activos críticos	≤ 15 minutos	≤ 4 horas
Alta	Incidentes con impacto significativo, pero sin interrupción total	≤ 30 minutos	≤ 8 horas
Media	Incidentes con impacto moderado	≤ 2 horas	≤ 24 horas
Baja	Incidentes de bajo impacto o consultas técnicas	≤ 4 horas	≤ 72 horas

Nota 1: El incumplimiento de los SLA podrá dar lugar a la aplicación de penalidades contractuales conforme a lo establecido por la entidad.

Nota 2: El contratista deberá entregar reportes mensuales de cumplimiento de SLA.

6. ARQUITECTURA DE LA SOLUCIÓN DE SEGURIDAD CIBERNÉTICA

6.1. Flexibilidad de Despliegue (Híbrido):

- Modelo de Implementación: La arquitectura debe permitir un despliegue flexible que se adapte a entornos On-Premise, Nube (Azure) y entornos híbridos, mediante el uso de sensores físicos o virtuales (Virtual Appliances).

- Visibilidad Unificada: Independientemente del tipo de despliegue, la arquitectura debe garantizar que la consola de gestión centralice la visibilidad de todos los entornos sin fragmentación de la información.

6.2. Escalabilidad Arquitectónica:

- Crecimiento Horizontal y Vertical: Capacidad de crecimiento horizontal (añadiendo más sensores para nuevos segmentos de red) y vertical (incrementando la capacidad de procesamiento de los nodos existentes) para absorber el aumento de tráfico o dispositivos en el MINTIC/FONTIC.

- Optimización de Recursos: El diseño arquitectónico de los sensores debe ser de "cero impacto" o "pasivo" (vía puerto SPAN o Mirror), asegurando que la recolección de datos no interfiera con el rendimiento de los dispositivos de red activos.

6.3. Estrategia de Recopilación de Datos:

- Ingesta Multi-fuente: La arquitectura debe estar diseñada para ingerir metadatos de red, logs de eventos, datos de tráfico en la nube (vía APIs o VPC Flow Logs) y eventos de identidad, proporcionando una visión holística del comportamiento digital de la entidad.

- Procesamiento en el "Edge": Los sensores deben ser capaces de realizar un análisis preliminar de los datos en el punto de captura para optimizar el ancho de banda hacia la consola central y permitir una detección en tiempo real.

6.4. Motor de Análisis Basado en IA:

- Núcleo de Aprendizaje No Supervisado: La arquitectura integra un motor de IA que utilice aprendizaje no supervisado para crear modelos de comportamiento (Línea Base) únicos para cada usuario y dispositivo de la entidad.
- Clasificación de Amenazas: El sistema clasifica automáticamente las anomalías detectadas según su nivel de criticidad y confianza, facilitando la priorización para el equipo de operación.

6.5. Componentes de Respuesta e Investigación:

- Módulos de Respuesta Autónoma: La arquitectura debe incluir componentes lógicos que permitan ejecutar acciones de respuesta inmediata (contención) directamente en la red o integrándose con los firewalls y el Directorio Activo.
- Repositorio de Análisis Forense: Cuenta con un almacenamiento seguro y estructurado de la telemetría de red que permita realizar investigaciones retroactivas sobre incidentes pasados.

6.6. Interoperabilidad y Conectividad:

- Ecosistema Abierto (APIs): La solución debe basarse en una arquitectura de API abierta (REST/JSON) que facilite el intercambio de información con otras plataformas de la OTI.
- Sincronización de Inteligencia: Compatibilidad nativa con protocolos estándar de la industria (STIX/TAXII, Syslog enriquecido) para la exportación de indicadores de compromiso y alertas hacia el SIEM institucional.

6.7. Seguridad de la Infraestructura de la Herramienta:

- Hardening y Cifrado: Todos los componentes de la arquitectura deben seguir prácticas de endurecimiento (hardening) de sistemas. Las comunicaciones entre sensores y consola deben estar protegidas mediante protocolos TLS 1.2 o superior.
- Control de Acceso Robusto: La arquitectura debe soportar la integración con servicios de identidad (LDAP/Azure AD) y permitir el control de acceso basado en roles (RBAC) con autenticación multifactor (MFA).

6.8. Alineación con Principios de Zero Trust:

- La solución deberá alinearse con los principios de arquitectura de seguridad Zero Trust, asegurando la verificación continua de usuarios, dispositivos y flujos de comunicación, así como la minimización de la confianza implícita dentro de la red.

7. GESTIÓN DE LOGS Y TELEMETRÍA DE LA SOLUCIÓN

7.1. Capacidades de Recopilación de Logs:

- Fuentes de Datos: Capacidad técnica de recolectar e integrar logs provenientes de diversas fuentes, incluyendo tráfico de red (metadatos), eventos de endpoints, registros de aplicaciones críticas, servicios en la nube (Azure/M365) y dispositivos de seguridad perimetral.
- Formatos Estándar: Soporte de forma nativa la ingesta y envío de logs en formatos estándar de la industria como Syslog (RFC 5424), JSON, CEF y LEEF, garantizando la compatibilidad con el ecosistema actual de la entidad.
- Procesamiento Continuo: La recopilación debe realizarse de manera continua y en tiempo real, asegurando que no existan brechas temporales en la visibilidad de la seguridad.

7.2. Almacenamiento y Retención Segura:

- Esquema de Almacenamiento: El contratista debe proveer una arquitectura de almacenamiento (local o en nube) que garantice la integridad y disponibilidad de los logs recolectados, evitando la pérdida de datos ante fallos de conexión.
- Periodo de Retención: La herramienta debe permitir la retención de logs y telemetría de red por un periodo mínimo de especificar tiempo, ej. 90 días en caliente para análisis inmediato, y opciones de archivado para cumplimiento normativo a largo plazo.
- Seguridad de los Registros: Se debe garantizar la inmutabilidad de los logs almacenados para evitar alteraciones, utilizando técnicas de cifrado y controles de acceso estrictos para asegurar la cadena de custodia de la información.

7.3. Análisis Avanzado y Correlación:

- Motor de Correlación en Tiempo Real: La herramienta debe analizar los grandes volúmenes de logs mediante algoritmos de IA para identificar patrones anómalos, ataques de fuerza bruta, movimientos laterales y comunicaciones con centros de comando y control (C2).
- Enriquecimiento de Alertas: Cada evento detectado debe estar enriquecido con contexto (direcciones IP, nombres de usuario, protocolos involucrados y severidad) para facilitar la labor de triaje del equipo de seguridad.

7.4. Interfaz de Visualización y Explotación de Datos:

- Consola de Gestión de Eventos: Proporcionar una interfaz web intuitiva que permita la búsqueda avanzada de logs mediante filtros dinámicos (por fecha, tipo de evento, gravedad, origen y destino).
- Dashboards Ejecutivos y Técnicos: Tableros de control que resuman el comportamiento de los logs y destaquen las alertas más críticas que requieran atención inmediata del administrador.

7.5. Integración con Ecosistema de Seguridad (SIEM/SOC):

- Interoperabilidad con SIEM: integración con la solución SIEM institucional del MINTIC/FONTIC, permitiendo el reenvío de alertas categorizadas para una gestión centralizada.
- Orquestación: La gestión de logs debe permitir la integración con herramientas de respuesta (SOAR) o firewalls para facilitar acciones de contención basadas en los hallazgos de los registros.

7.6. Soporte Técnico y Transferencia de Conocimiento:

- Documentación Técnica: El contratista debe entregar la documentación detallada sobre la estructura de los logs, diccionarios de datos y procedimientos de exportación.
- Capacitación Operativa: Incluir sesiones de transferencia de conocimiento para el personal de la OTI sobre la explotación de los logs, creación de reportes personalizados y mantenimiento del sistema de almacenamiento.

8. REPORTES Y ENTREGABLES DE GESTIÓN

El contratista deberá suministrar reportes periódicos y bajo demanda que permitan a la OTI y a los niveles ejecutivos del MINTIC/FONTIC analizar la postura de seguridad, la efectividad de la detección y el estado de salud de la solución. Los reportes se dividen en dos categorías principales:

8.1. Reportes Técnicos y Operativos:

- Reporte de Detección de Amenazas y Anomalías: Detalle pormenorizado de los incidentes detectados por la IA, incluyendo vectores de ataque, severidad (score), dispositivos/usuarios afectados y acciones de respuesta (autónomas o manuales) ejecutadas.

- Reporte de Higiene y Vulnerabilidades de Red: Informe sobre activos críticos con comportamientos riesgosos, protocolos inseguros detectados en la red y vulnerabilidades identificadas de acuerdo con el análisis de tráfico.

- Reporte de Cumplimiento (Compliance): Evaluación automatizada del estado de los controles de seguridad alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27001:2022.

- Reporte de Salud de la Plataforma: Estado de funcionamiento de los sensores, sondas y consolas, asegurando que el monitoreo se realiza sobre el 100% del alcance definido.

8.2. Reportes Ejecutivos de Gestión:

- Resumen Ejecutivo Mensual: Visión de alto nivel sobre la postura de seguridad de la entidad, destacando los riesgos mitigados más significativos y la evolución de la superficie de ataque.

- Análisis de Tendencias y Patrones: Gráficas comparativas que permitan identificar si las amenazas están aumentando, disminuyendo o cambiando de naturaleza a lo largo del tiempo.

- Indicadores de Gestión (KPIs): El contratista debe incluir métricas de valor como:

  - Número de alertas críticas detectadas vs. atendidas.

  - Tiempo promedio de respuesta y contención.

- Ahorro estimado en impacto operativo gracias a la detección temprana.

- Plan de Acción y Recomendaciones: Cada reporte mensual debe finalizar con una sección de recomendaciones tácticas y estratégicas sugeridas por el proveedor para robustecer la infraestructura de la entidad.

8.3. Características Técnicas de los Reportes:

- Automatización y Programación: Los informes deben poder programarse para envío automático a los correos institucionales definidos por la supervisión (diario, semanal o mensual).

- Personalización (Dashboards): La herramienta debe permitir la creación de tableros de control personalizados según las necesidades específicas de la OTI.

- Formatos de Exportación: Toda la información debe ser exportable en formatos editables y de presentación (PDF, Excel, CSV, JSON) para facilitar auditorías y análisis posteriores.

- Visualización de Datos: Uso obligatorio de elementos gráficos (mapas de calor, líneas de tiempo, grafos de relaciones) que faciliten la comprensión rápida de incidentes complejos.

8.4. Sustentación Mensual:

- El contratista deberá realizar una reunión mensual de sustentación de resultados con el supervisor del contrato, donde presentará el consolidado de las amenazas detectadas, las alertas atendidas y el estado de cumplimiento de los niveles de servicio (SLA).

9. PLATAFORMA DE INTELIGENCIA DE AMENAZAS (THREAT INTELLIGENCE)

La solución debe integrar una plataforma de inteligencia de amenazas de clase mundial que permita al MINTIC/FONTIC anticiparse a ataques modernos mediante el análisis de Tácticas, Técnicas y Procedimientos (TTP) utilizados por actores de amenazas globales.

9.1. Fuentes de Inteligencia (Feeds de Datos):

- Multifuente y Curada: La plataforma debe ingerir datos de múltiples fuentes confiables, incluyendo comunidades de código abierto (OSINT), feeds comerciales de reputación global y alertas de centros de respuesta a incidentes (CSIRTs) nacionales e internacionales.
- Inteligencia del Mundo Real: Debe incluir telemetría anonimizada de despliegues globales del fabricante, permitiendo que un ataque detectado en otra parte del mundo sirva para proteger proactivamente la infraestructura del Ministerio.

9.2. Niveles de Inteligencia Requeridos:

- Inteligencia Estratégica: Informes sobre tendencias de ciberamenazas dirigidas específicamente al sector gobierno, analizando los motivos de los atacantes y la evolución del panorama de riesgos en la región.
- Inteligencia Táctica (TTPs): Información detallada sobre las técnicas de ataque según el marco de MITRE ATT&CK, permitiendo identificar si un comportamiento anómalo en la red corresponde a una fase específica de una intrusión (ej. Movimiento lateral o Exfiltración).
- Inteligencia Operativa (IoC): Suministro constante de Indicadores de Compromiso actualizados, como direcciones IP maliciosas, dominios de Comando y Control (C2) y hashes de archivos malintencionados.

9.3. Capacidades de Análisis y Contextualización:

- Correlación Automática: Se debe cruzar automáticamente la inteligencia externa con la actividad interna de la red para identificar "coincidencias" (matches) que indiquen un compromiso activo.
- Priorización Basada en Riesgo: Clasificar las amenazas no solo por su peligrosidad global, sino por su relevancia específica según la infraestructura tecnológica y los activos críticos declarados por el MINTIC.
- Atribución y Contexto: Proporcionar detalles sobre los grupos de amenazas (Threat Actors) asociados a ciertos ataques, sus herramientas preferidas y sus objetivos probables, facilitando la toma de decisiones estratégicas.

9.4. Integración Operativa con la Herramienta:

- Actualización Dinámica: La plataforma de inteligencia debe actualizar en tiempo real los modelos de detección de la herramienta, sin requerir intervenciones manuales constantes o reinicios del sistema.
- Alertamiento Temprano: Notificar de manera inmediata cuando un Indicador de Compromiso global sea detectado dentro de la red institucional, activando los protocolos de respuesta correspondientes.
- Enriquecimiento Forense: Durante la investigación de un incidente, la herramienta debe mostrar automáticamente la información de inteligencia relacionada con los activos involucrados para acelerar el análisis de la causa raíz.

10. AUDITORÍA DE TRÁFICO DE RED Y COMUNICACIONES

Contar con capacidad avanzada de auditoría de tráfico de red y comunicaciones, permitiendo la detección de actividades maliciosas sutiles, la identificación de anomalías de comportamiento y la provisión de evidencia técnica para la investigación de incidentes. Esta capacidad es mandatoria para la protección de la información sensible y crítica gestionada por el MINTIC/FONTIC.

Características Requeridas de la Auditoría:

- Captura y Análisis de Tráfico en Tiempo Real: Realizar la inspección pasiva del tráfico de red (sin afectar la latencia), analizando protocolos estándar y críticos como HTTP, HTTPS (vía metadatos), DNS, FTP, SMTP, SMB, SSH, entre otros.

- Análisis Profundo de Protocolos (DPI - Deep Packet Inspection): Inspeccionar el contenido y las cabeceras de los paquetes de datos para identificar aplicaciones, usuarios, dispositivos y comportamientos maliciosos ocultos en flujos de comunicación aparentemente legítimos.

- Detección de Anomalías de Comportamiento: Utilizar modelos de aprendizaje automático para identificar patrones de comunicación inusuales, tales como conexiones a destinos externos sospechosos (Beaconing), transferencias masivas de datos no habituales o escaneos internos de red.

- Visibilidad de Tráfico Este-Oeste (Movimiento Lateral): La auditoría debe cubrir no solo el tráfico de salida a internet, sino fundamentalmente el tráfico interno entre servidores y segmentos de red, para detectar movimientos laterales de posibles atacantes.

- Identificación de Aplicaciones y Shadow IT: Clasificar automáticamente las aplicaciones que se ejecutan en la red, identificando aplicaciones en la nube, servicios no autorizados (Shadow IT) o herramientas de administración remota que representen un riesgo.

- Monitoreo y Perfilamiento de Usuarios/Dispositivos: Rastrear y perfilar la actividad de cada entidad en la red, estableciendo su "huella digital" de comportamiento normal para detectar cuando una cuenta o dispositivo ha sido comprometido.

- Investigación Forense y Línea de Tiempo: Proporcionar herramientas gráficas para la reconstrucción cronológica de incidentes (Forensic Loop), permitiendo identificar el origen de la amenaza, los activos afectados y la exfiltración potencial de datos.

- Cumplimiento Normativo Nacional: La capacidad de auditoría debe facilitar el cumplimiento de la Ley 1581 de 2012 (Protección de Datos Personales), el Modelo de Seguridad y Privacidad de la Información (MSPI) de la entidad y los controles de monitoreo de la norma ISO/IEC 27001:2022.

11. AUDITORÍA DE INFRAESTRUCTURA Y APLICATIVOS

Proporcionar una visibilidad profunda y un análisis continuo del comportamiento de la infraestructura de red (interna, perimetral y nube), así como de las aplicaciones que transitan por ella. El sistema debe cumplir con los siguientes requisitos técnicos:

11.1. Visibilidad y Mapeo Dinámico de Activos:

- Autodescubrimiento y Topología: Descubrir y mapear automáticamente la topología de la red en tiempo real, identificando cada dispositivo (servidores, estaciones, IoT, activos de red) y sus relaciones de comunicación sin necesidad de agentes.
- Monitoreo de Flujos de Red: Capacidad de identificar flujos de comunicación detallados entre dispositivos, usuarios y aplicaciones, permitiendo visualizar el mapa de dependencias de los servicios críticos de la entidad.
- Inspección Multi-protocolo: Análisis nativo de protocolos de red (TCP, UDP, ICMP) y protocolos de capa de aplicación (DNS, HTTP/S, SMB, FTP, SSH, etc.) para detectar usos indebidos o canales de comunicación no autorizados.
- Visibilidad Híbrida (Nube/On-Premise): Extender la visibilidad hacia los entornos de nube (Azure), monitoreando el tráfico hacia y desde las instancias virtuales y aplicaciones SaaS utilizadas por la entidad.

11.2. Detección Inteligente de Anomalías:

- Establecimiento de Línea Base (LSS): Uso de IA para crear un modelo de comportamiento normal para cada activo e infraestructura de red, permitiendo entender qué es "normal" en el contexto específico del MINTIC/FONTIC.
- Identificación de Desviaciones Críticas: Detectar automáticamente cambios significativos en el comportamiento que sugieran fallos de configuración, degradación de servicios o actividades maliciosas (ej. escaneos de puertos internos o picos inusuales de tráfico).
- Alertamiento Contextual: Generar alertas en tiempo real clasificadas por nivel de riesgo y confianza, evitando la fatiga de alertas mediante la agrupación de eventos relacionados.

11.3. Análisis y Control de Aplicaciones:

- Clasificación de Inventario de Software: Identificar y clasificar automáticamente las aplicaciones en ejecución, diferenciando entre herramientas corporativas autorizadas y aplicaciones no autorizadas (Shadow IT).
- Métricas de Consumo y Uso: Proporcionar visibilidad sobre el ancho de banda consumido por aplicación, usuarios activos y frecuencia de uso, facilitando la identificación de abusos de recursos o fugas de información.
- Evaluación de Riesgo de Aplicaciones: Identificar riesgos asociados a aplicaciones obsoletas, configuraciones inseguras o comportamientos que se desvíen de los estándares de seguridad de la entidad.

11.4. Correlación y Respuesta:

- Correlación Multi-fuente: La arquitectura debe permitir la correlación de eventos detectados en la red con telemetría de otras capas (nube, identidad) para identificar ataques complejos y persistentes.
- Capacidades de Investigación: Proveer interfaces gráficas que permitan a los analistas realizar "drill-down" en los incidentes para entender el alcance total de una amenaza sobre la infraestructura.

11.5. Interoperabilidad con el Ecosistema de Seguridad:

- Integración SIEM/SOAR: El contratista debe garantizar la integración con las plataformas de gestión de eventos y orquestación de la entidad para automatizar los flujos de respuesta (SOC).
- Sincronización con Escáneres de Vulnerabilidades: Capacidad de importar datos de escáneres de vulnerabilidades para priorizar alertas de red sobre activos que se saben vulnerables, optimizando el tiempo de respuesta.
- Gestión de Configuración y Cumplimiento: Integración con herramientas de gestión de configuración para verificar que los cambios en la infraestructura sigan las políticas de seguridad establecidas por la OTI.

12. DESCRIPCIÓN GENERAL DEL ALCANCE Y OBJETO A CONTRATAR

12.1. ALCANCE ESPECÍFICO DEL PROYECTO

El proyecto comprende el suministro, actualización, configuración y la operación gestionada de la solución de seguridad cibernética basada en Inteligencia Artificial (IA), diseñada para la detección y respuesta autónoma ante amenazas en la infraestructura del MINTIC/FONTIC.

1. Implementación y Configuración Técnica:

Instalación y puesta en marcha de la solución en entornos locales (On-Premise) y nube (Azure/M365).

Integración técnica bidireccional con el ecosistema de seguridad actual: SIEM, firewalls, herramientas de endpoint y plataformas de gestión de identidades.

Personalización de la herramienta mediante la definición de políticas de seguridad, umbrales de detección y flujos de trabajo de respuesta autónoma adaptados a la criticidad de los activos del Ministerio.

2. Operación, Detección y Respuesta Administrada:

Monitoreo Continuo 7x24: Supervisión ininterrumpida de la red, dispositivos y aplicaciones para identificar anomalías que representen un riesgo para la entidad.

Análisis de IA en Tiempo Real: Identificación de amenazas conocidas y desconocidas (Zero-days), ransomware, movimientos laterales, exfiltración de datos y amenazas internas mediante aprendizaje no supervisado.

Respuesta Autónoma y Contención: Ejecución de medidas de mitigación en tiempo real (bloqueo de tráfico malicioso, cuarentena quirúrgica de dispositivos) para detener la propagación de ataques sin afectar la continuidad del negocio.

Gestión de Incidentes: Análisis técnico de la causa raíz, determinación del alcance del impacto y suministro de recomendaciones de remediación inmediata.

3. Visibilidad y Análisis de Comportamiento:

Provisión de una visibilidad integral de la red (Tráfico Norte-Sur y Este-Oeste), identificando patrones de comportamiento de usuarios y dispositivos.

Capacidades de análisis forense digital para la reconstrucción de eventos de seguridad y cumplimiento de la cadena de custodia de la información.

4. Cumplimiento y Estándares de Seguridad:

Alineación de la solución con el Marco de Seguridad Digital de Colombia, la Ley 1581 de 2012 (Protección de Datos Personales), el MSPI y la norma ISO/IEC 27001:2022.

Generación de evidencias técnicas para soportar auditorías de cumplimiento normativo.

5. Escalabilidad y Flexibilidad:

Garantizar que la solución sea escalable para absorber el crecimiento del tráfico y los activos de la entidad durante la vigencia del contrato.

Flexibilidad técnica para integrarse con futuras tecnologías que la entidad decida implementar.

12.2. EXCLUSIONES

Hardware: El alcance no incluye la adquisición de hardware físico nuevo por parte del contratista. Se utilizará la infraestructura de servidores y virtualización existente en la entidad para el despliegue de las sondas y consolas virtuales.

12.3. ENTREGABLES DEL CONTRATO

Solución Implementada: Herramienta de seguridad configurada, integrada y operando bajo el modelo de servicio gestionado.

Documentación Técnica: Manuales de arquitectura, configuración, protocolos de administración y plan de respuesta a incidentes.

Informes de Gestión: Reportes mensuales de seguridad, análisis de amenazas detectadas, cumplimiento de niveles de servicio (SLA) y recomendaciones de mejora.

Transferencia de Conocimiento: Certificado de capacitación técnica y operativa para el personal designado por la OTI sobre el uso y explotación de la herramienta.

Reporte Final de Cierre: Documento consolidado que resuma la ejecución contractual, los logros alcanzados en la postura de seguridad y el estado final de la plataforma.

ANDRES DIAZ MOLINA
Jefe Oficina de Tecnologías de la Información.

Elaboró: *Jaime Alberto Aguillón – Contratista OTI*
Revisó: *Dayana Cardozo - Contratista OTI*
Revisó: *Liliana Carolina Perilla Amaya – Coordinadora GIT DE CIBERSEGURIDAD*

REGISTRO DE FIRMAS ELECTRONICAS

ANEXO TECNICO HERRAMIENTA DE CIBERSEGURIDAD 2026 ok

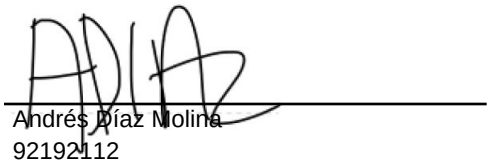
Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20260413-160906-5b0a48-73084457
Estado: Finalizado

Creación: 2026-04-13 16:09:06
Finalización: 2026-04-13 18:52:14

Escanee el código para verificación

Firma: jefe oficina de TI



Andrés Díaz Molina
92192112
adiazm@mintic.gov.co
Jefe de Oficina de Tecnologías de la Información
Ministerio de TIC

Revisión: revisión

Liliana Carolina Perilla Amaya
53067088
lcperilla@mintic.gov.co
Profesional Especializado
MINTIC

Revisión: Revision

DAYANA CARBONÓ CARBONÓ
52780885
dcarbono@mintic.gov.co
CONTRATISTA
MINTIC

Elaboración: Elaboracion

JAIME ALBERTO AGUILLON BARRAGAN
79515095
jaguillon@mintic.gov.co
Contratista
Ministerio de Tecnología de la Información y las Comunicaciones

REPORTE DE TRAZABILIDAD

ANEXO TECNICO HERRAMIENTA DE CIBERSEGURIDAD 2026 ok

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

Id Acuerdo: 20260413-160906-5b0a48-73084457
Creación: 2026-04-13 16:09:06
Estado: Finalizado
Finalización: 2026-04-13 18:52:14

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	JAIME ALBERTO AGUILLON BARRAGAN jaguillon@mintic.gov.co Contratista Ministerio de Tecnología de la Información y las C	Aprobado	Env.: 2026-04-13 16:09:09 Lec.: 2026-04-13 16:11:28 Res.: 2026-04-13 16:11:46 IP Res.: 190.145.189.98 Canal: Email
Revisión	DAYANA CARBONÓ CARBONÓ dcarbono@mintic.gov.co CONTRATISTA MINTIC	Aprobado	Env.: 2026-04-13 16:11:47 Lec.: 2026-04-13 17:32:09 Res.: 2026-04-13 17:32:12 IP Res.: 186.29.158.27 Canal: Email
Revisión	Liliana Carolina Perilla Amaya lcperilla@mintic.gov.co Profesional Especializado MINTIC	Aprobado	Env.: 2026-04-13 17:32:12 Lec.: 2026-04-13 17:34:29 Res.: 2026-04-13 17:34:33 IP Res.: 190.145.189.98 Canal: Email
Firma	Andrés Díaz Molina adiazm@mintic.gov.co Jefe de Oficina de Tecnologías de la Información Ministerio de TIC	Aprobado	Env.: 2026-04-13 17:34:33 Lec.: 2026-04-13 18:52:12 Res.: 2026-04-13 18:52:14 IP Res.: 186.154.35.146 Canal: AZSign