1. OBJETIVO

Definir un marco de trabajo para la gestión de la **inteligencia de amenazas**. Con el fin de mitigar el riesgo de ciberataques mediante la recopilación, el análisis y la difusión de información oportuna y relevante sobre amenazas, para la gestión proactiva y reactiva de amenazas avanzadas (como ataques APT, ransomware sofisticado, ingeniería social dirigida y ataques de día cero) que puedan impactar la confidencialidad, integridad y disponibilidad de la información de la Superintendencia.

2. ALCANCE

Este procedimiento es aplicable a los sistemas de información, correo electrónico, aplicaciones y servicios tecnológicos integrados con servicios de Directorio Activo.

Se utilizarán las siguientes herramientas para la implementación:

- Microsoft Defender: Para la protección de endpoints y la detección de amenazas.
- Microsoft Intune: Para la gestión de dispositivos móviles y la aplicación de políticas de seguridad.
- Sentinel (Correlacionador de Eventos): Para la agregación y correlación de eventos de seguridad.
- FortiAnalyzer: Para el análisis de tráfico de red, registro de eventos (logs) y generación de informes de seguridad.

3. DEFINICIONES

Amenaza Avanzada: Intento malicioso, persistente y complejo de violar la seguridad de un sistema informático, a menudo ejecutado por actores con recursos significativos y alta sofisticación técnica.

Verifique que este documento corresponda a la versión vigente antes de su uso

Indicador de Compromiso (IOC): Evidencia forense de un ataque o intrusión en un sistema o red (direcciones IP maliciosas, hashes de archivos, patrones de tráfico, etc.).

Inteligencia de Amenazas (Threat Intelligence): Información procesada y analizada sobre amenazas existentes o emergentes, actores, motivaciones y métodos, utilizada para mejorar las defensas.

4. DOCUMENTOS DE REFERENCIA

- GIN-PO-001 Documento de Políticas del SGI
- GIN-PO-003 Políticas de Seguridad y privacidad de la Información del SGSI
- GTI-GU-006 Gestión Incidentes

5. CONDICIONES GENERALES

5.1. Responsabilidades:

- **Oficial de Seguridad de la Información:** Es responsable de supervisar la implementación y el mantenimiento del procedimiento. Aprueba las fuentes de inteligencia de amenazas y asegura la correcta integración de las herramientas.
- **Equipo de Seguridad e Informática Forense:** Son los encargados de la ejecución del procedimiento, incluyendo la correlación, monitorización y el análisis periódico de amenazas y la respuesta a incidentes.
- **Administradores de Sistemas y Redes:** Colaboran en la configuración de las herramientas para asegurar una correcta recolección de datos.
- **Funcionarios y usuarios:** Notificar y reportar posibles eventos o incidentes de seguridad (por ejemplo, correos electrónicos sospechosos, comportamientos anómalos).
- **Mesa de Servicio:** Registrar los eventos o incidentes reportados por las diferentes fuentes.

5.2. Lineamientos Generales

A través del GC-PO-001 Documento de Políticas del SGI y los lineamientos generales en el documento GC-MO-001 Documento de Modelos del SGI, se establecen lineamientos para incrementar la capacidad de defensa ante amenazas y riesgos

Verifique que este documento corresponda a la versión vigente antes de su uso

actuales de seguridad digital, a través de las siguientes instancias de ayuda y soporte:

- El Comité de Seguridad Digital del que trata el Acuerdo 002 de 5 de junio de 2018 del Consejo para la Gestión y el Desempeño Institucional.
- La Coordinación Nacional de Seguridad Digital (Presidencia de la República)
- Las unidades cibernéticas de las Fuerzas Militares.
- Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, a través del Grupo de Respuestas a Emergencias Cibernéticas de Colombia - ColCERT.
- Equipo de respuesta a incidentes de seguridad informática CSIRT de Gobierno.
- CAI Virtual Policía Nacional de Colombia.
- Fiscalía General de la Nación y sus centros de investigación. En conjunto con estas entidades y en el momento que se requiera, se conformarán equipos que puedan ayudar a superar incidentes de seguridad digital.

5.3. Gestión e inteligencia de amenazas

5.3.1. Recopilación de Inteligencia de Amenazas

Fuentes de Datos Internas: Se obtendrá inteligencia de amenazas de las siguientes fuentes:

- **Microsoft Defender:** Proporciona datos sobre amenazas detectadas en los endpoints, vulnerabilidades y comportamientos maliciosos. Microsoft Defender for Endpoint (MDE) es una plataforma de seguridad de endpoints (Endpoint Detection and Response - EDR) que se centra en la prevención, detección, investigación y respuesta a amenazas avanzadas en tiempo real.
- **Sentinel:** Recibe eventos de seguridad de diversas fuentes, incluyendo firewalls, servidores, DLP, Defender, Entra-id y aplicaciones, que pueden indicar actividad sospechosa.
- **FortiAnalyzer:** Recopila información de tráfico de red, intentos de acceso no autorizado y otros eventos de seguridad del perímetro.
- **Intune:** Proporciona datos sobre el estado de cumplimiento y la postura de seguridad de los dispositivos móviles. Se enfoca en la gestión de

dispositivos y aplicaciones (Unified Endpoint Management - UEM) y en asegurar que estos cumplan con las políticas de seguridad de la organización.

- **PureVIew:** Proporciona información de directivas configuradas para la prevención de fuga de información - DLP o IRM (administración de riesgos de personas)

Fuentes de datos Externas: Se utilizarán feeds de inteligencia de código abierto (OSINT) y, si es posible, servicios de inteligencia de amenazas de terceros:

- Reportes de ciberseguridad del Colcert – MINTIC
- Suscripción a fuentes de inteligencia de amenazas reputadas (privadas y públicas) para mantenerse al tanto de nuevas tácticas, técnicas y procedimientos (TTPs) de atacantes.
- Integrar IOCs de estas fuentes en las herramientas de seguridad para una detección más rápida.
- Monitorización 24/7: este servicio se realizará a través de la contratación del SOC – Centro de Operaciones de Seguridad, y cuando no sea posible a través de la generación de alertas y envío de las mismas a los canales definidos como correo electrónico.

Entre las fuentes disponibles se puede considerar sin limitarse las siguientes:

FUENTE EXTERNA	DESCRIPCION	USO
Virus Total	Es una herramienta que proporciona un servicio rápido y eficaz para el análisis de archivos y URLs en busca de malware. Desde su lanzamiento en 2004 por Hispasec Sistemas, y su adquisición por Google en 2012, esta plataforma ha ganado una	* VirusTotal utiliza más de 70 motores antivirus y herramientas de análisis para detectar amenazas en archivos y URLs. Los informes muestran información exhaustiva sobre reputación,

Verifique que este documento corresponda a la versión vigente antes de su uso

	excelente reputación gracias a su confiabilidad y facilidad de uso.	detalles técnicos, relaciones y detecciones. Se puede Integrar su API y las versiones avanzadas permite automatizar análisis y obtener inteligencia de amenazas más profunda.
Abuse IP	AbuseIPDB es un proyecto administrado por Marathon Studios Inc. Su misión es ayudar a que la Web sea más segura proporcionando un repositorio central para que los webmasters, administradores del sistema y otras partes interesadas informen e identifiquen las direcciones IP asociadas a actividades malintencionadas en línea.	Acepta una dirección IP (v4 o v6) y proporciona información sobre la dirección IP consultada, incluida la versión, el país o región de origen, el tipo de uso, el ISP y el dominio. Se incluyen informes abusivos. AbuseIPDB - IP address abuse reports - Making the Internet safer, one IP at a time
Phish Report	Herramienta gratuita y de código abierto diseñada para analizar y gestionar sitios de phishing de manera eficiente.	Permite a los usuarios detectar, reportar y seguir el progreso de la eliminación de estos sitios, todo desde una interfaz sencilla Analizar un sitio de phishing - phish.report
CentralOps.net	Es una plataforma gratuita y sin anuncios que ofrece herramientas en línea para realizar diagnósticos de redes y dominios.	Es útil para administradores de sistemas, analistas de seguridad y profesionales de TI que necesitan realizar investigaciones rápidas sin instalar software adicional. Free online network tools - traceroute, nslookup, dig, whois lookup, ping - IPv6
mxtools	Plataforma integral y gratuita que ofrece herramientas avanzadas	Es útil para administradores de sistemas, analistas de seguridad y

Verifique que este documento corresponda a la versión vigente antes de su uso

	para diagnosticar y optimizar la infraestructura de correo electrónico, DNS y redes.	profesionales de TI que buscan mejorar la entregabilidad de correos electrónicos y garantizar el buen funcionamiento de sus servicios en línea. MX Lookup Tool - Check your DNS MX Records online - MxToolbox
Shodan.io	Su objetivo principal es recopilar información sobre dispositivos expuestos en la red, como cámaras, routers, servidores, sistemas de control industrial (ICS), IoT, bases de datos, entre otros	Shodan realiza escaneos continuos de direcciones IP en busca de puertos abiertos y banners, que contienen información técnica sobre los servicios en ejecución: software, versiones, mensajes de bienvenida, etc. Esta información se almacena en una base de datos que los usuarios pueden consultar con filtros como país, puerto, tipo de dispositivo, organización, software, entre otros. LevelBlue - Open Threat Exchange
AlienVault Open Threat Exchange (OTX)	es una plataforma colaborativa de inteligencia de amenazas desarrollada originalmente por AlienVault, actualmente parte de AT&T Cybersecurity. Se configura como una de las comunidades más grandes del mundo en este campo, donde miles de profesionales comparten y acceden libremente a datos de amenazas actualizados.	Opera como una plataforma gratuita basada en la nube, accesible mediante registro. OTX | La comunidad de inteligencia de amenazas más grande del mundo
ANY.RUN	Es una herramienta que proporciona un servicio rápido e interactivo para el análisis de archivos y URLs en busca de	Analizar archivos sospechosos (ejecutables, documentos, scripts, correos, etc.) en busca de malware.

Verifique que este documento corresponda a la versión vigente antes de su uso

	comportamientos maliciosos. Creada en 2016 y lanzada su versión comercial en 2018 por Aleksey Lapshin y su equipo, esta plataforma ha ganado gran reconocimiento en la comunidad de ciberseguridad gracias a su capacidad de permitir la interacción en tiempo real con las muestras analizadas y la extracción de indicadores de compromiso de manera sencilla y eficaz.	Revisar URLs y sitios web que puedan alojar phishing, exploits o descargas maliciosas. Observar el comportamiento del malware en tiempo real (procesos, conexiones de red, cambios en el registro, persistencia). Extraer IOCs (Indicadores de Compromiso) como dominios, IPs, hashes, rutas de archivos. Compartir análisis con otros investigadores o equipos SOC para respuesta a incidentes. Capacitación y entrenamiento de analistas de seguridad en un entorno seguro e interactivo. Adicional tiene conectores con Microsoft https://learn.microsoft.com/en-us/connectors/anyrunthreatintellig/ El conector permite a los equipos de seguridad y TI optimizar sus operaciones al incorporar las capacidades de inteligencia de amenazas de ANY.RUN en flujos de trabajo manuales y automatizados con aplicaciones como Defender for Endpoint y Sentinel.

5.3.2. Implementación de Herramientas de Detección Avanzada:

Verifique que este documento corresponda a la versión vigente antes de su uso

- **SIEM** – Sentinel (Security Information and Event Management): Recopilar y correlacionar registros de eventos de seguridad de todas las fuentes relevantes (firewalls, IDS/IPS, sistemas operativos, aplicaciones).
- **XDR** (Detección y respuesta Extendida): Monitorizar la actividad en los endpoints para detectar comportamientos anómalos y maliciosos.
- **IPS** (Intrusion Prevention Systems): Monitorear el tráfico de red en busca de patrones de ataque conocidos y anomalías.
- **Soluciones de Seguridad de Correo Electrónico y Navegación Web**: Filtrar contenido malicioso y detectar intentos de phishing o spear-phishing.
- **Análisis de Comportamiento de entidades de Usuarios (UEBA)**: Identificar desviaciones de las líneas base de comportamiento normal

5.3.3. Análisis y Correlación de Datos

1. **Sentinel (Correlacionador de Eventos):** Este sistema actuará como el centro de operaciones. Se configurará para recibir eventos de Defender, FortiAnalyzer e Intune.
2. **Reglas de Correlación:** Se crearán reglas de correlación personalizadas en Sentinel para identificar patrones de ataque. Por ejemplo, una regla podría correlacionar una alerta de malware de Defender con un intento de conexión sospechosa de FortiAnalyzer.
3. **Análisis de Vulnerabilidades:** La información de Microsoft Defender sobre vulnerabilidades se utilizará para priorizar la aplicación de parches y la mitigación de riesgos.
4. **Análisis de Comportamiento:** Se analizará el tráfico de red en FortiAnalyzer para detectar anomalías o patrones que no se ajusten a un comportamiento normal.

5.3.4. Toma de Decisiones y Respuesta

1. **Clasificación de Alertas**: Cuando se genere una alerta, el equipo de seguridad debe clasificarla según su nivel de criticidad (informativa, baja, media, alta, crítica).

Verifique que este documento corresponda a la versión vigente antes de su uso

2. **Investigación Inicial**: Realizar una investigación preliminar para determinar la validez de la alerta y si representa una amenaza real. Esto incluye:

    - Verificar los logs y eventos asociados
    - Consultar bases de datos de IOCs.
    - Analizar el contexto de la alerta.
    - Escalamiento: Si la alerta se clasifica como una posible amenaza avanzada, escalarla al equipo de respuesta a incidentes (ERI) para una investigación profunda.

3. **Generación de Alertas:** Sentinel generará alertas automatizadas cuando se detecten eventos o patrones que cumplan con las reglas de correlación.
4. **Respuesta a Incidentes:** Ante una alerta crítica, el equipo de seguridad iniciará el plan de respuesta a incidentes, de acuerdo con lo establecido en la guía **GTI-GU-006 GestionIncidentes**, se utilizará la información detallada de Defender y FortiAnalyzer para comprender el alcance del incidente.
5. **Actualización de Políticas:** La inteligencia de amenazas obtenida se utilizará para actualizar las políticas de seguridad. Por ejemplo, se podría configurar una nueva regla en el firewall (gestionado por FortiAnalyzer) para bloquear una dirección IP maliciosa o una política en Intune para restringir aplicaciones en dispositivos móviles.

5.3.5. Mejora Continua

1. **Revisión Periódica:** El Oficial de Seguridad de la Información revisará el procedimiento al menos una vez al año, o después de un incidente de seguridad mayor, para asegurar su efectividad o cuando haya cambios significativos en el entorno de amenazas, surjan nuevas fuentes internas o externas, cambios en la tecnología o los requisitos de la Superintendencia.
2. **Auditorías Internas**: Por tratarse del control A.5.17. Inteligencia de amenazas, control establecido en el Anexo de la Norma ISO 27001, se

Verifique que este documento corresponda a la versión vigente antes de su uso

debe Incluir el cumplimiento de este procedimiento en las auditorías internas del SGSI para asegurar su efectividad.

3. **Métricas de Desempeño:** Se establecerán métricas para evaluar la efectividad del procedimiento, como el número de amenazas detectadas, el tiempo de respuesta a incidentes y el número de falsos positivos. Los informes de FortiAnalyzer y Sentinel serán esenciales para esta tarea.

El indicador con el cual se mediará la gestión de la inteligencia de amenazas es:

Indicador	Descripción	Fórmula	Propósito	Ejemplo de Meta
Tasa de detección proactiva de amenazas	Mide el porcentaje de amenazas detectadas antes de que causen incidentes.	(Número de amenazas detectadas proactivamente / Total de amenazas identificadas) × 100	Evalúa la capacidad proactiva del procedimiento para anticipar riesgos.	Alcanzar al menos el 70% de detección proactiva en un año.

6. PROCEDIMIENTO

No.	Actividad	Responsable	Punto de Control	Registro
	Inicio			
1	**Recopilación de Inteligencia de Amenazas** Definir las fuentes internas y externas que se tendrán en cuenta para realizar la inteligencia de amenazas	OSI GRUPO DE SEGURIDAD E INFORMÁTICA FORENSE		Fuentes internas y externas
2	**Implementación de Herramientas de Detección Avanzada:** Realizar la implementación y administración de las herramientas adquiridas	GRUPO DE SEGURIDAD E INFORMÁTICA FORENSE		Reportes de Herramientas

Verifique que este documento corresponda a la versión vigente antes de su uso

3	**Análisis y Correlación de Datos** Definir y monitorear las alertas necesarias para identificar posibles eventos de seguridad	GRUPO DE SEGURIDAD E INFORMÁTICA FORENSE		Informe Herramienta de SIEM
4	**Toma de Decisiones y Respuesta** Activar la atención de los eventos e incidentes que se generen	GRUPO DE SEGURIDAD E INFORMÁTICA FORENSE OSI	X	Bitácora Incidentes de Seguridad
5	**Mejora Continua** Realizar la medición del proceso e implementar las mejoras a que haya lugar	GRUPO DE SEGURIDAD E INFORMÁTICA FORENSE		Indicadores de Medición
	Fin			

7. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
001	24-10-2025	Creación del documento: Se crea procedimiento para definir las acciones a realizar para dar cumplimiento al control de inteligencia de amenazas.

Elaboró	Revisó	Aprobó
Nombre: Leidy Clavijo Cargo: Contratista – Grupo de Seguridad e informática Forense Fecha: 20/10/2025	Nombre: Rocio Pedrozo Cargo: Coordinador Grupo de Seguridad e informática Forense Fecha: 20/10/2025	Nombre: Ricardo Fernelix Ríos Cargo: director tecnología de la información y las comunicaciones Fecha: 20/10/2025

Verifique que este documento corresponda a la versión vigente antes de su uso