1. OBJETIVO

Definir las actividades de monitoreo, análisis, clasificación y escalamiento de las alertas de seguridad generadas en la herramienta SIEM, con el fin de garantizar una respuesta oportuna y estandarizada por parte del Centro de Operaciones de Seguridad (SOC) ante eventos que puedan afectar la confidencialidad, integridad o disponibilidad de la información.

2. ALCANCE

Este procedimiento aplica a todas las alertas de seguridad generadas a partir de las fuentes integradas en la herramienta SIEM (incluyendo, entre otras, FortiAnalyzer y Microsoft Defender), así como a todo el personal del Grupo de Seguridad e Informática Forense, los analistas del SOC y las áreas responsables de la gestión y remediación de los casos escalados a través de la herramienta ITSM. Aplica desde la generación de la alerta hasta el cierre formal del caso.

3. RESPONSABILIDADES

Rol	Descripción	Responsabilidades clave
Analistas SOC – Primer respondiente (Monitoreo GSIF en caso de no contar con Tercero Contratado para la Gestión del SOC)	Encargado del monitoreo continuo de la consola de la herramienta SIEM y de la revisión diaria de alertas generadas. Para cada tipo de alerta, la matriz de alertas (Anexo 1) asigna un primer respondiente específico dentro del Grupo de Seguridad e Informática Forense.	• Consultar la consola de la herramienta SIEM de forma periódica. • Realizar el triage inicial (clasificar por severidad según la matriz). • Descartar falsos positivos evidentes según el criterio documentado. • Diligenciar la Plantilla de Requerimientos SOC (Anexo 2) y remitir el caso para análisis o escalamiento.
Grupo de Seguridad e Informática Forense (GSIF)	Equipo que realiza tanto el monitoreo/triage inicial (primer respondiente en caso de no contar con contrato SOC) como el análisis en profundidad de las alertas y determina el tratamiento a seguir.	• Analizar evidencia (logs de SIEM, FortiAnalyzer, Defender). • Confirmar si la alerta es un incidente real (verdadero positivo). • Definir la acción de contención/remediación según la matriz. • Escalar el caso a través de La herramienta ITSM al responsable correspondiente.

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

Rol	Descripción	Responsabilidades clave
		• Realizar labores de análisis forense cuando se requiera preservar evidencia.
Coordinador Grupo Seguridad e Informática Forense / Coordinador del SOC	Responsable de la operación general del SOC, cumplimiento del procedimiento y mejora continua.	• Supervisar el cumplimiento de los SLA. • Autorizar cambios a la matriz de alertas. • Reportar indicadores de gestión. • Escalar incidentes críticos a la Dirección de Seguridad/TI.
Responsables de gestión (dueños de plataforma: Redes, Infraestructura, Aplicaciones, TI)	Áreas técnicas a quienes se escala el caso a través de la herramienta ITSM para ejecutar la remediación.	• Recibir el caso asignado en La herramienta ITSM. • Ejecutar las acciones de contención/erradicaciones indicadas. • Actualizar el estado del caso y evidenciar el cierre. • Retroalimentar al SOC sobre causa raíz.
Mesa de Servicio / herramienta ITSM	Plataforma de gestión de casos utilizada para el registro, asignación, trazabilidad y cierre de los incidentes escalados.	• Registrar el caso con la información suministrada por el SOC. • Notificar al responsable asignado. • Mantener la trazabilidad de tiempos (SLA) hasta el cierre.

4. DEFINICIONES

Conceptos que se encuentran en la guía:

- **SOC (Centro de Operaciones de Seguridad)**: equipo y conjunto de procesos encargados del monitoreo, detección, análisis y respuesta ante eventos de seguridad de la información.
- **Alerta:** notificación generada por una herramienta de seguridad ante un evento o patrón que cumple una regla de detección.
- **Incidente de seguridad:** alerta confirmada como verdadero positivo que representa un riesgo real para la organización.
- **Falso positivo:** alerta generada por una condición legítima que no representa una amenaza real.

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

- **Triage:** proceso de clasificación inicial de una alerta según su severidad y probabilidad de ser un incidente real.
- **Escalamiento:** acción de trasladar la gestión de un caso, a través de La herramienta ITSM, al área o responsable competente para su remediación.
- **SIEM:** (por sus siglas en inglés, *Security Information and Event Management*, o Gestión de Información y Eventos de Seguridad) es una plataforma de ciberseguridad. Recopila, centraliza y analiza registros de datos y alertas de toda la red de una empresa en tiempo real para detectar y responder a amenazas con rapidez
- **SLA (Service Level Agreement):** tiempo máximo definido para atender, escalar o resolver una alerta según su severidad.
- **Matriz de alertas:** documento de referencia que relaciona cada tipo de alerta con su severidad, criterios de validación, acción a ejecutar y responsable de escalamiento.

5. GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD- SOC

5.1. Herramientas tecnológicas del SOC

El SOC opera sobre un ecosistema de herramientas integradas, cuya arquitectura general de flujo de información es la siguiente: FortiAnalyzer y Microsoft Defender (entre otras fuentes) envían sus logs y eventos a la herramienta SIEM, el cual los correlaciona y genera las alertas de seguridad; dichas alertas son gestionadas por el Grupo de Seguridad e Informática Forense y/o el contratista responsable de la gestión del SOC y, cuando se confirma un caso a atender, se escalan mediante La herramienta ITSM al responsable de la remediación.

Herramienta	Función dentro del procedimiento	Tipo de información / fuente
Herramienta SIEM	Plataforma SIEM/SOAR central del SOC. Correlaciona eventos, genera y consolida las alertas de seguridad a partir de múltiples fuentes de log. Configuración de Playbooks	Consola única de monitoreo diario; reglas de correlación y alertas de seguridad.
FortiAnalyzer	Fuente de logs de la infraestructura perimetral (firewalls Fortinet).	Logs de firewall, tráfico de red, intentos de intrusión, políticas de seguridad perimetral.

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

Herramienta	Función dentro del procedimiento	Tipo de información / fuente
	Envía eventos de red, tráfico e IPS/IDS al SIEM.	
Microsoft Defender (XDR/Endpoint)	Fuente de logs de protección de endpoints, identidad y correo. Envía alertas de malware, comportamiento anómalo y amenazas de identidad a SIEM.	Logs de endpoint, detecciones de malware, alertas de identidad (Entra ID), correo (Defender for Office 365).
Herramienta ITSM-Mesa de Servicios	Herramienta de gestión de casos/tickets utilizada para escalar la alerta ya analizada al responsable de la remediación.	Registro de casos, asignación, seguimiento de SLA, trazabilidad y cierre del incidente.

5.2. ACTIVIDADES PARA LA GESTIÓN DEL SOC

A continuación, se describe el flujo general de gestión de alertas del SOC, desde su generación hasta el cierre del caso:

#	Actividad	Descripción	Responsable
1	Monitoreo continuo	Se realiza la ingesta permanente de registros (logs) provenientes de FortiAnalyzer, Microsoft Defender y demás fuentes de información hacia la plataforma SIEM para su análisis y correlación.	Plataformas / SIEM
2	Generación de la alerta	La herramienta SIEM correlaciona los eventos recibidos con base en las reglas de detección configuradas y genera las alertas correspondientes.	SIEM (automático)
3	Consulta diaria de alertas	El primer respondiente asignado accede diariamente a la consola SIEM para revisar las alertas generadas durante el período analizado.	Primer respondiente (GSIF)
4	Validación inicial	Verificar que la alerta contenga la información necesaria, que la fuente esté operativa y que no corresponda a errores de ingesta, duplicidades o fallas de correlación.	Primer respondiente (GSIF)
5	Triage y clasificación	Se efectúa el análisis inicial de la alerta, clasificándola de acuerdo con su nivel de severidad (Alta, Media, Baja o Informativa) y validando si corresponde	Primer respondiente (GSIF)

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

#	Actividad	Descripción	Responsable
		a un falso positivo identificado en la matriz de alertas.	
6	Análisis especializado	Las alertas que requieren una revisión más profunda son remitidas al Grupo de Seguridad e Informática Forense o al Grupo de Sistemas y Arquitectura de Tecnología, según su naturaleza.	Grupo de Seguridad e Informática Forense / Grupo de sistemas y arquitectura de tecnología.
7	Recolección y preservación de evidencias	Se recopilan registros, indicadores de compromiso (IOC), evidencias y artefactos digitales necesarios para soportar el análisis y la trazabilidad del caso.	GSIF
8	Determinación del caso	Se determina si la alerta corresponde a un evento de seguridad o a un incidente de seguridad y se define el tratamiento correspondiente de acuerdo con la matriz de alertas.	Seguridad e Informática Forense
9	Escalamiento, Notificación y comunicación	Se diligencia la Plantilla de Requerimientos SOC (Anexo 2) y se registra el caso en la herramienta ITSM, adjuntando la documentación correspondiente y se informa a las áreas responsables, propietarios de activos o partes interesadas sobre el incidente identificado y las acciones requeridas definido en la matriz de alertas.	Seguridad e Informática Forense
10	Seguimiento y control	Se realiza seguimiento al ticket y a los compromisos definidos hasta la implementación de las acciones correctivas.	GSIF
11	Gestión y remediación	El responsable asignado ejecuta las acciones de contención, mitigación, erradicación o corrección requeridas y actualiza el estado del caso en la herramienta ITSM.	Responsable de la plataforma / TI
12	Validación de efectividad	Se confirma que los indicadores de compromiso desaparecieron, que la amenaza fue contenida y que no existen alertas relacionadas activas.	GSIF

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

#	Actividad	Descripción	Responsable
13	Verificación y cierre	Una vez implementadas las acciones correctivas, el responsable verifica la efectividad de la remediación y procede con el cierre formal del caso en la herramienta ITSM.	Responsable de la plataforma / TI
14	Lecciones aprendidas	Para los incidentes clasificados con severidad alta o crítica, se documentan las causas identificadas, las oportunidades de mejora y los ajustes requeridos en las reglas de detección o en la matriz de alertas.	Coordinador del SOC
15	Mejora continua	Se actualizan reglas de correlación, listas de exclusión, casos de uso, procedimientos e indicadores según los hallazgos obtenidos.	Coordinador SOC / GSIF

5.2.1.Monitoreo continuo y consulta de alertas

El Centro de Operaciones de Seguridad (SOC) realiza el monitoreo continuo de los eventos de seguridad mediante la consola de la herramienta SIEM. El primer respondiente designado de acuerdo con la Matriz de Alertas (Anexo 1) deberá efectuar el seguimiento permanente de las alertas generadas y, como mecanismo de control, garantizar al menos una validación formal diaria de los eventos registrados en la plataforma.

Para las alertas clasificadas con severidad Alta o Crítica, la herramienta SIEM deberá contar con mecanismos de notificación en tiempo real, tales como correo electrónico, mensajería instantánea o integración con la herramienta ITSM institucional, con el fin de garantizar su atención oportuna y reducir el tiempo de respuesta ante posibles incidentes de seguridad de la información.

La consulta de alertas deberá quedar soportada mediante los registros generados por la herramienta SIEM o por los mecanismos de auditoría definidos para tal fin, asegurando la trazabilidad de las actividades de monitoreo realizadas por el personal responsable.

5.2.2.Triage y clasificación inicial

Cada alerta se clasifica según los niveles de severidad definidos en esta guía (numeral 5.3) y se contrasta contra la matriz de alertas (Anexo 1) para identificar si corresponde

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

a un patrón ya documentado, su acción recomendada y si existen criterios conocidos de falso positivo.

5.2.2. Análisis por el Grupo de Seguridad e Informática Forense

Las alertas que no se descartan en el triage inicial son remitidas al Grupo de Seguridad e Informática Forense, quien realiza el análisis técnico correspondiente: revisión de logs de origen (SIEM, FortiAnalyzer, Defender), correlación con otros eventos, identificación de indicadores de compromiso (IoC) y determinación de la táctica/técnica asociada (referencia MITRE ATT&CK cuando aplique).

5.2.3. Diligenciamiento de la Plantilla de Requerimientos SOC

Una vez analizada la alerta, el Grupo de Seguridad e Informática Forense diligencia la Plantilla de Requerimientos SOC (Anexo 2), registrando: fecha y hora del evento, activo o cuenta comprometida, dirección IP, tipo de evento, severidad SIEM, número de ticket La herramienta ITSM, descripción del evento, acciones realizadas por el SOC, acciones requeridas por parte del especialista y recomendaciones del equipo GSIF. Este formato es el insumo oficial que se anexa al caso escalado.

5.2.4. Escalamiento a través de la Herramienta ITSM

Confirmado el caso como verdadero positivo, o cuando se requiera la intervención de un área técnica para su remediación, el Grupo de Seguridad e Informática Forense o los Analistas del SOC registran el caso en la herramienta ITSM anexando la Plantilla de Requerimientos SOC diligenciada, e indicando el área/responsable a quien se asigna de acuerdo con la matriz de alertas y los tiempos de SLA definidos.

5.2.5. Gestión, remediación y cierre

El responsable asignado ejecuta la acción de contención, erradicación o recuperación indicada y actualiza el estado del caso en la herramienta ITSM. El SOC verifica la efectividad de la remediación antes de proceder al cierre formal. Para incidentes de severidad Alto se documentan las lecciones aprendidas y, de ser necesario, se ajustan las reglas de correlación en la herramienta SIEM o se actualiza la matriz de alertas.

5.3. Niveles de severidad y tiempos de atención (SLA)

Severidad (SIEM)	Criterio	Tiempo máx. de triage (GSIF)	Tiempo máx. de escalamiento (Aranda)
Alto	Compromiso activo o de alta probabilidad de impacto: malware confirmado, exfiltración de datos, movimiento lateral, ataques dirigidos a identidades críticas (DCSync, password spray, etc.).	15 minutos	30 minutos
Media	Comportamiento anómalo que requiere validación adicional antes de confirmar impacto (ej. actividad sospechosa de correo, ejecución de scripts no habituales).	1 hora	2 horas
Baja	Eventos con bajo riesgo o hallazgo ya mitigado automáticamente por la herramienta (ej. malware puesto en cuarentena).	4 horas	8 horas
Informativo	Eventos de registro/consulta sin riesgo inmediato, o resultado benigno de una investigación automatizada.	1 día hábil	No aplica (registro y seguimiento de tendencia)

5.4. Matriz de alertas de seguridad

Con el fin de estandarizar la respuesta del equipo ante cada tipo de alerta y servir como base de conocimiento para todos los integrantes del SOC, se mantiene una matriz de alertas que relaciona, para cada tipo de alerta: la categoría, la fuente de detección, la frecuencia histórica, la severidad, el primer respondiente del Grupo de Seguridad e Informática Forense, los criterios para identificar falsos positivos, la acción inmediata a ejecutar y el área o responsable a quien se debe escalar el caso en la herramienta ITSM.

La matriz vigente se construyó a partir del histórico real de incidentes de la herramienta SIEM (3.198 registros, periodo comprendido entre el 28 de enero y el 31 de julio de 2026) y de la asignación actual de primer respondiente del equipo GSIF, cubriendo 94 tipos de alerta distintos. Se administra como un documento vivo en un archivo de Excel independiente (GTI-FM-XXX. Matriz de Alertas SOC), de forma que pueda ser consultada y actualizada ágilmente por todo el equipo. El Anexo 1 de este procedimiento presenta un extracto de dicha matriz a manera de referencia.

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

La actualización de la matriz de alertas debe realizarse: (i) cada vez que se cree una nueva regla de correlación en la herramienta SIEM, (ii) después de cada incidente que evidencie un tipo de alerta no documentado, y (iii) como mínimo semestralmente, como parte del proceso de mejora continua del SOC. Toda modificación debe ser aprobada por el coordinador del grupo de Seguridad e informática Forense.

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

Anexo 1. Extracto de la matriz de alertas (datos reales de herramienta SIEM)

El presente extracto muestra alertas reales tomadas del histórico de la herramienta SIEM, con su severidad, fuente, primer respondiente y acción asociada. La versión completa (94 tipos de alerta) se gestiona en el archivo GTI-FM-XXX Matriz de Alertas SOC.xlsx.

Alerta (nombre real en SIEM)	Severidad	Fuente	Primer respondiente	Acción inmediata (GSIF)	Escala a (La herramienta ITSM)
Suspected DCSync attack (replication of directory services)	Alto	Microsoft Defender for Identity	Pedro	Validar el usuario/host y la IP de origen; bloquear la cuenta o forzar cambio de contraseña si corresponde.	Administración de Identidades
Multi-stage incident involving Initial access & Credential access	Alto	AAD Identity Protection	Jeny	Verificar el remitente/enlace y el resultado de la acción automática de Defender.	Seguridad de Correo / Mesa de Servicio
Password Spray involving one user	Alto	AAD Identity Protection	Jeny	Validar el usuario/host y la IP de origen; bloquear la cuenta o forzar cambio de contraseña si corresponde.	Administración de Identidades
'Cerdigent' high-severity malware was detected	Baja	Antivirus	Andres	Confirmar que el archivo fue puesto en cuarentena o eliminado; verificar ejecución previa.	Infraestructura / Ciberseguridad Endpoint
Connection to a custom network indicator	Informativo	TI personalizada	Perzonalizado	Bloquear el indicador (IP/dominio) y aislar el host de origen mientras se confirma el alcance.	Redes / Seguridad Perimetral

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

Anexo 2. Plantilla de Requerimientos SOC

Formato oficial que los analistas del SOC o el Grupo de Seguridad e Informática Forense diligencia una vez analizada cada alerta, y que se anexa al caso escalado en la herramienta ITSM (ver numeral 5.2.4.). El archivo editable se gestiona de forma independiente ("Plantilla_Requerimientos_SOC.xlsx").

CENTRO DE OPERACIONES DE SEGURIDAD – SOC - GSIF	
INFORMACIÓN	**DETALLE**
Fecha y hora del evento	
Activo o cuenta comprometida	
Dirección IP	
Tipo de Evento	
Severidad SIEM	Informativo / Baja / Media / Alto
No Ticket La herramienta ITSM	
Descripción del Evento	
Acciones Realizadas por el SOC - GSIF	
Acciones Requeridas por parte del Especialista	
Recomendaciones del Grupo GSIF	

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

6. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
001	11/09/2026	Se crea la primera versión de la guía de gestión del SOC

Elaboró	Revisó	Aprobó
Nombre: Leidy A. Clavijo Cargo: Contratista – Grupo de Seguridad e informática Forense Fecha: 31 de agosto de 2026	Nombre: Rocio Pedrozo Cargo: Coordinador Grupo Seguridad e informática Forense Fecha: 31 de agosto de 2026	Nombre: Ricardo Ríos Rosales Cargo: director de Tecnología de la Información y las Comunicaciones Fecha: 11 de septiembre de 2026

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