

## INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

### 1. OBJETIVO

Establecer el procedimiento y lineamientos para la **identificación, detección, registro, análisis y clasificación** de incidentes de seguridad de la información dentro de la organización, con el fin de responder de manera oportuna y minimizar los impactos tecnológicos, operativos, legales y reputacionales.

### 2. ALCANCE

Este documento aplica a:

- Todos los usuarios internos, contratistas y terceros que utilicen los sistemas de información o accedan a la red de la organización.
- Equipos, aplicaciones, servicios en la nube, redes internas y recursos informáticos.
- Toda información tratada, almacenada o transmitida.

### 3. DEFINICIONES

#### 3.1 Evento de Seguridad

Cualquier alerta, comportamiento o señal anómala detectada en un sistema, red o aplicación que podría indicar un problema de seguridad.

**Ejemplos:**

- Intentos de inicio de sesión fallidos.
- Alertas del antivirus.
- Conexiones inusuales.

#### 3.2 Incidente de Seguridad

Un evento o conjunto de eventos que comprometen, o podrían comprometer, la **confidencialidad, integridad, disponibilidad o trazabilidad** de la información.

**Ejemplos:**

- Acceso no autorizado.
- Infección por malware.
- Exfiltración de datos personales.
- Caída de servicios críticos.
- Vulneración de datos personales (requiere análisis de notificación ante la SIC y MINTIC).

### 3.3 Indicadores de Compromiso (IoC)

Elementos técnicos que permiten identificar actividad maliciosa o no autorizada.

Ej.: IPs maliciosas, hashes de malware, procesos sospechosos.

## 4. PRINCIPIOS RECTORES DEL PROCESO

- **Detección temprana:** reducir el tiempo entre el inicio del incidente y su reconocimiento.
- **Registro obligatorio:** todos los eventos deben registrarse.
- **Preservación de evidencia:** la información técnica debe conservarse íntegra.
- **Confidencialidad:** solo el personal autorizado debe conocer los detalles.
- **Trazabilidad:** todas las acciones deben quedar documentadas.
- **Conformidad legal:** atención a normas colombianas de protección de datos personales.

## 5. FUENTES DE DETECCIÓN E IDENTIFICACIÓN

### 5.1 Fuentes Automáticas

La organización contará con sistemas que generen alertas automáticas:

- **SIEM** o plataforma de correlación de eventos.
- **EDR/XDR** para monitoreo de endpoints.
- **Antivirus y antimalware.**
- **Firewall/IDS/IPS.**
- **Sistemas de detección de anomalías de red.**
- **Logs de servidores, bases de datos, AD, VPN y aplicaciones.**
- **Sistemas cloud (Azure/AWS/GCP) con alertas nativas.**

### 5.2 Fuentes Humanas

- Reportes de usuarios internos.
- Alertas del área de TI o Mesa de Ayuda.
- Hallazgos de auditoría interna o externa.
- Notificaciones de proveedores críticos.

- Alertas del **CSIRT-Colombia** o entidades CERT.

## 6. PROCEDIMIENTO DE IDENTIFICACIÓN

La identificación es la primera fase del proceso de gestión de incidentes. Consta de:

### 6.1 Recepción del Evento

Un evento puede recibirse por:

- Alerta automática,
- Reporte manual,
- Sistema de monitoreo,
- Proveedor externo,
- Aviso de autoridad.

### 6.2 Análisis Inicial (Triage)

El analista o responsable deberá:

1. Validar si la alerta es real.
2. Revisar logs relacionados.
3. Identificar si el comportamiento corresponde a actividad normal.
4. Determinar si el evento tiene potencial impacto.

El triage debe realizarse en un tiempo máximo de **30 minutos**, salvo circunstancias justificadas.

## 7. CRITERIOS PARA DETERMINAR SI ES INCIDENTE

### 7.1 Indicadores Técnicos de Riesgo

- Múltiples intentos fallidos de autenticación.
- Elevación de privilegios sin justificación.
- Instalación de software desconocido.
- Procesos inusuales o conexiones externas anómalas.
- Tráfico irregular fuera de horarios laborales.
- Cambios no autorizados en configuraciones.

- Detección de archivos ejecutables sospechosos.

## 7.2 Impacto Potencial

- Afectación a datos personales (riesgo regulatorio según Ley 1581/2012).
- Interrupción total o parcial de un servicio crítico.
- Acceso no autorizado a información confidencial.
- Alteración o pérdida de integridad de la información.
- Exposición pública de datos.

## 7.3 Probabilidad de Explotación

- Existencia de vulnerabilidades sin parche.
- Coincidencia con indicadores de compromiso conocidos.
- Ataques activos en la región reportados por CSIRT-Colombia.

Si el evento cumple uno o más de estos criterios, **se declara incidente de seguridad**.

## 8. REGISTRO DEL EVENTO / INCIDENTE

Todo evento debe registrarse en el **Registro de Incidentes** con:

- Fecha y hora.
- Usuario o fuente que lo detectó.
- Tipo de evento.
- Sistemas afectados.
- Evidencias (logs, capturas, archivos hash).
- Clasificación inicial (Evento / Incidente).
- Analista a cargo.
- Observaciones.

El registro debe mantenerse seguro, con integridad garantizada y acceso restringido.

## 9. INDICADORES DE COMPROMISO (IoC)

La organización mantendrá un repositorio de IoC actualizado periódicamente, incluyendo:

- IPs, dominios o URLs maliciosas.
- Hashes de malware.
- Firmas de ataques conocidos.
- Patrones de comportamiento anómalo.
- Procesos, puertos y servicios no habituales.

Los IoC deben integrarse al SIEM y EDR.

## 10. HERRAMIENTAS PARA LA IDENTIFICACIÓN

Se debe disponer de al menos:

- Consola EDR/XDR.
- SIEM.
- Firewall con IDS/IPS.
- Sistemas de monitoreo de integridad (FIM).
- Dashboards de tráfico en tiempo real.
- Alertas automáticas basadas en reglas.

## 11. ASEGURAMIENTO DE EVIDENCIA

Para garantizar la cadena de custodia se deben seguir estas pautas:

- Preservar logs sin alteraciones.
- Generar hash de archivos relevantes.
- Registrar la fuente y fecha de captura.
- Almacenar la evidencia en repositorios protegidos.
- Evitar apagar sistemas comprometidos si afecta la evidencia.

## 12. ESCALAMIENTO

El incidente debe escalar inmediatamente a:

- Responsable de Seguridad de la Información.

- Líder del proceso afectado.
- Alta Dirección (según criticidad).

Si hay afectación a datos personales, se activa análisis para determinar **reporte a la SIC** según obligación legal colombiana.

### 13. CAPACITACIÓN EN DETECCIÓN TEMPRANA

Todo el personal debe capacitarse para identificar señales como:

- Mensajes extraños solicitando contraseña.
- Comportamientos inusuales del equipo.
- Archivos modificados sin intervención del usuario.
- Lentitud o bloqueos anormales.
- Ventanas emergentes o aplicaciones no instaladas.

Los usuarios son un sensor clave dentro del SGSI.

### 14. CONFIDENCIALIDAD DE LA INFORMACIÓN DEL INCIDENTE

La información del incidente debe manejarse bajo estricta confidencialidad.  
Solo el personal autorizado podrá acceder a los detalles.

Divulgar información sin autorización constituye falta disciplinaria.

### 15. CUMPLIMIENTO LEGAL Y AUDITORÍA

Este procedimiento responde a las exigencias de:

- Ley 1581 de 2012 – Protección de Datos Personales.
- Decreto 1377 de 2013.
- Decreto 1074 – Compilatorio de normas TIC.
- Ley 1273 de 2009 – Delitos informáticos.
- Guías del CSIRT Nacional – MinTIC.
- Estándares ISO/IEC 27001 y 27002.

Se realizarán auditorías internas anuales para verificar el cumplimiento del proceso.

## **16. RESPONSABILIDADES**

### **Usuarios**

- Reportar cualquier anomalía o posible incidente.

### **Área de TI**

- Monitorear sistemas y generar alertas.
- Preservar evidencias.

### **Responsable de Seguridad de la Información**

- Liderar el análisis y clasificación final.
- Coordinar la respuesta.
- Evaluar notificaciones obligatorias ante autoridades.

### **Alta Dirección**

- Aprobar recursos y decisiones estratégicas.