CURADURÍA URBANA PRIMERA DE SINCELEJO
Sucre - Colombia

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

VIGENCIA 2025

Basado en ISO/IEC 27035 - Gestión de Incidentes de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información (MSPI) - MinTIC

www.curaduriaprimerasincelejo.com.co

CONTROL DE VERSIONES

VERSIÓN	FECHA	DESCRIPCIÓN	ELABORADO POR
1.0	[DD/MM/2025]	Versión inicial del Procedimiento de Gestión de Incidentes	[Responsable]

TABLA DE CONTENIDO

1. OBJETIVO

Establecer un procedimiento sistemático para la identificación, reporte, análisis, contención, erradicación, recuperación y documentación de los incidentes de seguridad de la información que se presenten en la Curaduría Urbana Primera de Sincelejo, minimizando su impacto y previniendo su recurrencia.

2. ALCANCE

Este procedimiento aplica a todos los incidentes de seguridad de la información que afecten o puedan afectar:

- La confidencialidad, integridad o disponibilidad de los activos de información.
- Los sistemas de información, equipos y redes de la entidad.
- El sitio web institucional y servicios digitales.
- Los datos personales de ciudadanos y usuarios.
- La continuidad de las operaciones de la Curaduría.

3. DEFINICIONES

TÉRMINO	DEFINICIÓN
Evento de seguridad	Ocurrencia identificada en un sistema, servicio o red que indica una posible violación de la política de seguridad o falla de controles.
Incidente de seguridad	Uno o varios eventos de seguridad no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una amenaza.
Amenaza	Causa potencial de un incidente no deseado que puede resultar en daño a un sistema u organización.
Contención	Acciones para limitar el alcance y magnitud de un incidente de seguridad.
Erradicación	Eliminación de la causa raíz del incidente de los sistemas afectados.
Recuperación	Restauración de los sistemas y operaciones a su estado normal.

4. CLASIFICACIÓN DE INCIDENTES

4.1 Por Tipo de Incidente

TIPO	DESCRIPCIÓN	EJEMPLOS
Código malicioso	Infección por virus, ransomware, troyanos, gusanos u otro malware	Ransomware, virus, spyware
Acceso no autorizado	Intrusión a sistemas, cuentas o áreas restringidas sin permiso	Hacking, robo de credenciales
Denegación de servicio	Ataques que impiden el acceso a servicios o recursos	DDoS, saturación de red
Ingeniería social	Engaño a usuarios para obtener información o acceso	Phishing, vishing, pretexting
Fuga de información	Divulgación no autorizada de información confidencial	Filtración de datos, robo de info
Abuso de privilegios	Uso indebido de permisos por usuarios autorizados	Acceso indebido a expedientes
Daño físico	Destrucción o deterioro de equipos o instalaciones	Robo de equipos, vandalismo
Falla de sistemas	Interrupción de servicios por fallas técnicas	Caída de servidor, falla de disco

4.2 Por Nivel de Severidad

NIVEL	SEVERIDAD	CRITERIOS	TIEMPO RESP.
1	**CRÍTICO**	Afecta procesos críticos, pérdida masiva de datos, compromiso grave de confidencialidad	**< 1 hora**
2	**ALTO**	Afecta varios sistemas o usuarios, interrupción significativa del servicio	**< 4 horas**
3	**MEDIO**	Afecta un sistema o proceso, impacto limitado en la operación	**< 8 horas**
4	**BAJO**	Impacto menor, se resuelve con procedimientos estándar	**< 24 horas**

5. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDADES
Todos los colaboradores	• Reportar inmediatamente cualquier evento o incidente sospechoso • Preservar evidencia (no apagar equipos sin indicación) • Seguir las instrucciones del equipo de respuesta
Responsable de Seguridad	• Coordinar la respuesta a incidentes • Clasificar la severidad del incidente • Decidir sobre escalamiento • Documentar el incidente y lecciones aprendidas
Líder Técnico / Webmaster	• Ejecutar acciones técnicas de contención y erradicación • Recuperar sistemas afectados • Preservar logs y evidencia digital • Implementar controles correctivos
Curador Urbano	• Aprobar acciones de alto impacto (apagar sistemas, notificar autoridades) • Autorizar comunicaciones externas • Asignar recursos adicionales si se requieren
Área Jurídica	• Asesorar sobre implicaciones legales • Coordinar notificaciones a autoridades (COLCERT, SIC) • Gestionar denuncias si corresponde

6. FASES DEL PROCEDIMIENTO

6.1 FASE 1: PREPARACIÓN

Actividades preventivas para estar preparados ante incidentes:

#	ACTIVIDAD	RESPONSABLE
1.1	Mantener actualizada la información de contacto del equipo de respuesta	Resp. Seguridad
1.2	Capacitar al personal sobre identificación y reporte de incidentes	Resp. Seguridad
1.3	Mantener herramientas de respuesta disponibles (antivirus, backups, logs)	Líder Técnico
1.4	Realizar simulacros periódicos de respuesta a incidentes	Resp. Seguridad

6.2 FASE 2: IDENTIFICACIÓN Y REPORTE

#	ACTIVIDAD	RESPONSABLE
2.1	Detectar el evento de seguridad (usuario, sistema de monitoreo, etc.)	Cualquier colaborador
2.2	Reportar inmediatamente al Responsable de Seguridad (correo, teléfono, presencial)	Quien detecta
2.3	Recopilar información inicial: ¿qué?, ¿cuándo?, ¿dónde?, ¿quién detectó?	Resp. Seguridad
2.4	Verificar si es un incidente real o falsa alarma	Resp. Seguridad
2.5	Clasificar el tipo e impacto del incidente	Resp. Seguridad
2.6	Registrar el incidente en el formato de reporte (Anexo A)	Resp. Seguridad

6.3 FASE 3: CONTENCIÓN

#	ACTIVIDAD	RESPONSABLE
3.1	Aislar el equipo o sistema afectado de la red (si aplica)	Líder Técnico
3.2	Preservar evidencia (NO apagar equipos, copiar logs, capturas de pantalla)	Líder Técnico
3.3	Cambiar credenciales comprometidas inmediatamente	Líder Técnico
3.4	Bloquear direcciones IP o usuarios maliciosos (si se identifican)	Líder Técnico
3.5	Evaluar si se requiere activar el Plan de Continuidad del Negocio	Resp. Seguridad

6.4 FASE 4: ERRADICACIÓN

#	ACTIVIDAD	RESPONSABLE
4.1	Identificar la causa raíz del incidente	Líder Técnico
4.2	Eliminar el malware, código malicioso o vulnerabilidad explotada	Líder Técnico
4.3	Aplicar parches de seguridad o actualizaciones necesarias	Líder Técnico
4.4	Verificar que no existan backdoors o persistencia del atacante	Líder Técnico

6.5 FASE 5: RECUPERACIÓN

#	ACTIVIDAD	RESPONSABLE
5.1	Restaurar sistemas desde backups limpios (si es necesario)	Líder Técnico
5.2	Verificar el funcionamiento correcto de los sistemas restaurados	Líder Técnico
5.3	Reconectar sistemas aislados a la red de forma gradual	Líder Técnico
5.4	Monitorear intensivamente durante las primeras 24-48 horas	Resp. Seguridad
5.5	Comunicar a usuarios afectados el restablecimiento del servicio	Resp. Seguridad

6.6 FASE 6: LECCIONES APRENDIDAS

#	ACTIVIDAD	RESPONSABLE
6.1	Documentar completamente el incidente (cronología, acciones, resultados)	Resp. Seguridad
6.2	Realizar reunión post-incidente con el equipo involucrado	Resp. Seguridad
6.3	Identificar mejoras en controles, procedimientos o capacitación	Resp. Seguridad
6.4	Actualizar la matriz de riesgos si se identificaron nuevas amenazas	Resp. Seguridad
6.5	Cerrar formalmente el incidente y archivar la documentación	Resp. Seguridad

7. DIAGRAMA DE FLUJO DEL PROCEDIMIENTO

[El diagrama de flujo se presenta de forma simplificada a continuación]

INICIO: Detección del evento
↓
1. REPORTE al Responsable de Seguridad
↓
2. VERIFICACIÓN: ¿Es un incidente real?
↓ SÍ NO → Cerrar como falsa alarma
3. CLASIFICACIÓN de tipo y severidad
↓
4. CONTENCIÓN: Aislar, preservar evidencia
↓
5. ERRADICACIÓN: Eliminar causa raíz
↓
6. RECUPERACIÓN: Restaurar sistemas
↓
7. LECCIONES APRENDIDAS: Documentar y mejorar
↓
FIN: Cierre del incidente

8. TIEMPOS DE RESPUESTA

SEVERIDAD	RESPUESTA	CONTENCIÓN	RESOLUCIÓN
CRÍTICO	< 15 min	< 1 hora	< 4 horas
ALTO	< 30 min	< 4 horas	< 24 horas
MEDIO	< 2 horas	< 8 horas	< 48 horas
BAJO	< 8 horas	< 24 horas	< 72 horas

9. COMUNICACIÓN Y ESCALAMIENTO

9.1 Matriz de Escalamiento

SEVERIDAD	NOTIFICAR A	ENTIDADES EXTERNAS
CRÍTICO	Curador Urbano (inmediato), Área Jurídica	COLCERT, Fiscalía (si hay delito), SIC (si hay datos personales)
ALTO	Curador Urbano (< 4 horas)	COLCERT (si es ciberataque)
MEDIO	Informe en próxima reunión	No requerido
BAJO	Registro en bitácora	No requerido

9.2 Contactos para Reporte Externo

- COLCERT (Centro Cibernético Policial): contacto@colcert.gov.co
- CAI Virtual: caivirtual.policia.gov.co
- Superintendencia de Industria y Comercio (datos personales): contactenos@sic.gov.co

10. REGISTRO Y DOCUMENTACIÓN

Todos los incidentes de seguridad deben ser documentados y conservados. La documentación incluye:

- Formato de Reporte de Incidentes (Anexo A) completamente diligenciado.
- Evidencia digital preservada (logs, capturas, archivos maliciosos aislados).
- Comunicaciones realizadas durante la gestión del incidente.
- Informe de lecciones aprendidas.

Tiempo de retención: Mínimo 5 años o según lo establecido en las Tablas de Retención Documental.

11. INDICADORES DE GESTIÓN

INDICADOR	FÓRMULA / MEDICIÓN	META
Tiempo promedio de respuesta	Suma de tiempos de respuesta / Número de incidentes	< 30 minutos
Tiempo promedio de resolución	Suma de tiempos de resolución / Número de incidentes	< 24 horas
Incidentes recurrentes	Incidentes del mismo tipo repetidos / Total incidentes	< 10%
Efectividad de controles	Incidentes evitados / Intentos detectados	≥ 90%
Cumplimiento de SLA	Incidentes resueltos en tiempo / Total incidentes	≥ 95%

ANEXO A - FORMATO DE REPORTE DE INCIDENTES DE SEGURIDAD

INFORMACIÓN GENERAL	
Número de incidente:	INC-2025-____
Fecha y hora de detección:	
Reportado por:	
Medio de reporte:	☐ Correo ☐ Teléfono ☐ Presencial ☐ Sistema
CLASIFICACIÓN	
Tipo de incidente:	☐ Malware ☐ Acceso no autorizado ☐ Phishing ☐ Fuga info ☐ Otro: ____
Severidad:	☐ Crítico ☐ Alto ☐ Medio ☐ Bajo
Sistemas/activos afectados:	
DESCRIPCIÓN	
Descripción del incidente:	
Impacto observado:	
ACCIONES TOMADAS	
Acciones de contención:	
Acciones de erradicación:	
Acciones de recuperación:	
CIERRE	
Fecha y hora de resolución:	
Causa raíz identificada:	
Lecciones aprendidas:	
Acciones preventivas:	
Responsable del cierre:	Firma: _____

URL de Publicación: https://curaduriaprimerasincelejo.com.co/transparencia/seguridad-digital/gestion-incidentes