

**Procedimiento de Gestión de Incidentes de Seguridad de la Infiormación**

**PROYECTO: SOFTWARE PARA LA CREACIÓN DE LA APLICACIÓN “ALERTA MUJER”**

**INTEGRANTES:**

**LUIS DAVID CONDE SANCHEZ FREINIER CARDONA PEREZ ANDRES FELIPE CUELLAR GOMEZ**

**INSTRUCTOR:**

**Javier Humberto Pinto Diaz**

**SERVICIO NACIONAL DE APRENDIZAJE – SENA**

**ANALISIS Y DESARROLLO DE SOFTWARE – 3145555**

**2025**

TABLA DE CONTENIDO

1. **Propósito y Alcance**
   1. **Propósito**
   2. **Alcance**
2. **Defiinición y Clasifiicación del Incidente**
   1. **Niveles de Gravedad**
3. **Fases del Proceso de Gestión de Incidentes**
   1. **Fase 1: Detección y Reporte**
   2. **Fase 2: Análisis y Evaluación**
   3. **Fase 3: Contención**
   4. **Fase 4: Erradicación y Recuperación**
   5. **Fase 5: Lecciones Aprendidas (Post-Incidente)**
4. **Pruebas y Revisión**

**Procedimiento de Gestión de Incidentes de Seguridad de la Infiormación (Control 5.24)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Propietario del Proceso** | **Control ISO 27001** |
| 1.0 | 2025-10-02 | Administrador de Operaciones (DevOps) | 5.24 Gestión de incidentes de seguridad de la información |

# Propósito y Alcance

## Propósito

Definir un proceso estructurado para la detección, el reporte, la respuesta, la contención y la recuperación de cualquier evento que comprometa la **Confidencialidad**, la **Integridad** o la **Disponibilidad (RNF1.1)** de los activos de "Alerta Mujer", priorizando la protección de los datos **CONFIDENCIALES (Control 5.12)** de las usuarias.

## Alcance

Aplica a todos los activos del **Inventario (Control 5.9)** y a todo el personal (Desarrolladores, DevOps, Líder de Proyecto) en todas las fases de desarrollo y operación.

# Defiinición y Clasifiicación del Incidente

Un **Incidente de Seguridad** es cualquier evento adverso que interrumpe la operación normal del proyecto o viola la **Política de Seguridad Marco**.

## Niveles de Gravedad

La clasificación determina la urgencia de la respuesta.

|  |  |  |  |
| --- | --- | --- | --- |
| **Nivel** | **Impacto en el** | **Ejemplo** | **Tiempo Máximo** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Servicio** |  | **de Respuesta** |
| **CRÍTICO (Nivel 3)** | Fuga de Datos CONFIDENCIALES  (PII/GPS) o caída total de la Base de Datos. | Ataque de Inyección SQL exitoso o *Ransomware* en el servidor. | **< 15 Minutos** (El DevOps debe ser notificado inmediatamente por SMS o llamada). |
| **ALTO (Nivel 2)** | Pérdida de una funcionalidad crítica o denegación parcial del servicio. | Un *bug* en el servidor impide que el 50% de las usuarias envíen la alerta o caída de un servicio externo (Proveedor). | **< 1 Hora** |
| **MEDIO/BAJO**  **(Nivel 1)** | Fallo de funcionalidad no crítica o detección de vulnerabilidad sin explotación. | Falla menor en la BD de *Logs* o detección de un CVE de riesgo medio (Control 5.7). | **< 24 Horas** (Generar un Ticket de Seguridad). |

# Fases del Proceso de Gestión de Incidentes

El proceso de respuesta se divide en seis fases obligatorias, con el **Administrador de Operaciones (DevOps)** como el líder técnico de la respuesta.

## Fase 1: Detección y Reporte

**Objetivo:** Identificar la anomalía y escalar al responsable.

1. **Detección:** El incidente puede ser detectado por:
   * **Monitoreo Automático:** Alertas de la nube (CPU alta, tráfico inusual, BD caída).
   * **Usuario Final:** Reporte de fallo de la aplicación o comportamiento anómalo.
   * **Inteligencia de Amenazas (Control 5.7):** Detección de una vulnerabilidad crítica que está siendo explotada activamente en la industria.
2. **Reporte:** El Líder del Proyecto o el Desarrollador que detecte el problema debe notificar inmediatamente al **DevOps** por el canal de comunicación crítica (ej. grupo de chat interno o llamada).

## Fase 2: Análisis y Evaluación

**Objetivo:** Determinar la gravedad y el alcance del impacto.

1. **Clasificación:** El DevOps clasifica el incidente según la Sección 2.1 (Nivel 1, 2 o 3).
2. **Activo Afectado:** Identificar qué activos del **Inventario (Control 5.9)** están comprometidos (ej. INF-001 PII, HW-001 Servidor).
3. **Registro:** El incidente debe ser registrado en el sistema de seguimiento con fecha, hora, clasificación y descripción inicial.

## Fase 3: Contención

**Objetivo:** Detener la amenaza y evitar mayor daño.

1. **Aislamiento:** Para incidentes **CRÍTICOS**, el DevOps debe tomar medidas técnicas inmediatas (ej. bloquear una IP maliciosa en el *firewall*, aislar el servidor de producción de la red de desarrollo).
2. **Backup:** Asegurar que la última copia de seguridad íntegra de la BD (Control 5.23) no haya sido comprometida antes de que el ataque empeore.

## Fase 4: Erradicación y Recuperación

**Objetivo:** Eliminar la causa raíz y restaurar la operación normal.

1. **Erradicación:** El equipo de Desarrollo corrige la vulnerabilidad (Control 8.27) y el DevOps limpia los artefactos maliciosos del sistema.
2. **Recuperación:** Se restaura el servicio y, si fue necesario, se aplica el *backup* de la BD. El DevOps verifica el funcionamiento normal antes de reabrir el acceso a todos los usuarios.
3. **Notificación de Escalada (Control 5.6):** Para incidentes **CRÍTICOS**, el Líder del Proyecto debe notificar a los **Grupos de Interés Interno (SENA)** para coordinar la respuesta institucional.

## Fase 5: Lecciones Aprendidas (Post-Incidente)

**Objetivo:** Prevenir la recurrencia.

1. **Reunión Post-Incidente:** En un plazo no mayor a **48 horas** después de la recuperación, el equipo se reúne para revisar:
   * ¿Funcionó el plan de contención?
   * ¿Cuál fue la causa raíz (ej. contraseña débil, *input* no sanitizado)?
   * ¿Qué cambios se deben hacer al SGSI (ej. mejorar el *firewall*, cambiar la Política 5.10)?
2. **Actualización del SGSI:** Se genera un **plan de acción** con tareas asignadas para modificar procedimientos, código o configuraciones para evitar que la vulnerabilidad sea explotada de nuevo.

# 4. Pruebas y Revisión

1. **Simulacros:** Se recomienda al Líder del Proyecto ejecutar simulacros de incidentes (ej. simular una inyección SQL o una denegación de servicio) al menos **una vez al ciclo formativo** para evaluar la efectividad del tiempo de respuesta.
2. **Evidencia de Cumplimiento:** Los *tickets* de seguridad cerrados y las actas de las reuniones de "Lecciones Aprendidas" sirven como prueba de que el Control 5.24 está operativo.

LIDER DEL PROYECTO. EQUIPO DE TRABAJO. EQUIPO DE TRABAJO.