Procedimiento de Notificación de Incidentes de Seguridad

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

Procedimiento de Notificación de Incidentes de Seguridad (Control 6.8)

Versión	Fecha	Propietario del Proceso	Control ISO 27001
1.0	2025-10-03	Líder del Proyecto / Todo el Personal	6.8 Notificación de incidentes de seguridad de la información

1. Propósito y Alcance

1.1 Propósito

Asegurar que cualquier evento de seguridad percibido, ya sea un fallo, una sospecha o un incidente confirmado, sea notificado de manera oportuna, clara y completa por cualquier miembro del equipo al **Líder del Proyecto** y al **Administrador de Operaciones (DevOps)** para su análisis y mitigación inmediata.

1.2 Alcance

Este procedimiento es de aplicación obligatoria para **todo el personal** involucrado en el diseño, desarrollo, operación o gestión de los activos del proyecto "Alerta Mujer".

2. Definición y Ejemplos de Eventos de Seguridad

Un **Evento de Seguridad** es cualquier suceso en el sistema que pueda indicar un fallo de la seguridad o una posible violación de las políticas. No todos los eventos son incidentes, pero todos deben ser notificados.

Categoría	Definición	Ejemplo en "Alerta Mujer"
Fallo de Política/Control	Un control de seguridad no se aplicó o falló.	El *password hash* de un usuario se filtró

		accidentalmente en un log de prueba.
Fallo Técnico/Error	Un componente del sistema se comporta de forma inesperada.	Un Desarrollador descubre que una librería de cifrado tiene una vulnerabilidad (CVE) publicada.
Acceso No Autorizado	Intento o éxito de acceso a un activo sin la debida autorización.	El Administrador de Operaciones nota accesos fallidos masivos al servidor por SSH (*Brute Force*).
Phishing / Ingeniería Social	Solicitudes sospechosas que buscan obtener información sensible.	Un correo electrónico llega al equipo pidiendo credenciales del servidor haciéndose pasar por el SENA.

3. Mecanismo y Formato de Notificación

El equipo debe utilizar la vía más rápida para notificar al Líder del Proyecto y al DevOps simultáneamente.

3.1 Canal de Notificación

El canal primario para la notificación inmediata es el **grupo de chat CRÍTICO** del proyecto o, en su defecto, un correo electrónico con la etiqueta **[ALERTA SEGURIDAD]** en el asunto, dirigido a:

- Líder del Proyecto.
- Administrador de Operaciones (DevOps).

3.2 Información Mínima Requerida (5W)

Para que el DevOps pueda actuar rápidamente, la notificación debe contener la siguiente información obligatoria:

1. **QUÉ (*What*):** Descripción concisa del evento o anomalía observada.
    - *Ejemplo: "La página de login está devolviendo un error 500 después de introducir caracteres especiales."*
2. **DÓNDE (*Where*):** Activo afectado (Módulo de la App, servidor de BD, Repositorio Git, Cuenta de Proveedor).

    - *Ejemplo: "Servidor de Producción (HW-001) / API de autenticación."*
3. **CUÁNDO (*When*):** Fecha y hora estimada de la detección.
4. **QUIÉN (*Who*):** Nombre y Rol del reportante.
5. **CÓMO (*How*):** Pasos para reproducir el fallo o qué se estaba haciendo cuando ocurrió.
    - *Ejemplo: "Estaba probando la sanitización de inputs del formulario de registro."*

> ⚠**Recordatorio Crítico:** Nunca se deben incluir contraseñas, claves de API o datos CONFIDENCIALES de usuarias reales en el cuerpo del mensaje de notificación. Solo se hace referencia al activo afectado.

4. Flujo de Respuesta Inmediata

Una vez recibida la notificación, se activa el **Procedimiento de Contacto (Control 5.6)** y el **Manual de Gestión de Incidentes (Control 5.24)**:

1. **Reporte (Todo el Personal):** El reportante notifica de inmediato (Sección 3.2).
2. **Recepción y Triage (DevOps/Líder):** El DevOps valida la información y determina si es un incidente **CRÍTICO** que requiere Contención.
3. **Contención (DevOps):** Si se confirma la amenaza, el DevOps inicia la Fase 1 del Protocolo de Respuesta (Contención, 15 minutos).
4. **Registro:** El Líder del Proyecto abre un registro formal del incidente con la información inicial de la notificación y asigna las Acciones Correctivas.

5. Evidencia de Cumplimiento

La evidencia de que el Control 6.8 está implementado incluye:

- **Registro de Reporte:** El hilo del grupo de chat o el correo electrónico que contiene la información mínima requerida (5W).
- **Lecciones Aprendidas:** El registro del incidente (Control 5.24) que demuestra que la notificación inicial (el reporte) fue procesada y llevó a una acción correctiva formal.
- **Simulacros:** La documentación de los **Simulacros de Incidentes (Control 5.33)** donde se verifica que el personal sabe cómo y a quién notificar en tiempo y forma.