

# Procedimiento de Gestión de la Inteligencia de Amenazas

### 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**

### Alcance

1. **Clasificación de la Inteligencia de Amenazas**
2. **Ciclo de Vida de la Inteligencia de Amenazas** 4.1Fase I: Recolección (Monitoreo Semanal) 4.2Fase II: Análisis y Priorización

### Indicadores de cumplimiento

**Procedimiento de Gestión de la Inteligencia de Amenazas (Control 5.7)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Propietario del Proceso** | **Control ISO 27001** |
| 1.0 | 2025-10-02 | Administrador de Operaciones (DevOps) | 5.7 Inteligencia de amenazas |

# Propósito

Definir los pasos operativos para la recopilación, el análisis, la priorización y la aplicación de contramedidas basadas en la Inteligencia de Amenazas relevante para el proyecto "Alerta Mujer". El objetivo final es reducir la **Ventana de Exposición** (el tiempo que el sistema permanece vulnerable) al mínimo posible.

# Alcance

Este procedimiento es de aplicación obligatoria para el **Administrador de Operaciones (*DevOps*)** (responsable de la recolección y análisis) y el equipo de **Desarrollo (*Devs*)** (responsable de la mitigación e implementación).

# Clasifiicación de la Inteligencia de Amenazas

La inteligencia se clasifica según su origen y su impacto potencial en el proyecto:

|  |  |  |  |
| --- | --- | --- | --- |
| **Nivel de Inteligencia** | **Fuente Principal (Control 5.6)** | **Ejemplo de Amenaza** | **Acción Requerida** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Estratégica** | Boletines de tendencias de seguridad móvil (OWASP). | Tendencia creciente de ataques de *phishing* dirigidos a Apps de seguridad. | Actualizar la formación del equipo (Control 6.3) y la interfaz de usuario. |
| **Operacional** | Alertas de Seguridad del SENA. | Detección de una intrusión en el *firewall* del entorno de *hosting*. | Aislamiento inmediato de la red y Contención del incidente (Control 5.6, Fase 1). |
| **Técnica (CRÍTICA)** | NIST NVD (CVE),  boletines de Android/iOS. | Nuevo *bug* crítico (CVE) en la librería de *hashing* de contraseñas utilizada. | **Parcheo obligatorio e inmediato** de código (Control 8.27). |

# Ciclo de Vida de la Inteligencia de Amenazas

## Fase I: Recolección (Monitoreo Semanal)

* + **Responsable:** Administrador de Operaciones (*DevOps*).
  + **Actividad:** Monitoreo semanal (mínimo) de las fuentes de la Categoría C (Inteligencia Externa) y registro de las alertas de la Categoría A (Interno Crítico - SENA) si son emitidas.
  + **Registro:** Toda alerta potencialmente relevante debe ser registrada en un sistema de seguimiento interno (ej. una hoja de cálculo o un *backlog* de seguridad) con su ID de fuente (ej. ID de CVE).

## Fase II: Análisis y Priorización

* + **Responsable:** Administrador de Operaciones, con consulta al Líder del Proyecto.
  + **Actividad:** Evaluar el impacto. Una amenaza es **Relevante** si afecta a:

1. El sistema operativo móvil (Android) soportado por la aplicación.
2. La base de datos (BD) o la infraestructura de *hosting*.
3. Las librerías de terceros (cifrado, autenticación) utilizadas.
   * **Priorización (Riesgo):** Las amenazas se priorizan siguiendo una escala de riesgo (Bajo, Medio, Alto, **Crítico**). Cualquier amenaza que comprometa la **Confidencialidad de la PII (RNF4.2)** o la **Disponibilidad 24/7 (RNF1.1)** se clasifica automáticamente como **CRÍTICA**.

## Fase III: Producción (Generación de Tickets de Seguridad)

* + **Responsable:** Administrador de Operaciones.
  + **Actividad:** Generar un **Ticket de Seguridad formal** para cada amenaza relevante y clasificada como Media o superior. El ticket debe incluir:

1. Descripción concisa del problema (ej. "Inyección SQL de día cero").
2. **Activo Afectado** (ej. "Módulo de Login/BD de usuarios").
3. **Acción Específica Requerida** (ej. "Actualizar librería X a versión Y" o "Añadir sanitización de *input* al formulario de login").

### Asignación:

* + - **Devs:** Tareas de codificación segura (Control 8.27).
    - **DevOps:** Tareas de configuración de servidor (*hardening*, Control 8.9).

## Fase IV: Mitigación y Cierre

* + **Responsable:** Equipo de Desarrollo o Equipo de Operaciones, según la asignación del ticket.
  + **Actividad:** Implementar la corrección, realizar pruebas (Control 8.29) y documentar la acción tomada.
  + **Verificación:** El Administrador de Operaciones verifica que la vulnerabilidad haya sido mitigada y cierra el ticket, marcando la **Fecha de Cierre**.

# Indicadores de Cumplimiento

El éxito de la Inteligencia de Amenazas se mide con la **Velocidad de Reacción**:

### Métrica: Tiempo Promedio de Parcheo (TPP).

* **Definición:** TPP es el tiempo que transcurre desde que se detecta y registra una amenaza (Fase I) hasta que se implementa y verifica su mitigación (Fase IV).
* **Objetivo del Proyecto:** El TPP para amenazas de riesgo **CRÍTICO** debe ser inferior a **72 horas**.

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