Procedimiento de Gestión de la Seguridad en el Ciclo de Vida del Proyecto

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 Gestión de la Seguridad en el Ciclo de Vida del Proyecto (Control 5.8)

Versión	Fecha	Propietario del Proceso	Control ISO 27001
1.0	2025-10-02	Líder del Proyecto / Docente Guía	5.8 Gestión de seguridad de la información del proyecto

1. Propósito

Garantizar que los requisitos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad) identificados en la **Política Marco (5.1)** se aborden y mantengan durante todas las fases de desarrollo e implementación del proyecto "Alerta Mujer", desde el diseño inicial hasta el despliegue en producción.

2. Alcance

Este procedimiento aplica a todo el equipo del proyecto: **Líder, Desarrolladores (*Devs*), Administrador de Operaciones (*DevOps*) y Docente Guía**.

3. Integración de la Seguridad por Fases (DevSecOps)

La seguridad se trata como una actividad continua y no como un paso final. La siguiente tabla describe las tareas obligatorias de seguridad en cada fase del ciclo de vida del proyecto:

Fase del Proyecto	Tarea Obligatoria de Seguridad	Responsable Principal	Control ISO Relacionado
I. Definición y Diseño	**Análisis de Requisitos de Seguridad:** Revisar y aprobar los Requisitos No Funcionales de Seguridad (**RNF4.1 - Cifrado**, **RNF1.1 - Disponibilidad 24/7**) antes de iniciar el código.	Líder del Proyecto	8.26 (Requisitos de la aplicación)
II. Implementación (Codificación)	**Principios de Codificación Segura:** Los *Devs* deben seguir las guías de **OWASP Top 10** (ej. sanitización de *inputs* para evitar Inyección SQL).	Desarrolladores (*Devs*)	8.27 (Principios de codificación segura)
III. Pruebas y Aseguramiento	**Pruebas de Seguridad (Pen-Testing):** Realizar pruebas funcionales y de seguridad (ej. intentar inyectar código en formularios, verificar que el	Desarrolladores / DevOps	8.29 (Pruebas de seguridad)

	hashing funciona).		
IV. Despliegue (Producción)	**Revisión de Configuración Segura (*Hardening*):** DevOps debe verificar que el servidor de producción cumpla con las configuraciones de seguridad antes de recibir tráfico real.	Administrador de Operaciones (*DevOps*)	8.9 (Gestión de la configuración)
V. Operación y Mantenimiento	**Gestión de Vulnerabilidades (Control 5.7):** Monitoreo continuo de amenazas externas (CVEs) y aplicación de parches.	Administrador de Operaciones (*DevOps*)	5.7 (Inteligencia de amenazas)

4. Gestión de Riesgos y Cambios de Seguridad

4.1. Evaluación de Riesgos Inicial (Diseño)

Durante la Fase I, el Líder del Proyecto debe realizar una **Evaluación de Impacto en la PII (DPIA)** (aunque sea simplificada) para determinar qué activos (datos de usuarias, coordenadas, evidencia) son los más críticos. Esto guiará las decisiones de cifrado y

autenticación.

4.2. Gestión de Cambios de Seguridad

Cualquier cambio propuesto que afecte a un control de seguridad debe ser aprobado formalmente:

- **Cambios Críticos:** Cualquier cambio en las tecnologías de cifrado (ej. cambiar el algoritmo de *hashing*) o en los protocolos de red (ej. deshabilitar TLS) debe ser aprobado por el **Docente Guía** y el **Líder del Proyecto** antes de ser implementado.
- **Documentación:** El cambio, la razón del cambio y la aprobación deben quedar registrados en el sistema de *versionamiento* de código (Control 8.28).

5. Documentación y Revisión

5.1. Evidencia de Cumplimiento

La evidencia de que el Control 5.8 está activo incluye:

- **Actas de Reunión:** Documentos que muestren que los requisitos de seguridad fueron revisados y aprobados en la Fase I (Diseño).
- **Revisiones de Código (*Code Reviews*):** La evidencia de que un par revisó el código de un desarrollador específicamente buscando fallos de seguridad.
- **Resultados de Pruebas:** Los reportes de las pruebas de penetración o de seguridad realizadas en la Fase III.

5.2. Revisión del Procedimiento

Este procedimiento debe ser revisado por el Líder del Proyecto y el Docente Guía **al final de cada ciclo de desarrollo (o *sprint*)** para asegurar que sigue siendo adecuado para el estado actual del proyecto.