



## **GESTIÓN DE LA CONFIGURACIÓN**

**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**
- 2. Procedimiento de Configuración Segura (*Hardening*)**
  - 2.1 Definición de Estándares de Hardening**
  - 2.2 Control de Cambios en la Configuración**
  - 2.3 Gestión del Hardening de la Aplicación**

## CONTROL: 8.9 GESTIÓN DE LA CONFIGURACIÓN

### 1. Propósito

El control 8.9 exige la definición, documentación e implementación de un proceso formal de **Gestión de la Configuración** para mantener la seguridad (*hardening*) de los sistemas y servicios. El objetivo es evitar el uso de configuraciones predeterminadas (*defaults*) inseguras o innecesarias que son fuentes comunes de vulnerabilidades (ej. contraseñas por defecto, servicios abiertos al público).

Para "Alerta Mujer", la implementación de este control es esencial para:

- **Reducir la Superficie de Ataque:** Desactivar servicios no esenciales en servidores, *firewalls* y la Base de Datos.
- **Integridad:** Asegurar que solo se utilizan componentes aprobados y con configuraciones verificadas.
- **Cumplimiento:** Servir como base para las revisiones de seguridad y las auditorías de cumplimiento.

### 2. Procedimiento de Configuración Segura (*Hardening*)

El proceso de gestión de la configuración se centrará en dos áreas: **Estándares de Configuración** y **Control de Cambios**.

#### 2.1. Definición de Estándares de *Hardening*

Se crearán y mantendrán **Líneas Base de Configuración Segura** para cada componente crítico de la arquitectura de "Alerta Mujer".

Componente	Requisito de <i>Hardening</i> Específico	Control Faltante Relacionado
<b>Servidores de Aplicación (Backend)</b>	<b>Desactivación de servicios innecesarios</b> (ej. deshabilitar acceso <i>root</i> directo, eliminar usuarios por defecto).	8.2 (Acceso privilegiado), 8.19 (Seguridad de red).
<b>Base de Datos (BD)</b>	<b>Modificación de la contraseña por defecto</b> del usuario administrador, limitación estricta de las IPs que pueden conectarse (Control 8.21).	8.2 (Acceso privilegiado), 8.21 (Separación de redes).

Componente	Requisito de <i>Hardening</i> Específico	Control Faltante Relacionado
<b>Entorno de Ejecución (Contenedores/VMs)</b>	Uso de la <b>última versión estable y hardened</b> del sistema operativo. Configurar el <i>firewall</i> local para <b>denegar por defecto</b> todo el tráfico excepto el esencial.	8.19 (Seguridad de red).
<b>Dispositivos de Red (Firewalls, Load Balancers)</b>	Desactivar la gestión remota no cifrada, asegurar la configuración de los servicios de red (DNS/NTP).	8.20 (Seguridad de servicios de red).

## 2.2. Control de Cambios en la Configuración

Para garantizar que los sistemas se mantengan seguros después del despliegue:

- **Gestión de la Configuración como Código (IaC):** Siempre que sea posible, las configuraciones (servidores, *firewalls*) deben gestionarse como código (ej. Terraform, Ansible). Esto garantiza la **inmutabilidad** y la trazabilidad (Control 8.28).
- **Revisión y Aprobación: Todo cambio** a la Línea Base de Configuración (ej. apertura de un nuevo puerto, instalación de *software*) debe ser revisado por el equipo de seguridad y aprobado antes de su implementación (Control 5.36).
- **Auditoría de Desviación:** Se implementarán herramientas automatizadas para **monitorear la configuración en vivo** de los sistemas y alertar al equipo de seguridad (Control 8.16) si un sistema se desvía de su Línea Base aprobada (ej. si alguien habilita un puerto prohibido).

## 2.3. Gestión del *Hardening* de la Aplicación

Aunque el Control 8.27 cubre el código, el 8.9 se asegura de la configuración de la App en el dispositivo.

- **Permisos de la Aplicación:** La App Móvil debe solicitar solo los **permisos absolutamente necesarios** (ej. GPS, Cámara, Micrófono). La gestión de estos permisos en el manifiesto de la aplicación debe ser revisada por seguridad antes de cada despliegue.
- **Deshabilitar Funciones de Depuración:** Asegurar que los puertos de depuración (*debugging ports*) y los *logs* internos detallados **estén deshabilitados** en el código de producción (Control 8.27).

LIDER DEL PROYECTO.

EQUIPO DE TRABAJO.

EQUIPO DE TRABAJO.