

**SEPARACIÓN DE REDES**

**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. **Principios de Separación de Redes**
   1. **Implementación de Firewall y ACLs**



# CONTROL: 8.21 SEPARACIÓN DE REDES

1. **Propósito**

El control 8.21 exige la **separación lógica o física de las redes** de los sistemas de información para mantener los servicios esenciales aislados de las redes menos seguras (ej. desarrollo) o menos controladas.

Para el proyecto "Alerta Mujer", la implementación de la separación de redes es esencial para:

* + **Aislamiento de Riesgos:** Garantizar que una vulnerabilidad o un ataque exitoso en el entorno de **Desarrollo/Prueba** no pueda acceder directamente o comprometer el entorno de **Producción** que maneja la información sensible y el servicio de alerta.
  + **Confidencialidad:** Proteger la Base de Datos (BD) de Producción (que contiene PII y evidencia cifrada) del acceso no autorizado desde segmentos de red con menos controles de seguridad.
  + **Disponibilidad:** Asegurar que el tráfico de la **Red de Administración** (que podría ser utilizado por DevOps o DBAs) no interfiera con el rendimiento o la latencia de la **Red de Producción** (la comunicación App-Servidor).

# Principios de Separación de Redes

La arquitectura de red del *backend* de "Alerta Mujer" (servidores de aplicación y BD) debe implementarse mediante una **separación lógica** utilizando subredes (VLANs o Subnets en entornos de nube) y reglas estrictas de *firewall*.

Se establecerán y aislarán al menos tres redes críticas:

|  |  |  |
| --- | --- | --- |
| Red / Segmento | Propósito | Reglas de Aislamiento Clave |
| **1. Red de Producción** | Aloja la aplicación en vivo, la BD de usuarias y los servicios de alerta. | **Prohibido el acceso**  **entrante** desde las Redes 2 y 3, excepto puertos específicos para monitoreo. Acceso solo a la App Móvil (puerto HTTPS 443). |
| **2. Red de Desarrollo/Prueba** | Aloja entornos de *staging*  y desarrollo. Maneja | **Prohibido el tráfico saliente** a la Red de Producción (Bloqueo Total). Requiere el |

|  |  |  |
| --- | --- | --- |
| Red / Segmento | Propósito | Reglas de Aislamiento Clave |
|  | datos no productivos o enmascarados. | control 8.31 (Separación de Entornos). |
| **3. Red de**  **Administración/Operación** | Utilizada por el personal de DevOps/DBA para  tareas de mantenimiento, *patching* y gestión de logs. | **Acceso estrictamente**  **controlado** (listas blancas de IPs, VPN obligatoria) y limitado a los servicios y puertos esenciales (SSH/RDP, Gestión de BD). |

* 1. **Implementación de *Firewall* y ACLs**

Se utilizarán **Listas de Control de Acceso (ACLs)** y reglas de *firewall* para forzar la separación y controlar estrictamente el flujo de tráfico entre las redes definidas:

* + - **Regla de Oro: Negar por defecto** el tráfico entre todos los segmentos (1, 2, y 3).
    - **Permitir Excepciones:** Solo se permitirán explícitamente las comunicaciones necesarias (ej. la Red de Administración puede enviar tráfico al servidor de Producción únicamente a los puertos de gestión y solo después de autenticación fuerte).
    - **Inspección de Tráfico:** Se recomienda la implementación de un *firewall* de aplicación (*Web Application Firewall - WAF*) para inspeccionar el tráfico que ingresa a la Red de Producción desde la App Móvil.

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

