

SEPARACIÓN DE LOS ENTORNOS DE DESARROLLO, PRUEBA Y PRODUCCIÓN

**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. **Objetivo**
2. **Definición y Segregación de Entornos**
3. **Controles Técnicos de Segregación**

PROCEDIMIENTO A8.31: SEPARACIÓN DE LOS ENTORNOS DE DESARROLLO, PRUEBA Y PRODUCCIÓN

1. **Objetivo**

Garantizar la **segregación estricta** de los entornos de **Desarrollo**, **Pruebas/Staging** y **Producción** para el *software* "ALERTA MUJER", asegurando que las actividades de codificación y prueba no afecten la **disponibilidad**, **integridad** y **confidencialidad** del sistema en vivo y sus datos sensibles.

1. **Definición y Segregación de Entornos**

Se establecen tres entornos principales, cada uno con una función, política de datos y control de acceso definidos:

|  |  |  |  |
| --- | --- | --- | --- |
| **ENTORNO** | **FUNCIÓN PRINCIPAL** | **POLÍTICA DE DATOS** | **CONTROL DE ACCESO** |
| **1.**  **DESARROLLO** | Codificación local (Visual Studio Code) y pruebas unitarias por parte del equipo de desarrollo. | **SOLO** datos falsos y enmascarados.  **PROHIBIDO** el  acceso a cualquier dato real. | Freinier, Luis David, Andrés Felipe. |
| **2. PRUEBAS / STAGING** | Pruebas de integración, rendimiento y auditorías de seguridad  (*pentesting*). | Datos **enmascarados** y anonimizados (copia estructurada de Producción). | Desarrolladores, QA y Auditores autorizados. |
| **3.**  **PRODUCCIÓN** | Operación de la aplicación en vivo para las usuarias finales. | **SOLO** datos reales y sensibles de las usuarias. | **MÁXIMO CONTROL.**  Exclusivo para Operaciones, sin  acceso directo a código o desarrollo. |

1. **Controles Técnicos de Segregación**

Para reforzar la separación y evitar la contaminación de entornos, se aplican los siguientes controles:

|  |  |  |
| --- | --- | --- |
| **Control** | **Descripción** | **Responsable** |
| **Aislamiento de Red** | La base de datos de Producción debe tener un  **Firewall** configurado para **bloquear explícitamente** cualquier conexión proveniente de direcciones IP asociadas a los entornos de **Desarrollo** local de los programadores. | Equipo de  Operaciones/TI |
| **Gestión de Credenciales** | Las credenciales de acceso a la base de datos de Producción solo deben existir y ser accesibles para el entorno de **Producción** (mediante un **Gestor de Secretos**). Está **prohibido** codificar o almacenar credenciales de Producción en el código del repositorio (GitHub) o en máquinas de Desarrollo. | Freinier Cardona (Líder) |
| **Separación Física** | Cada entorno debe ejecutarse en infraestructura, servidores y bases de datos **físicamente o**  **lógicamente separados** (ej. diferentes máquinas virtuales, diferentes bases de datos o diferentes cuentas de nube). | Equipo de  Operaciones/TI |

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