PROTECCIÓN DE SISTEMAS DURANTE PRUEBAS DE AUDITORÍA

1. Objetivo

Garantizar que toda actividad de prueba de seguridad o auditoría (***pentesting* / escaneo de vulnerabilidades**) se realice sin comprometer la **confidencialidad, integridad o disponibilidad** de los datos y servicios que las usuarias de "ALERTA MUJER" utilizan en el ambiente de producción.

2. Entornos de Pruebas Seguras

Principio: Nunca se realizarán pruebas intrusivas de seguridad directamente en el ambiente de **PRODUCCIÓN**.

Ambiente	Propósito	Restricciones de Uso
PRODUCCIÓN	Operación real de la aplicación.	**PROHIBIDO** realizar escaneos, pruebas de penetración o pruebas de estrés.
PRE-PRODUCCIÓN / STAGING	Ambiente espejo y aislado de Producción.	**AMBIENTE AUTORIZADO** para pruebas de seguridad destructivas o de alto impacto.

3. Gestión de Datos para Auditoría

Técnica Elegida: Enmascaramiento de Datos.

Requisito de Datos	Control de Seguridad Aplicado
Confidencialidad	La base de datos del ambiente de pruebas (Pre-Producción) debe ser una copia fiel de la estructura de Producción, pero los datos sensibles deben ser **enmascarados**.
Enmascaramiento	Se utilizará la técnica de **enmascaramiento de datos** para reemplazar la **Información de Identificación Personal (IIP)** (ej. nombres, ubicaciones exactas, teléfonos) con datos falsos, pero manteniendo el formato original y la integridad lógica de la basede datos.

Requisito de Datos	Control de Seguridad Aplicado
Aislamiento	La copia de la base de datos de pruebas debe ser independiente y no tener conectividad de red con el ambiente de Producción.

4. Proceso de Solicitud y Aprobación Formal

Toda actividad de prueba de seguridad debe seguir este flujo de autorización para garantizar la protección del sistema:

FASE	TAREA	RESPONSABLE	DOCUMENTACIÓN REQUERIDA
Solicitud	El Auditor o Equipo de Seguridad solicita formalmente la prueba.	Auditor Líder/Equipo de Seguridad	**Plan de Prueba:** Alcance, tipo de prueba, fecha y hora de inicio/fin, y el impacto esperado.
Aprobación	Revisión de la solicitud, confirmación del ambiente de pruebas (Pre-Producción) y verificación de que el enmascaramiento de datos se haya realizado correctamente.	**Freinier Cardona (Líder) y Luis David Conde (Desarrollador)**	**Aprobación Formal:** Documento firmado o correo electrónico que dé luz verde explícita para la prueba.
Ejecución y Monitoreo	El auditor ejecuta la prueba **únicamente** en el ambiente de Pre-Producción. El equipo de Operaciones supervisa el ambiente de Producción.	Auditor / Equipo de Operaciones	**Registro de Logs** en Producción: Monitorear cualquier actividad anómala o pico de rendimiento para confirmar el aislamiento.
Post-Prueba	El ambiente de pruebas se restablece o se elimina para evitar la persistencia de datos o vulnerabilidades explotadas.	Equipo de Desarrollo	**Informe de Resultados** de la auditoría y plan de mitigación de vulnerabilidades.

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