Procedimiento de Pruebas de Cumplimiento (Control 5.33)

Versión	Fecha	Propietario del Proceso	Control ISO 27001
1.0	2025-10-02	Líder del Proyecto	5.33 Pruebas de cumplimiento

1. Propósito y Alcance

1.1 Propósito

Asegurar que las políticas, procedimientos y controles de seguridad definidos para el proyecto "Alerta Mujer" se cumplen rigurosamente y funcionan como se espera. Esto confirma la validez del **Sistema de Gestión de Seguridad de la Información (SGSI)** y protege la **Integridad** y **Confidencialidad** de los datos.

1.2 Alcance

Este procedimiento aplica a todos los controles establecidos en la **Política de Seguridad Marco (Control 5.2)** y los procedimientos asociados (5.7, 5.12, 5.23, 5.24, etc.).

2. Métodos de Verificación de Cumplimiento

El proyecto utilizará dos métodos principales para verificar el cumplimiento, ambos liderados por el **Líder del Proyecto** o el **Docente Guía** como auditor interno.

2.1 Auditoría Documental y de Configuración (Semanal/Mensual)

Esta prueba es una revisión sistemática para confirmar que las tareas de seguridad programadas se están ejecutando y documentando correctamente.

Control a Probar	Rol Responsable	Frecuencia	Criterio de Aceptación (Evidencia)

5.7 (Inteligencia de Amenazas)	DevOps	Semanal	Evidencia de monitoreo (captura de pantalla) de las fuentes de CVEs y la generación de **Tickets de Seguridad** relacionados.
5.12 (Clasificación de Datos)	Desarrolladores	Mensual	Verificación del uso de datos anonimizados en el entorno de **Desarrollo/Prueba** (Control 8.33).
5.23 (Seguridad en la Nube)	DevOps	Mensual	Confirmación de que las **reglas del *firewall*** del proveedor de la nube cumplen con la política de *Deny-All*.
5.21 (Credenciales de Proveedores)	DevOps	Trimestral	Evidencia de que las **claves de API** de producción son distintas a las de desarrollo y están almacenadas de forma segura (Control 5.31).
8.28 (Control de Versiones)	Desarrolladores	Continua	Verificación de que **todo cambio en el código** tiene una revisión (*Code Review*)document ada antes de la fusión a la rama principal.

2.2 Pruebas de Resiliencia y Respuesta (Trimestral)

Estas pruebas evalúan la funcionalidad de los controles de seguridad críticos en escenarios simulados.

Control a Probar	**Tipo de Prueba/Simulacro**	**Rol Liderando**	**Criterio de Aceptación (Éxito)**
5.24 (Gestión de Incidentes)	**Simulacro de Fuga de Datos (Nivel CRÍTICO)**	Líder del Proyecto	El tiempo de contención (Fase 3) es **inferior a 15 minutos** y se genera la documentación de "Lecciones Aprendidas".
8.14 (Continuidad Operacional)	**Simulacro de Caída de BD**	DevOps	El servicio debe conmutar exitosamente a la **transmisión por SMS** (RF7) y la funcionalidad crítica permanece activa.
8.29 (Pruebas de Seguridad)	**Prueba de Penetración Básica**	Desarrollador Líder	Pruebas de inyección SQL y XSS no deben retornar errores o revelar información sensible (Control 8.27).
5.23 (Backup)	**Prueba de Restauración**	DevOps	Restauración exitosa del último

			backup de datos CONFIDENCIALES en un entorno de prueba en **menos de 2 horas**.

3. Planificación y Documentación de Hallazgos

3.1 Plan de Pruebas

Al inicio de cada ciclo formativo, el Líder del Proyecto debe generar un **Plan de Pruebas** que defina:

1. Las fechas exactas de las pruebas trimestrales.
2. El alcance detallado de la prueba (ej. "Se probará solo el módulo de autenticación contra *Brute Force*").
3. El equipo que participará.

3.2 Reporte de No Conformidad y Acciones Correctivas

1. **Hallazgo:** Si una prueba de cumplimiento falla (ej. el *firewall* no estaba configurado correctamente, o la respuesta al incidente tardó 30 minutos), se registra como una **No Conformidad**.
2. **Acción Correctiva:** El Líder del Proyecto asigna al rol responsable (DevOps, Dev) una **Acción Correctiva** con una fecha límite de implementación.
3. **Seguimiento:** El Líder debe verificar que la Acción Correctiva se haya implementado y que la nueva prueba de cumplimiento sea exitosa antes de cerrar el hallazgo.

4. Evidencia de Cumplimiento

La evidencia de que el Control 5.33 se está aplicando incluye:

- El Plan de Pruebas trimestral.
- Los reportes de las Pruebas de Resiliencia (ej. "Simulacro de Incidente CRÍTICO - 2025-10-30") que documenten el tiempo de respuesta.
- El registro de los hallazgos de **No Conformidad** y las Acciones Correctivas asociadas.