CONTROL: 8.8 GESTIÓN DE VULNERABILIDADES TÉCNICAS

1. Propósito

El control 8.8 exige un **proceso formal y recurrente** para identificar, evaluar y tratar las **vulnerabilidades técnicas** en el *software* (aplicación móvil, *backend*), sistemas operativos, y componentes de red. El objetivo es reducir el riesgo de que atacantes exploten debilidades conocidas.

Para una aplicación crítica como "Alerta Mujer", la gestión de vulnerabilidades es esencial para:

- **Disponibilidad (5.26):** Asegurar que los sistemas de alerta y la BD se mantengan operativos y no sean paralizados por *exploits*.
- **Seguridad de la Plataforma:** Gestionar proactivamente las vulnerabilidades de Android/iOS y las librerías de terceros utilizadas.

2. Procedimiento de Gestión de Vulnerabilidades (Ciclo de Vida)

El proceso de gestión de vulnerabilidades se implementará como un ciclo continuo de cuatro fases: **Identificación, Evaluación, Tratamiento y Monitoreo**.

2.1. Fase 1: Identificación (Detección y *Scanning*)

Se utilizarán métodos proactivos para descubrir vulnerabilidades:

- **Fuentes de Inteligencia de Amenazas (5.7 faltante):** Suscripción a alertas de seguridad de los proveedores de tecnología (ej. Google/Android Security Bulletins, CVE, NVD).
- **Escaneo de Vulnerabilidades Recurrente:** Se realizarán escaneos automatizados a nivel de la infraestructura (*backend*, servidores) y la aplicación:
    - **Frecuencia: Mensual** como mínimo.
    - **Alcance:** Escanear servidores de aplicación, Base de Datos, y dispositivos de red.
- **Análisis de Dependencias:** Uso de herramientas para escanear y catalogar las **librerías de terceros** (dependencias) de la aplicación y el *backend*, buscando versiones conocidas con vulnerabilidades.

2.2. Fase 2: Evaluación y Priorización

No todas las vulnerabilidades son igualmente críticas. Deben ser evaluadas y priorizadas:

- **Clasificación de Riesgo:** Toda vulnerabilidad debe ser calificada usando el **Sistema de Puntuación de Vulnerabilidad Común (CVSS)** para determinar su severidad (Crítica, Alta, Media, Baja).
- **Análisis de Impacto:** El Propietario de Datos y el Responsable de Riesgos (5.2) deben evaluar el **impacto potencial** de la explotación de la vulnerabilidad en los activos críticos (BD, servicio de alerta).
-

Severidad	**Objetivo de Tiempo de Tratamiento (*SLA*)**
Crítica (CVSS 9.0-10.0)	Menos de **72 horas** para aplicar el parche o una mitigación.
Alta (CVSS 7.0-8.9)	Menos de **7 días** para aplicar el parche.
Media/Baja	Incluir en el ciclo de *patching* mensual o la próxima versión (RF).

2.3. Fase 3: Tratamiento (*Patching* y Mitigación)

El tratamiento de las vulnerabilidades debe ser formalizado como un cambio controlado (5.36).

- **Pruebas (8.29):** Antes de aplicar cualquier parche de seguridad en Producción, debe ser probado en el **Entorno de Staging/Prueba** (8.31 faltante) para asegurar que no introduce nuevas vulnerabilidades o fallos de funcionalidad.
- **Aplicación de Parches:** El equipo de DevOps/Operaciones es responsable de aplicar los parches según los **Tiempos de Tratamiento** establecidos.
- **Mitigación:** Si no se puede aplicar un parche de inmediato, se debe implementar una mitigación (ej. reglas de *firewall* temporal, desactivación de un servicio) para reducir el riesgo hasta que el parche sea viable (Control 8.9).

2.4. Fase 4: Monitoreo y Verificación

- **Monitoreo Post-Parche:** Después de la aplicación de un parche crítico, el equipo de monitoreo (8.16) debe vigilar activamente los *logs* para detectar cualquier anomalía o fallo en el sistema.
- **Re-Escaneo:** El sistema debe ser **re-escaneado** para verificar que la vulnerabilidad se haya cerrado efectivamente.

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