CONTROL: 8.7 PROTECCIÓN CONTRA *MALWARE*

1. Propósito

El control 8.7 requiere la implementación de medidas tecnológicas y operativas para proteger los sistemas y la información contra el *malware* (incluidos virus, *ransomware*, y *spyware*). La infección por *malware* en el *backend* o en los sistemas de desarrollo podría comprometer la **confidencialidad** (ej. robo de datos de la BD), la **integridad** (ej. alteración del código fuente) y la **disponibilidad** (ej. *ransomware* en servidores de alerta).

Para "Alerta Mujer", este control se enfoca en asegurar los **servidores de *backend*** y el **entorno de *build*** (donde se compila el código) para evitar que el *malware* afecte la calidad y seguridad de la aplicación distribuida.

2. Procedimiento de Protección contra *Malware*

La protección se implementará en dos frentes: la infraestructura de producción y el ciclo de vida de desarrollo.

2.1. Protección de la Infraestructura de *Backend* (Servidores y BD)

Los servidores de producción y la BD (alojados en la Red de Producción, Control 8.21) requieren la defensa más estricta:

- **Software Antimalware/Antivirus (AV):** Se instalará una solución AV probada y de grado empresarial en todos los servidores de aplicación y de administración (Red 3, Control 8.21).
    - **Configuración:** El *software* AV debe configurarse para **ejecutar escaneos completos periódicos** (ej. semanalmente) y **monitoreo en tiempo real** (*real-time scanning*).
    - **Actualizaciones:** Las bases de datos de firmas de *malware* deben **actualizarse automáticamente** al menos diariamente (Control 8.8).
- **Restricción de Ejecución:** Se implementará una política de **Lista Blanca de Aplicaciones** (*Application Whitelisting*) en el *backend* de Producción. Esto limitará la ejecución solo a los programas y librerías esenciales, bloqueando automáticamente cualquier *software* no autorizado, que es un método altamente efectivo contra *ransomware* y *malware* desconocido.
- **Aislamiento de Navegación:** El personal administrativo y de operaciones **NO** debe utilizar los servidores de *backend* ni de administración para la navegación web general o el correo electrónico, reduciendo el vector de infección.

2.2. Protección en el Ciclo de Desarrollo y *Build*

Es crucial prevenir que el *malware* se introduzca en el código fuente o en la aplicación final.

- **Escaneo de Código Fuente (CI/CD):** Se integrará un escáner de *malware* en la *pipeline* de Integración Continua (CI).
    - **Propósito:** Escanear el repositorio de código (Control 8.28) y las librerías de terceros (dependencias) antes de la compilación para detectar código malicioso inyectado o paquetes comprometidos.
- **Entorno de *Build* Aislado:** El servidor o contenedor de *build* (donde se compila el APK/IPA) debe ser un **entorno limpio, efímero y desechable**. No debe reutilizarse para otras tareas para evitar la contaminación cruzada.
- **Control de Cifrado (8.24):** El *malware* a menudo busca robar datos. La correcta implementación del **cifrado en reposo y en tránsito** mitiga el impacto si un *malware* logra acceder a los datos.

2.3. Gestión de Incidentes de *Malware*

- **Respuesta:** La detección de *malware* activará inmediatamente el **Plan de Gestión de Incidentes de Seguridad (5.24 faltante)**.
- **Cuarentena:** Los archivos o sistemas sospechosos deben ser puestos en **cuarentena o aislados de la red** (Control 8.21) automáticamente para evitar la propagación.