CONTROL: 8.16 ACTIVIDADES DE MONITOREO

1. Propósito

El control 8.16 exige la **monitorización activa** y la revisión periódica de los registros (*logs* y eventos) generados por los sistemas de información, redes y aplicaciones (control 8.15), con el objetivo de **detectar actividades inusuales o ataques en curso** en tiempo real.

Para una aplicación de emergencia como "Alerta Mujer", el monitoreo activo es fundamental para la **Disponibilidad (5.26)** y la **Integridad (5.25)**, permitiendo:

- **Detección Temprana:** Identificar intentos de *phishing*, inyección SQL, o accesos no autorizados antes de que causen daños.
- **Respuesta a Incidentes:** Proporcionar los datos necesarios para activar el Plan de Gestión de Incidentes (Control 5.24 faltante).

2. Procedimiento de Aplicación del Control 8.16

La aplicación de este control requiere un sistema de Gestión de Eventos e Información de Seguridad (**SIEM**) o una solución de monitoreo centralizado.

2.1. Definición de Eventos Críticos a Monitorear

Se establecerá una lista prioritaria de eventos que, al ocurrir, deben generar una alerta inmediata (Reglas de Correlación):

Componente	Eventos Críticos (Amonestar)	Impacto de Seguridad
Autenticación	**Múltiples fallos de inicio de sesión** (5 veces en 1 minuto) en la App o el panel de administración.	Ataque de Fuerza Bruta (8.5).
Alertas de Emergencia	**Activación masiva de alertas** desde una sola cuenta o IP en un corto período de tiempo.	Ataque de Denegación de Servicio (DoS) o uso malintencionado del servicio (5.26).
Base de Datos (BD)	Ejecución de comandos no autorizados (ej. DROP TABLE, SELECT * de la tabla PII) o aumento repentino en el tráfico de salida.	Fuga de datos (RNF4.2) o Inyección SQL (8.27).
Administración	**Uso de cuentas privilegiadas** (ej. Root, DBA) fuera de las ventanas de mantenimiento programado.	Compromiso del Acceso Privilegiado (8.2 faltante).
Sistema de Red	Cambios de configuración en el *firewall* (8.19) o fallos en la sincronización NTP (8.20).	Compromiso de la infraestructura crítica.

2.2. Implementación de una Solución de Monitoreo Centralizado

- **Recopilación (8.15):** Los *logs* de los diferentes sistemas (servidores web, BD, *firewalls*, App móvil) deben ser normalizados y enviados de forma segura (cifrado en tránsito) a un repositorio centralizado de *logs*.
- **Monitoreo Continuo:** La plataforma SIEM o herramienta similar debe aplicar las **Reglas de Correlación** (definidas en 2.1) sobre el flujo de datos en tiempo real.
- **Alertas Automatizadas:** Ante la detección de un evento o patrón crítico, el sistema debe generar una alerta que se dirija al **equipo de respuesta a incidentes** (equipo SOC o DevOps de guardia) a través de un canal seguro y de alta disponibilidad (ej. SMS, llamada automatizada, servicio de *pager*).

2.3. Revisión Periódica y Reportes

- **Revisión Diaria:** El equipo de seguridad y operaciones debe revisar diariamente los **eventos de bajo riesgo** (ej. fallos de conexión aislados) para identificar tendencias.
- **Reporte Mensual:** Se generará un reporte de seguridad que incluya: el número de incidentes detectados, las fuentes de ataque más comunes y las tendencias de tráfico, para informar a la dirección sobre el estado de la seguridad (5.4).

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