

**CONTROL DE REGISTRO DE EVENTOS**

**PROYECTO: SOFTWARE PARA LA CREACIÓN DE LA APLICACIÓN “ALERTA MUJER”**

**INTEGRANTES:**

**LUIS DAVID CONDE SANCHEZ FREINIER CARDONA PEREZ ANDRES FELIPE**

**CUELLAR GOMEZ**

**INSTRUCTOR:**

**Javier Humberto Pinto Diaz**

**SERVICIO NACIONAL DE APRENDIZAJE – SENA**

**ANALISIS Y DESARROLLO DE SOFTWARE – 3145555**

**2025**

TABLA DE CONTENIDO

1. **Propósito**
2. **Procedimiento de Aplicación del Control**
   1. **Alcance y Detalle de Eventos a Registrar**
   2. **Protección e Integridad del Registro (Logging)**
   3. **Retención**

# CONTROL: 8.15 CONTROL DE REGISTRO DE EVENTOS

1. **Propósito**

El control 8.15 requiere que la aplicación y sus sistemas de soporte generen, almacenen y protejan registros (*logs*) detallados de las actividades y eventos. Estos *logs* son fundamentales para:

* + **Trazabilidad Forense:** Servir como evidencia legal (Control 5.25) en caso de un incidente de seguridad o un mal uso del servicio de alerta.
  + **Auditoría:** Permitir la revisión de la actividad de los usuarios y administradores, especialmente en torno a datos sensibles.
  + **Detección (8.16):** Proporcionar la información necesaria para el monitoreo activo y la detección de patrones de ataque en tiempo real.

# Procedimiento de Aplicación del Control 8.15

Se establecerá una **Política de Registro de Eventos** que defina qué se registra, cómo se protege y por cuánto tiempo se retiene.

# Alcance y Detalle de Eventos a Registrar

Los sistemas de información de "Alerta Mujer" deben registrar, como mínimo, los siguientes eventos críticos con el detalle especificado:

|  |  |  |
| --- | --- | --- |
| Sistema | Eventos Críticos a Registrar | Detalle del *Log* Requerido |
| **App Móvil / Autenticación** | Intentos de **inicio de sesión exitosos y fallidos**. | Fecha/Hora precisa, IP de origen, ID de Usuario, Tipo de fallo (si aplica). |
| **Servidor de Alertas** | **Activación y cancelación** de alertas de emergencia. | Fecha/Hora precisa (sincronizada por NTP), ID de Usuario, Coordenadas GPS del evento, Estado del *backend*. |
| **Base de Datos (BD)** | **Accesos a datos sensibles** (PII), cambios de privilegios, y comandos de administración (ej. *SELECT*, *UPDATE*, *DELETE*). | ID de Usuario que ejecutó la acción (ej. DBA), Sentencia SQL ejecutada o tabla afectada, Resultado. |

|  |  |  |
| --- | --- | --- |
| Sistema | Eventos Críticos a Registrar | Detalle del *Log* Requerido |
| **Gestión de Evidencia** | **Acceso a la evidencia multimedia** (foto/video/audio) por parte de administradores o autoridades. | Fecha/Hora, ID de Usuario (Administrador), Archivo de evidencia accedido, Propósito del acceso. |
| **Sistema** | Cambios en la configuración del servidor, aplicación de parches o reinicios. | Usuario que realizó el cambio, Componente afectado, Resultado. |

# Protección e Integridad del Registro (*Logging*)

Los *logs* son un activo de seguridad y deben ser protegidos contra la manipulación o eliminación (Control 5.30).

* + - **Protección contra Alteración:** Los *logs* deben escribirse en modo **"Append- Only"** (solo añadir), y solo los usuarios privilegiados del sistema de gestión de *logs* (SIEM o centralizador) deben tener permiso para escribir. El **equipo de**

**desarrollo NO debe tener permisos para modificar o eliminar *logs*** de producción.

* + - **Sincronización de Tiempo:** Todos los sistemas deben sincronizar su reloj con una **fuente de tiempo segura (NTP)** (Control 8.20) para garantizar que los *logs* de la App, el Servidor y la BD sean correlacionables.
    - **Almacenamiento Seguro:** Los *logs* deben ser transferidos inmediatamente después de su generación a un **servidor de *log* centralizado y aislado** (Control 8.21), y almacenados en un formato cifrado.

# Retención

La duración de la retención de los *logs* debe basarse en requisitos regulatorios (si aplican) y la necesidad forense.

* + - **Duración:** Los *logs* operativos deben retenerse por un mínimo de **90 días** para monitoreo activo (8.16). Los *logs* de auditoría (ej. accesos a PII y alertas) deben retenerse por un mínimo de **un año** para propósitos forenses.
    - **Respaldo:** Los *logs* deben ser respaldados periódicamente y la retención debe incluir los *logs* de **respaldo** (Control 8.13).

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