CONTROL: 8.3 INFORMACIÓN DE ACCESO A LA INFORMACIÓN

1. Propósito

El control 8.3 exige la protección de los accesos a información crítica, especialmente por parte de cuentas privilegiadas (operadores, administradores, DBAs). La **información de acceso** (quién, cuándo y por qué accede) debe ser registrada y revisada.

Para "Alerta Mujer", la aplicación de este control es vital para:

- **Trazabilidad Forense:** Registrar de manera irrefutable qué administrador accedió a la PII, el historial de alertas, o la evidencia multimedia (Control 5.25).
- **Control de Privilegios:** Reforzar el principio de **Mínimo Privilegio** y asegurar que los operadores solo acceden a los datos cuando es estrictamente necesario y con un propósito justificado.
- **Confidencialidad (5.31):** Proteger los datos sensibles de accesos internos no autorizados.

2. Procedimiento de Control de Acceso y *Logging*

Este control se implementa mediante la integración de la gestión de acceso con el sistema de registro de eventos (Control 8.15) y el monitoreo (Control 8.16).

2.1. Definición del Alcance Sensible

La información de acceso debe registrarse obligatoriamente para los siguientes activos que requieren protección por parte de los operadores:

Activo Sensible	Ubicación de Acceso	Rol que Requiere Acceso
Datos de Identificación Personal (PII)	Base de Datos (BD) y Paneles de Administración (CU-13).	Administrador, Soporte.
Historial de Alertas y Coordenadas	BD y Paneles de Monitoreo (CU-12, CU-14).	Administrador, Soporte, Monitoreo.
Evidencia Multimedia (Fotos/Audio)	Servidor de Archivos Seguros y BD (RF6.3).	Administrador, Soporte (solo con autorización).

Activo Sensible	Ubicación de Acceso	Rol que Requiere Acceso
Claves de Cifrado y Configuración	Servidores de Aplicación y Secret Manager.	DevOps.

2.2. Requisitos de Registro de Accesos (*Logging*)

Todo acceso de un operador a la información sensible debe generar un *log* inmutable y detallado (Control 8.15). El *log* debe incluir obligatoriamente:

- **Identidad Única:** El nombre de usuario único del operador (Control 5.16), no cuentas compartidas.
- **Fecha/Hora:** Sello de tiempo preciso y sincronizado (Control 8.20).
- **Origen:** Dirección IP de donde se originó el acceso (ej. VPN de la Red de Administración, Control 8.21).
- **Acción:** La consulta específica ejecutada (ej. SELECT * FROM USUARIOS WHERE ID=123) o la funcionalidad accedida en el panel.
- **Resultado:** Éxito o fracaso del acceso.
- **Justificación (Recomendado):** Si es posible, se debe requerir que el operador ingrese la razón o el *ticket* de soporte por el cual necesita acceder al dato antes de ejecutar la acción.

2.3. Revisión y Monitoreo de los Accesos

- **Revisión Periódica:** El **Propietario de Datos o el Responsable de Riesgos (5.2)** debe revisar el *log* de accesos privilegiados al menos **mensualmente** para detectar patrones inusuales (ej. un administrador accediendo a 500 cuentas en una hora).
- **Alertas Críticas (8.16):** El sistema de monitoreo debe generar una **alerta inmediata** si se detectan accesos a la BD fuera del horario laboral o accesos a las claves de cifrado, activando el Plan de Gestión de Incidentes (Control 5.24).
- **Retención:** Los *logs* de acceso a información sensible deben retenerse por un período de **un año** para auditorías forenses, según la política de retención (Control 8.15).

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