CONTROL: 8.2 DERECHOS DE ACCESO PRIVILEGIADO

1. Propósito

El control 8.2 exige que la asignación y el uso de **derechos de acceso privilegiado** (aquellos que permiten saltarse los controles del sistema, como acceso a la BD de producción, al *firewall* o al código fuente) estén estrictamente controlados, restringidos y monitoreados.

Para "Alerta Mujer", la correcta implementación de este control garantiza que:

- **Confidencialidad:** Solo el personal autorizado pueda ver, modificar o extraer datos sensibles de la Base de Datos (PII, evidencia).
- **Integridad y Disponibilidad:** Se previenen cambios no autorizados en la configuración crítica del servidor o la BD que puedan comprometer el servicio de alerta 24/7.

2. Procedimiento de Gestión de Accesos Privilegiados

La gestión de estos derechos se basará en el principio de **Mínimo Privilegio (PoLP)** y **Necesidad de Saber**.

2.1. Definición y Asignación de Privilegios

- **Identificación de Roles Privilegiados:** Se definen formalmente los roles que requieren acceso de "superusuario" en el entorno de Producción:
    - **DBA/Administrador de BD:** Acceso completo a la BD (tablas, *logs*, configuración).
    - **DevOps/SysAdmin:** Acceso *root*/SSH a los servidores de aplicación y *firewalls*.
    - **Administrador de Aplicación (Soporte L3):** Acceso al panel de administración para gestión de usuarios (CU-11) y monitoreo de alertas (CU-12/CU-14).
- **Asignación de Cuentas Únicas (5.16):** Cada individuo debe tener su **propia cuenta privilegiada nominativa**, nunca se deben compartir cuentas de *root* o administradores genéricos.
- **Justificación Formal:** La asignación de derechos privilegiados debe ser **aprobada por el Propietario del Activo** (5.2) y documentada con la justificación del negocio y el período de validez.

2.2. Restricciones Técnicas y de Acceso

- **Acceso Temporal (*Just-in-Time Access*):** El acceso privilegiado a Producción (servidores o BD) debe ser **revocable por defecto** y solo activarse cuando es necesario para una tarea específica y documentada.
    - **Mecanismo:** El acceso solo se habilitará por un **tiempo limitado** (ej. 4 horas) y automáticamente revocado después, forzando al operador a solicitarlo de nuevo para cada intervención.

- **Método de Acceso Seguro (8.19):** El acceso a Producción debe ser a través de un **canal seguro obligatorio** (ej. VPN o *Bastion Host*), y siempre requerirá **Autenticación Multifactor (MFA)**.
- **Separación (8.21):** El acceso privilegiado a Producción debe originarse únicamente desde la **Red de Administración/Operación** (Red 3), aislada de la red de Desarrollo y Prueba.

2.3. Auditoría y Revisión (Monitoreo Activo)

El uso de los derechos privilegiados debe ser monitoreado y revisado con la máxima prioridad.

- **Registro de Auditoría (8.3 y 8.15): Todas las acciones** realizadas por una cuenta privilegiada (incluyendo comandos de *shell*, consultas a la BD, cambios de configuración) deben ser registradas detalladamente y de forma inmutable.
- **Monitoreo Activo (8.16):** El sistema de Monitoreo/SIEM debe generar **alertas de prioridad Crítica** por cualquier actividad sospechosa o fuera del horario normal de trabajo en una cuenta privilegiada.
- **Revisión Periódica:** Los **logs de acceso privilegiado** deben ser revisados diariamente por el equipo de seguridad y formalmente por la dirección (5.4) al menos **mensualmente** para detectar patrones de abuso.
- **Revocación (Offboarding):** Los derechos privilegiados deben **revocarse inmediatamente** si el rol o la necesidad del operador termina (ej. cambio de puesto o desvinculación).