**Control: 8.10 Eliminación de la información**

## 1. Propósito

El control 8.10 exige el **borrado seguro** de la información, *software* y otros activos cuando ya no sean necesarios o su retención ya no sea legalmente permisible. Este proceso debe asegurar que la información sea **irrecuperable** utilizando métodos técnicos.

Para "Alerta Mujer", la aplicación de este control es fundamental para cumplir con la **privacidad (5.31)** y el derecho de cancelación de datos personales. Específicamente, asegura que al eliminar una cuenta, los datos altamente sensibles (PII, coordenadas históricas y evidencia multimedia) sean borrados de forma definitiva y no puedan ser recuperados por medios forenses o ataques futuros.

## 2. Procedimiento de Borrado Seguro

Se establecerá un **Procedimiento de Eliminación Segura de Datos** que se activará bajo dos escenarios:

1. **Cierre de Cuenta por la Usuaria:** Cuando la usuaria solicita la eliminación de su cuenta.
2. **Fin de Retención:** Cuando la información de *logs* o evidencia cumple su periodo de retención obligatorio y debe ser purgada.

### 2.1. Definición de la Información Sensible a Eliminar

Los siguientes activos requieren un borrado seguro e irrecuperable:

| Activo | Ubicación de Almacenamiento | Clasificación de Confidencialidad |
|---|---|---|
| **Datos de Identificación Personal (PII)** (Nombre, Teléfono, Datos de Contacto) | Base de Datos (BD) de Producción | Alto |
| **Historial de Coordenadas GPS** | BD de Producción | Alto |
| **Evidencia Multimedia** (Fotos, Audio, Video) | Almacenamiento de Objetos/Archivos Seguros | Crítico |

| Activo | Ubicación de Almacenamiento | Clasificación de Confidencialidad |
|---|---|---|
| **Copia de Seguridad de la BD** | Almacenamiento de *Backup* (8.13) | Alto |

### 2.2. Métodos de Borrado Seguro

Para los datos almacenados digitalmente, se utilizarán métodos de **sanitización de datos** que cumplan con estándares industriales.

- **Para la Base de Datos (BD):**
    - **Registro Principal:** La eliminación de los registros de PII y coordenadas no será un simple DELETE o DROP. Se aplicará una técnica de **sobreescritura lógica** (ej. reemplazar el registro con datos aleatorios o ceros **antes** de la eliminación) para ofuscar el dato original en el medio de almacenamiento subyacente.
- **Para Archivos Multimedia (Evidencia):**
    - **Almacenamiento de Archivos:** Para archivos almacenados en discos virtuales o almacenamiento de objetos, se utilizarán funciones API que garanticen la eliminación a bajo nivel. En entornos de nube, se confirmará que el proveedor cumple con estándares de borrado seguro (*data sanitization*).
- **Para Copias de Seguridad (8.13):**
    - Se implementará un proceso automatizado para que, tras la eliminación de la cuenta en la BD activa, las copias de seguridad afectadas marquen los datos de esa usuaria para su **destrucción o expiración forzada** cuando dichas copias de seguridad alcancen su fecha de purga.

### 2.3. Proceso de Confirmación y Trazabilidad

- **Confirmación de Usuario:** El proceso de eliminación solo se ejecutará después de una **confirmación fuerte** por parte de la usuaria (ej. ingreso de la contraseña actual, o *token* de verificación enviado por correo).

- **Registro de Borrado:** Se debe generar un **registro de auditoría inmutable (log)** que confirme que el proceso de borrado seguro se ha completado, incluyendo la fecha, hora y el ID de la cuenta eliminada (Control 8.15).

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