

# COPIA DE SEGURIDAD DE LA INFORMACIÓN

**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**

**SERVICIONACIONAL DE APRENDIZAJE – SENA**

**ANALISIS Y DESARROLLO DE SOFTWARE – 3145555**

**2025**

TABLA DE CONTENIDO

1. **Propósito**
2. **Procedimiento de Aplicación del Control**
   1. **Definición de Alcance y Frecuencia**

# Protección de las Copias de Seguridad

* 1. **Pruebas de Recuperación y Restauración (Simulación de Incidentes)**

# CONTROL: 8.13 COPIA DE SEGURIDAD DE LA INFORMACIÓN

1. **Propósito**

El control 8.13 exige la implementación y el mantenimiento de **copias de seguridad** de la información, *software* y otros activos de seguridad para **proteger contra la pérdida de datos** (por fallos, desastres naturales o ataques maliciosos).

Para el proyecto "Alerta Mujer", la copia de seguridad es crítica para garantizar la **Disponibilidad (RNF6)** de la aplicación y la **Integridad (5.25)** de la evidencia sensible y los datos personales (PII). El objetivo es poder restaurar el servicio y todos los datos en un tiempo definido (*Recovery Time Objective - RTO*) en caso de una falla catastrófica.

# Procedimiento de Aplicación del Control 8.13

Se establecerá una **Política de Copias de Seguridad y Recuperación** que cubrirá los datos de la Base de Datos (BD) y el código fuente.

# Definición de Alcance y Frecuencia

|  |  |  |  |
| --- | --- | --- | --- |
| Activo Crítico | Tipo de Copia de Seguridad | Frecuencia | Ubicación de Almacenamiento |
| **Base de Datos (BD) de Producción** (PII, Alertas, Evidencia) | **Completa Diaria** e **Incremental/Diferencial por hora**. | Diaria (completa), Horaria (incremental). | Almacenamiento geográficamente redundante y aislado (principio de 3-2-1). |
| **Código Fuente** (Repositorio principal) | Completa. | Diaria (Ya cubierto por 8.28 como *snapshot*). | Almacenamiento *offline* o aislado del VCS principal. |
| **Logs de**  **Auditoría** (8.15) | Completa. | Diaria. | Almacenamiento inmutable y diferente al de la BD. |

**Retención:** Las copias de seguridad de la BD se retendrán por un período de **30 días**. Las copias de seguridad del código fuente y los *logs* de auditoría críticos se retendrán según el Control 8.28 y 8.15.

# Protección de las Copias de Seguridad

Las copias de seguridad son el objetivo principal de los atacantes y deben ser protegidas rigurosamente.

* + - **Aislamiento (*Air Gapping* Lógico):** Las copias de seguridad deben almacenarse en un segmento de red **aislado** de la red de Producción (Control 8.21), sin conectividad de escritura directa.
    - **Cifrado:** Todas las copias de seguridad deben estar **cifradas en reposo**

utilizando un algoritmo fuerte, y las claves de cifrado deben gestionarse de forma segura y separada de los datos de *backup*.

* + - **Acceso Restringido:** Solo las cuentas de servicio automáticas o los administradores con el **mínimo privilegio** (Control 8.2 faltante) deben tener acceso a leer o modificar las copias de seguridad.

# Pruebas de Recuperación y Restauración (Simulación de Incidentes)

Una copia de seguridad es inútil si no puede ser restaurada.

* + - **Frecuencia de Pruebas:** Se realizará una **prueba de restauración completa** en un entorno aislado (no de Producción) al menos **trimestralmente** o después de un cambio importante en la BD o la infraestructura.
    - **Procedimiento Documentado:** Se debe mantener un **procedimiento detallado y aprobado** para la recuperación de desastres (DRP) que defina los pasos, los roles responsables y el tiempo objetivo (*RTO*) de restauración.
    - **Verificación:** La prueba debe verificar que la aplicación funciona correctamente después de la restauración y que la integridad de la PII y la evidencia multimedia se mantiene.

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