Procedimiento de Seguridad de la Información para el Uso de Servicios en la Nube

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

Procedimiento de Seguridad de la Información para el Uso de Servicios en la Nube (Control 5.23)

Versión	Fecha	Propietario del Proceso	Control ISO 27001
1.0	2025-10-02	Administrador de Operaciones (DevOps)	5.23 Seguridad de la información para el uso de servicios en la nube

1. Propósito y Alcance

1.1 Propósito

Establecer las directrices operacionales para proteger la información y los activos críticos de "Alerta Mujer" alojados o gestionados a través de servicios en la nube (PaaS, IaaS o SaaS), garantizando la continuidad de la **Confidencialidad** y la **Disponibilidad** (RNF1.1) del servicio.

1.2 Alcance

Aplica a todos los servicios de computación en la nube utilizados por el proyecto, listados en el **Inventario de Activos (Control 5.9)**, incluyendo:

- Bases de datos en la nube (ej. Firestore, Realtime Database).
- Servicios de alojamiento y despliegue del *backend*.
- Servicios de autenticación y notificación.

2. Modelo de Responsabilidad Compartida (CRÍTICO)

La seguridad del proyecto depende tanto de los controles del equipo interno como de los controles del proveedor de la nube. Este modelo define las obligaciones de cada parte:

Componente de	Responsabilidad	Responsabilidad	Rol Responsable

Seguridad	**del Proveedor Cloud (Freeware)**	**del Equipo "Alerta Mujer"**	
Seguridad Física	Servidores, redes de infraestructura y climatización.	N/A	N/A
Sistema Operativo/Hipervisor	Parcheo de la infraestructura base del servidor.	N/A	N/A
Datos (INF-001, INF-002)	Disponibilidad y protección contra pérdida física (copias de seguridad internas).	**Cifrado** del contenido, Integridad y Control de Acceso (5.18).	Líder / DevOps
Configuración del Servicio	Configuración de *Firewall* virtual, políticas de acceso y roles de usuario (IAM).	**Administración** de la Configuración (*Hardening* - 8.9).	DevOps
Credenciales/Tokens	Autenticación de los administradores del servicio.	Gestión de **Contraseñas** y **Claves de API** (Control 5.21).	DevOps

3. Controles Técnicos de Seguridad en la Nube (Control 5.21)

El Administrador de Operaciones (*DevOps*) debe implementar y mantener los siguientes controles en el entorno de la nube:

3.1 Hardening y Configuración Segura (Control 8.9)

1. **Reglas de Firewall:** Se configurarán las reglas de acceso del *firewall* virtual para **denegar todo el tráfico por defecto** (*Deny-All*) y solo permitir conexiones explícitamente necesarias (ej. puerto HTTPS 443).

2. **Cifrado en Reposo:** El DevOps debe activar las configuraciones nativas del servicio en la nube para asegurar que los datos **CONFIDENCIALES** (INF-001, INF-002, INF-003) estén cifrados en reposo, incluso en los planes gratuitos.
3. **Registro de Actividad (*Logging* - Control 8.3):** Se activará y monitoreará el registro de actividad de la consola de administración de la nube para detectar accesos inusuales o cambios de configuración no autorizados.

3.2 Segregación de Entornos

Se mantendrá una **separación lógica y de credenciales** entre el entorno de Producción y el de Desarrollo/Pruebas, utilizando cuentas de servicio o proyectos de la nube distintos.

3.3 Gestión de Copias de Seguridad (Backup)

- **Política:** Aunque el proveedor ofrece disponibilidad, el equipo de "Alerta Mujer" debe configurar y verificar una **política de *backup* propia** para los datos clasificados como **CONFIDENCIALES** (INF-001/002) que garantice la posibilidad de restauración rápida (Disponibilidad RNF1.1).
- **Retención:** Las copias de seguridad deben ser retenidas según la política de retención de datos del proyecto (a definir).

4. Plan de Gobernanza y Salida de la Nube (Exit Plan)

Esta sección garantiza que la información se puede recuperar si el servicio en la nube se suspende o se termina.

4.1 Plan de Contingencia y Migración

El Líder del Proyecto debe documentar un **Plan de Salida** que especifique los pasos para recuperar y migrar los datos críticos a otra plataforma o *stack* tecnológico si el proveedor:

1. Cancela el plan gratuito sin previo aviso.
2. Introduce un cambio que compromete la seguridad (ej. deja de soportar TLS 1.2 o superior).

4.2 Verificación de Exportación

El DevOps debe verificar **al menos trimestralmente** la funcionalidad de exportación masiva de los datos **CONFIDENCIALES** de la base de datos de la nube, asegurando que la información pueda ser extraída en un formato utilizable y seguro (ej. CSV cifrado o JSON).