Procedimiento de Seguridad en la Gestión de Proveedores (Controles 5.19 al 5.22)

Versión	Fecha	Propietario del Proceso	Controles ISO 27001
1.0	2025-10-02	Líder del Proyecto / Administrador de Operaciones (DevOps)	5.19, 5.20, 5.21, 5.22

1. Propósito y Alcance

1.1 Propósito

Asegurar que los riesgos introducidos por el uso de servicios externos, *freeware* o librerías de terceros (Proveedores) sean identificados, evaluados y mitigados. El objetivo es mantener la **Confidencialidad** (Cifrado de PII) y la **Disponibilidad** (24/7) del servicio "Alerta Mujer", independientemente de que se utilicen planes gratuitos.

1.2 Alcance

Este procedimiento aplica a todos los proveedores y servicios externos críticos listados en el **Inventario de Activos (Control 5.9)**, incluyendo:

- **Hosting Cloud:** Servicios de base de datos o *backend* (ej. Firebase, Azure, AWS Free Tier).
- **Librerías de Terceros:** Librerías de código abierto utilizadas para funcionalidades críticas (ej. cifrado, geolocalización, autenticación).
- **Servicios de Comunicación:** APIs o servicios gratuitos para el envío de notificaciones (SMS, *Push*).

2. Evaluación de Riesgos y Selección (Control 5.19)

Esta fase se centra en la diligencia debida antes de utilizar un servicio *freeware*.

2.1 Criterios de Evaluación

Antes de adoptar un servicio o librería, el Líder del Proyecto y el Administrador de Operaciones deben evaluar los siguientes criterios:

1. **Seguridad y Certificación (Crítico):** ¿El proveedor publica alguna certificación de seguridad (ej. ISO 27001, SOC 2)? Si es una librería, ¿tiene un historial de parches rápidos para vulnerabilidades (Control 5.7)?
2. **Ubicación del Dato (Crítico):** ¿Dónde se alojarán los datos clasificados como **CONFIDENCIALES (Control 5.12)**? Se debe preferir *hosting* dentro de jurisdicciones con alta protección de datos, si es posible.
3. **Reputación y Soporte:** ¿El proveedor o la librería tienen una comunidad de usuarios activa y documentación de calidad?
4. **Riesgo de Bloqueo (*Vendor Lock-in*):** ¿Qué tan fácil sería migrar a otro servicio si el plan gratuito se suspende o si se detecta un fallo de seguridad grave?

2.2 Requisito Mínimo de Seguridad

Todo proveedor que maneje datos **CONFIDENCIALES** (INF-001 PII, INF-002 GPS) debe cumplir al menos con los siguientes requisitos:

- Garantizar la transmisión de datos mediante **TLS/HTTPS (RNF4.1)**.
- Permitir la configuración de un **cifrado fuerte** para datos en reposo.

3. Seguridad en el Acuerdo y Obligaciones (Control 5.20)

Para el *freeware*, el "acuerdo" es la aceptación formal de sus términos.

3.1 Revisión de Términos y Condiciones (ToS)

El Líder del Proyecto debe revisar y documentar las secciones clave de los Términos de Servicio (ToS) y la Política de Privacidad del proveedor:

1. **Propiedad del Dato:** Confirmar que el proveedor **no reclama propiedad** sobre los datos cargados por los usuarios de "Alerta Mujer".
2. **Responsabilidad en Caso de Fuga:** Entender el alcance de la responsabilidad del proveedor en caso de una fuga de datos.
3. **Cambios en el Servicio:** Documentar el procedimiento que el proveedor utiliza para notificar **cambios en la seguridad** o la interrupción del servicio gratuito.

3.2 Documentación de las Obligaciones

Se debe mantener un registro (en el Inventario de Activos o anexo) que contenga:

- Nombre del Proveedor (Ej. Firebase Cloud Messaging).

- URL de los Términos de Servicio y fecha de la última revisión.
- Extracto de las cláusulas relativas a la privacidad y seguridad.

4. Gestión Operacional de la Seguridad (Control 5.21)

Esta fase asegura que se apliquen los controles de seguridad mientras el servicio está activo.

4.1 Gestión de Credenciales y Accesos

- **Administrador de Operaciones (DevOps) Responsable:** El DevOps es el único responsable de la gestión de las claves y *tokens* de acceso a los servicios externos.
- **Mínimo Privilegio (8.2):** Los accesos configurados a las APIs y servicios deben tener el **mínimo de permisos** necesarios. Por ejemplo, si un *token* solo necesita leer logs, no debe tener permisos de escritura.
- **Almacenamiento Seguro:** Las claves de API deben ser almacenadas de forma segura (ej. en variables de entorno o en un *Vault*), nunca directamente en el código fuente (Control 5.31).

4.2 Segregación de Entornos

Las cuentas y credenciales utilizadas para el entorno de **Producción** deben ser **distintas** a las utilizadas para los entornos de Desarrollo y Prueba.

5. Monitoreo y Gestión del Cambio (Control 5.22)

El Administrador de Operaciones garantiza la continuidad y el cumplimiento de la seguridad.

5.1 Monitoreo de Disponibilidad

El DevOps debe monitorear activamente el **Estado de Disponibilidad** del servicio externo.

- **Actividad:** Verificar semanalmente la **página de estado** (Status Page) del proveedor de *hosting* y de la BD para detectar interrupciones programadas o incidentes.
- **Respuesta (RNF1.1):** Cualquier interrupción que afecte la **Disponibilidad 24/7** debe ser tratada como un incidente de seguridad (Control 5.6).

5.2 Gestión de Cambios del Proveedor

Si el proveedor notifica un cambio en sus términos o servicios, el Líder del Proyecto debe:

1. **Reevaluación:** Evaluar si el cambio afecta la seguridad o la disponibilidad del servicio "Alerta Mujer".
2. **Mitigación:** Si el cambio introduce un riesgo (ej. el servicio gratuito limita el tráfico), el equipo debe proponer un plan de mitigación (ej. optimización, migración) antes de la fecha límite impuesta por el proveedor.

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