Procedimiento de Concienciación, Educación y Formación en Seguridad (Control 6.3)

Versión	Fecha	Propietario del Proceso	Control ISO 27001
1.0	2025-10-03	Líder del Proyecto	6.3 Concienciación, educación y formación en seguridad de la información

1. Propósito y Alcance

1.1 Propósito

Establecer un programa de formación y concienciación que complemente la educación formal recibida en el SENA, enfocándose en los requisitos de seguridad específicos del proyecto "Alerta Mujer". El objetivo es asegurar que todo el personal posea el conocimiento técnico y la conciencia de riesgos necesarios para proteger la **Confidencialidad** de las usuarias.

1.2 Alcance

Aplica a todos los miembros del equipo del proyecto.

2. Modelo de Responsabilidad Compartida con el SENA

Área de Formación	Responsabilidad	Evidencia de Cumplimiento

Educación General en Ciberseguridad	**SENA (Entidad Formadora)**	Certificado de Competencias o Títulos de Formación (evidencia de base).
Concienciación Específica del Proyecto	**Líder del Proyecto**	Acta de Reunión de Concienciación Semanal.
Formación Técnica por Rol	**Rol Asignado (DevOps/Devs)**	Documentación del cumplimiento de tareas (Control 5.35) y Cierre de Tickets de Seguridad (Control 5.7).

3. Matriz de Concienciación Específica del Proyecto

El Líder del Proyecto debe asegurar que el equipo esté consciente de los siguientes puntos clave, que son únicos para "Alerta Mujer":

Tema de Concienciación	Propósito de Seguridad	Roles Involucrados	Frecuencia Mínima
Clasificación de Datos CONFIDENCIALES	Entender que la pérdida de Coordenadas GPS (INF-002) es un incidente CRÍTICO y debe ser cifrada siempre (Control 5.12).	Todos	Inicio de Ciclo Formativo
Riesgos del Servicio Freeware	Conocer las limitaciones del *hosting* en la nube (ej. límites de tráfico, riesgo de cierre de cuenta) y la importancia del **Plan de Salida**	Líder, DevOps	Anual o por Cambio de Proveedor

	(Control 5.23).		
Protocolo de Respuesta a Incidentes (5.24)	Conocer los pasos exactos y el tiempo máximo (15 minutos) para la **Contención de la Amenaza** si ocurre una fuga.	Todos	Tras cada Simulacro (Control 5.33)
Ingeniería Social/Phishing	Alertar sobre correos o mensajes dirigidos al equipo que busquen obtener credenciales del servidor (Control 5.31).	Todos	Cuando se detecte una campaña de *phishing*

4. Requisitos de Formación Técnica y Aplicación por Rol

Esta sección garantiza que la formación teórica se traduce en acción práctica dentro del proyecto.

4.1. Desarrollador Líder (Devs)

El Desarrollador Líder es responsable de buscar y aplicar formación en:

1. **Codificación Segura (*Secure Coding*):** Comprensión profunda de las 10 principales vulnerabilidades de OWASP y cómo prevenirlas en el lenguaje de programación principal del proyecto.
    - **Evidencia:** El cumplimiento se demuestra al cerrar los **Tickets de Seguridad** generados por la **Inteligencia de Amenazas (Control 5.7)** que requieran correcciones en el código (Control 8.27).
2. **Anonimización de Datos (Control 8.33):** Conocer técnicas para enmascarar o anonimizar la PII de las usuarias de forma irreversible para usarla en el entorno de Prueba.

4.2. Administrador de Operaciones (DevOps)

El DevOps es responsable de buscar y aplicar formación en:

1. **Hardening de Sistemas Operativos:** Conocimiento detallado de los comandos y configuraciones para asegurar el servidor y la base de datos (ej. uso de ufw, deshabilitar SSH con contraseña).
    - **Evidencia:** Cumplimiento de la **Guía de Configuración Segura** (Control 5.35) y la confirmación de la configuración *Deny-All* en el *firewall* virtual (Control 5.23).
2. **Monitoreo y Loggin:** Entendimiento de cómo usar las herramientas de la nube para monitorear el consumo de recursos y auditar los logs (Control 5.34).

5. Mantenimiento y Evidencia de Cumplimiento

1. **Evidencia Formal del SENA:** La evidencia principal del conocimiento técnico y la educación general en seguridad se demostrará mediante la presentación del **Registro de Notas de Evaluaciones** del programa y el **Certificado Final de Tecnólogo** (una vez obtenido).
2. **Registro de Asistencia Interna:** El Líder del Proyecto mantendrá un registro de la asistencia a las reuniones de **Concienciación Específica** (Sección 3) para demostrar la transferencia de conocimiento interno del proyecto.
3. **Actualización Anual:** Este procedimiento se revisa anualmente o cuando se introduce una tecnología nueva (ej. un nuevo proveedor de SMS o una nueva base de datos).

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