Clasificación de la Información

Versión	Fecha	Propietario del Proceso	Control ISO 27001
1.0	2025-10-02	Líder del Proyecto	5.12 Clasificación de la información

1. Propósito

Establecer un esquema formal para la **clasificación de la información** manejada por el proyecto "Alerta Mujer". Esto asegura que los controles de seguridad (ej. cifrado, control de acceso, retención) sean aplicados de manera proporcionada y efectiva, priorizando los datos más sensibles.

2. Alcance

Este procedimiento aplica a todos los activos de **Tipo Información** registrados en el **Inventario de Activos (Control 5.9)**, incluyendo datos en reposo (BD) y datos en tránsito (comunicaciones).

3. Esquema de Clasificación de la Información

El proyecto "Alerta Mujer" utilizará un esquema de clasificación basado en el impacto potencial si se pierde la **Confidencialidad** o la **Integridad** de la información:

Nivel de Clasificación	Descripción del Impacto	Requisitos de Seguridad Obligatorios
CONFIDENCIAL	Impacto CRÍTICO. La pérdida o fuga de estos datos causaría daño legal (protección de datos) y reputacional grave a las usuarias y al SENA.	**Cifrado en reposo y en tránsito (RNF4.1).** Acceso restringido (*Need-to-Know*, Control 5.18).

RESTRINGIDO	Impacto ALTO/MEDIO. El acceso no autorizado a estos datos compromete la propiedad intelectual del proyecto o la seguridad operacional.	Control de acceso estricto. Almacenamiento con control de versiones (Control 8.28) y protección de la Integridad (Control 5.25).
INTERNO	Impacto BAJO. Información necesaria para la operación diaria. La pérdida no compromete legalmente a las usuarias ni al SENA.	Protección estándar de red y autenticación básica.
PÚBLICO	Impacto NULO. Información diseñada para ser compartida (ej. Manuales).	Se aplica la Integridad (evitar alteraciones), pero no la Confidencialidad.

4. Clasificación de Activos de Información Crítica

El Líder del Proyecto asignará la clasificación y la registrará en la tabla de inventario (Control 5.9).

Activo (ID 5.9)	**Datos Incluidos**	**Clasificación Asignada**	**Justificación para la Protección**
INF-001	PII de Usuarias (Nombres, Teléfonos, Contraseña en *hash*).	**CONFIDENCIAL**	Datos personales sensibles. Requiere Cifrado en Reposo (Hashing) y TLS.
INF-002	Coordenadas/Historial GPS y Ubicación de Alerta.	**CONFIDENCIAL**	Revela la ubicación física de las usuarias. Requiere el mayor nivel de protección contra fugas.

INF-003	Evidencia Multimedia (Audio/Video de la alerta).	**CONFIDENCIAL**	Evidencia altamente sensible. Requiere inviolabilidad (Integridad) y Logs de Acceso (8.3).
SW-001	Código Fuente de la Aplicación (Repositorio Git).	**RESTRINGIDO**	Proteger la propiedad intelectual y la lógica de seguridad del código cerrado.
INF-004	Logs de Auditoría (Accesos fallidos, actividad de administradores).	**RESTRINGIDO**	Vital para la investigación de incidentes. Debe ser protegido de alteraciones (Integridad).
INF-005	Manuales de Usuario o Preguntas Frecuentes.	**PÚBLICO**	Información destinada a la descarga libre.

5. Implementación de los Controles de Clasificación

El Administrador de Operaciones y los Desarrolladores deben usar esta clasificación para aplicar los siguientes controles tecnológicos:

1. **Control de Acceso (5.18):** Se asegurará que solo los roles con necesidad de conocer (*Need-to-Know*) y con la debida autorización (Control 5.2) tengan acceso a los datos **CONFIDENCIALES**.
2. **Datos de Prueba (8.33):** Los datos clasificados como **CONFIDENCIALES** y **RESTRINGIDOS** nunca deben ser usados en el entorno de Prueba o Desarrollo a menos que hayan sido previamente **anonimizados o enmascarados**.
3. **Manejo de Activos (5.14):** La transferencia o manipulación de cualquier información **CONFIDENCIAL** debe realizarse siempre a través de canales seguros y cifrados (VPN, TLS/HTTPS).

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