

Procedimiento de Documentación de Procedimientos Operativos (Control 5.35)

Versión	Fecha	Propietario del Proceso	Control ISO 27001
1.0	2025-10-02	Líder del Proyecto	5.35 Documentación de procedimientos operativos

1. Propósito y Alcance

1.1 Propósito

Establecer un estándar para la creación, mantenimiento y accesibilidad de la documentación de los procedimientos operativos esenciales para el proyecto "Alerta Mujer". Esto garantiza la **continuidad operativa (RNF1.1)**, la **integridad** de los sistemas y la transferencia de conocimiento entre el equipo formativo.

1.2 Alcance

Este procedimiento aplica a todos los **procedimientos técnicos y operativos** que impactan la **Confidencialidad**, la **Integridad** y la **Disponibilidad** de los activos (Control 5.9).

Ejemplos de documentación obligatoria:

- Proceso de Despliegue a Producción.
- Procedimiento de Copia de Seguridad (*Backup*) y Restauración (Control 5.23).
- Guía de Configuración Segura (*Hardening*) del Servidor.
- Manual de Respuesta a Incidentes (Control 5.24).

2. Requisitos para la Documentación Operativa

La documentación de los procedimientos operativos debe cumplir con los siguientes criterios

obligatorios para ser considerada válida:

2.1 Estructura del Documento

Todo procedimiento operativo debe incluir obligatoriamente:

1. **Título y Control Asociado:** Título claro que identifique la tarea (ej. "Procedimiento de Hardening del Servidor Linux") y el control ISO 27001 relacionado (ej. Control 8.9).
2. **Rol Responsable:** Identificación del rol que ejecuta la tarea (ej. Administrador de Operaciones - DevOps).
3. **Objetivo:** El resultado esperado de ejecutar el procedimiento (ej. "Garantizar que solo el puerto 443 esté abierto al tráfico externo").
4. **Pasos Detallados:** Lista de pasos numerados y exactos. **Debe incluir los comandos o herramientas específicos** a utilizar (ej. `ssh root@<IP_servidor>`, seguido de `ufw enable`).
5. **Verificación:** Un paso final que confirme que la tarea se realizó correctamente (ej. "Verificar con `ss -tln` que los puertos listados son solo los necesarios").

2.2 Accesibilidad y Repositorio

1. **Repositorio Central:** Toda la documentación operativa debe estar almacenada en un repositorio de control de versiones (ej. Repositorio Git del proyecto) o una plataforma de documentación compartida por el equipo.
2. **Acceso:** La documentación debe ser de fácil acceso para todos los miembros del equipo que necesiten ejecutar o entender la tarea.

2.3 Mantenimiento y Revisión

1. **Revisión por Eventos de Cambio:** La documentación debe ser revisada y actualizada inmediatamente si:
 - Se cambia el **Servidor de Producción** (HW-001).
 - Se modifica una **librería crítica** (SW-001).
 - Un **incidente de seguridad (Control 5.24)** expone un fallo en el procedimiento.
2. **Revisión Programada:** El Líder del Proyecto debe revisar y aprobar formalmente la documentación al menos **una vez cada ciclo formativo** o cada 6 meses.

3. Matriz de Documentación Operativa Crítica

El siguiente es un registro de los procedimientos que deben ser documentados por el equipo, con el **Administrador de Operaciones (DevOps)** como responsable primario de su creación y mantenimiento.

Procedimiento Operativo	Control ISO Relacionado	Rol Responsable	Evidencia de Cumplimiento
-------------------------	-------------------------	-----------------	---------------------------

Procedimiento de Despliegue	8.32 (Gestión de Cambios)	DevOps	Registro del <i>pipeline</i> de CI/CD que muestre el despliegue automático.
Procedimiento de Backup y Restauración	5.23 (Servicios en la Nube)	DevOps	Registro de la ejecución trimestral de la Prueba de Restauración (Control 5.33).
Hardening de Servidor/Firewall	8.9 (Hardening de Configuración)	DevOps	Captura de pantalla de la configuración actual del <i>firewall</i> virtual.
Instalación y Configuración del Entorno de Desarrollo	N/A (Operacional)	Desarrolladores	Documento de pasos claros para un nuevo desarrollador.
Proceso de Anonimización de Datos	8.33 (Datos de Prueba)	Desarrolladores	Script utilizado para enmascarar los datos CONFIDENCIALES en el entorno de prueba.

4. Evidencia de Cumplimiento

La evidencia de que el Control 5.35 está implementado incluye:

- El repositorio central que aloja todos los documentos operativos.
- Los registros de cambios (*commits*) en la documentación que demuestran que las revisiones se realizan tras un cambio o un incidente.
- El **Acta de Revisión** del Líder del Proyecto confirmando la validez de la documentación.

LIDER DEL PROYECTO.

EQUIPO DE TRABAJO.

EQUIPO DE TRABAJO.