
5 Pasos para Preparar tu Auditoría ISO 27001

Guía práctica para responsables de compliance y seguridad de la información

Paso 1 — Revisión del alcance (SoA)

- Confirmar que el alcance del SGSI sigue vigente (procesos, ubicaciones, sistemas incluidos)
- Revisar que cada control del Anexo A esté marcado como aplicable o no aplicable, con justificación
- Verificar que los controles aplicables tengan evidencia real de implementación
- Actualizar el SoA si hubo cambios organizacionales (nuevos sistemas, proveedores, sedes)

Paso 2 — Evidencia documental

- Recopilar registros de al menos los últimos 3–6 meses (logs, actas, formularios)
- Verificar que las políticas estén firmadas, con fecha y versión vigente
- Confirmar evidencia de capacitación y concientización del personal
- Revisar registros de gestión de incidentes, con al menos un caso documentado y cerrado
- Validar evidencia de control de accesos (altas, bajas, revisiones periódicas)

Paso 3 — Auditoría interna previa

- Programar la auditoría interna 4–6 semanas antes de la externa
- Asignar un auditor interno independiente del área auditada, o externo si no hay recursos
- Documentar hallazgos con clasificación: mayor, menor u observación
- Verificar que el informe de auditoría interna esté firmado y archivado

Paso 4 — Revisión por la dirección

- Confirmar que existió una reunión formal de revisión por la dirección en el periodo
- Verificar que el acta incluya: resultados de auditorías, estado de riesgos, cambios en el contexto, oportunidades de mejora
- Asegurar que existan decisiones y responsables asignados, no solo discusión
- Archivar el acta como evidencia disponible para el auditor

Paso 5 — Plan de acción para no conformidades

- Contar con un procedimiento documentado de tratamiento de no conformidades
- Verificar que cada no conformidad previa tenga causa raíz, acción correctiva, plazo y responsable
- Confirmar cierre o seguimiento activo de las acciones pendientes
- Preparar evidencia de lecciones aprendidas aplicadas al SGSI

Plantilla de seguimiento

Completa este cuadro antes de la auditoría para tener una visión rápida del estado de cada paso.

Ítem	Estado	Responsable	Fecha límite	Evidencia disponible	
SoA actualizado					
Evidencia documental completa					
Auditoría interna realizada					
Revisión por la dirección documentada					
No conformidades cerradas o en seguimiento					