GUÍA 01 / PREPARACIÓN

Cómo preparar tu empresa para ISO 27001

Una guía de trabajo para PYMES que quieren organizar el proyecto antes de comenzar.

Qué conseguirás

Al terminar podrás describir tu objetivo, proponer un alcance inicial, identificar a las personas que deben participar y reunir información útil para una primera valoración. No necesitas tener el sistema ya implantado para realizar este ejercicio.

Qué es un SGSI

Un sistema de gestión de la seguridad de la información (SGSI) organiza cómo se identifican y tratan los riesgos, se asignan responsabilidades y se comprueban los resultados. ISO/IEC 27001:2022 establece sus requisitos. Puede aplicarse a organizaciones de distintos tamaños y sectores. [1]

Cómo utilizar esta guía

Reúne a una persona de dirección y a quienes conocen los procesos y la tecnología. Completa las preguntas con datos disponibles; anota lo que no sabes y quién puede aclararlo. Los pasos y formatos de esta guía son recomendaciones prácticas de NEXT, no una secuencia obligatoria de la norma.

Recorrido	Resultado que prepararás
1. Objetivo, alcance y equipo	Una ficha inicial del proyecto.
2. Información y prioridades	Un inventario de fuentes y decisiones pendientes.
3. Plan de arranque	Acciones con responsable y fecha.

Idea clave: empezar bien consiste en conocer tu situación y organizar el trabajo. Comprar herramientas o acumular documentos no sustituye esa preparación.

01 / DEFINIR

Aclara el objetivo, el alcance y el equipo

1. Explica por qué quieres iniciar el proyecto

¿Lo solicita un cliente? ¿Buscas reducir interrupciones, ordenar responsabilidades o preparar una certificación? Escribe el resultado esperado y distingue una fecha deseada de un compromiso contractual. Evita prometer una fecha de certificación antes de conocer la situación.

2. Propón un alcance inicial

Describe la entidad, los servicios y procesos que quieres incluir, las ubicaciones y el trabajo remoto. Identifica las aplicaciones y proveedores de los que dependen. La propuesta de alcance deberá revisarse con el contexto y las interfaces reales; no excluyas una dependencia solo porque la gestiona un tercero.

Pregunta	Ejemplo ficticio: asesoría de 25 personas
¿Qué servicio queremos proteger?	Gestión contable y documental prestada a clientes.
¿Dónde y con qué herramientas?	Una oficina, trabajo remoto, correo y repositorio en la nube; aplicación contable externa.
¿Qué dependencias debemos revisar?	Proveedor informático, plataforma contable y comunicaciones.
¿Quién debe decidir?	Dirección, responsable de operaciones y responsables de los procesos afectados.

3. Reserva personas y tiempo

Designa una persona coordinadora y un interlocutor de dirección. Identifica a quienes pueden explicar compras, personal, operaciones y sistemas. Acuerda tiempo para entrevistas, decisiones y revisiones. Una misma persona puede asumir varias funciones si se definen y se dispone de capacidad.

No olvides el contexto

Considera necesidades de clientes, proveedores y otras partes interesadas. La enmienda de 2024 incorpora la evaluación de la relevancia del cambio climático en el contexto del sistema y recuerda que las partes interesadas pueden tener requisitos relacionados. Documenta tu valoración según tu situación. [2]

02 / REUNIR

Prepara información útil, sin crear papeles de más

Localiza lo existente y registra su responsable y ubicación. Esta lista es orientativa; no implica que cada elemento deba ser un documento independiente.

Información de partida	Qué conviene localizar
Actividad e información	Servicios, flujos de trabajo, tipos de datos y procesos críticos.
Sistemas y proveedores	Equipos y aplicaciones, servicios externos, contratos y contactos.
Personas y accesos	Roles, altas y bajas, permisos y acuerdos de confidencialidad existentes.
Protección y recuperación	Medidas implantadas, copias de seguridad y resultados de pruebas de recuperación.
Incidentes y cambios	Problemas recientes, interrupciones, reclamaciones y cambios previstos.
Requisitos y compromisos	Cláusulas de clientes y obligaciones identificadas; valida su interpretación con quien corresponda.

Convierte las dudas en preguntas concretas

En vez de escribir “las copias están bien”, pregunta cuándo se recuperó por última vez un archivo y dónde está el resultado de la prueba. En vez de “el proveedor lleva la seguridad”, identifica qué tareas tiene contratadas y qué controles conserva tu organización.

Primeras prioridades: ejemplo ficticio

Si detectas cuentas de personas que ya no trabajan en la empresa, registra la incidencia y acuerda su revisión con el responsable. Si nadie conoce el procedimiento de recuperación, asigna una comprobación. Estas acciones iniciales no sustituyen la evaluación formal de riesgos.

Comparte la documentación mediante un canal acordado y con acceso limitado. Para solicitar una primera valoración suele bastar información general, sin contraseñas ni datos personales de clientes.

03 / ACTUAR

Tu hoja de preparación y el siguiente paso

Completa esta ficha en una reunión de arranque. Copia las respuestas a tu herramienta habitual para poder mantenerlas.

Campo	Respuesta / decisión pendiente
Objetivo y motivo del proyecto	_____
Servicios, sedes y dependencias	_____
Coordinación y apoyo de dirección	_____
Fecha deseada y condicionantes	_____
Tres dudas que debemos resolver	_____ _____
Primera acción, responsable y fecha	_____ _____

Antes de pedir una propuesta

Comprueba que puedes explicar el objetivo, el alcance provisional y la disponibilidad del equipo. Pide que la propuesta distinga consultoría, actuaciones técnicas, auditoría interna y certificación externa, e indique entregables y responsabilidades. La certificación corresponde a una entidad independiente. [3]

Cómo continuar con INET NEXT

Con esta información podemos revisar tu punto de partida y valorar un diagnóstico o un proyecto de implantación. Accede a Contacto desde la web de INET NEXT y describe tu necesidad; no es necesario enviar documentación sensible en la primera consulta.

Referencias y alcance de esta guía

[1] ISO: ISO/IEC 27001:2022

[2] ISO: Enmienda 1:2024

[3] ISO: Certification

Consulta: 23/09/2026. Contenido divulgativo propio: no reproduce ni sustituye la norma, una evaluación completa del SGSI o una auditoría de certificación.