CHECKLIST

Implantación de ISO 27001

30+ puntos clave para revisar si tu SGSI está bien planteado, se aplica en la práctica y está preparado para avanzar hacia la auditoría.

Cómo utilizar esta checklist
Revisa cada punto y marca el estado que mejor refleje la situación actual. No es una auditoría ni una certificación: es una herramienta de revisión para detectar aspectos que conviene mantener, revisar o priorizar antes de avanzar.

Estados de revisión

☐ Correcto	El punto está definido y funciona adecuadamente.
☐ Revisar	Existe, pero necesita actualización, mejora o mayor consistencia.
☐ Prioridad	No está resuelto o existe una debilidad que conviene abordar antes de avanzar.

Organización: _____ Fecha: _____

Responsable de la revisión: _____

1. Alcance del SGSI

Marca el estado de cada punto y anota, si es necesario, la acción que debería realizarse.

Comprobación	Estado	Notas / acción
El alcance del SGSI está definido de forma clara y documentada.	☐ C ☐ R ☐ P	
El alcance identifica los procesos, servicios, información, sistemas, ubicaciones o unidades organizativas relevantes.	☐ C ☐ R ☐ P	
Las exclusiones o límites del alcance tienen una justificación coherente con el contexto y los objetivos de la organización.	☐ C ☐ R ☐ P	
El alcance refleja cómo funciona realmente la empresa y no solo una estructura diseñada para la certificación.	☐ C ☐ R ☐ P	
Las personas implicadas conocen qué actividades y áreas quedan dentro del SGSI.	☐ C ☐ R ☐ P	
Se han revisado las dependencias con proveedores, servicios externos u otras áreas de la organización.	☐ C ☐ R ☐ P	

Resumen del bloque — Correctos: _____ Revisar: _____ Prioridades: _____
Observaciones: _____

2. Gobierno, responsabilidades y recursos

Marca el estado de cada punto y anota, si es necesario, la acción que debería realizarse.

Comprobación	Estado	Notas / acción
La Dirección conoce el propósito, alcance y objetivos del SGSI y respalda su implantación.	☐ C ☐ R ☐ P	
Existe una persona o función claramente responsable de coordinar el SGSI.	☐ C ☐ R ☐ P	
Las responsabilidades de seguridad de la información están definidas y no dependen de una única persona.	☐ C ☐ R ☐ P	
Las áreas implicadas en el alcance participan cuando sus procesos o decisiones afectan al SGSI.	☐ C ☐ R ☐ P	
Se han asignado recursos suficientes —personas, tiempo, presupuesto y herramientas— para mantener el sistema.	☐ C ☐ R ☐ P	
La implantación no se gestiona exclusivamente como un proyecto técnico de IT.	☐ C ☐ R ☐ P	
Existe un mecanismo para escalar decisiones, riesgos o incumplimientos a los responsables adecuados.	☐ C ☐ R ☐ P	

Resumen del bloque — Correctos: _____ Revisar: _____ Prioridades: _____
Observaciones: _____

3. Análisis y tratamiento de riesgos

Marca el estado de cada punto y anota, si es necesario, la acción que debería realizarse.

Comprobación	Estado	Notas / acción
Se ha establecido un método definido para identificar, analizar y evaluar los riesgos de seguridad de la información.	☐ C ☐ R ☐ P	
El análisis parte de los procesos, información, activos y circunstancias reales de la organización.	☐ C ☐ R ☐ P	
Los riesgos identificados tienen un responsable y una valoración coherente con el método utilizado.	☐ C ☐ R ☐ P	
Los criterios para aceptar o tratar los riesgos están definidos.	☐ C ☐ R ☐ P	
Existe un plan de tratamiento que relaciona los riesgos con las medidas o controles seleccionados.	☐ C ☐ R ☐ P	
Las decisiones sobre controles pueden justificarse en función de los riesgos y necesidades de la organización.	☐ C ☐ R ☐ P	
El análisis de riesgos se revisa cuando existen cambios relevantes en procesos, tecnología, organización o contexto.	☐ C ☐ R ☐ P	
Los resultados del análisis de riesgos se utilizan para tomar decisiones y no se mantienen únicamente como un documento.	☐ C ☐ R ☐ P	

Resumen del bloque — Correctos: _____ Revisar: _____ Prioridades: _____
Observaciones: _____

4. Documentación, controles y aplicación real

Marca el estado de cada punto y anota, si es necesario, la acción que debería realizarse.

Comprobación	Estado	Notas / acción
Las políticas y procedimientos del SGSI están adaptados a la organización y no son simples documentos genéricos.	☐ C ☐ R ☐ P	
La documentación describe procesos y responsabilidades que realmente se aplican.	☐ C ☐ R ☐ P	
Los controles definidos tienen un responsable y una forma concreta de aplicación.	☐ C ☐ R ☐ P	
Las personas que deben aplicar los controles conocen sus responsabilidades.	☐ C ☐ R ☐ P	
Los procedimientos y controles se integran, cuando es posible, en la operativa habitual de la empresa.	☐ C ☐ R ☐ P	
Existe evidencia de que los controles documentados se están ejecutando.	☐ C ☐ R ☐ P	
La documentación se mantiene actualizada cuando cambian los procesos o las responsabilidades.	☐ C ☐ R ☐ P	
Se evita crear documentación que nadie utiliza o que no puede demostrarse en la práctica.	☐ C ☐ R ☐ P	

Resumen del bloque — Correctos: _____ Revisar: _____ Prioridades: _____
Observaciones: _____

5. Evidencias, auditoría interna y preparación

Marca el estado de cada punto y anota, si es necesario, la acción que debería realizarse.

Comprobación	Estado	Notas / acción
Se ha definido qué evidencias deben conservarse para demostrar la aplicación de los controles.	☐ C ☐ R ☐ P	
Las evidencias disponibles son suficientes para demostrar que los procesos y controles funcionan.	☐ C ☐ R ☐ P	
Se han identificado y gestionado las desviaciones o incumplimientos detectados durante la implantación.	☐ C ☐ R ☐ P	
Se ha realizado una auditoría interna o una revisión equivalente antes de afrontar la auditoría de certificación.	☐ C ☐ R ☐ P	
Los resultados de la auditoría interna se han analizado y se han definido acciones cuando ha sido necesario.	☐ C ☐ R ☐ P	
La Dirección revisa el funcionamiento del SGSI y dispone de información para tomar decisiones.	☐ C ☐ R ☐ P	
Las acciones pendientes tienen responsables y seguimiento.	☐ C ☐ R ☐ P	
La organización puede explicar y demostrar cómo funciona el SGSI sin depender únicamente de la persona que lideró la implantación.	☐ C ☐ R ☐ P	

Resumen del bloque — Correctos: _____ Revisar: _____ Prioridades: _____
Observaciones: _____

De la revisión a la acción

Esta checklist permite identificar puntos que conviene mantener, revisar o priorizar. El siguiente paso no debería ser simplemente acumular documentación, sino comprobar que el SGSI está adaptado al contexto de la organización, que los riesgos están gestionados y que los controles se aplican y pueden demostrarse.

Si has marcado varios puntos como “Revisar” o “Prioridad”, puede ser útil realizar una revisión más detallada antes de avanzar hacia la auditoría.

¿Necesitas ayuda para implantar ISO 27001?

BcnSoluciona
Acompañamos a las organizaciones en el diseño e implantación de su SGSI, desde el análisis inicial hasta la preparación para la auditoría.