GUÍA 02 / DOCUMENTACIÓN

Cómo preparar una Declaración de Aplicabilidad

Una guía práctica para conectar riesgos, controles y evidencias en tu SGSI.

Qué es la SoA

La Declaración de Aplicabilidad (SoA, por sus siglas en inglés) reúne los controles necesarios, la justificación de su inclusión y si están implantados. También justifica las exclusiones de controles del Anexo A. Este contenido se vincula a la cláusula 6.1.3 d) de ISO/IEC 27001:2022. [1, 2]

Qué conseguirás con esta guía

Podrás preparar las entradas, elegir una estructura de trabajo y redactar una primera ficha de control. Encontrarás ejemplos ficticios para distinguir necesidad, implantación y evidencia. No se incluye el catálogo de controles ni se reproduce el texto de la norma.

Tres documentos que deben conectarse

La evaluación de riesgos explica qué puede afectar a la información. El plan de tratamiento organiza las respuestas, acciones y recursos. La SoA recoge las decisiones sobre controles. Mantén referencias entre ellos para evitar versiones contradictorias.

Pregunta	Dónde buscar la respuesta
¿Qué necesitamos tratar?	Evaluación de riesgos y requisitos identificados.
¿Qué controles necesitamos y por qué?	Declaración de Aplicabilidad.
¿Quién hará lo pendiente y cuándo?	Plan de tratamiento o registro de acciones relacionado.

Base de referencia: ISO/IEC 27001:2022, considerando su enmienda de 2024. Los ejemplos y el diseño de fichas son propuestas de NEXT, no modelos oficiales de ISO.

01 / PREPARAR

De la información de partida a las decisiones

1. Reúne las entradas

Trabaja con el alcance del SGSI, la evaluación de riesgos, las decisiones de tratamiento y los requisitos identificados. Localiza también las medidas existentes y quién puede demostrar cómo funcionan. Si faltan entradas, anota la duda y su responsable antes de dar por definitiva una decisión.

2. Selecciona y contrasta

Determina los controles necesarios y compáralos con el Anexo A para detectar omisiones. No limites la selección al catálogo si hacen falta controles propios o de otras fuentes. El Anexo A sirve de contraste, no sustituye el análisis de tu organización. [3]

3. Separa aplicabilidad y estado

Un control necesario puede estar pendiente. La falta de presupuesto o de implantación no lo convierte en “no aplicable”. Registra la necesidad y enlaza la actuación pendiente. Del mismo modo, un servicio externalizado exige analizar las responsabilidades compartidas, no excluir automáticamente sus controles.

4. Redacta una razón que pueda entenderse

Una justificación útil conecta una necesidad concreta con la medida elegida. Evita frases vacías como “porque lo pide ISO”. Para una exclusión, describe la situación que hace innecesario el control y qué información permite sostenerla; reevalúala si cambia esa situación.

Evita	Mejor enfoque de redacción
“Aplica por seguridad”.	“Necesario para reducir el riesgo de acceso a expedientes por cuentas no autorizadas”.
“No aplica: está externalizado”.	Identifica qué realiza el proveedor, qué verificas y qué conserva tu empresa.
“Implantado: existe una política”.	Indica cómo se aplica, quién lo comprueba y qué registro lo demuestra.

02 / ESTRUCTURAR

Una ficha sencilla para cada decisión

El formato puede ser una hoja de cálculo o una herramienta documental. Lo importante es mantener contenido coherente y localizable. Separa el contenido esencial de los campos auxiliares que proponemos para trabajar. [2]

Campo	Qué escribir
Control necesario / referencia	Identificación inequívoca y correspondencia con el Anexo A u otra fuente.
Justificación de inclusión	Riesgo, requisito o necesidad concreta que atiende.
Estado de implantación	Si está implantado; si está pendiente o parcial, explica qué falta.
Exclusión del Anexo A	Motivo específico cuando se considera innecesario un control de referencia.
Responsable (auxiliar)	Persona o función que mantiene y verifica la medida.
Evidencia (auxiliar)	Referencia a registros o comprobaciones, con fecha cuando proceda.
Acción / riesgo (auxiliar)	Identificador del riesgo o requisito y de la acción pendiente.
Versión y revisión (gestión)	Fecha, autor, aprobación interna e historial de cambios según vuestro procedimiento.

Convención de estados propuesta

Puedes usar “Implantado”, “Parcial” y “Pendiente”, definiendo qué significa cada uno. En “Parcial”, indica que aún no está completamente implantado y describe la parte que falta. “Excluido” es una decisión de aplicabilidad, no un grado de implantación.

Protege el detalle sensible

Enlaza a las evidencias en su ubicación controlada. Evita copiar contraseñas, configuraciones sensibles o datos de clientes en la SoA. Si debes compartirla, valora el destinatario y el nivel de detalle autorizado.

03 / EJEMPLOS

Cómo se ve una decisión bien documentada

Casos ficticios de una asesoría que usa aplicaciones en la nube. Los nombres son descriptivos, no títulos oficiales del Anexo A. Deben contrastarse con el alcance y los requisitos de cada organización.

Ejemplo A / Gestión de bajas de acceso

Decisión: control necesario. **Motivo:** reducir el riesgo R-04 de que una persona desvinculada acceda a expedientes. **Estado:** parcial; se cancelan cuentas principales, pero no existe una comprobación de todas las aplicaciones. **Responsables:** personal comunica la baja y sistemas la ejecuta. **Evidencia disponible:** tickets de dos bajas recientes. **Acción A-07:** completar la relación de aplicaciones y verificar la próxima baja con fecha acordada.

Ejemplo B / Recuperación de información

Decisión: control necesario. **Motivo:** responder al riesgo R-09 de pérdida de expedientes. **Estado:** implantado para el repositorio incluido en este ejemplo. **Evidencia:** registro de ejecución de copias y prueba de restauración satisfactoria del 10/09/2026, con alcance y resultado. **Seguimiento:** revisar cambios de datos, herramientas y necesidades de recuperación. Una prueba aislada no acredita por sí sola la eficacia permanente.

Ejemplo C / Una exclusión que debe revisarse

Para el control relativo a codificación segura, una posible exclusión requeriría comprobar que en el alcance no se desarrolla código ni se encarga desarrollo a terceros, y que tampoco existen scripts o automatizaciones que lo hagan relevante. Esa conclusión debe quedar sustentada. Usar software comercial no elimina la necesidad de revisar proveedores, configuraciones, accesos y otros controles aplicables.

Comprobación de coherencia

¿La justificación se entiende sin hablar con quien la escribió? ¿El estado coincide con la evidencia? ¿Lo pendiente tiene una acción? ¿La decisión seguiría siendo válida si se incorpora una aplicación nueva o un proveedor cambia el servicio?

04 / MANTENER

Revisa, valida y conserva una versión útil

Antes de cerrar una versión, utiliza estas preguntas como revisión interna orientativa:

- ¿El alcance y la evaluación de riesgos utilizados están identificados?
- ¿Se han contrastado los controles necesarios con el Anexo A?
- ¿Las inclusiones y exclusiones tienen razones concretas?
- ¿Los estados describen la situación real y las evidencias son localizables?
- ¿Las actuaciones pendientes están conectadas con responsables y seguimiento?
- ¿La versión ha sido revisada por las personas responsables y aprobada según vuestro proceso?

Cuándo volver a revisarla

Establece una revisión planificada y desencadénala también ante cambios relevantes: nuevo servicio, proveedor, incidente, riesgo o hallazgo de auditoría. Registra qué cambió, por qué y quién lo validó. No existe una periodicidad mensual universal propuesta en esta guía.

Siguiente paso con INET NEXT

Si ya tienes una SoA, podemos revisar su coherencia y el estado documentado. Si empiezas desde cero, primero aclararemos las entradas necesarias. Consulta la página Declaración de Aplicabilidad o Contacto en la web de INET NEXT.

Referencias y alcance de esta guía

[1] ISO: ISO/IEC 27001:2022

[2] Grupo de prácticas de auditoría: nota educativa sobre SoA (2022)

[3] Grupo de prácticas de auditoría: nota educativa sobre Anexo A (2022)

[4] ISO: Enmienda 1:2024

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

Las notas educativas [2] y [3] no son normas ni interpretaciones oficialmente avaladas por ISO; sus referencias antiguas deben leerse en su contexto. Para aplicar requisitos, consulta la edición vigente de la norma.