

Dazr Compliance · Ficha de producto · SGSI y controles

Un SGSI que funciona con controles recurrentes.

Cada control de ISO 27001, RGPD, NIS2 y ocho marcos más se convierte en un control recurrente con responsable, fecha de vencimiento, evidencias y un recordatorio. Aprueba tu declaración de aplicabilidad, vincula los controles a los riesgos, políticas y procesos que cubren, y consulta en el panel la cobertura por marco.

ISO 27001 · Control A.5.18



Access rights

Access rights to information and assets provisioned, reviewed, modified and removed in accordance with the access-control policy.

● **Abierto** ISO 27001 Válida hasta el 26 dic 2026

Asignado a

 mark.jansen@bright ▼

Fecha de vencimiento

06/10/2026



Se repite

No se repite

Cada mes

Cada 3 meses

Cada 6 meses

Cada año

Evidencia

Cuenta como cubierto hasta **26 dic 2026**

Funciones principales

- ✓ **11 marcos** en un único espacio de trabajo: ISO 27001:2022 (93 controles del Anexo A más cláusulas 4-10), RGPD, NIS2, NEN 7510, DORA, EU AI Act, ISO 27701, ISO 22301, SOC 2, BIO y PCI DSS.
- ✓ **Evidencias** como notas, enlaces y archivos, con fecha de validez y alertas de caducidad.
- ✓ **Vínculos y procesos:** conecta controles, riesgos, políticas, procesos, activos, proveedores y actividades de tratamiento.
- ✓ **Controles recurrentes** con responsable, fecha de vencimiento, descripción, recomendación y periodicidad de revisión.
- ✓ **Declaración de aplicabilidad** con justificación por control, versiones aprobadas, PDF y XLSX.
- ✓ **Panel:** controles cubiertos por marco, cobertura a lo largo del tiempo y lo que requiere tu atención ahora.

Controles recurrentes con responsables

- Asigna un responsable y una fecha de vencimiento. El responsable recibe un correo cuando se le asigna el control, 7 días antes de que venza y cada semana mientras está vencido.
- Elige una periodicidad: una vez, cada mes, cada 3 meses, cada 6 meses o cada año. Enterprise define su propio intervalo por control.
- Al completar un control, sus evidencias se bloquean y se programa el siguiente ciclo, de modo que el historial de cada revisión permanece intacto.
- Los comentarios por control mantienen la conversación junto a las evidencias; los auditores externos también pueden comentar.
- Desde Basic, añade tus propias tareas junto a los controles del marco, para el trabajo que ningún estándar prescribe.

Declaración de aplicabilidad

Marca cada control de ISO 27001 como aplicable o no, indica el motivo (evaluación de riesgos, requisito legal o contractual, requisito de negocio o buena práctica) y registra el estado de implantación: implantado, parcial, planificado o no implantado. Excluir un control exige una justificación, como espera la cláusula 6.1.3 d. Los controles excluidos desaparecen de tu lista de controles y de la cobertura.

Aprueba una versión cuando la declaración de aplicabilidad esté lista: Dazr conserva cada versión aprobada con quién la aprobó y cuándo, y la exporta en PDF o XLSX. Incluido desde Basic.

Controles, riesgos, políticas y procesos, vinculados

Todo en el espacio de trabajo puede apuntar a todo lo demás: controles, riesgos, políticas, procesos, activos, proveedores y actividades de tratamiento. Un riesgo muestra los controles que lo tratan, una política muestra los controles que respalda y un proceso muestra los controles, riesgos y activos de los que depende. Los vínculos también los ven los auditores, en solo lectura.

El **registro de procesos** (Pro y Enterprise) enumera tus procesos de negocio con una descripción, una criticidad y un responsable, hasta 500 por espacio de trabajo, para que el trabajo de continuidad y de riesgos cuelgue de los procesos que importan.

Declaración de aplicabilidad

Para cada control, registra si se aplica a tu organización, por qué y hasta qué punto está implementado (ISO/IEC 27001:2022, cláusula 6.1.3 d). Los controles excluidos desaparecen de la lista de controles, la cobertura, los recordatorios y la preparación.

Marco ISO 27001
PDF CSV Excel
Marcar la SuA como aprobada

90 aplicables · 3 excluidos · 0 sin justificación
Aprobada v1 por samuel.davies@brightwater.example el 2 oct 2026

Todos 93 Aplicables 90 Excluidos 3 Sin justificación 0
Buscar código, título o justificación...

Control	Título	Aplicable	Justificación	Implementación	Evidencia	Última revisión
5. CONTROLES ORGANIZATIVOS (37)						
☐	A.5.1 Policies for information security	☒	Exigido por la evaluación d	Implementado	0	-
	Añade detalles (opcional)					
☐	A.5.2 Information security roles and responsibilities	☒	Exigido por la evaluación d	Implementado	0	-
	Añade detalles (opcional)					
☐	A.5.3 Segregation of duties	☒	Exigido por la evaluación d	Parcialmente	0	9 jul 2026
	Añade detalles (opcional)					
☐	A.5.4 Management responsibilities	☒	Requisito legal o contractu	Implementado	0	2 jun 2026

Plataforma

- ✓ Alojado en la UE, desarrollado por Dazr en Italia
- ✓ Registros cifrados en reposo con AES-256-GCM
- ✓ Acceso con Google, Microsoft o un código por correo
- ✓ Roles: propietario, administrador, miembro, auditor
- ✓ Registro de actividad con búsqueda y exportación
- ✓ Inglés, neerlandés, italiano, alemán, francés, español y polaco