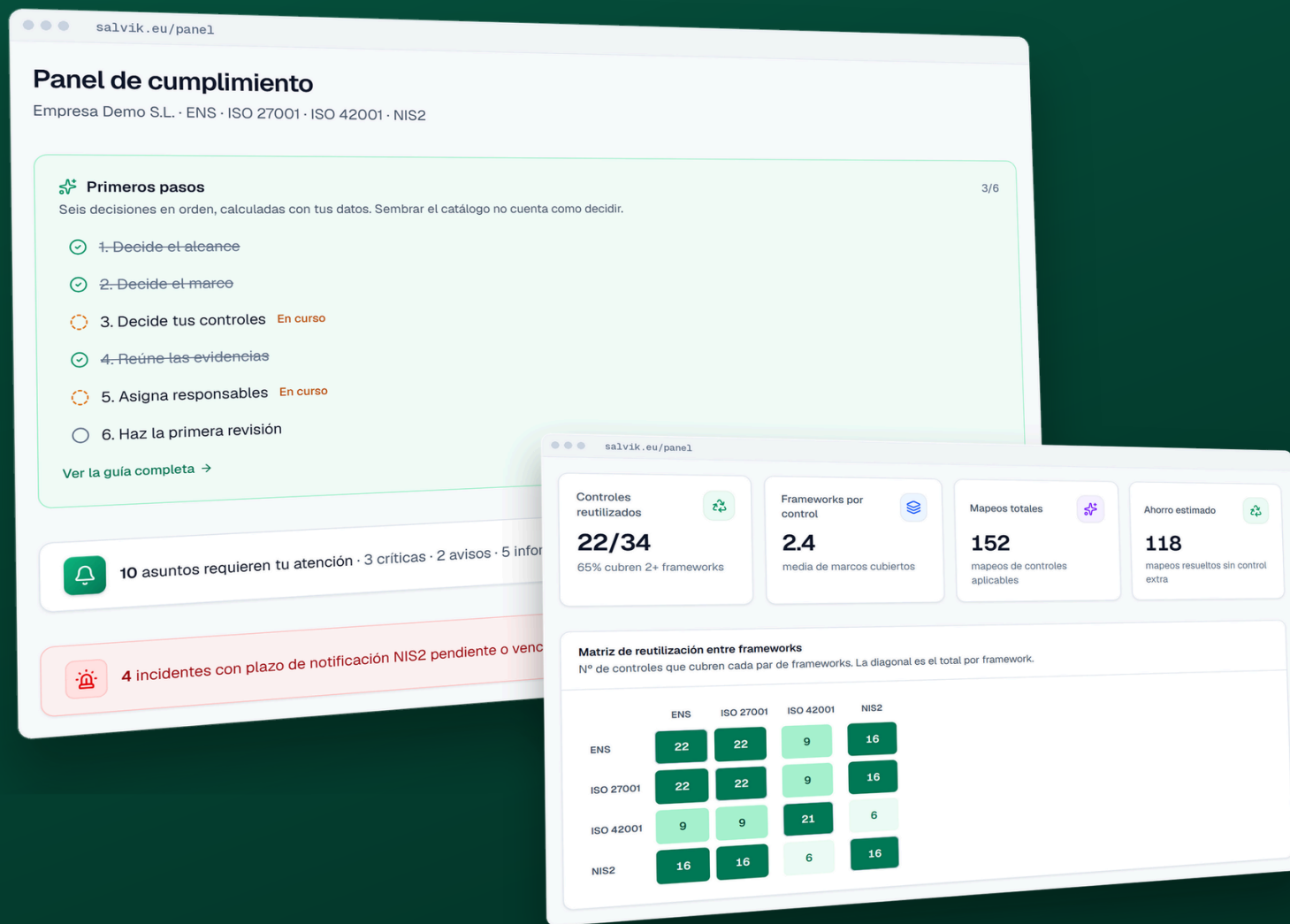


De cero a auditoría con **Salvik**

ISO 27001, ISO 42001, NIS2 y ENS en un solo sistema. Un recorrido completo por la plataforma, paso a paso, con una empresa de ejemplo.



Panel de cumplimiento
Empresa Demo S.L. · ENS · ISO 27001 · ISO 42001 · NIS2

Primeros pasos 3/6
Seis decisiones en orden, calculadas con tus datos. Sembrar el catálogo no cuenta como decidir.

- 1. Decide el alcance
- 2. Decide el mapeo
- 3. Decide tus controles **En curso**
- 4. Reúne las evidencias
- 5. Asigna responsables **En curso**
- 6. Haz la primera revisión

[Ver la guía completa →](#)

10 asuntos requieren tu atención · 3 críticas · 2 avisos · 5 info

4 incidentes con plazo de notificación NIS2 pendiente o vencido

Controles reutilizados 22/34
65% cubren 2+ frameworks

Frameworks por control 2.4
media de marcos cubiertos

Mapeos totales 152
mapeos de controles aplicables

Ahorro estimado 118
mapeos resueltos sin control extra

Matriz de reutilización entre frameworks
Nº de controles que cubren cada par de frameworks. La diagonal es el total por framework.

	ENS	ISO 27001	ISO 42001	NIS2
ENS	22	22	9	16
ISO 27001	22	22	9	16
ISO 42001	9	9	21	6
NIS2	16	16	6	16

SALVIK EN UNA PÁGINA

Deja de hacer cuatro veces el mismo trabajo.

Si tu empresa tiene que cumplir ISO 27001, ENS, NIS2 o ISO 42001, lo habitual es llevar cada norma por su lado: su hoja de cálculo, sus controles, sus evidencias y su auditoría. Y buena parte del trabajo se repite. La misma copia de seguridad, la misma política de accesos o el mismo registro de riesgos responden a requisitos de varias normas a la vez.

Salvik parte de esa idea. Cada control queda conectado con los requisitos de todas tus normas —los del catálogo ya vienen conectados—, así que lo trabajas una vez y cuenta para todas. A partir de ahí te guía en el orden correcto, te avisa de lo que caduca o vence, usa la IA para el trabajo pesado (planes Pro y Auditado) y, si la contratas, un auditor certificado revisa y firma tus controles para tu auditoría interna.



Las cuatro normas, ya cargadas

265 requisitos de ISO 27001, ISO 42001, NIS2 y ENS, y un catálogo de 26 controles ya conectados a 95 de ellos.



Un control, varias normas

El cruce entre normas se mide: ves qué controles sirven para varias a la vez.



Tu primera semana, en orden

Seis decisiones guiadas —alcance, marco, controles, evidencias, responsables y revisión— calculadas con tus datos.



Avisos antes de que sea tarde

Evidencias por caducar, controles sin prueba, riesgos sin tratar y plazos de notificación NIS2.



IA con permiso y con rastro

Redacta políticas, borradores de notificación y respuestas a cuestionarios (Pro y Auditado). Apagada hasta que la enciendes; cada envío queda registrado.



Auditoría interna firmada

En el plan Auditado, un Lead Auditor certificado revisa y firma tus controles, y cualquiera puede verificar el informe.



Lo que Salvik no hace

Salvik no certifica: la certificación solo la emite un organismo de certificación (acreditado, si quieres reconocimiento internacional). Tampoco decide por ti qué controles necesitas. Te da el sistema para gestionar tu cumplimiento y, si la contratas, una revisión de controles firmada por un auditor certificado para tu auditoría interna (cláusula 9.2).



Cómo leer este manual

Cada capítulo es un paso del recorrido. Las capturas llevan números que corresponden a los pasos y a la leyenda. Todo lo que ves está en la demo pública: abre salvik.eu/panel y síguelo en paralelo, sin registrarte. Las capturas son del 27 de septiembre de 2026; las fechas y los plazos de la demo avanzan con el calendario.

CONTENIDO

Índice

01	Conoce a Empresa Demo S.L.	4
PARTE I · ARRANQUE		
02	Crea tu cuenta	7
03	Tu primera semana, en orden	8
04	Elige tus marcos	9
05	Define el alcance y genera tu SoA inicial	10
06	Tus controles: un catálogo ya conectado	11
07	Un control, cuatro normas	13
PARTE II · DÍA A DÍA		
08	Evidencias: la prueba de que cada control funciona	15
09	Alertas y tareas: Salvik te dice qué toca	16
10	Riesgos: la matriz y su tratamiento	17
11	Políticas: redacta con IA, revisa y aprueba	18
12	Incidentes: los plazos de NIS2, bajo control	19
13	RegWatch: qué cambia en la normativa y a qué puede afectarte	20
PARTE III · INTELIGENCIA ARTIFICIAL		
14	Descubre la IA que ya se usa en tu empresa	22
15	Inventario y gobierno de la IA	24
16	Cuestionarios de seguridad de clientes, con IA	26
PARTE IV · AUDITORÍA Y DIRECCIÓN		
17	Auditoría interna firmada y verificable	28
18	Revisión por la dirección	31
19	Trust Center: tu postura de seguridad, a la vista	32
PARTE V · ORGANIZACIÓN		
20	Equipo, roles y tus datos	35
·	Tu primera semana con Salvik	36
·	Planes y precios	37

Conoce a Empresa Demo S.L.

Todo el manual sigue a la misma empresa ficticia. Así ves cómo encaja cada pieza con datos de trabajo, no con pantallas vacías.



Empresa Demo S.L.

Tecnología / SaaS · unas 60 personas

Vende software a banca, aseguradoras y Administración pública.

Por qué necesita cada norma

ISO 27001	Sus clientes grandes la piden en cada contrato.
ENS	Vende a la Administración: sin ENS no hay licitación.
NIS2	Da servicio a entidades esenciales: las exigencias le llegan por la cadena de suministro.
ISO 42001	Usa IA en su producto —un asistente de atención al cliente y un modelo de detección de fraude— y en el día a día.

Es una empresa en marcha, no un escaparate perfecto: sigue los cuatro marcos con 34 controles (los 26 del catálogo y 8 propios de su sistema de gestión de IA), ya ha pasado una primera auditoría interna de ejemplo de ISO 27001, tiene ISO 42001 lista para auditar y el panel le dice por dónde seguir.

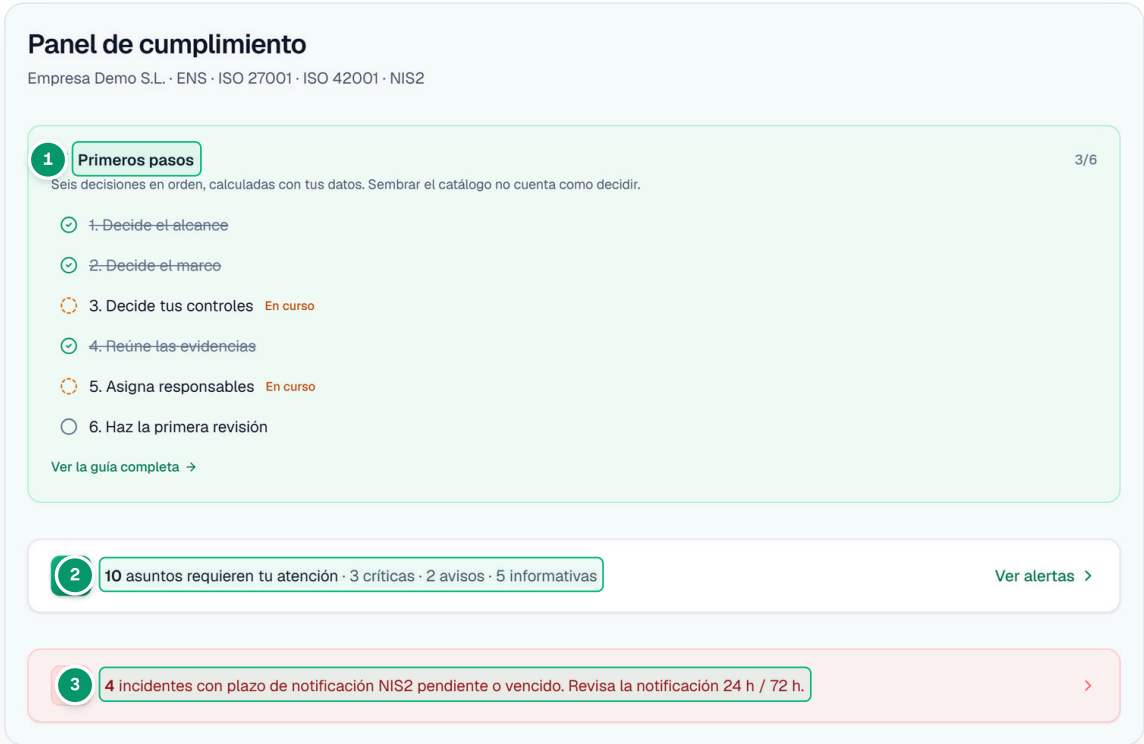


Figura 1. El panel de cumplimiento de Empresa Demo S.L.

- 1

Primeros pasos: las seis decisiones del arranque, con su estado real.
- 2

Resumen del centro de alertas, por gravedad.
- 3

Aviso de plazos NIS2: incidentes con notificación pendiente o vencida.

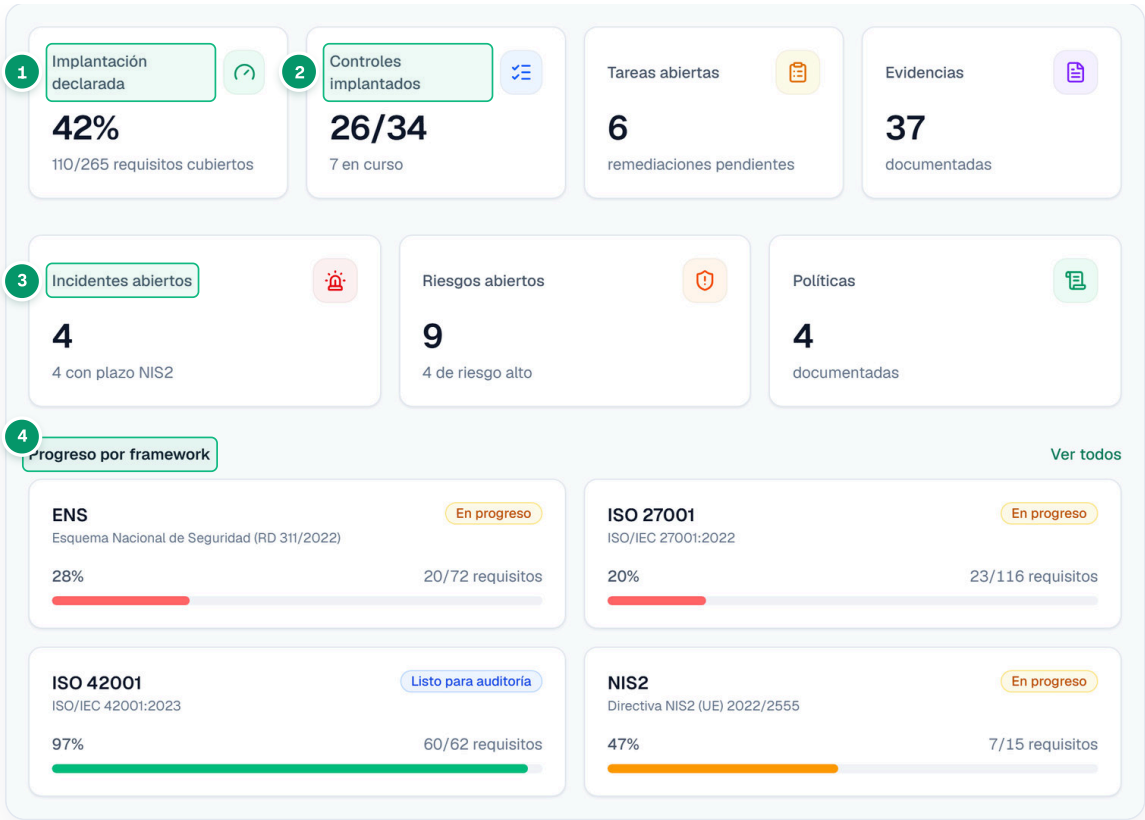


Figura 2. Indicadores y avance de cada marco.

- 1

Implantación declarada: requisitos con un control que la organización declara implantado.
- 2

Controles implantados y en curso.
- 3

Incidentes abiertos y cuántos tienen plazo NIS2.
- 4

Avance de cada marco, con sus requisitos cubiertos.



Síguelo en la demo

Todas las pantallas de este manual son de la demo pública. Ábrela en salvik.eu/panel y recorre cada capítulo en paralelo, sin registrarte.

PARTE I · ARRANQUE

Tu primera semana

Del registro a tu primera Declaración de Aplicabilidad.

02 Crea tu cuenta

03 Tu primera semana, en orden

04 Elige tus marcos

05 Define el alcance y genera tu SoA inicial

06 Tus controles: un catálogo ya conectado

07 Un control, cuatro normas

CAPÍTULO 2 · ARRANQUE

Crea tu cuenta

Correo, contraseña y dentro. Sin tarjeta y sin instalar nada.

Crear cuenta

1 Email

Contraseña

2 Acepto el [aviso legal y las condiciones de uso](#). He leído la [política de privacidad](#).

Tratamos tus datos para darte acceso al servicio y prestarlo (ejecución del contrato). No te pedimos consentimiento para eso ni te enviamos publicidad por darte de alta.

3 Crear cuenta gratis

4 Sin tarjeta. El nombre de tu organización lo ajustas dentro, en un paso.

¿Ya tienes cuenta? [Entrar](#)

- 1 Entra en **salvik.eu** y pulsa «Empezar gratis».
- 2 Escribe tu correo de trabajo y una contraseña **1**.
- 3 Acepta el aviso legal y las condiciones de uso **2** y pulsa «Crear cuenta gratis» **3**.
- 4 Confirma tu correo con el enlace que te llega.
- 5 Pon el nombre de tu organización **4** y elige tu ruta de arranque: lo verás en el capítulo siguiente.

Figura 3. Alta en salvik.eu.



La prueba gratuita

Dura 7 días, es gratis y sin tarjeta, y usa el plan Base: un marco, sin IA, RegWatch ni Trust Center, y hasta tres personas. Si después contratas, sigues donde lo dejaste: no se pierde nada de lo que hayas registrado.



Consejo

Invita a tu equipo desde el principio (capítulo 20): en la prueba caben tres personas. Cada invitación es un enlace personal, de un solo uso.

Tu primera semana, en orden

Salvik te marca seis decisiones en orden y calcula con tus datos cuáles están hechas.

La primera pregunta es si ya tienes un sistema de gestión en marcha. Si ya lo tienes (ruta A), se trata de trasladarlo a Salvik; si empiezas de cero (ruta B), Salvik te acompaña paso a paso. Cada paso se adapta a la ruta que elijas.

Puesta en marcha

Tu primera semana, en orden: alcance, marco, controles, evidencias, responsables y revisión

3 de 6 decisiones hechas

[Guía en PDF](#)

Siguiente: **3. Decide tus controles**. 33 de 34 controles decididos.

El estado se calcula con lo registrado en Salvik. Refleja lo que has decidido y documentado aquí, no el nivel de cumplimiento ni la opinión de un auditor.

1

¿Ya tenéis un sistema de gestión en marcha?

Elige tu ruta y cada paso te dirá qué cambia para ti.

✓

Paso 1. Decide el alcance

2

15 min (ruta A) / 1-2 h (ruta B)

3

Terminado cuando:

4

Error típico:

Qué parte de la organización entra: sedes, procesos, sistemas y personas. Todo lo demás depende de esto.

Se toma como alcance la evidencia «Alcance y contexto del SGIA v1.0». Si no lo es, renómbrala.

En Evidencias hay una entrada con «alcance» en el nombre y su enlace abre el documento.

Poner «toda la empresa» sin haberlo pensado. Luego tendrás que justificar controles en sitios que nadie ha revisado.

[Ir a Evidencias y Riesgos →](#)

Figura 4. Puesta en marcha: la guía de la primera semana.

1

La ruta: ya hay sistema de gestión (A) o se empieza de cero (B).

2

Tiempo estimado del paso, según la ruta.

3

«Terminado cuando»: el criterio con el que Salvik da el paso por hecho.

4

«Error típico»: lo que más se repite en las implantaciones.

1. Decide el alcance 15 min (A) · 1-2 h (B)	2. Decide el marco 15 min	3. Decide tus controles 2-3 h
4. Reúne las evidencias 1-2 h	5. Asigna responsables 45 min	6. Haz la primera revisión 1 h

**Ojo**

El porcentaje de avance refleja lo que has registrado en Salvik, no el nivel de cumplimiento ni la opinión de un auditor. Úsalo para saber qué atacar, no como una nota.

**¿Prefieres ir acompañado?**

«Puesta en marcha desde cero»: una sesión de trabajo para dejar Salvik montado y a tu equipo formado. **499 € + IVA**, pago único.

salvik.eu

8

CAPÍTULO 4 · ARRANQUE

Elige tus marcos

ISO 27001, ISO 42001, NIS2 y ENS vienen cargados con sus requisitos. Sigues solo los que te aplican.

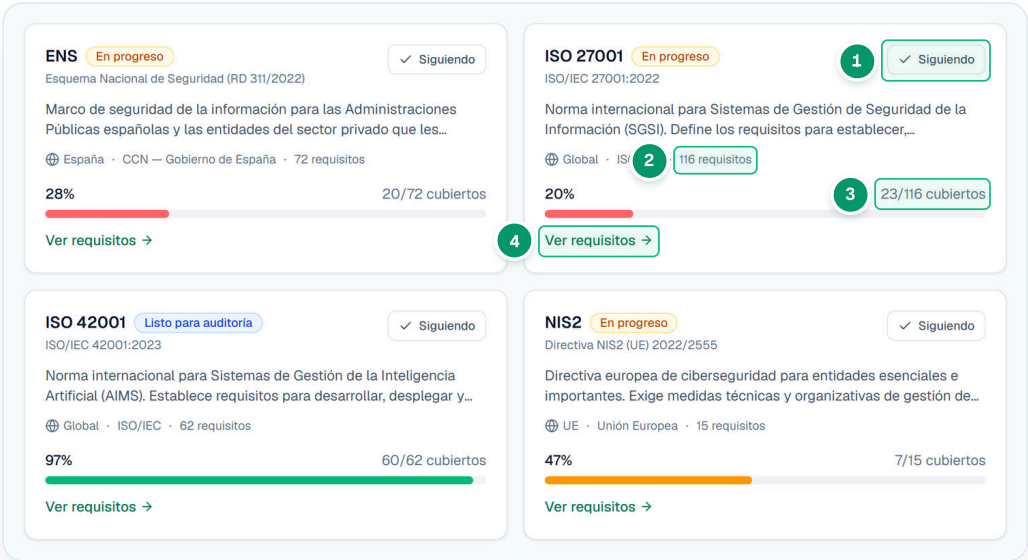


Figura 5. Frameworks: los cuatro marcos, con su avance.

- 1 «Siguiendo»: activa o desactiva cada marco.
- 2 Número de requisitos del marco.
- 3 Requisitos que ya cubren tus controles.
- 4 «Ver requisitos»: el detalle, uno a uno.

Cada marco trae su catálogo: ISO 27001 con 116 requisitos (las cláusulas 4 a 10 y los 93 controles del Anexo A), ISO 42001 con 62, NIS2 con 15 y el ENS con 72 medidas. Un mismo control de tu catálogo puede cubrir requisitos de varios; lo verás en el capítulo 7.

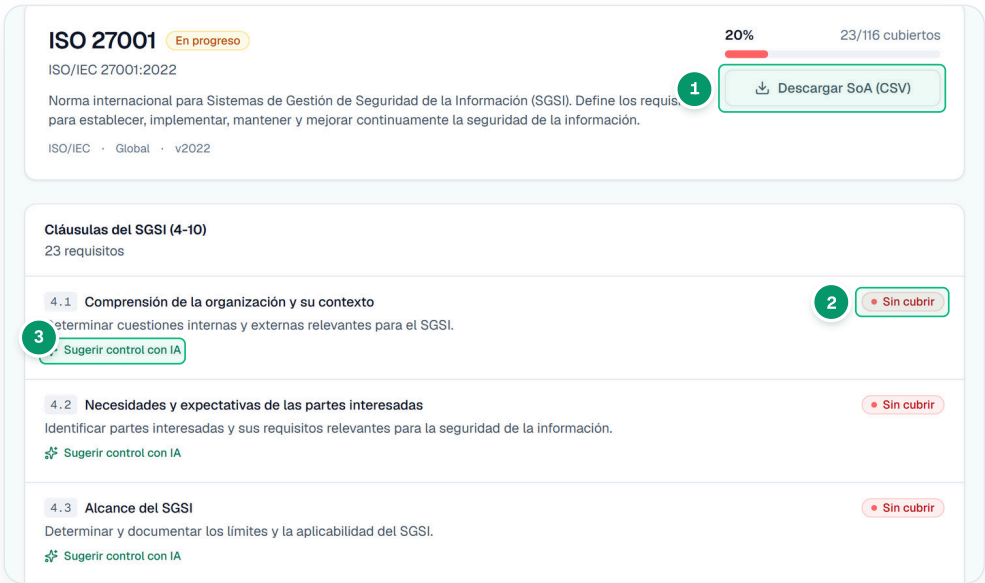


Figura 6. Los requisitos de ISO 27001 y su Declaración de Aplicabilidad.

- 1 «Descargar SoA (CSV)»: la Declaración de Aplicabilidad del marco, para trabajar sobre ella.
- 2 Requisitos que todavía no cubre ningún control.
- 3 «Sugerir control con IA»: propone un control para cubrir el hueco.



Según tu plan

El plan Base, y también la prueba, incluye un marco; Pro y Auditado, los cuatro. «Sugerir control con IA» está en Pro y Auditado.

CAPÍTULO 5 · ARRANQUE

Define el alcance y genera tu SoA inicial

Cuenta lo básico de tu organización y parte de una SoA inicial que después ajustas control a control.

- 1 Abre el **Asistente SoA** y rellena el perfil de alcance: sector **1**, «¿Usáis sistemas de IA?» **2** y «¿Sois proveedor del sector público?» **3**.
- 2 Pulsa «Generar SoA inicial» **4**: todos los controles del catálogo quedan como aplicables, salvo los de IA si no la usáis, y el resultado te recomienda ISO 42001 o el ENS según tus respuestas.
- 3 Revisa cada control en Controles (capítulo 6) y ajusta su aplicabilidad —aplicable, no aplicable o parcial— con su justificación.
- 4 Sube a Evidencias el documento de alcance, con «alcance» en el nombre: así la guía da por hecho el primer paso.
- 5 Descarga la SoA de cada marco desde Frameworks cuando la necesites (capítulo 4).

Figura 7. Asistente «de cero a SoA».

La Declaración de Aplicabilidad (SoA, por sus siglas en inglés) es el documento que dice qué controles aplican a tu organización y por qué. El asistente te da un punto de partida en segundos; las decisiones, y su justificación, son tuyas.



Consejo

No pongas «toda la empresa» como alcance sin haberlo pensado: después tendrás que justificar controles en sitios que nadie ha revisado.

CAPÍTULO 6 · ARRANQUE

Tus controles: un catálogo ya conectado

Empiezas con un catálogo de 26 controles ya conectados con los requisitos que cubren. Tú decides su estado real.

Controles

4

Exportar controles

Controles internos unificados. Cada uno puede satisfacer requisitos de varios frameworks (cross-mapping).

Código	Control	Estado	Respons	Cubre frameworks	Requisitos	Evidencias
1 AC-01	Control de acceso y gestión de identidades Control de acceso	2 Implantado	3 Usuario Demo	ENSISO 27001NIS2	7	1
AC-02	Autenticación multifactor (MFA) Control de acceso	Implantado	Usuario Demo	ENSISO 27001NIS2	4	1
AI-01	Política y gobernanza de IA Gobernanza de IA	Implantado	Usuario Demo	ISO 42001	6	2
AI-02	Evaluación de impacto de sistemas de IA Gobernanza de IA	Implantado	Usuario Demo	ISO 42001	5	2
AI-03	Inventario y clasificación de sistemas de IA Gobernanza de IA	Implantado	Usuario Demo	ENSISO 27001ISO 42001	4	1

Figura 8. Controles: el catálogo unificado.

- 1

Cada control, con su código y su nombre.
- 2

Estado real de cada control.
- 3

Los marcos que cubre.
- 4

«Exportar controles» a CSV.

Abre un control para ver su ficha. Ahí decides su estado (sin empezar, en curso, implantado o no aplica), su aplicabilidad en la SoA (aplicable, no aplicable o parcial), su responsable, su eficacia y cada cuánto se revisa.

RSK-01

Enc1

Aplicable

3

Eficacia

45%

Gestión de riesgos de seguridad

Gestión de riesgos

Metodología de análisis y tratamiento de riesgos aplicada periódicamente, con registro de riesgos mantenido.

2

Responsable: Usuario Demo

Versión 1.0

Revisión: Anual

Última revisión: —

4

Grafo de evidencia

Trazabilidad de un vistazo: requisito → control → evidencia → responsable → alerta.

REQUISITOS

6

en 4 frameworks

ENSISO 27001ISO 42001NIS2

→

RSK-01

Gestión de riesgos de seguridad

Encurso

Usuario Demo

→

EVIDENCIAS

1

1 vigentes

Registro de riesgos y plan de ...

ALERTAS DE ESTE CONTROL

Sin alertas activas.

Figura 9. Ficha del control RSK-01, «Gestión de riesgos de seguridad».

1

Estado y aplicabilidad (SoA).

2

Responsable, versión y frecuencia de revisión.

3

Eficacia del control (0-100).

4

Grafo de evidencia: requisito → control → evidencia → responsable → alerta.

salvik.eu

11

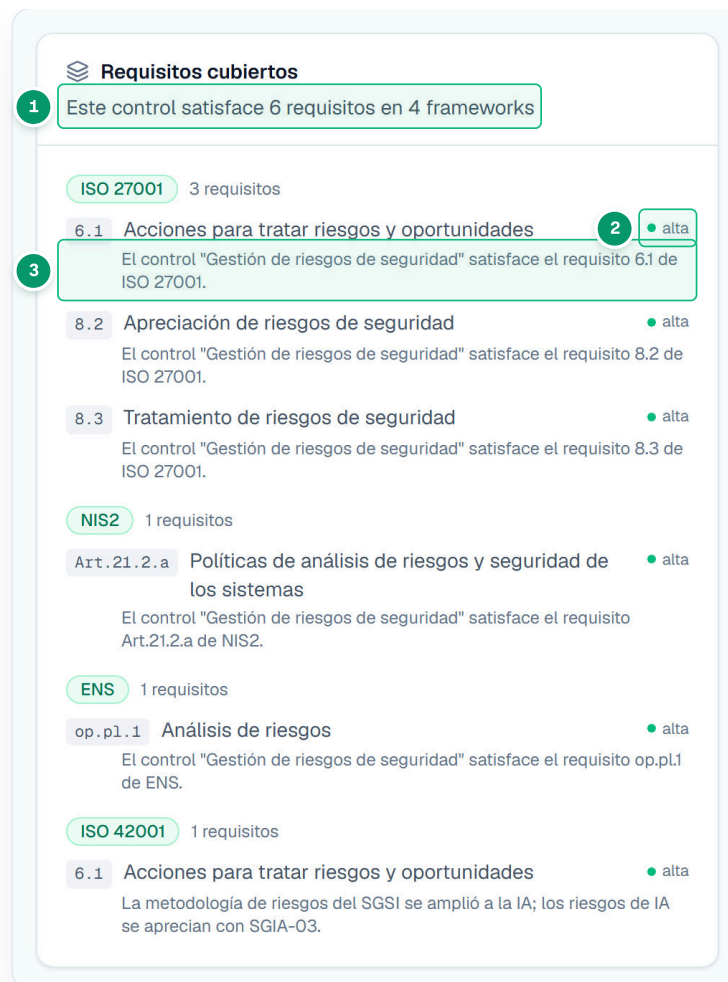


Figura 10. Qué requisitos cubre RSK-01.

- 1 Cuántos requisitos y marcos cubre el control.
- 2 Confianza de cada vínculo (alta, media o baja).
- 3 La referencia exacta del requisito y una nota del vínculo.

 Ojo

Marcar «implantado» para que suba el porcentaje no sirve: Salvik lo permite sin evidencia, un auditor no. Por eso un control implantado sin evidencia queda señalado como «Pendiente de evidencia».

Con IA (planes Pro y Auditado)

«Análisis de brecha con IA»: describe cómo lo haces hoy y la IA evalúa qué falta para cumplir el control.

Si un control tiene una atestación de auditoría vigente y lo cambias, queda «en deriva»: hay que volver a atestarlo, y el informe final que se apoyaba en esa atestación queda revocado.

CAPÍTULO 7 · LA IDEA CLAVE

Un control, cuatro normas

La razón de ser de Salvik, medida: cuánto trabajo reutilizas entre normas.

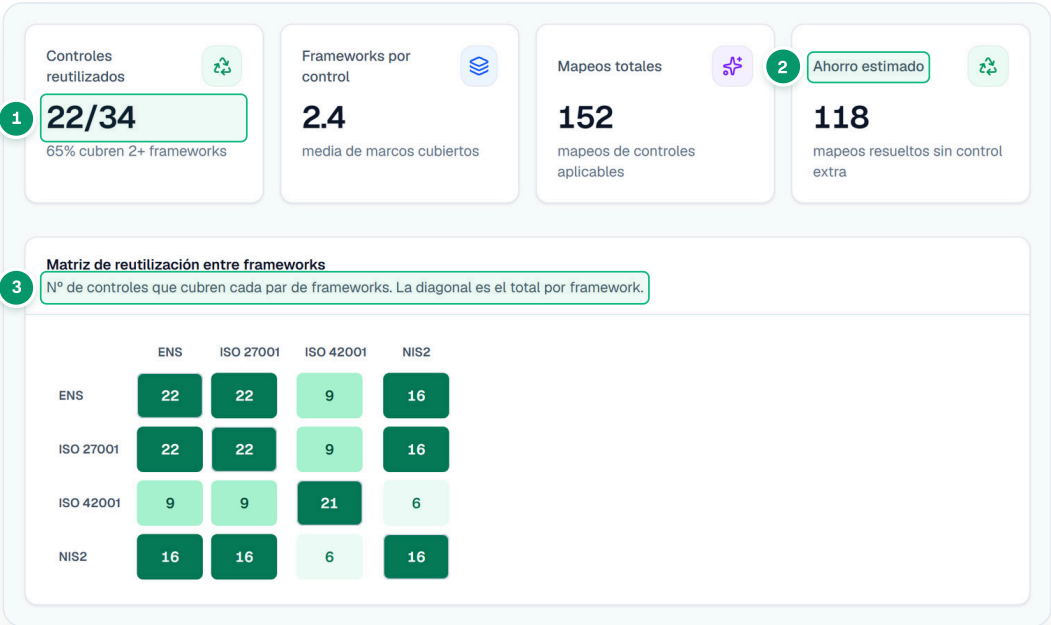


Figura 11. Cobertura cruzada de Empresa Demo S.L.

- 1** Controles reutilizados: 22 de 34 cubren dos o más marcos.
- 2** Ahorro estimado: vínculos con requisitos que el cruce cubre sin crear un control más.
- 3** Matriz: cuántos controles comparten cada par de marcos. La diagonal es el total de cada uno.

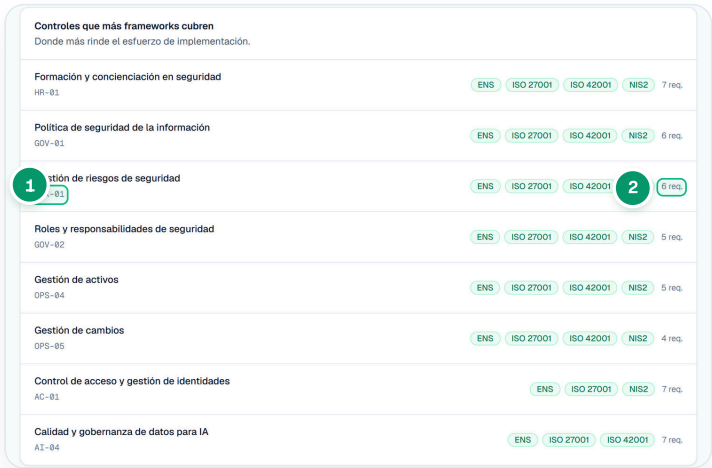


Figura 12. Los controles que más marcos cubren.

- 1** RSK-01 cubre los cuatro marcos.
- 2** Número de requisitos que cubre.



Qué ganas

Un ejemplo: RSK-01 cubre las cláusulas 6.1, 8.2 y 8.3 de ISO 27001, la 6.1 de ISO 42001, el artículo 21.2.a de NIS2 y la medida op.pl.1 del ENS. Lo implantas y lo evidencias una vez, y avanzas en las cuatro normas. En Empresa Demo, los 34 controles suman 152 vínculos con 138 requisitos: el cruce le ahorra crear un control para cada uno.



PARTE II · DÍA A DÍA

El sistema, vivo

Evidencias, avisos, riesgos, políticas, incidentes y cambios normativos.

-
- 08 Evidencias: la prueba de que cada control funciona
 - 09 Alertas y tareas: Salvik te dice qué toca
 - 10 Riesgos: la matriz y su tratamiento
 - 11 Políticas: redacta con IA, revisa y aprueba
 - 12 Incidentes: los plazos de NIS2, bajo control
 - 13 RegWatch: qué cambia en la normativa y a qué puede afectarte

Evidencias: la prueba de que cada control funciona

Cada control implantado necesita una prueba. Salvik la guarda, la vincula a sus controles y te avisa antes de que caduque.



Figura 13. Evidencias de Empresa Demo S.L.

- 1

«Añadir evidencia»: documento, captura, configuración, registro, política o enlace.
- 2

Controles a los que sirve: una misma evidencia vale para varios.
- 3

Fecha de caducidad, si la tiene.
- 4

«Exportar evidencias» a CSV.
- 1

Pulsa «Añadir evidencia» 1 y elige el tipo.
- 2

Sube el fichero (hasta 25 MB) o indica dónde está.
- 3

Vincúlala a los controles que demuestra 2.
- 4

Si la prueba tiene validez limitada —un certificado, un escaneo trimestral—, pon su fecha de caducidad 3: el centro de alertas te avisará antes.

Al subir un fichero, Salvik calcula su huella digital (SHA-256). Es lo que usa después la auditoría para dejar fijado exactamente qué se revisó. Borrar una evidencia exige un motivo, y queda constancia de quién, cuándo y por qué.

**Consejo**
Enlaza la prueba mínima. Si se cuela algo sensible, como datos personales que no hacen falta, bórralo desde Evidencias.

Alertas y tareas: Salvik te dice qué toca

No hace falta recordar qué vence ni qué falta: Salvik lo calcula a partir de lo que registras.



Figura 14. Centro de alertas.

- 1

Alertas por gravedad: críticas, avisos e informativas.
- 2

Un plazo de notificación NIS2 vencido.
- 3

Cada alerta lleva su acción para resolverla.
- 4

Un plazo que vence pronto: Salvik avisa antes, no solo cuando ya es tarde.

El centro de alertas vigila los plazos de notificación NIS2 (los próximos y los vencidos), los controles implantados sin evidencia, las evidencias caducadas o por caducar, los riesgos altos sin tratar, los sistemas de IA de alto riesgo en producción, los requisitos que ningún control cubre y los cambios normativos importantes.

Las tareas son las acciones para cerrar cada hueco: van ligadas a un control, con responsable, prioridad y vencimiento. Las que vencen aparecen también en el centro de alertas.



Figura 15. Tareas de remediación.

- 1

Control al que pertenece la tarea.
- 2

Responsable.
- 3

Vencimiento.

Riesgos: la matriz y su tratamiento

El registro de riesgos que piden ISO 27001, ISO 42001 y ENS, con su matriz y su plan de tratamiento.

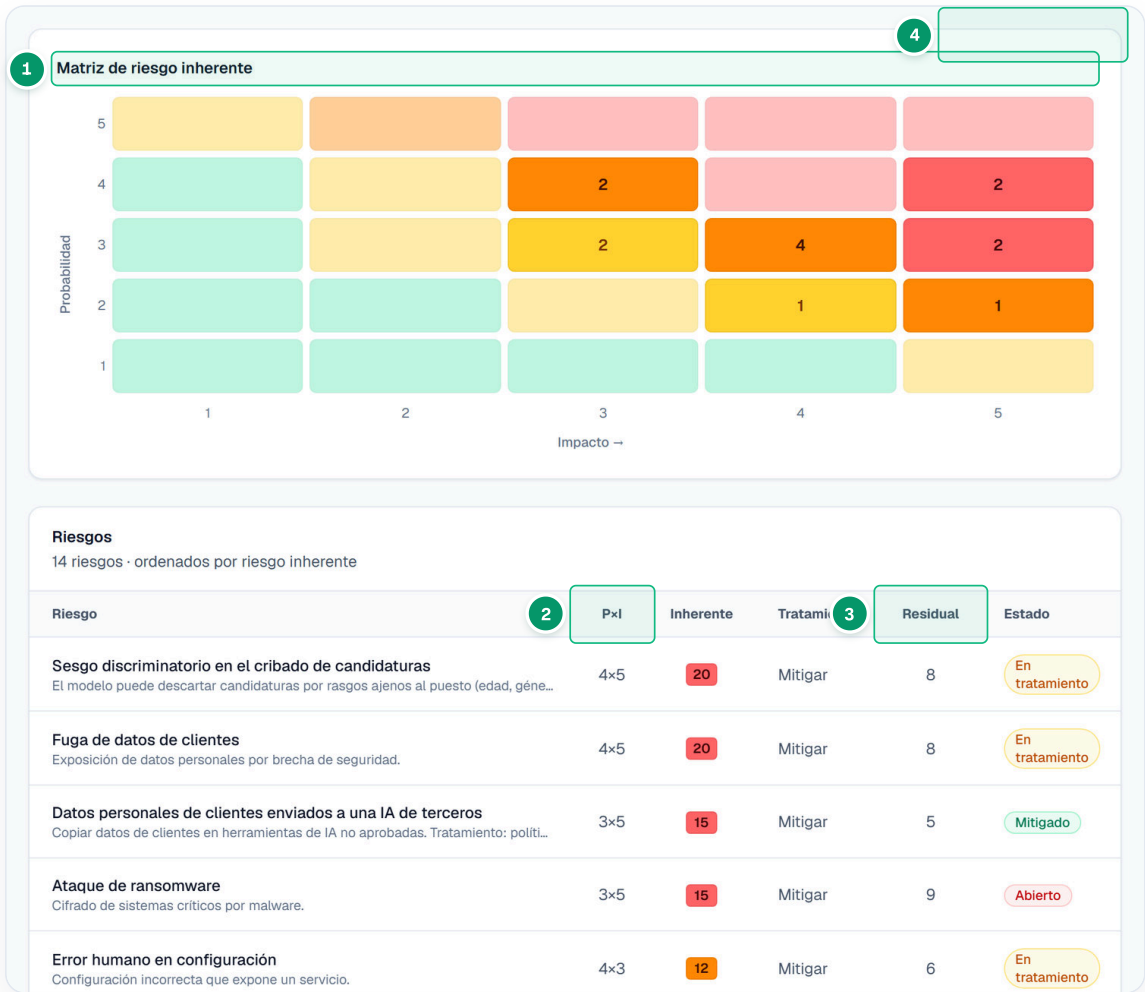


Figura 16. Registro de riesgos.

- 1 Matriz de riesgo inherente: probabilidad × impacto.
- 2 Probabilidad e impacto de cada riesgo.
- 3 Riesgo residual tras el tratamiento.
- 4 «Exportar riesgos» a CSV.

Cada riesgo tiene su valoración inherente, un tratamiento (mitigar, aceptar, transferir o evitar), su riesgo residual, un estado y un responsable. Los riesgos altos que siguen abiertos saltan al centro de alertas.

Políticas: redacta con IA, revisa y aprueba

Un borrador de política en segundos, que tu equipo revisa, aprueba y versiona.

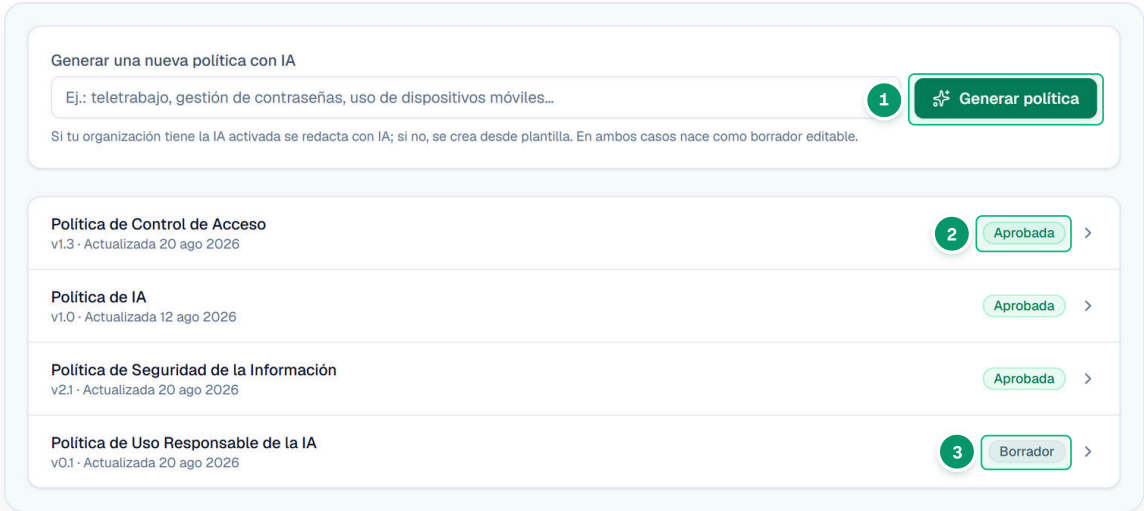


Figura 17. Políticas de Empresa Demo S.L.

- 1

«Generar política»: describe qué necesitas y la IA redacta el borrador.
- 2

Políticas aprobadas, con su versión y su fecha.
- 3

Borradores pendientes de revisión.



Figura 18. Una política aprobada.

- 1

Estado y versión.
- 2

Fechas de actualización y de aprobación.
- 3

Estructura: objeto, alcance, responsabilidades, directrices, cumplimiento y revisión.

Si la IA de tu organización está apagada, la política se crea desde una plantilla. En los dos casos nace como borrador editable: nada cuenta hasta que alguien de tu equipo la revisa y la aprueba. La redacción con IA está en los planes Pro y Auditado.

Incidentes: los plazos de NIS2, bajo control

Registra el incidente y Salvik calcula cada plazo de notificación de NIS2: la alerta temprana, la notificación y el informe final.



Figura 19. Incidentes, con su plazo NIS2 (captura del 27-sep-2026).

- 1 Lo que exige NIS2 (art. 23), siempre a la vista.
- 2 Un incidente reciente, con la notificación en plazo.
- 3 Un plazo vencido, en rojo.
- 4 «Registrar incidente».

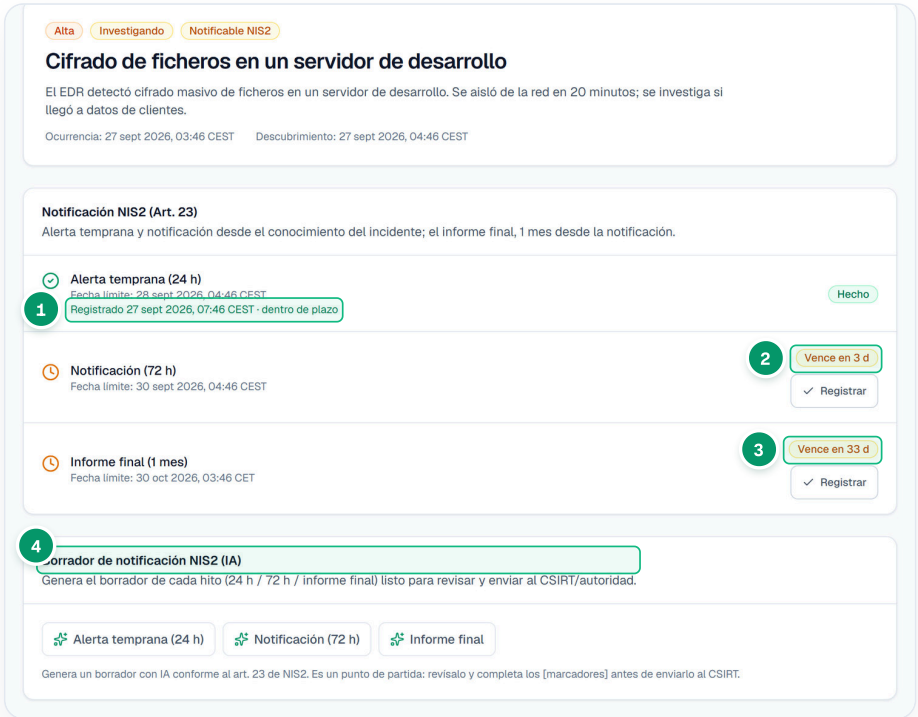


Figura 20. Un incidente notificable, con sus tres plazos.

- 1 Alerta temprana (24 h), registrada dentro de plazo.
- 2 Notificación (72 h): cuánto queda.
- 3 Informe final: un mes desde la notificación.
- 4 Borrador de cada notificación, redactado con IA y listo para revisar.

Las 24 h y las 72 h cuentan desde que se tiene conocimiento del incidente; el informe final, un mes desde la notificación. Cuando envías cada comunicación, la registras y queda la trazabilidad para el auditor. Salvik aplica los plazos del artículo 23 de la Directiva NIS2; en España, la ley que la transpone sigue en tramitación.

 **Con IA (planes Pro y Auditado)**
El borrador de notificación sigue el artículo 23 de NIS2 y deja entre corchetes lo que tienes que completar antes de enviarlo al CSIRT.

RegWatch: qué cambia en la normativa y a qué puede afectarte

Los cambios normativos que importan, los controles que podrían verse afectados y la acción recomendada.



Figura 21. Un cambio normativo: el «Ómnibus digital» del Reglamento de IA.

- 1** Posible impacto en tu organización.
- 2** Controles tuyos que podrían verse afectados.
- 3** Acción recomendada, en lenguaje claro.

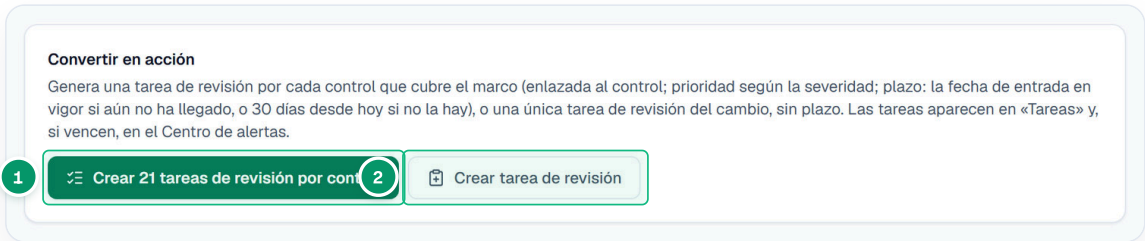


Figura 22. De la lectura a la acción.

- 1** Una tarea de revisión por cada control, con plazo.
- 2** O una única tarea de revisión del cambio.

RegWatch es un boletín curado a mano por Salvik a partir de fuentes oficiales. Salvik señala los controles que podrían verse afectados; qué tocar lo decides tú.



Según tu plan

RegWatch está en los planes Pro y Auditado.



PARTE III · INTELIGENCIA ARTIFICIAL

La IA, a la vista

Descubre la IA que ya se usa, gobiérnala y úsala con permiso.

-
- 14 Descubre la IA que ya se usa en tu empresa
 - 15 Inventario y gobierno de la IA
 - 16 Cuestionarios de seguridad de clientes, con IA

Descubre la IA que ya se usa en tu empresa

Antes de gobernar la IA hay que saber dónde está. Salvik la busca en exportaciones que ya tienes.

El Reglamento europeo de IA también afecta a quien usa IA, no solo a quien la fabrica: según el uso, por ejemplo, las obligaciones de transparencia del artículo 50 se aplican desde agosto de 2026. Y la ISO 42001 parte de saber qué sistemas de IA entran en el alcance. No puedes cumplir con lo que no sabes que existe.

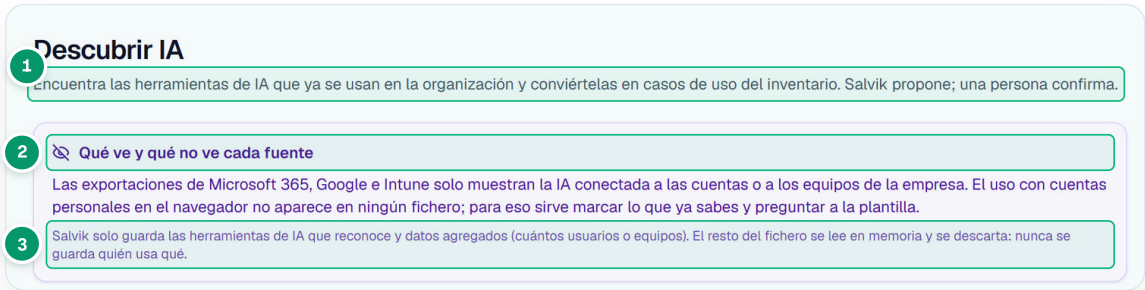


Figura 23. Descubrir IA.

- 1 Salvik propone; una persona confirma.
- 2 Qué ve cada fuente y qué no.
- 3 Privacidad: solo herramientas reconocidas y datos agregados; nunca quién usa qué.
- 1 Exporta tus datos: el script de Salvik para Microsoft 365 (solo lectura), una exportación de Entra ID, Google Workspace o Intune, o un extracto de gastos de la tarjeta de empresa.
- 2 Impórtalo en «Descubrir IA». Salvik reconoce las herramientas de un catálogo de 135 y descarta el resto del fichero.
- 3 Revisa cada candidata: confírmala, descártala con un motivo o déjala pendiente.
- 4 Da de alta cada uso confirmado como caso de uso del inventario (capítulo 15).

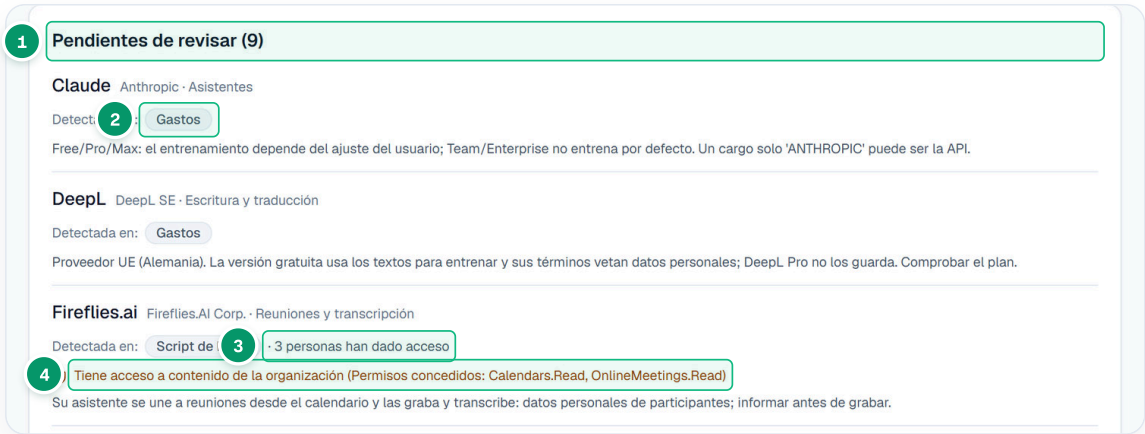


Figura 24. Herramientas detectadas, pendientes de revisar.

- 1 Herramientas pendientes de revisar.
- 2 Dónde se detectó; aquí, en el extracto de gastos.
- 3 Cuántas personas le han dado acceso con su cuenta de empresa.
- 4 Aviso cuando la herramienta puede leer contenido: calendario, reuniones...



Figura 25. Herramientas confirmadas.

- 1 Herramientas confirmadas por una persona.
- 2 Datos agregados de la detección.
- 3 Casos de uso del inventario ligados a la herramienta.



En la demo

En Empresa Demo, el script de Microsoft 365 y tres meses de gastos encontraron 12 herramientas, y el equipo declaró otras dos (Microsoft 365 Copilot y GitHub Copilot): de ChatGPT y la API de OpenAI a la IA que viene dentro de Slack, Notion o Miro, y dos transcritores de reuniones con acceso al calendario. Cuatro están confirmadas, una descartada y nueve esperan revisión.



Según tu plan

«Descubrir IA» está incluido en todos los planes, también en la prueba.

Inventario y gobierno de la IA

Cada uso de la IA, con su finalidad, su riesgo y su responsable. Y la IA de Salvik, con permiso y con rastro.

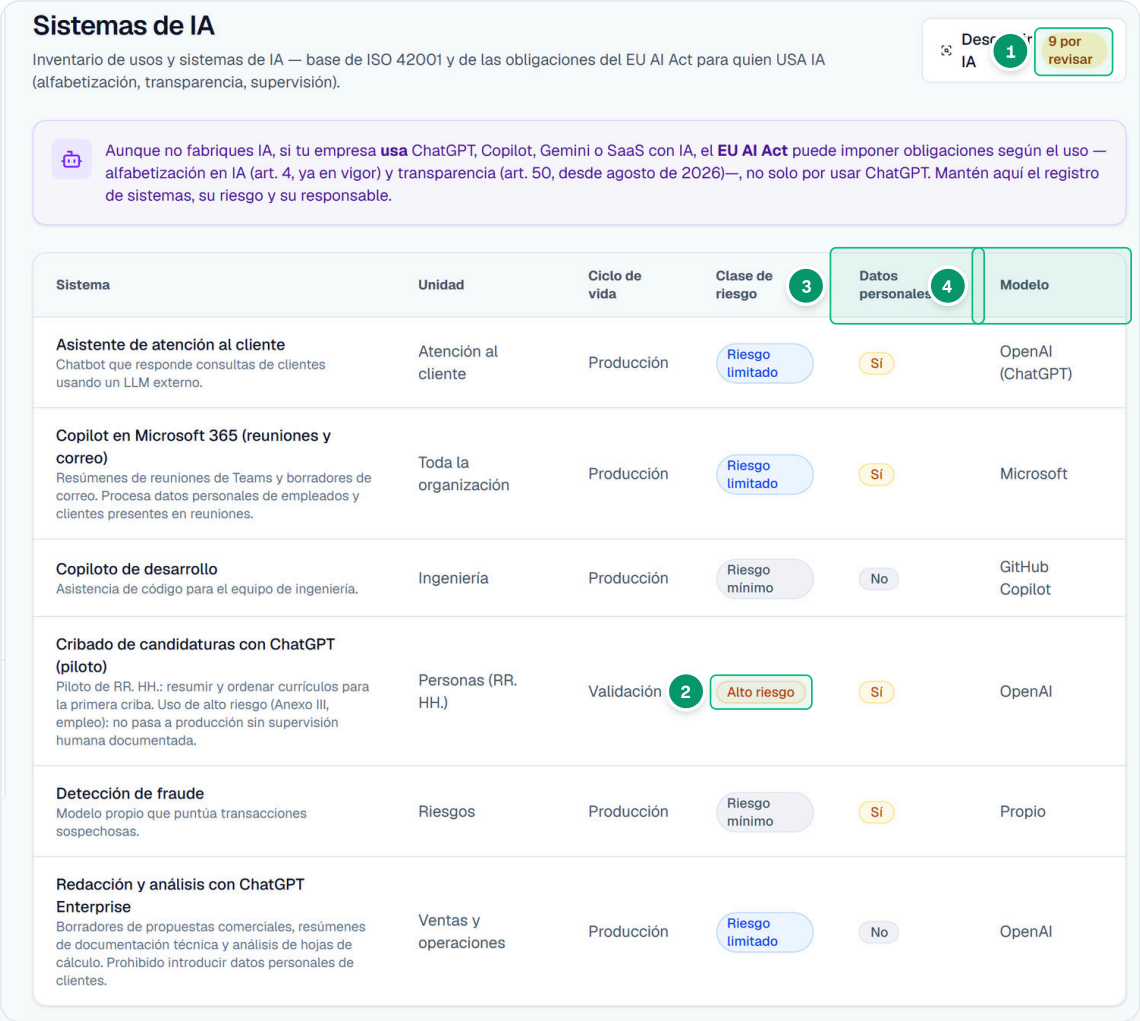


Figura 26. Inventario de sistemas de IA.

- 1

Acceso a «Descubrir IA», con las herramientas por revisar.
- 2

Clase de riesgo de cada sistema; aquí, un piloto de alto riesgo.
- 3

Si trata datos personales.
- 4

Modelo o proveedor.

Una fila por finalidad: usar ChatGPT para redactar ofertas y usarlo para cribar currículos son dos casos de uso con obligaciones distintas; el segundo es de alto riesgo según el Reglamento de IA, porque afecta al empleo.

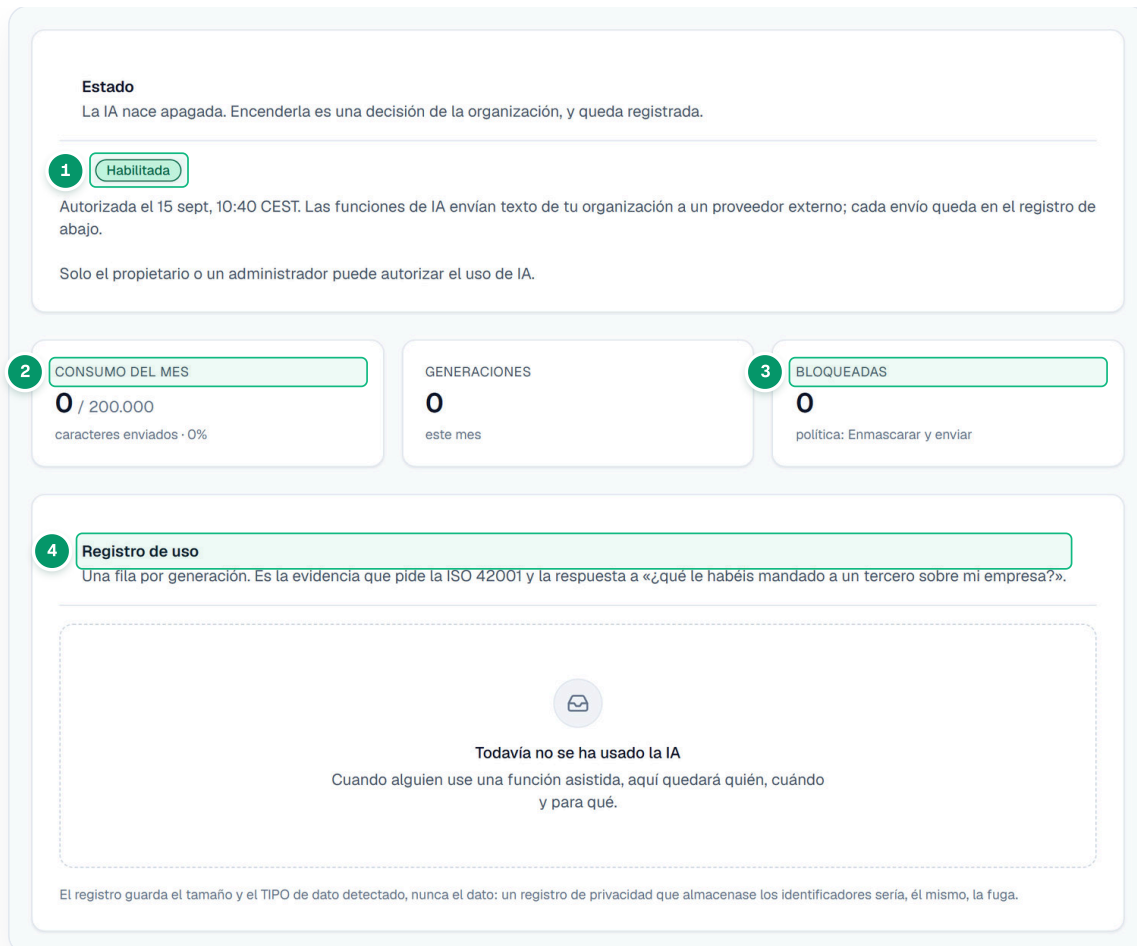


Figura 27. Gobierno de IA.

- | | |
|---|--|
| <p>1 La IA nace apagada; encenderla es una decisión que queda registrada.</p> | <p>2 Consumo del mes.</p> |
| <p>3 Envíos bloqueados por la política de datos sensibles.</p> | <p>4 Registro de uso: una fila por generación.</p> |

Tú eliges qué pasa si un texto lleva identificadores personales (correos, DNI o NIE, IBAN, teléfonos o tarjetas): bloquear el envío, que es lo que viene por defecto; sustituirlos por marcadores como [CORREO] o [DNI] antes de enviarlo, o enviarlo tal cual (no recomendado). No detecta nombres ni otros datos: revisa lo que pegas. El registro guarda el tamaño y el tipo de dato detectado, nunca el dato.



Qué ganas

Respondes con datos a la pregunta más incómoda que te puede hacer un auditor o un cliente: «¿Qué le habéis mandado a un tercero sobre mi empresa?».

CAPÍTULO 16 · INTELIGENCIA ARTIFICIAL

Cuestionarios de seguridad de clientes, con IA

Pega hasta 20 preguntas por tanda y Salvik redacta cada respuesta citando tus controles.

Pega las preguntas del cuestionario (una por línea)

1 ¿Cifráis los datos de clientes en reposo y en tránsito?
¿Exigís MFA para todos los accesos administrativos?
¿Cómo notificáis un incidente de seguridad que nos afecte?
¿Usáis IA con datos de clientes? ¿Con qué garantías?

2 **Responder cuestionario** 3 Modo IA activo: respuestas redactadas por IA que citan tus controles.

Figura 28. Cuestionarios de seguridad.

- 1 Las preguntas del cuestionario, una por línea (hasta 20 por tanda).
- 2 «Responder cuestionario».
- 3 Modo IA activo: respuestas redactadas por IA que citan tus controles.

Cada respuesta se apoya en los controles que tienes registrados e indica con qué confianza (alta, media o baja). Tú revisas cada respuesta antes de enviar nada: una persona siempre en el bucle.



Según tu plan

La redacción con IA, en los planes Pro y Auditado. En Base, las preguntas se emparejan con tus controles por palabras clave.

IV

PARTE IV · AUDITORÍA Y DIRECCIÓN

Cerrar el ciclo

Auditoría interna firmada, revisión por la dirección y Trust Center.

-
- 17 Auditoría interna firmada y verificable
 - 18 Revisión por la dirección
 - 19 Trust Center: tu postura de seguridad, a la vista

CAPÍTULO 17 · AUDITORÍA

Auditoría interna firmada y verificable

La revisión de controles para tu auditoría interna (cláusula 9.2): la IA propone borradores de hallazgos, un auditor certificado revisa y firma, y cualquiera puede verificar el informe.



Qué es y qué no es

Una revisión de los controles del alcance con la metodología de ISO 19011, firmada por un auditor competente e imparcial. No constituye por sí sola el programa de auditoría interna que exige la cláusula 9.2, ni es una certificación: esa la emite un organismo de certificación (acreditado, si quieres reconocimiento internacional).

- 1 La dirección aprueba el **programa** de auditoría interna (cláusula 9.2.2).
- 2 Se abre el **encargo**: alcance, marcos y declaración de imparcialidad. Quien implantó tus controles no puede auditarlos.
- 3 Trabajo de campo: Salvik congela la relación de evidencias de cada control, con la huella de cada fichero, y la IA puede proponer borradores de hallazgos.
- 4 El auditor revisa cada hallazgo y **atesta control a control**, con su firma.
- 5 Informe final con **sello de tiempo**. Solo sale como «final» si todo el alcance está atestado; si no, queda como borrador sin atestar.
- 6 Cualquiera lo **verifica** con su enlace: se recalculan la huella del informe y la de cada atestación con sus evidencias.



Figura 29. El encargo de ejemplo de Empresa Demo S.L.

- | | |
|--|---|
| 1 El encargo de auditoría interna de ISO 27001 (cl. 9.2). | 2 Cobertura atestada: 17 de 17 controles del alcance. |
| 3 Consola del auditor, donde se revisan hallazgos y se atesta. | 4 El informe final, firmado. |

Informe de auditoría interna

1Final

Encargo: EJEMPLO · Auditoría interna ISO/IEC 27001:2022 (cl. 9.2) · Empresa ficticia de demostración · Tipo: Auditoría interna (9.2) · Marcos: ISO27001

2Generado: 26 sept 2026, 20:06 CEST · Cobertura atestada: 17/17 (100%)

AUDITOR

Ana Martín (auditora ficticia · EJEMPLO)

Lead Auditor ISO/IEC 27001:2022 (ficticia) (verificada)Lead Auditor ISO/IEC 42001:2023 (ficticia) (verificada)

3DECLARACIÓN DE IMPARCIALIDAD

"Declaro que actúo con objetividad e imparcialidad (ISO 19011). El auditor declaró el 14-09-2026 no haber implantado, configurado ni asesorado los controles incluidos en el alcance, ni dentro ni fuera de esta plataforma. Esa declaración es suya y no la verifica el sistema. Divulgación: 17 de los 17 controles del alcance tenían, a fecha de esta firma, un código coincidente con el catálogo de plantillas de la plataforma. La plataforma aporta el enunciado del control; su implantación, su configuración y su evidencia son del cliente, y es sobre eso sobre lo que se audita." — 26 sept 2026, 20:06 CEST

CONTROLES Y ATESTACIONES

4Observación

5AC-01 — Control de acceso y gestión de identidades

"La gestión de identidades y el principio de mínimo privilegio están implantados. Observación: falta la revisión de derechos de acceso del último trimestre y la política no fija su frecuencia; conviene fijarla y retomar la revisión trimestral (A.5.18)."

Atestado: 26 sept 2026, 20:06 CEST · Válida hasta: 26 sept 2027, 20:06 CEST

root: 418d4e348893b4094d8c0e81d7ef9cab...

Observación: Revisión de derechos de acceso sin evidencia del último trimestre — La última revisión de derechos de acceso documentada es la del 1.er trimestre de 2026 (acta de abril). No consta ninguna revisión posterior ni el motivo de su omisión. La Política de Control de Acceso (v1.3) exige revisiones periódicas sin fijar su frecuencia, y la práctica de la organización es trimestral.

Conforme

AC-02 — Autenticación multifactor (MFA)

"Comprobada en el proveedor de identidad la política que exige MFA a todos los usuarios, sin exclusiones, y verificada en una muestra de 10 inicios de sesión de administradores del último mes. Cumple A.8.5."

Atestado: 26 sept 2026, 20:06 CEST · Válida hasta: 26 sept 2027, 20:06 CEST

root: 426fe1e12114baafd2be97d650e97c2d...

Figura 30. El informe de auditoría interna.

1

Estado del informe: final.

2

Cobertura atestada del alcance.

3

Declaración de imparcialidad del auditor.

4

Conclusión de cada control; aquí, una observación.

5

Fecha de la atestación y hasta cuándo vale.

TIPO	CONTROL	HALLAZGO DEL EJEMPLO
No conformidad menor	OPS-02	Vulnerabilidades críticas fuera del plazo de corrección definido
Observación	AC-01	Revisión de derechos de acceso sin evidencia del último trimestre
Observación	BC-01	Pruebas de restauración sin periodicidad definida
Observación	HR-01	Seguimiento incompleto de la formación anual
Observación	DEV-01	Desarrollo seguro solo en el repositorio principal
Oportunidad de mejora	OPS-03	Centralizar registros y alertar sobre eventos de autenticación
Oportunidad de mejora	RSK-01	Vincular cada riesgo con los controles que lo tratan
Conforme	10 controles	Cada uno con su conclusión y la evidencia revisada

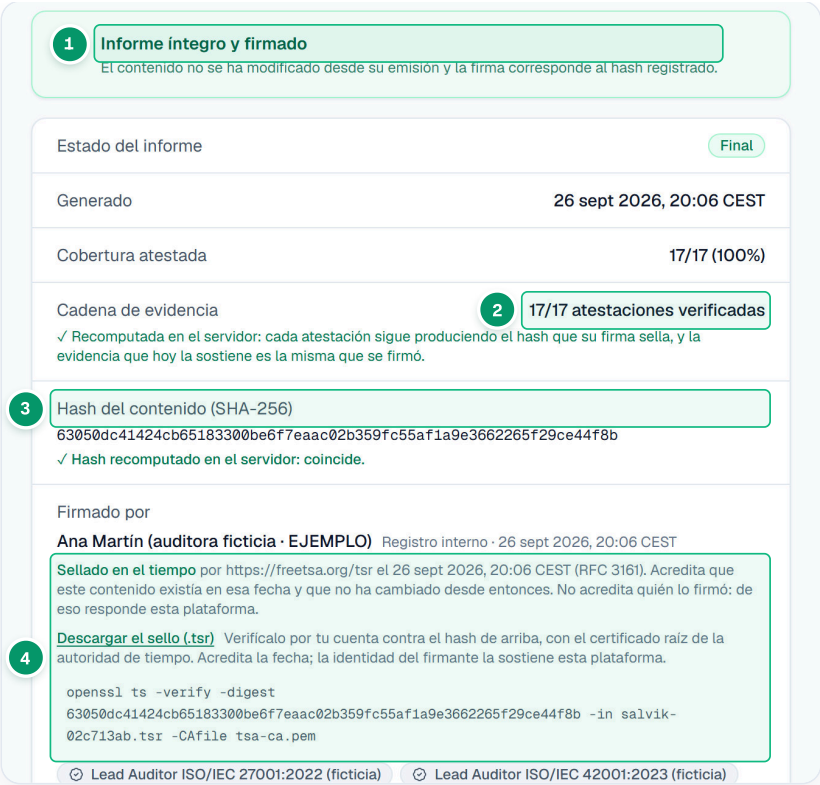


Figura 31. La verificación pública del informe.

- 1** Resultado: informe integro y firmado.

3 Huella (hash) del contenido del informe.
- 2** Cadena de evidencia: cada atestación se recalcula en el servidor.

4 Sello de tiempo RFC 3161 de una autoridad externa, descargable.



En la demo

La auditoría de Empresa Demo es un EJEMPLO sobre una empresa ficticia, firmado por una auditora ficticia. En tu organización la firma un Lead Auditor certificado.



Según tu plan

Plan Auditado: dos marcos al año, incluidos. También se contrata suelta: **2.200 € + IVA** por ciclo de dos marcos y **900 € + IVA** por marco adicional.

Revisión por la dirección

La reunión que cierra el ciclo (cláusula 9.3), con los datos de entrada ya preparados.

Al convocarla, Salvik reúne y congela los datos de entrada: estado de las acciones, resultados de la auditoría interna, incidentes, riesgos, cambios normativos y avance de cada marco. La dirección completa lo demás, registra sus decisiones y los cambios en el sistema de gestión, y cierra el acta.

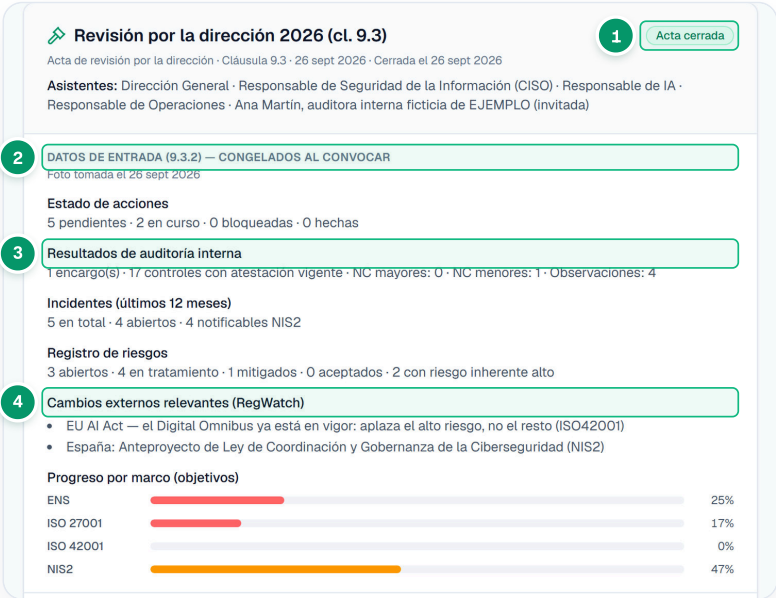


Figura 32. Acta de la revisión por la dirección: los datos de entrada.

- 1

Acta cerrada: información documentada.
- 2

Datos de entrada que reúne Salvik (9.3.2), congelados al convocar.
- 3

Resultados de la auditoría interna.
- 4

Cambios normativos relevantes, desde RegWatch.

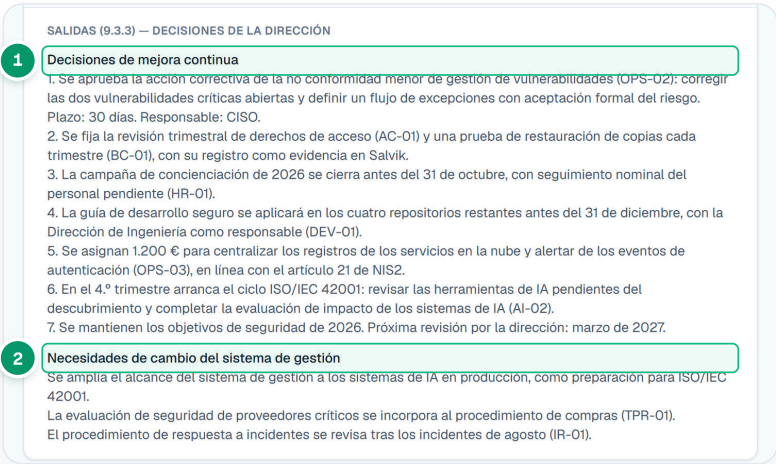


Figura 33. Las salidas: decisiones de la dirección.

- 1

Decisiones de mejora continua (9.3.3).
- 2

Cambios necesarios en el sistema de gestión.



Qué ganas

Junto con la auditoría interna, el acta cerrada es lo que pide el organismo de certificación antes de la fase 1. Y la preparas en una reunión, no en una semana.



En la demo

El acta es un EJEMPLO de la empresa ficticia; la auditora invitada también es ficticia. Planes Pro y Auditado.

Trust Center: tu postura de seguridad, a la vista

Una página pública —el Centro de Confianza— para que tus clientes comprueben tu estado sin pedírtelo por correo.

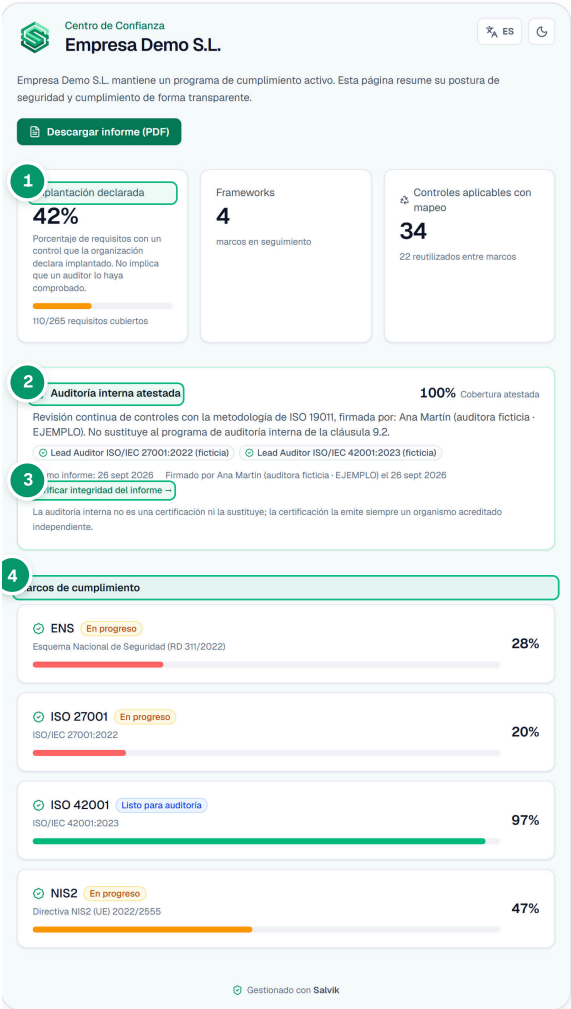


Figura 34. El Centro de Confianza público de Empresa Demo S.L.

- 1 Tus clientes ven la implantación declarada **1**, con la aclaración de que no implica que un auditor lo haya comprobado.
- 2 Si tienes un informe final de auditoría interna firmado, ven su sello **2** y pueden verificarlo ellos mismos **3**.
- 3 Ven también tus marcos y su avance **4**, y pueden abrir un informe imprimible.
- 4 Compártelo en tus propuestas y en tu web: es un enlace, no un documento que caduca.

Estado

El Trust Center nace cerrado. Publicarlo es una decisión tuya.

1

Publicado

Es accesible para cualquiera que tenga el enlace. Publicado el 20 ago 2026.

2

ENLACE PÚBLICO

https://salvik.eu/trust/demo

Verlo como lo ve un cliente →

Solo el propietario o un administrador puede cambiar esto.

Qué se publica

Y, sobre todo, qué no.

3

Se publica

· Nombre de la organización y sector

· Marcos adoptados y su estado

· Porcentaje de requisitos cubiertos

· Número de controles

· El sello de auditoría, si hay informe final firmado

4

No se publica

· Evidencias ni documentos

· Controles concretos ni su detalle

· Hallazgos, no conformidades ni riesgos

· Incidentes

· Personas del equipo

Figura 35. Qué se publica y qué no.

1

Nace cerrado: publicarlo es una decisión tuya.

2

El enlace público para compartir.

3

Lo que se publica...

4

...y, sobre todo, lo que no.

Se publica el nombre y el sector, los marcos y su estado, el porcentaje de requisitos cubiertos, el número de controles y el sello de auditoría si hay informe final firmado. No se publican evidencias, controles concretos, hallazgos, riesgos, incidentes ni personas del equipo.

Según tu plan

Planes Pro y Auditado.

salvik.eu

33



PARTE V · ORGANIZACIÓN

Tu equipo y tus datos

Roles, invitaciones y dónde vive cada dato.

20 Equipo, roles y tus datos

Equipo, roles y tus datos

Invita a tu equipo con el rol justo y conoce en todo momento dónde están tus datos.

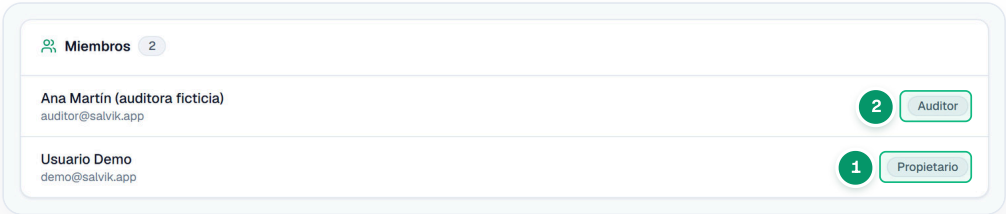


Figura 36. Miembros de la organización.

- 1 Propietario de la organización.
- 2 Auditor: hace la auditoría y no puede tocar tus controles ni tus evidencias.

Hay cinco roles: propietario, administrador, miembro, auditor y solo lectura. Cada invitación es un enlace propio, de un solo uso. El plan Base incluye un usuario (tres durante la prueba); Pro, diez; Auditado, ilimitados.

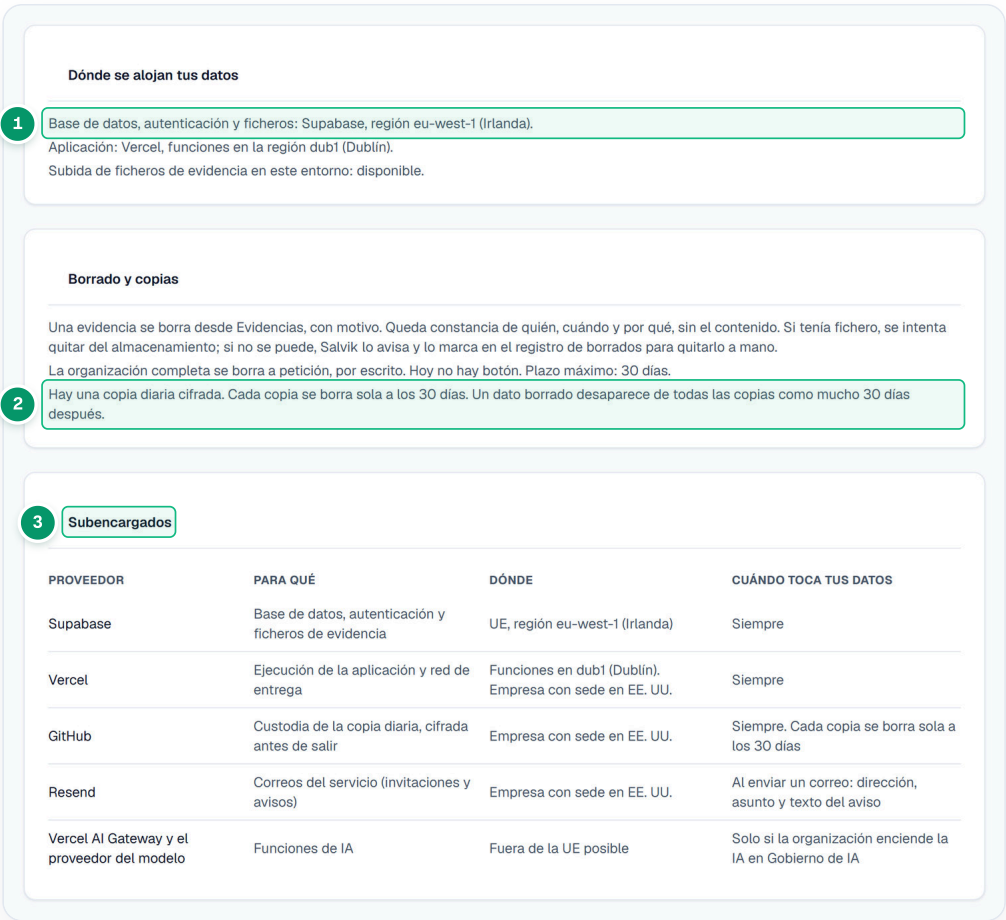


Figura 37. Datos y privacidad.

- 1 Base de datos, autenticación y ficheros, en la UE (Irlanda).
- 2 Copia diaria cifrada, que se borra sola a los 30 días.
- 3 Subencargados: quién toca tus datos, para qué y dónde.

Tus datos son tuyos: exporta a CSV los controles, riesgos, evidencias e incidentes, y la SoA de cada marco, cuando quieras.

✓ **Por defecto, cerrado**
La IA y el Trust Center vienen apagados: nada sale hacia un proveedor de IA ni se publica sin que alguien con permiso lo decida.

PARA EMPEZAR

Tu primera semana con Salvik

Un plan realista para pasar de cero a un sistema en marcha durante la prueba de 7 días.

CUÁNDO	QUÉ HACES	TIEMPO
Día 1	Crea la cuenta, elige tu ruta y tu primer marco. Invita a tu equipo.	30 min
Día 2	Decide el alcance y genera la SoA inicial con el asistente.	De 15 min a 2 h
Día 3	Decide tus controles: estado, aplicabilidad y responsable.	2-3 h
Día 4	Vincula una evidencia a cada control implantado.	1-2 h
Día 5	Asigna responsables y tareas, descarga la SoA y haz la primera revisión.	1-2 h
Después	Riesgos, políticas y «Descubrir IA». Con Pro o Auditado, también la IA y el Trust Center.	A tu ritmo



¿Prefieres ir acompañado?

Con la «Puesta en marcha desde cero» dejamos tu Salvik montado y a tu equipo formado en una sesión de trabajo (499 € + IVA).

PLANES

Planes y precios

Precios por organización, sin IVA. Base y Pro, al mes o al año y sin permanencia; Auditado, solo anual.

	BASE	PRO	AUDITADO
Precio	95 €/mes o 950 €/año	245 €/mes o 2.450 €/año	4.650 €/año solo anual
Marcos	1	Los 4	Los 4
Usuarios	1	10	Ilimitados
Controles, evidencias, riesgos, incidentes y alertas	✓	✓	✓
Descubrir IA e inventario de IA	✓	✓	✓
IA, RegWatch, Trust Center y revisión por la dirección	—	✓	✓
Auditoría interna firmada	Aparte	Aparte	2 marcos al año, incluida

Servicios

Puesta en marcha desde cero

Una sesión de trabajo para dejar Salvik montado y a tu equipo formado.

499 € + IVA · pago único

Auditoría interna firmada, suelta

Un ciclo de revisión de controles de dos marcos, firmado por un Lead Auditor certificado, para tu auditoría interna.

2.200 € + IVA · marco adicional, 900 € + IVA

Prueba gratuita: 7 días con el plan Base, sin tarjeta. Salvik no certifica: la certificación la emite un organismo de certificación. La auditoría interna firmada es una revisión de controles con la metodología de ISO 19011 para tu programa de auditoría interna (cláusula 9.2 de ISO 27001 e ISO 42001).

Empieza hoy



Mira la demo

salvik.eu/panel

Empresa Demo S.L., sin registrarte.



Pruébalo

salvik.eu

7 días gratis, sin tarjeta.



Hablemos

info@salvik.eu

Te respondemos personalmente.



Escanea para abrir la demo