sealpath
Smart Protection for Sensitive Data

ESTUDIO ESPECIALIZADO · PRIMERA EDICIÓN

Estado de la protección del dato 2026

Radiografía del control de la información, la colaboración y la exposición a IA



Qué controlan hoy las organizaciones sobre su información sensible y qué cambia con la IA.

Prólogo de Luis Ángel del Valle, CEO de SealPath

Cuando planteamos este estudio nos hicimos una pregunta sencilla: ¿cómo protegen hoy las organizaciones su información sensible, ahora que la IA generativa ha entrado en su día a día? Se lo preguntamos a CISOs y responsables de seguridad y sistemas de varios países. Gracias a todos: este informe es suyo antes que nuestro.

La fotografía tiene luces y sombras. Las organizaciones han avanzado mucho en el control del acceso: la gran mayoría aplica mínimo privilegio y retira el acceso a quien se marcha. Pero ese control pierde fuerza cuando la información sale del lugar donde se creó: cuando se comparte con un tercero, cuando un empleado se va con lo que manejaba o cuando alguien la introduce en una herramienta de IA. Casi la mitad de los participantes confirma que esto último ya ha ocurrido, y siete de cada diez organizaciones con política de uso de IA no la respaldan con un bloqueo técnico.

A esto se suman dos fuerzas que marcarán los próximos años: una presión regulatoria que ya no se limita a ISO 27001 y al RGPD, con NIS2 en primer plano, y una exigencia creciente de soberanía sobre dónde se guarda y se procesa la información, también cuando la procesa una IA.

Hemos intentado devolver algo útil: una fotografía honesta de dónde está el sector, con los límites de los datos a la vista y sin hablar de productos. No hay una respuesta única; cada organización parte de un sitio distinto. Os invitamos a leer estos resultados como un espejo: comparar vuestra situación con la del conjunto, ver dónde estáis más expuestos y decidir por dónde empezar.



Luis Ángel del Valle

CEO de SealPath

Índice

1. **Prólogo** 2

2. **Resumen ejecutivo** 4

3. **El dato y su control** 5

   Capacidades y madurez 7

   Tecnologías y cobertura 10

4. **El dato fuera de la organización** 11

   Exposición e incidentes 13

5. **IA y exposición** 15

6. **Gobierno y barreras** 18

7. **Conclusiones y agenda del CISO** 20

8. **Participantes y metodología** 22

9. **Anexos y glosario** 24

10. **Enfoque SealPath** 27

Cinco ideas para llevarse del informe

Patrón común: los controles están pensados para el lugar donde se guarda la información, no para los lugares a los que viaja (un tercero, un empleado que se marcha, una herramienta de IA).

36%

Cambia permisos tras el envío

Se controla el acceso, no el documento

El 85% aplica mínimo privilegio, pero solo el 14% sabe dónde están sus copias. Y ocho de cada diez se declaran en madurez gestionada o superior. (P11, P13)

La información sensible ya llega a la IA

El 48% lo confirma. El 78% tiene política de uso, pero solo el 26% aplica bloqueo técnico y el 15% confía en que se cumpla. (P4, P5)

Tener tecnología no es estar cubierto

El 91% tiene alguna tecnología desplegada, pero solo el 42% la considera eficaz y el 59% admite que no frena, o solo en parte, la fuga hacia la IA. (P9)

Terceros, bajas y agentes: puntos ciegos

El 46% puede revocar lo compartido con terceros. El 48% no sabe con certeza qué se lleva quien se marcha. (P10, P12)

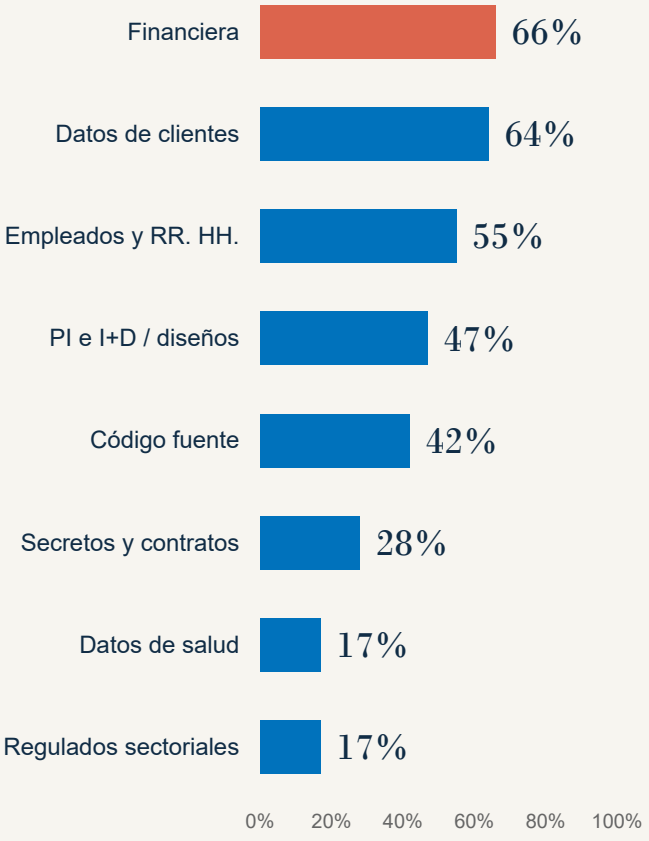
La soberanía ya es criterio de compra

El 83% la considera importante u obligatoria y el 72% la exige también a la IA que procesa datos sensibles. (P14)

2 de cada 3 organizaciones guardan su información más valiosa en local

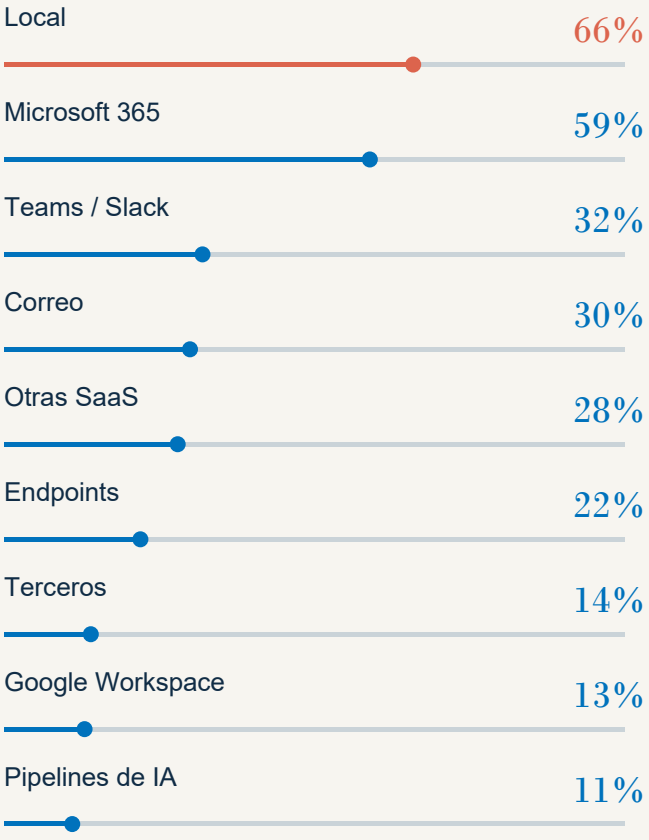
Información financiera (66%) y datos de clientes (64%) encabezan lo que se considera más valioso; PII (Información Personal Identificable) e I+D (47%) y código fuente (42%) completan el núcleo. Esa información reside a la vez en local (66%), Microsoft 365 (59%), herramientas de colaboración (32%) y correo (30%).

Tipos de información



Selección múltiple: se podían marcar varias opciones; los porcentajes no suman 100%.

Dónde reside



Selección múltiple: se podían marcar varias opciones; los porcentajes no suman 100%.

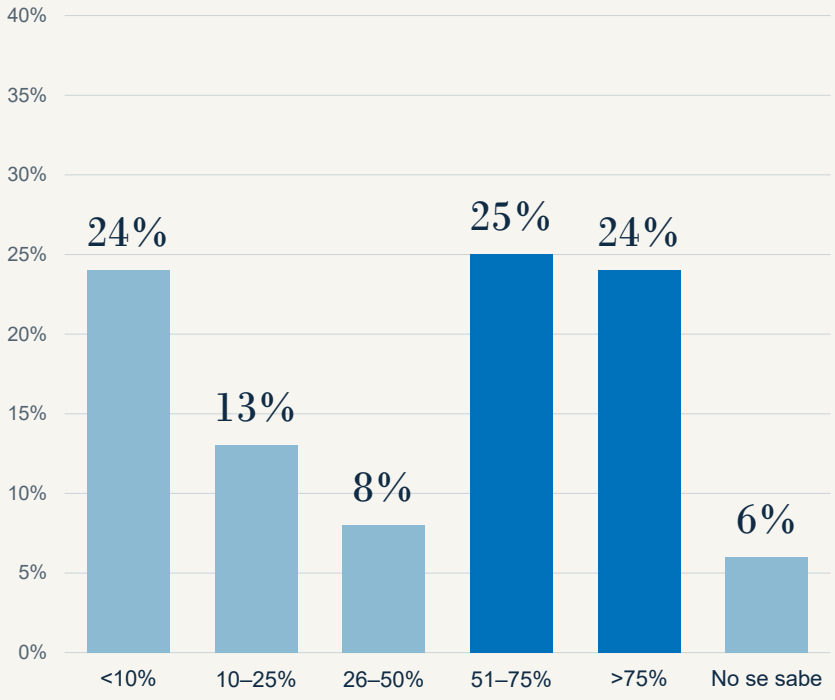
Un patrón a tener en cuenta

Quienes señalan la PI, la I+D o el código fuente como su información más valiosa declaran más capacidades de control que el resto (página 09).

1 de cada 4 organizaciones apenas ha clasificado su información sensible

La cobertura está polarizada: el 24% ha clasificado menos del 10% de su información sensible y otro 24%, más del 75%. El método mixto es el más citado (40%) y solo el 18% clasifica con herramienta automática.

Porción de información clasificada



Porcentajes aproximados.

Clasificar ayuda a ver

Entre quienes tienen clasificada más de la mitad de su información sensible, la exposición confirmada a la IA es más frecuente (en torno al 50%, frente al 40% del resto).

Una posible explicación: quien clasifica más también detecta mejor lo que llega a la IA.

Método empleado

Mixto	**40%**
Manual	**31%**
Automático	**18%**
No clasificamos	**11%**

Qué conviene comprobar

Elegir un archivo sensible y revisar su etiqueta, el criterio utilizado y el control que activa. Repetir la prueba después de descargarlo ayuda a comprobar hasta dónde llega la política.

P11 · Sobre un documento sensible (dentro o fuera de la organización), ¿qué capacidades de protección y control puede ejercer hoy?

Solo el 36% de los participantes puede cambiar permisos tras enviar

El 85% declara mínimo privilegio y el 72% auditoría de accesos. Las capacidades que acompañan al documento una vez descargado o enviado son minoritarias: cambiar permisos (36%), protección persistente (21%) y saber dónde están las copias (14%).

Mínimo privilegio



85%

Auditoría general



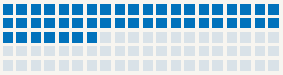
72%

Revocación



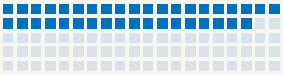
69%

Caducidad



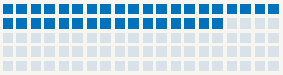
47%

Bloquear copia / impresión



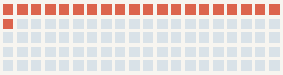
38%

Cambiar permisos



36%

Protección persistente



21%

Localizar las copias

14%

Ninguna

6%

No lo sabemos

6%

Cada cuadrado representa aproximadamente un punto porcentual.

Selección múltiple: se podían marcar varias opciones; los porcentajes no suman 100%.

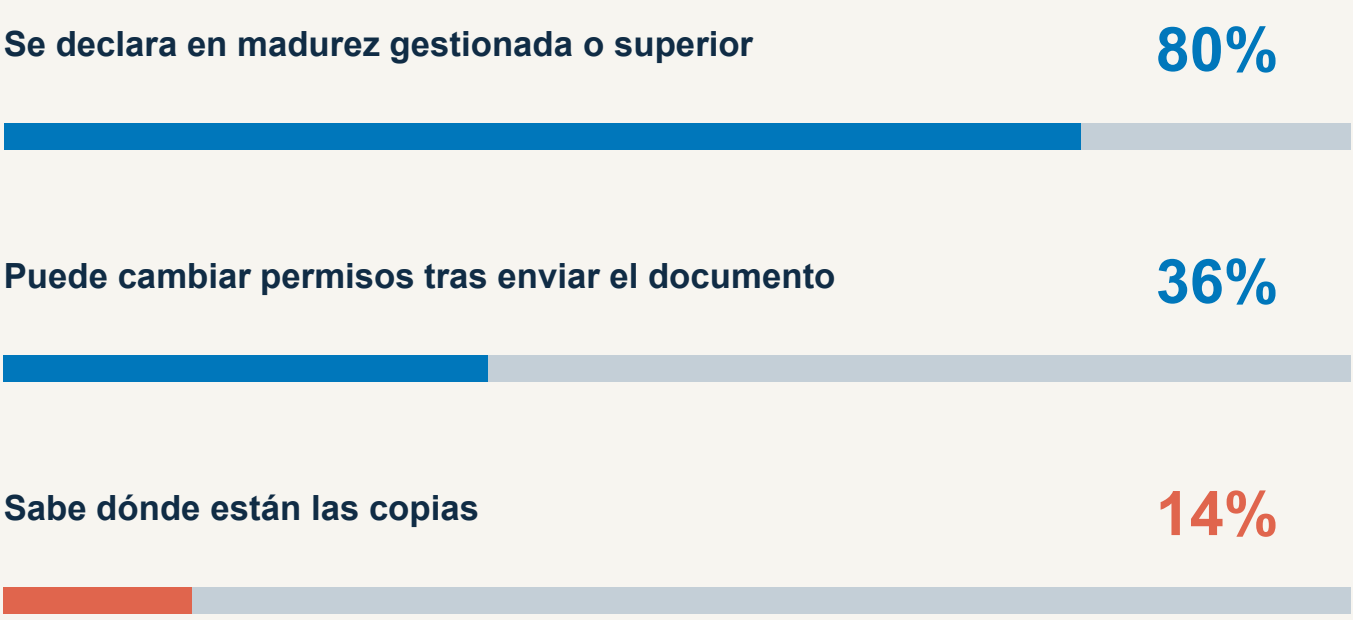
El acceso está controlado, pero los documentos, incluso menos aún

El 69% declara poder revocar accesos, pero solo el 36% puede cambiar permisos sobre un documento ya enviado. Definición de cada control en el glosario (página 26).

8 de cada 10 participantes consideran que su organización tiene una madurez alta en protección del dato

El 50% se sitúa en madurez gestionada, el 20% en avanzada y el 10% en optimizada; el 20% restante, en niveles inicial o básico. Sin embargo, solo el 36% puede cambiar permisos sobre un documento ya enviado y el 14% sabe dónde están sus copias.

Madurez declarada frente a capacidades sobre el documento



El grupo más maduro tampoco escapa

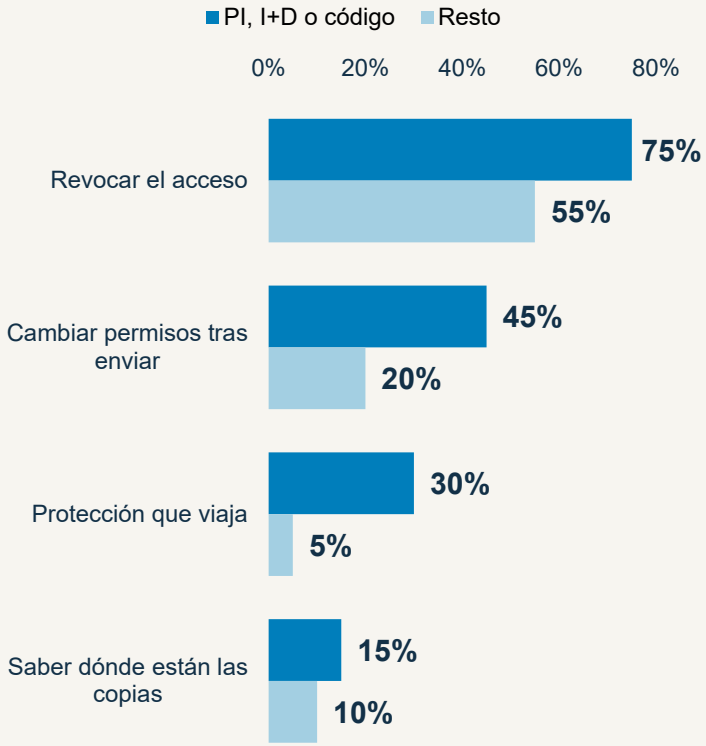
Entre quienes se declaran avanzados u optimizados, cambiar permisos tras el envío es más habitual (en torno al 55%, frente al 25% del resto), pero saber dónde están las copias sigue siendo excepcional.

Capacidades autodeclaradas. El grupo avanzado u optimizado es reducido: lectura orientativa.

Quien custodia PII y código tiene más control, pero no sobre el documento

La hipótesis de que la información más valiosa estaría peor controlada no se confirma. Quienes señalan la PI, la I+D o el código fuente como su información más valiosa declaran más capacidades de control, aunque la protección que acompaña al documento sigue siendo minoritaria.

Capacidades de control según lo más valioso



Una posible lectura

Quien identifica su PI y su código como lo más valioso parece invertir más en controlarlo.

Aun así, la protección que acompaña al documento sigue siendo minoritaria también en este grupo (en torno al 30%).

Base: quienes marcan PI, I+D o código fuente entre su información más valiosa, frente al resto.

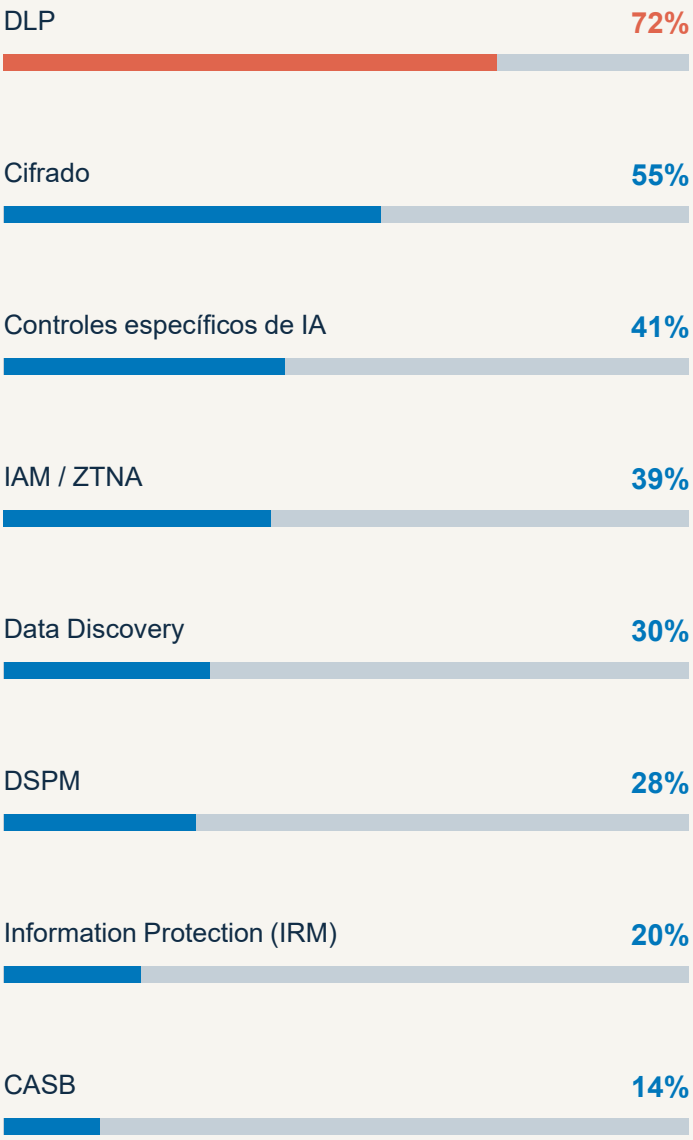
Qué se considera más valioso

Financiera (66%) y datos de clientes (64%) encabezan; PI e I+D (47%) y código fuente (42%) completan el núcleo.

El 91% de las organizaciones tiene tecnología; solo el 42% la ve eficaz

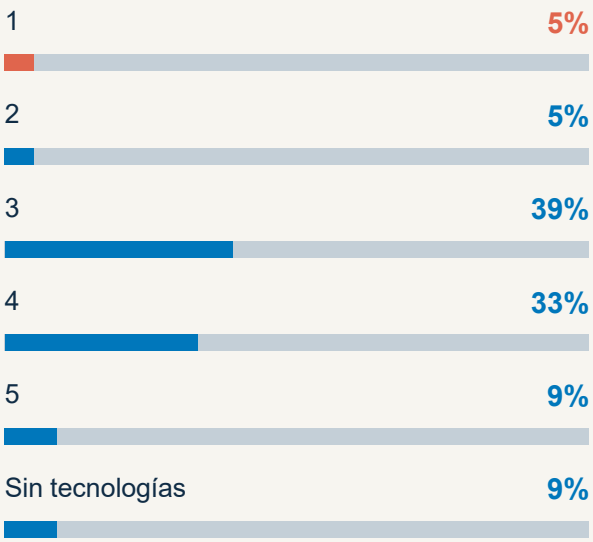
El 91% tiene al menos una tecnología de protección, con DLP (72%) y cifrado (55%) a la cabeza. Solo el 42% valora el conjunto como bastante o muy eficaz (4–5), y el 59% admite que no frena, o solo en parte, la fuga de información hacia la IA.

Tecnologías declaradas

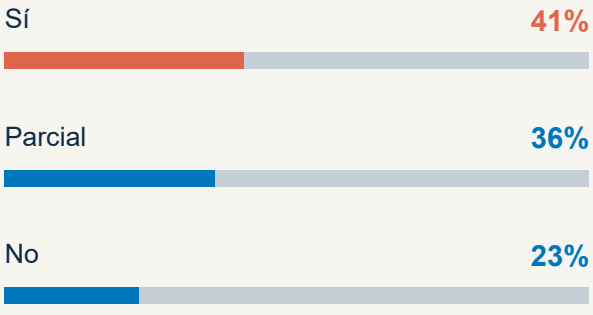


Eficacia global (1–5)

1: menor eficacia percibida · 5: mayor



¿Frena la fuga hacia IA?



Selección múltiple: se podían marcar varias opciones; los porcentajes no suman 100%.

Porcentajes aproximados.

El 72% de las organizaciones comparte información sensible con terceros, menos del 50% puede revocar accesos

El 72% comparte información sensible con terceros al menos ocasionalmente. El cifrado (68%) y los permisos por usuario (62%) son los controles más citados; revocar el acceso (46%) y auditar el acceso del tercero (32%), bastante menos.

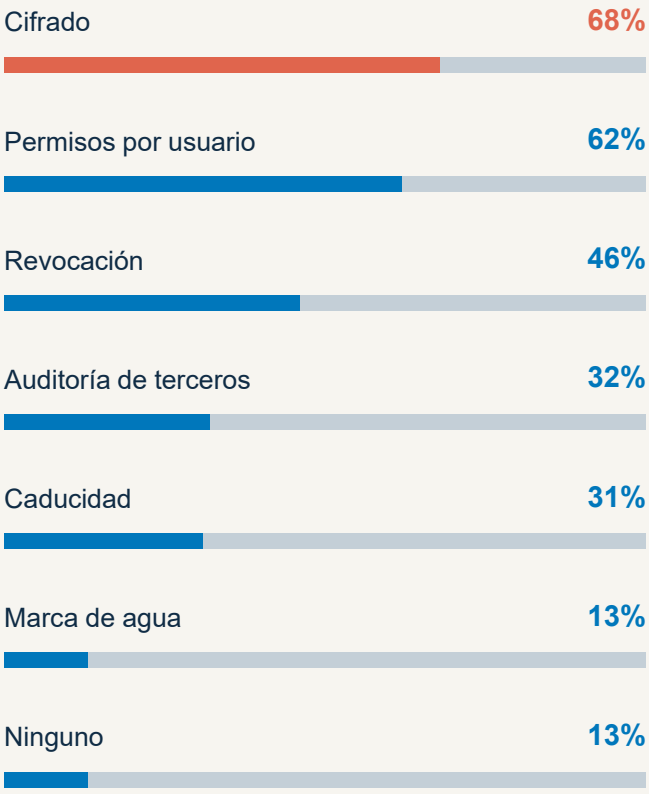


Frecuencia de colaboración

Muy frecuentemente	15%
Frecuentemente	17%
Ocasionalmente	40%
Raramente	18%
Nunca	10%

Porcentajes aproximados.

Control conservado



Selección múltiple: se podían marcar varias opciones; los porcentajes no suman 100%.

Terceros y NIS2

NIS2 exige gestionar el riesgo de la cadena de suministro. Revocar y auditar el acceso de terceros a lo compartido forma parte de esa gestión.

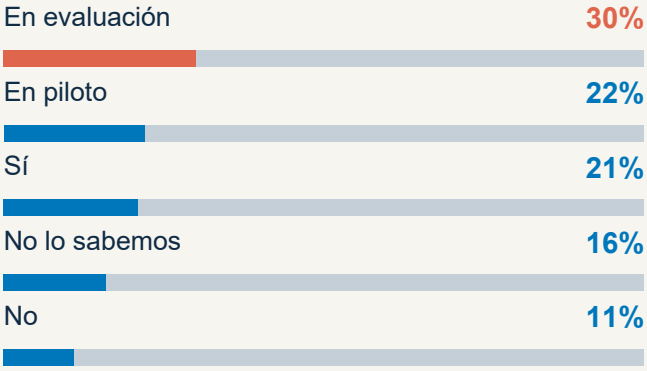
El 48% de los participantes no sabe con certeza qué se lleva quien se marcha

El 84% retira siempre el acceso a quien deja la organización, pero solo el 52% puede reconstruir qué información se ha llevado. Los agentes de IA abren un frente similar: más de la mitad de quienes ya los usan o prueban no puede auditarlos por completo.

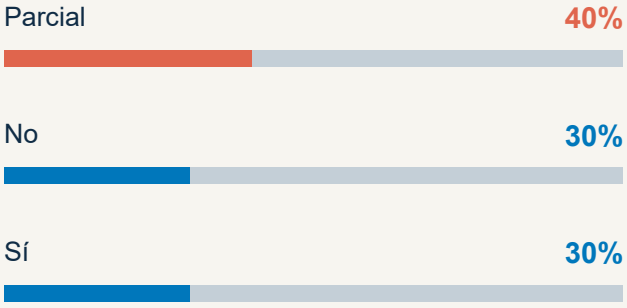
Empleados que dejan la organización

Respuesta	Revocación	Trazabilidad
Sí / siempre	84%	52%
Parcial	10%	42%
No	6%	6%

Agentes de IA con acceso



Auditoría de ese acceso



Acceso concedido a agentes o copilotos de IA sobre repositorios corporativos, y capacidad de auditar ese acceso. Porcentajes aproximados.

Dos datos relacionados

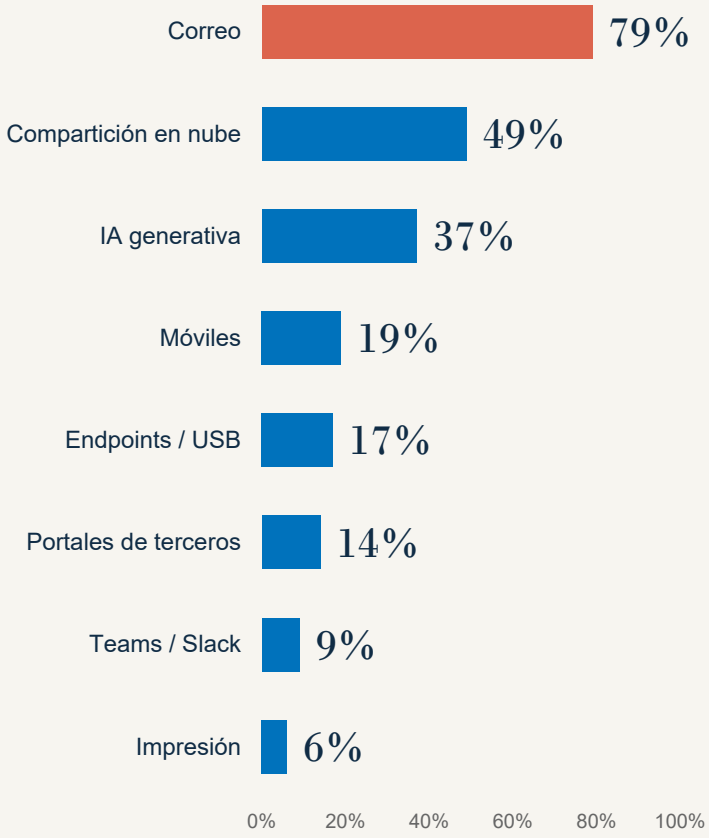
Con agentes activos o en piloto: auditoría completa 40%, parcial 35%, ninguna 20% y sin respuesta 5%. Entre quienes comparten con terceros, el 85% revoca siempre las bajas y el 49% declara trazabilidad.

P7 · ¿Cuáles son sus principales canales de exposición de información sensible y por cuáles ha sufrido un incidente en 24 meses?

El correo es el primer canal de exposición y la IA ocupa el tercer lugar

El correo (79%) y la compartición en nube (49%) encabezan los canales de exposición percibidos. La IA generativa (37%) ya aparece en tercer lugar, por delante de móviles, USB y portales de terceros. Percepción e incidentes reales se presentan por separado.

Canales percibidos



Selección múltiple: se podían marcar varias opciones; los porcentajes no suman 100%.

Incidentes declarados

No	**72%**
Sí	**11%**
Prefiero no responder	**11%**
No lo sabemos	**6%**

Incidente declarado: incidente confirmado o reportable por la organización.

Del canal señalado a la respuesta

El correo también aparece como canal principal en el pequeño grupo con incidentes confirmados. Conviene revisar destinatarios, permisos y capacidad de retirar acceso.

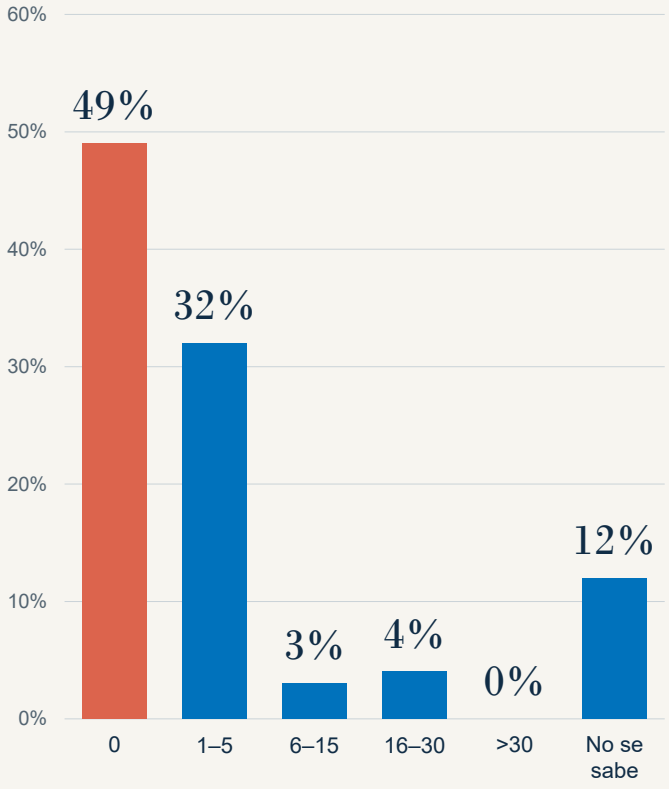
Canales confirmados: selección múltiple sobre un subgrupo reducido. Lectura orientativa.

P8 · ¿Cuántos incidentes de exposición o pérdida de información sensible estima que sufre al mes, y espera que aumenten en 2026?

El 39% de los consultados estima que su organización sufre eventos de exposición cada mes

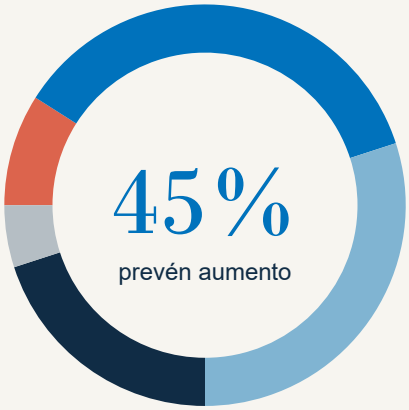
El 39% estima al menos un evento de exposición al mes y el 45% espera que aumenten en 2026; solo el 5% prevé una reducción. Las estimaciones mensuales recogen eventos potenciales, no incidentes confirmados.

Incidentes estimados al mes



Incidentes estimados: eventos potenciales de exposición. No equivalen a incidentes confirmados.

Expectativa para 2026



Aumentarán mucho	9%
Aumentarán	36%
Se mantendrán	30%
No lo sabemos	20%
Disminuirán	5%

Porcentajes aproximados.

45% espera un aumento o un aumento fuerte. Aproximadamente el 20% no sabe cómo evolucionará.

La expectativa de aumento invita a revisar la capacidad de detección y respuesta. Las estimaciones recogen la percepción de los participantes sobre la evolución de la exposición.

El 96% de las organizaciones utiliza o prueba la IA generativa

El 96% declara IA generativa en uso o en piloto. Copilotos corporativos (64%), análisis documental (56%) y asistentes de código (51%) son los usos más extendidos, y el 22% ya trabaja con agentes autónomos.

Adopción de IA

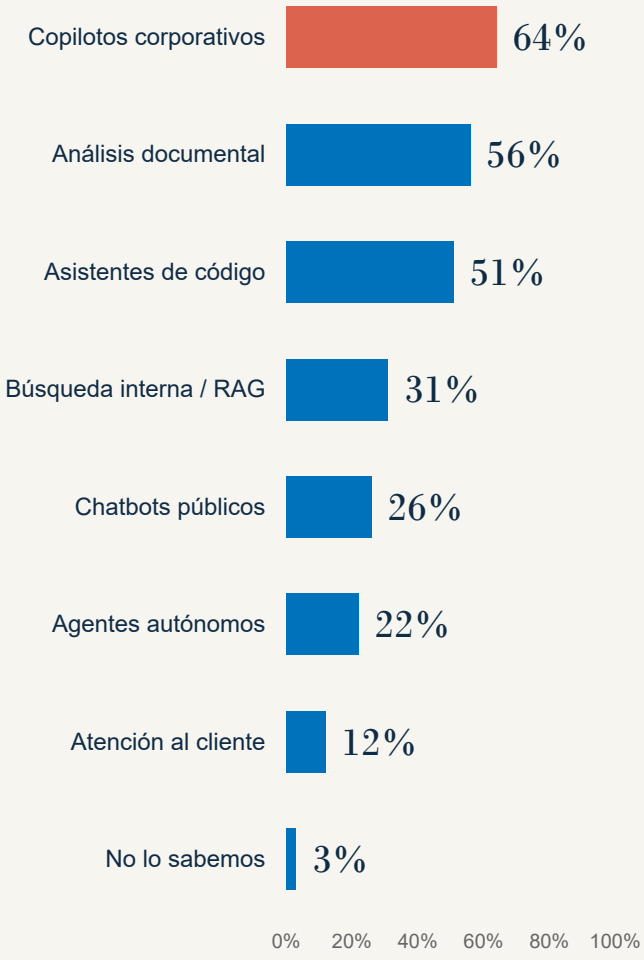
96%

Declara IA en uso o en piloto

El indicador reúne el uso extendido, el uso puntual y las iniciativas en piloto. Describe presencia de IA, no el grado de madurez de sus controles.

Porcentaje agregado, calculado antes de redondear.

Usos declarados



Selección múltiple: se podían marcar varias opciones; los porcentajes no suman 100%.

Agentes: el siguiente frente

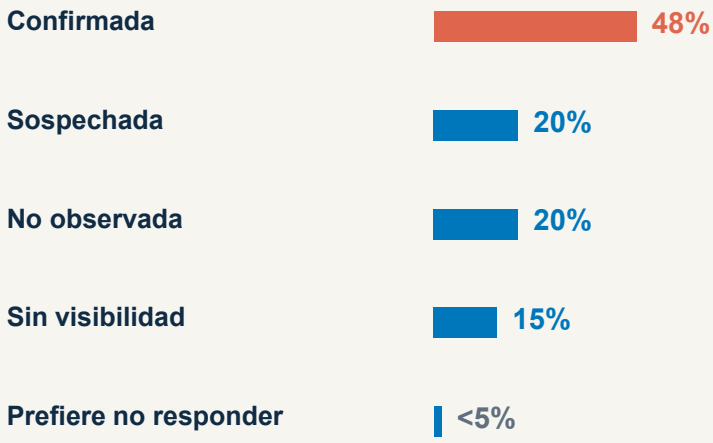
El 22% ya usa agentes autónomos. Su acceso a repositorios y su auditoría se analizan en la página 12.

P4 + P6 · ¿Tiene constancia de que se haya introducido información sensible en herramientas de IA? ¿Ve cuáles se usan?

El 48% de los participantes confirma que se ha introducido información sensible en herramientas de IA

La exposición confirmada convive con sospechas y falta de visibilidad: solo el 41% tiene visibilidad completa de las herramientas de IA que se usan. Introducir información en una herramienta de IA no implica por sí solo un incidente: depende del destino y de la autorización.

Exposición declarada a IA





Porcentajes aproximados.

Visibilidad sobre herramientas de IA

Parcial	**44%**
Completa	**41%**
No lo sabemos	**9%**
No	**6%**

Porcentajes aproximados.

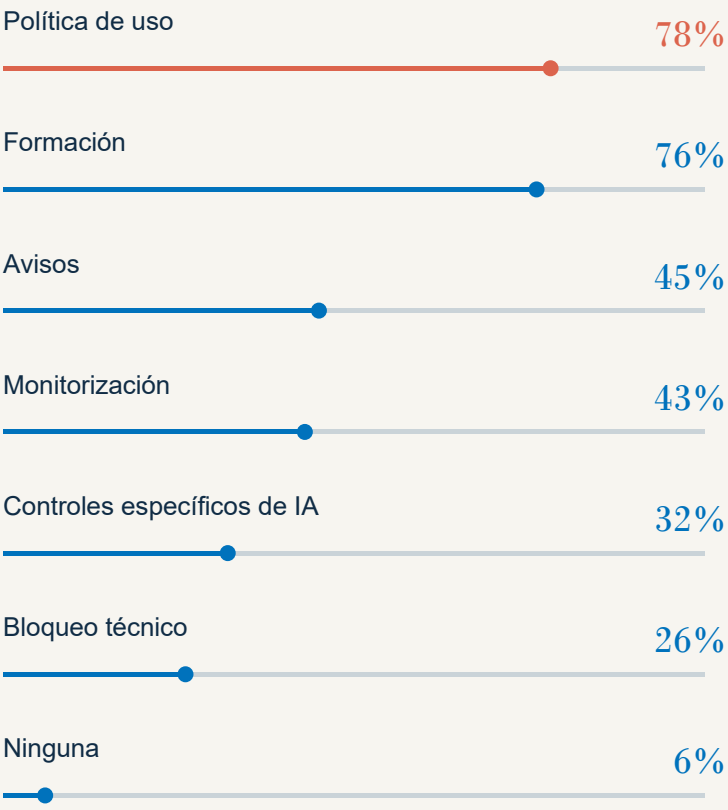
La fuga hacia la IA rara vez se registra como incidente: dos de cada tres participantes que confirman exposición a la IA declaran no haber sufrido ningún incidente de exposición en los últimos 24 meses.

P5 · ¿Qué medidas tiene para evitar que información sensible se introduzca en herramientas de IA, y confía en que se cumplan?

El 78% de las organizaciones tiene política de uso de IA, pero solo el 26% aplica bloqueo técnico

El 78% dispone de política de uso de IA y el 76% forma a sus empleados, pero solo el 26% aplica bloqueo técnico de la subida. La confianza en que la política se cumpla es mayoritariamente media (55%) y solo el 15% la considera alta.

Medidas declaradas



Selección múltiple: se podían marcar varias opciones. Los porcentajes pueden superar el 100%.

Confianza en el cumplimiento



Base: respuestas a esta pregunta.

28%

de quienes tienen política marcan también bloqueo técnico.

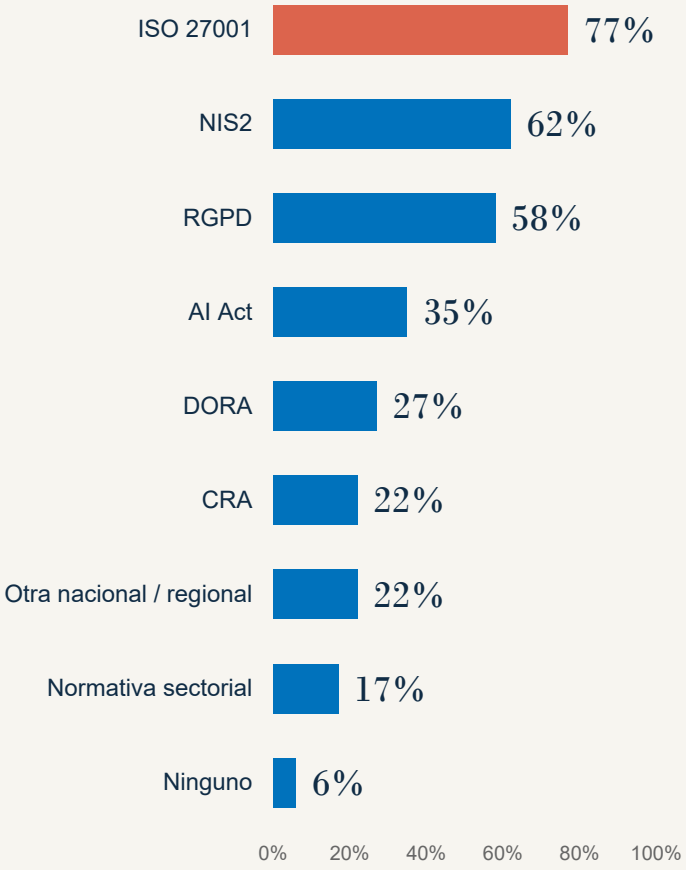
La política necesita respaldo técnico

Entre quienes tienen política y contestan sobre confianza, el 20% expresa confianza alta. Una prueba de subida permite comprobar el comportamiento del control en un flujo real.

El 83% de los participantes considera la soberanía del dato importante u obligatoria

El 40% la trata ya como requisito obligatorio y el 72% la extiende a las herramientas de IA que procesan datos sensibles. ISO 27001 (77%), NIS2 (62%) y RGPD (58%) son los marcos que más impulsan la inversión en protección del dato.

Marcos que impulsan inversión



Selección múltiple: se podían marcar varias opciones; los porcentajes no suman 100%.

Peso de la soberanía

Requisito obligatorio	**40%**
Criterio importante	**43%**
Lo valoramos, no es decisivo	**6%**
No es un factor	**2%**
No lo sabemos	**9%**

Porcentajes aproximados.

Jurisdicción exigida

Región (p. ej., UE)	**44%**
País de la organización	**38%**
Indiferente	**10%**
Contrato o normativa	**8%**

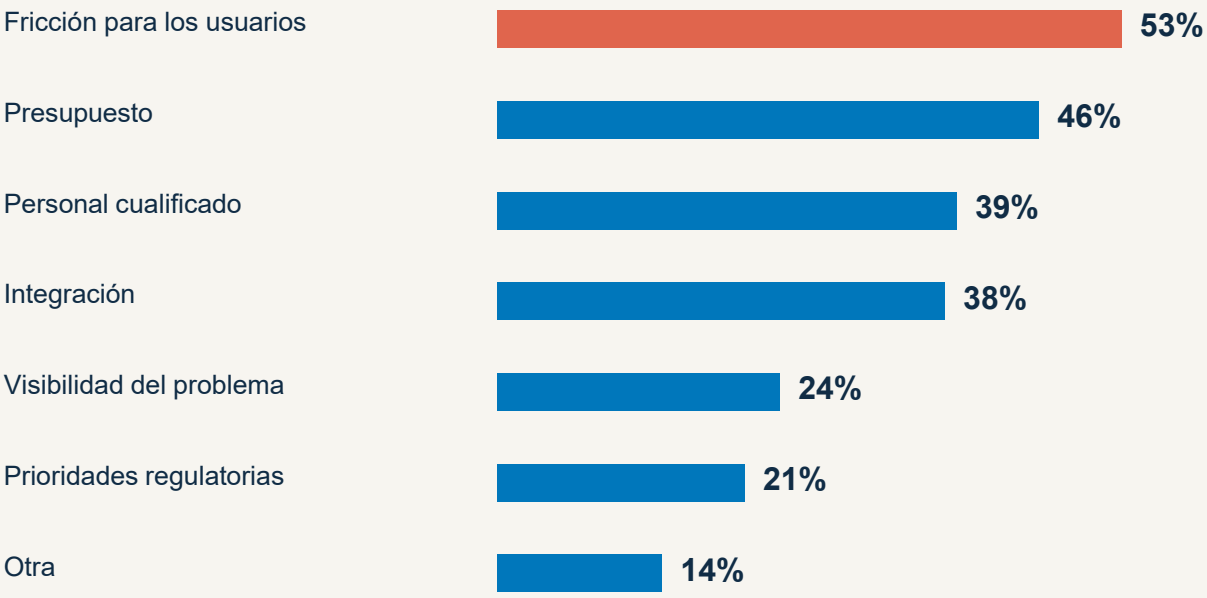
Porcentajes aproximados.

¿A qué se aplica el requisito de soberanía? A los datos almacenados (77%), a las herramientas de IA que procesan datos sensibles (72%), a los servicios en la nube (68%) y a proveedores y terceros (59%). Solo el 7% no aplica ningún requisito. Selección múltiple.

P15 · ¿Cuál es la principal barrera para mejorar la protección de la información sensible en su organización durante 2026?

La fricción para los usuarios y el presupuesto son las principales barreras para mejorar la protección del dato

La fricción para el usuario (53%) y el presupuesto (46%) encabezan las barreras, seguidas de la falta de personal cualificado (39%) y la integración (38%). La tabla inferior las desglosa según el marco regulatorio citado.



Selección múltiple: se podían marcar varias opciones; los porcentajes no suman 100%.

Barreras entre quienes citan cada marco

Marco	Presupuesto	Fricción	Integración
NIS2	51%	49%	47%
DORA	60%	44%	60%
AI Act	46%	52%	39%
ISO 27001	52%	55%	41%

Selección múltiple dentro de cada grupo. Una organización puede citar varios marcos

La experiencia de usuario y el esfuerzo de integración condicionan la adopción de controles de protección.

Agenda del CISO: seis comprobaciones

Cómo usarla: cada comprobación parte de lo que hacen sus pares según el estudio, indica qué revisar en su organización y qué evidencia demuestra que el control funciona. Si no puede obtener la evidencia, ha identificado una carencia.

01

Política de IA con respaldo técnico

Dato del estudio: El 78% tiene política de uso de IA, pero solo el 26% aplica bloqueo técnico y el 15% confía plenamente en que se cumpla.
Qué comprobar: Si cada herramienta de IA autorizada admite solo la información prevista, con una prueba de subida con información ficticia.

Evidencia: resultado de la prueba en una herramienta autorizada y en otra no autorizada.

02

Agentes de IA antes de conectarlos

Dato del estudio: El 43% ya da acceso a agentes de IA o lo está probando, y solo el 30% puede auditarlo por completo.
Qué comprobar: Qué puede leer cada agente, con qué identidad actúa y qué registro deja, antes de conectarlo a un repositorio.

Evidencia: inventario de agentes, permisos asignados y registro de accesos.

03

Salidas de personal con trazabilidad

Dato del estudio: El 84% retira el acceso a quien se marcha, pero el 48% no sabe con certeza qué se ha llevado.
Qué comprobar: Si el proceso de baja incluye revisar la actividad reciente sobre información sensible, en coordinación con RR. HH.

Evidencia: checklist de baja con revisión de accesos y descargas recientes.

Agenda del CISO: terceros y despliegue

El resultado de las seis comprobaciones es una lista priorizada de carencias reales, no supuestas, con la que justificar decisiones e inversiones ante la dirección.

04

Terceros: el control tras el envío

Dato del estudio: El 72% comparte información sensible con terceros y solo el 46% puede revocar ese acceso.
Qué comprobar: Si al cerrar una colaboración se retira el acceso a lo ya compartido, dentro de la gestión de la cadena de suministro que exige NIS2.

Evidencia: registro de lo compartido por tercero y resultado de la retirada del acceso.

05

Despliegue con usuarios y soporte

Dato del estudio: La fricción para el usuario (53%) y el presupuesto (46%) encabezan las barreras.
Qué comprobar: En un piloto con usuarios representativos, si completan la tarea y cuánto tardan antes de extender el control, y si el presupuesto incluye el soporte.

Evidencia: tarea completada, fricción observada y esfuerzo de integración o ayuda.

06

Soberanía y evidencias

Dato del estudio: El 83% considera la soberanía importante u obligatoria y el 72% la aplica a la IA que procesa datos sensibles.
Qué comprobar: Qué información queda sujeta al requisito y dónde se almacena o procesa, también en servicios de IA y en terceros.

Evidencia: condiciones del proveedor, ubicaciones y responsable de cada requisito.

Una convocatoria especializada

Trabajo de campo: julio y agosto de 2026. Estudio de SealPath centrado en profesionales de seguridad y tecnología.

1.052

CISOs y profesionales de seguridad contactados

Los gráficos utilizan las respuestas recibidas en cada pregunta.



Perfiles de seguridad y tecnología

CISO	35% · Dirección de seguridad de la información
CIO	25% · Dirección de Sistemas de Información
Responsables de seguridad	15% · Gestión de la seguridad
Responsables de IT	20% · Gestión de sistemas y servicios de IT

Predominan los perfiles de CISO y dirección de seguridad, seguidos de CIO y responsables de IT. El estudio profundiza en controles concretos sobre el documento.

Otros perfiles, 5%. Metodología en la página 23.

Cómo interpretar los resultados

Estudio exploratorio de SealPath. Trabajo de campo: julio y agosto de 2026. Convocatoria dirigida a 1.052 CISOs y profesionales de seguridad.

Base de cálculo

Los porcentajes se calculan sobre las respuestas de cada pregunta. En selección múltiple, una misma organización podía indicar varias opciones.

Presentación de porcentajes

Porcentajes expresados en enteros. En selección múltiple pueden superar el 100%. Los indicadores con bases diferentes no deben sumarse.

Cruces y ausencias

Los cruces describen respuestas de las mismas organizaciones. Su base puede variar según las preguntas contestadas. Los cruces sobre grupos reducidos se presentan como lectura orientativa.

Alcance de la interpretación

Participación voluntaria y datos autodeclarados. La convocatoria no equivale a la base de respuestas. El estudio no estima representatividad del mercado, causalidad ni eficacia objetiva de productos.

Alcance del informe

Primera edición. Cada página indica la pregunta de la que procede y los términos técnicos se definen en el glosario (página 26). Para próximas ediciones se mantendrán las preguntas clave para comparar tendencias.

Dónde se concentra la información sensible

Coincidencias entre tipos de información y entornos seleccionados por los participantes.

Tipo de información	Local	M365	GWS	SaaS	Equipos	Colab.	Correo	Terc.	IA
Financiera	MA	MA	B	M	M	M	M	B	B
Datos de clientes	MA	A	B	M	M	M	M	M	B
Empleados y RR. HH.	MA	A	B	M	M	M	M	B	B
Prop. intelectual / I+D	A	A	B	M	M	M	M	B	B
Código fuente	A	A	B	M	B	M	B	B	B
Secretos y contratos	M	M	B	M	M	M	M	B	B
Datos de salud	M	B	B	B	B	B	B	B	B
Regulados sectoriales	B	M	B	B	B	M	B	B	B

GWS: Google Workspace. Colab.: Teams / Slack. Terc.: terceros.

B Baja	**M** Moderada	**A** Alta	**MA** Muy alta
Menos del 10%	10% a menos del 25%	25% a menos del 40%	40% o más

Comparativa por segmento

Las organizaciones grandes y los perfiles de seguridad declaran más control técnico.

	Bloqueo técnico de IA	Trazabilidad en bajas	Protección que viaja
Menos de 1.000 empleados	10%	40%	15%
1.000 o más empleados	50%	75%	30%
Seguridad	35%	65%	30%
IT y otros	10%	35%	<5%

Grupos de base reducida: lectura orientativa. Intensidad según la escala superior.

Sectores, regiones y organizaciones

La participación reúne perfiles de varios países, con mayor presencia de la península ibérica. Los siguientes gráficos describen la composición del estudio.

Sector



Participación geográfica

Representación mayoritaria del sur de Europa

El resto procede de otros países europeos y, en menor medida, de fuera de Europa.

Tamaño de la organización



Porcentajes aproximados.

Glosario de términos

Definiciones breves de los controles y conceptos que aparecen en el informe, en el sentido en que se utilizan en el cuestionario.

Mínimo privilegio: cada persona accede solo a la información que necesita para su función.

Auditoría de accesos: registro de quién accede a la información, cuándo y desde dónde.

Revocación del acceso: retirada de un permiso ya concedido, por ejemplo a una cuenta, una carpeta o un enlace compartido. No implica por sí sola poder retirar el acceso a una copia ya descargada o enviada.

Cambiar permisos tras el envío: modificar lo que un destinatario puede hacer con un documento después de habérselo enviado.

Caducidad: el acceso expira automáticamente en una fecha o tras un plazo.

Protección persistente: el cifrado y los permisos acompañan al propio archivo, esté dentro o fuera de la organización ("protección que viaja con el documento").

Trazabilidad: capacidad de reconstruir qué información se ha consultado, descargado o llevado y por quién.

Clasificación y etiquetado: identificación del nivel de sensibilidad de la información y marcado para aplicarle una política.

DLP: prevención de pérdida de datos: detecta y bloquea movimientos de información sensible por canales como correo, web o USB.

CASB: control del uso de servicios en la nube y de la información que se sube a ellos.

DSPM: descubrimiento de dónde reside la información sensible, sobre todo en la nube, y de quién tiene acceso.

IAM / ZTNA: gestión de identidades y accesos, y acceso a aplicaciones basado en verificación continua ("confianza cero").

IRM / Information Protection: cifrado y permisos aplicados al documento para controlar su uso.

Shadow AI: uso de herramientas de IA no aprobadas por la organización.

Agentes de IA: sistemas de IA que realizan tareas de forma autónoma y pueden acceder a repositorios corporativos.

Soberanía del dato: requisito de que la información y su procesamiento, incluida la IA, permanezcan bajo una jurisdicción determinada.

Protección persistente en una arquitectura por capas

La protección ligada al documento aborda el control posterior al envío. Repositorios, clasificación y controles del canal conservan funciones complementarias.



Capa	Función principal
Repositorio e identidad	Custodia y autorización del acceso al original.
Clasificación	Identificación de sensibilidad y aplicación de políticas.
DLP	Control de movimientos y usos en superficies cubiertas.
DSPM	Descubrimiento de exposición y permisos excesivos.
CASB / SWG	Controles sobre servicios nube y tráfico supervisado.
IRM / EDRM	Cifrado, permisos y trazabilidad en la copia protegida.

SealPath vincula cifrado, permisos y trazabilidad al documento protegido. Permite conservar control tras compartirlo y revocar el acceso según la política aplicada. Su función complementa la protección del repositorio y del canal.

Límites: no evita fotografías de pantalla o transcripción manual. El modo offline puede retrasar la revocación; las restricciones dependen de formato, aplicación y sistema operativo.

sealpath™
Smart Protection for Sensitive Data

SOBRE SEALPATH

Seguridad centrada en el dato

SealPath es una compañía europea líder que está revolucionando la seguridad de los datos corporativos al combinar una protección persistente con una gran facilidad de uso. Posee la confianza de organizaciones en más de 30 países y más de una década de experiencia prestando servicios a empresas de renombre del Euro Stoxx 50 y la lista Fortune 500. Cada día protege millones de documentos con soluciones avanzadas. SealPath destaca por hacer posible que la protección centrada en el dato sea accesible para todos, reducir riesgos, garantizar el cumplimiento normativo y permitir la colaboración segura.

www.sealpath.com
info@sealpath.com