dpi
DATA PRIVACY INSTITUTE

isms forum

VII

Estudio sobre el nivel de madurez en la aplicación de **Reglamento General de Protección de Datos**

Observatorio de la **Privacidad**

Participantes

Director

Carlos A. Sáiz

Participantes

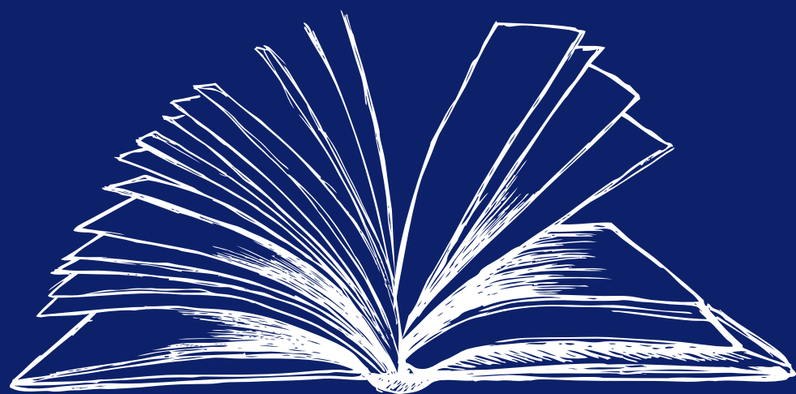
Álvaro Medina
Carlos Cabre
Cristina Köhler
Edison Hernández
Óscar López
Pilar Castillejo
Soraya Juarez
Víctor Antunes
Xabier Alberdi

Gestión del proyecto

Beatriz García

Diseño y maquetación

Susana Marín



La VII edición del Estudio sobre el Nivel de Madurez en la Aplicación del RGPD constituye un punto de inflexión en la trayectoria del Observatorio de la Privacidad. Tras seis ediciones consecutivas analizando la evolución del cumplimiento en organizaciones públicas y privadas, esta nueva entrega se presenta con una perspectiva más estratégica, integradora y orientada a la toma de decisiones reales dentro de la función de privacidad.

El estudio **consolida un recorrido de años en los que se ha acompañado la evolución del rol del DPO**, la profesionalización de los equipos de privacidad y la incorporación progresiva de modelos de gobernanza más robustos. Esta edición profundiza en esa línea, ofreciendo una visión que no solo describe el nivel de madurez alcanzado, sino que permite entender las dinámicas que lo explican: la presión regulatoria creciente, la evolución organizativa, la sofisticación tecnológica y, en última instancia, la necesidad de reforzar la resiliencia operativa en torno a los datos.

Para los profesionales de la privacidad, especialmente quienes asumen funciones de DPO o lideran unidades de cumplimiento y riesgo, esta edición aporta una radiografía que busca ir más allá del diagnóstico clásico. El enfoque metodológico se ha diseñado para ofrecer una lectura útil para la planificación anual, la priorización de iniciativas, la justificación presupuestaria, la interlocución con dirección y la construcción de hojas de ruta de madurez basadas en evidencia comparada.

En definitiva, pretende ser una herramienta práctica que responda a la necesidad real de disponer de métricas fiables y tendencias verificables sobre gobernanza, eficiencia y alineamiento regulatorio en un contexto cada vez más exigente.

01

Enfoque metodológico
y novedades de esta edición

1.1.

Muestra y alcance del estudio

La composición de la muestra mantiene un equilibrio que permite comparar prácticas entre organizaciones muy diversas en tamaño, sector y capacidad operativa. La presencia relevante de grandes corporaciones, unida a la participación de organizaciones medianas y pequeñas, facilita una lectura transversal del grado de madurez RGPD. Todo ello permite a los DPO situar su organización en un marco de referencia sólido, comprensible y útil para identificar fortalezas, brechas y prioridades de mejora.

1.2.

Novedades de esta edición

Esta edición incorpora avances significativos que enriquecen el análisis:

- **Mayor granularidad en los indicadores de madurez**, con métricas que permiten observar la evolución real del cumplimiento y no solo su estado estático.
- **Integración de indicadores tecnológicos**, fundamentales para evaluar la automatización de procesos, el uso de herramientas avanzadas y la eficiencia del programa de cumplimiento.
- **Bloque específico dedicado a la gobernanza de la Inteligencia Artificial,** alineado con el nuevo Reglamento de IA, que permite entender cómo convergen los marcos de privacidad y tecnología en la práctica diaria.
- Revisión y ajuste del modelo de madurez, incorporando **nuevas dimensiones de riesgo, responsabilidad y supervisión interna.**

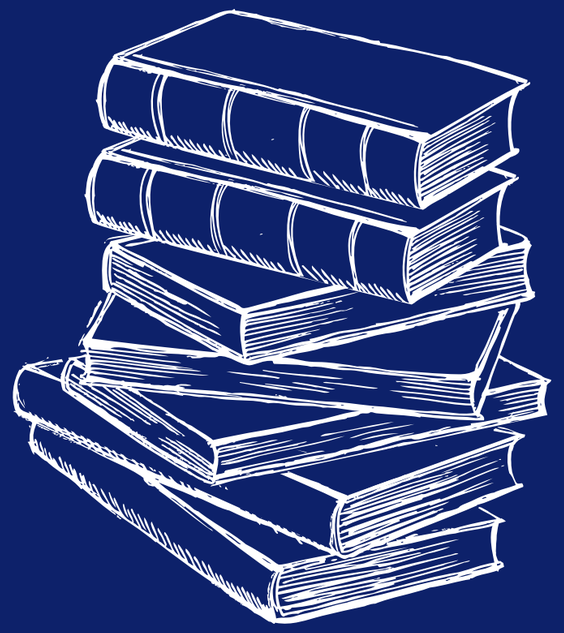
1.3.

Alineación con tendencias **regulatorias europeas**

La metodología empleada se alinea con la evolución del marco regulatorio europeo, en particular:

- el **fortalecimiento del RGPD** como estándar global,
- la integración de requisitos derivados del **Reglamento de IA,**
- el auge de normativas de **resiliencia digital (DORA) y seguridad (NIS2),**
- y la **necesidad de reforzar** la trazabilidad, la responsabilidad proactiva y el control interno.

Esta alineación permite que el Estudio no solo refleje el estado actual del cumplimiento, sino que se convierta en una herramienta predictiva: **ayuda a anticipar qué capacidades debe reforzar una organización para afrontar con éxito los retos regulatorios de los próximos años.**



02

Tipología
de la muestra

2.1.

Distribución por **número de empleados**

La composición de la muestra del VII Estudio refleja una distribución empresarial amplia y equilibrada, lo que permite obtener una visión representativa del grado de madurez en protección de datos en organizaciones con distintos niveles de complejidad operativa y estructuras de gobierno heterogéneas.

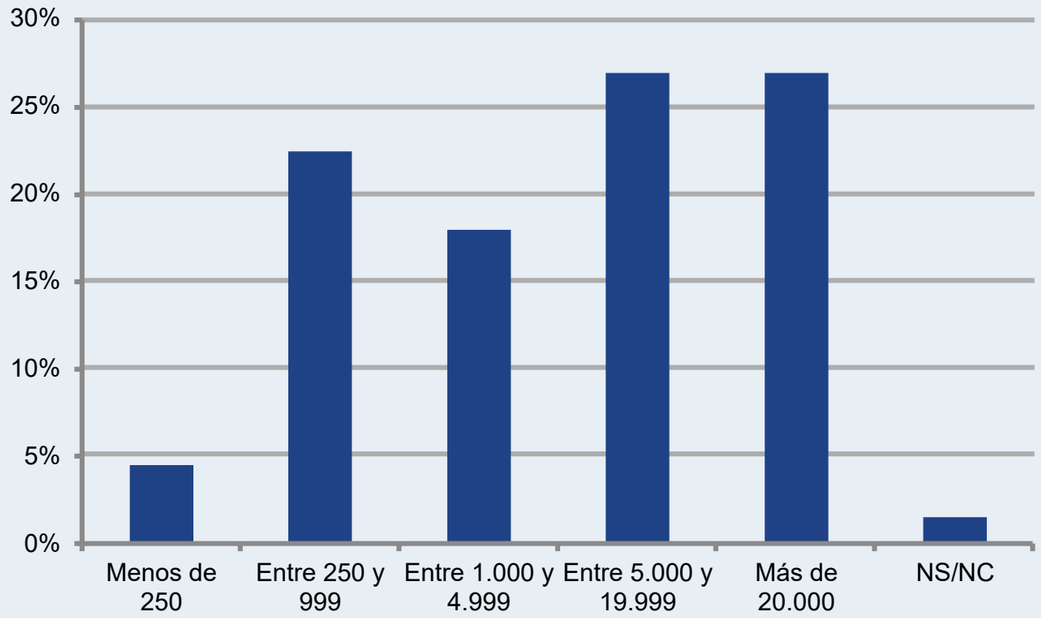
En términos de dimensión corporativa, se observa una participación particularmente significativa de empresas de gran escala: cerca de un tercio de los encuestados pertenece a organizaciones con entre 5.000 y 19.999 empleados, destacando el peso que tienen las entidades multinacionales en la consolidación de modelos avanzados de cumplimiento. Un porcentaje prácticamente equivalente corresponde a compañías con más de 20.000 trabajadores, lo que reafirma la relevancia de los grandes grupos empresariales en la muestra analizada.

Asimismo, un bloque relevante de participantes procede de organizaciones de tamaño intermedio. Las empresas con entre 250 y 999 empleados representan más de una quinta parte del total, mientras que las que cuentan con entre 1.000 y 4.999 trabajadores suponen algo menos de una quinta parte. Este segmento aporta una perspectiva esencial sobre cómo las estructuras medianas están adaptando sus capacidades internas para responder a las obligaciones del RGPD, especialmente en materia de gobernanza, control interno y gestión del riesgo.

La presencia de compañías pequeñas, aquellas con menos de 250 empleados, es más reducida, situándose en torno al 5%. Pese a su menor peso cuantitativo, este grupo resulta especialmente relevante para identificar retos de implementación ligados a recursos limitados o modelos organizativos menos formalizados. Por último, el porcentaje de respuestas clasificadas como NS/NC es residual, lo que contribuye a una interpretación robusta de los datos agregados.

En conjunto, **la distribución demuestra una participación sólida tanto de grandes corporaciones como de empresas de tamaño medio,** lo que garantiza un análisis metodológicamente equilibrado y alineado con la realidad del tejido empresarial que opera en España y a nivel internacional.

Ilustración 1: **Tamaño de la compañía**



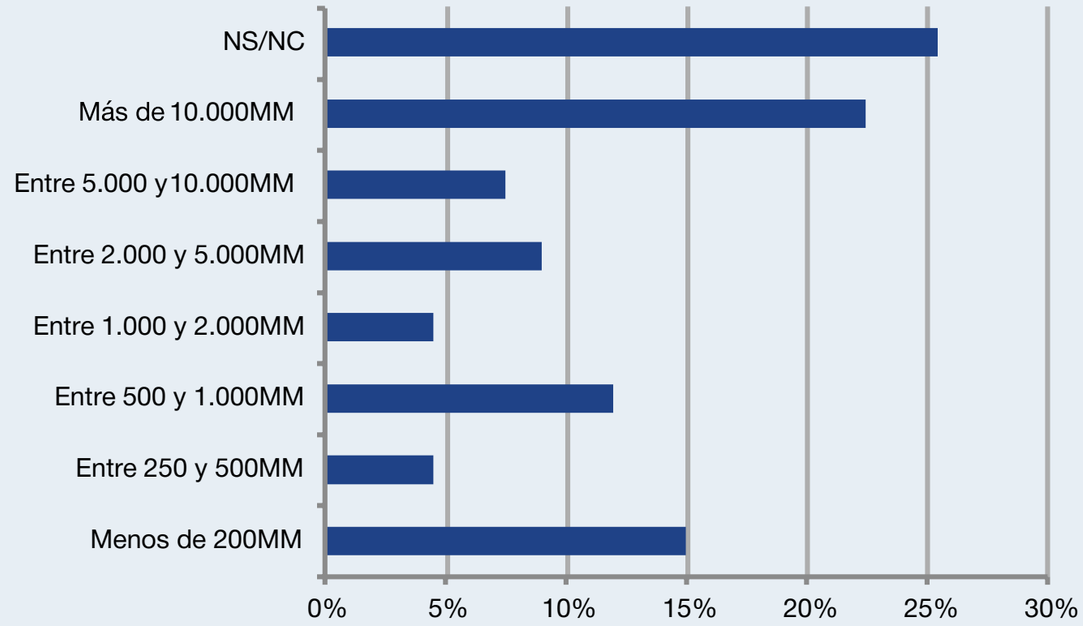
2.2.

Distribución por **ingresos anuales**

La distribución por ingresos muestra una participación especialmente elevada de organizaciones que no facilitan este dato (NS/NC, 26%), algo habitual en encuestas con información financiera sensible. Entre las respuestas declaradas, destacan las empresas con más de 10.000 millones de euros (22%), lo que evidencia un peso significativo de corporaciones de gran escala. Los tramos intermedios, de 2.000 a 5.000 millones y de 500 a 1.000 millones, presentan valores moderados, mientras que las compañías con ingresos menores de 200 millones de euros representan alrededor del 15%.

En conjunto, la muestra combina **organizaciones con alta capacidad financiera con otras de menor dimensión económica**, permitiendo analizar la madurez RGPD en contextos de recursos muy diferentes.

Ilustración 2: **Facturación de la compañía**



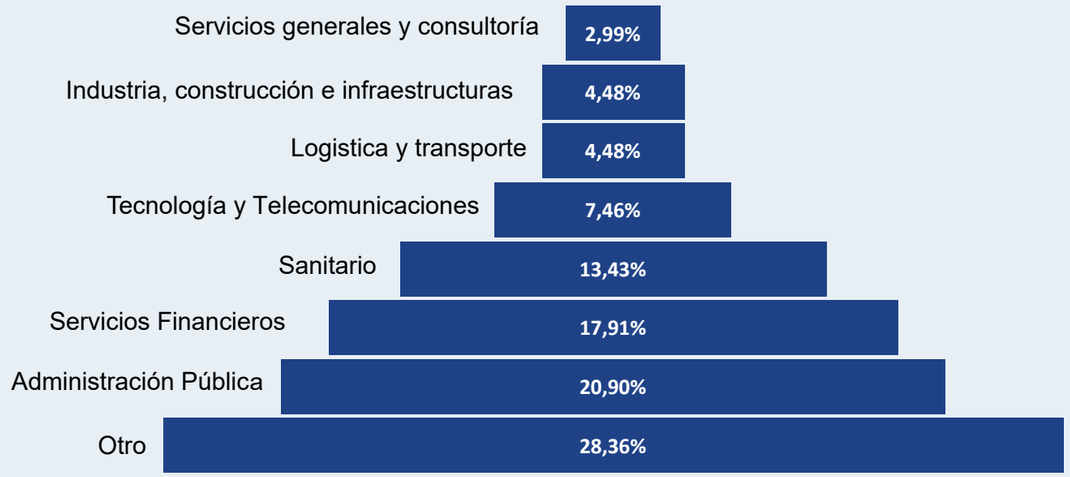
2.3.

Distribución por **sector de actividad**

La distribución sectorial evidencia una muestra amplia y diversa, con especial concentración en la categoría “Otros”, donde los participantes detallaron sectores como retail (incluyendo alimentación), seguros, distribución, entretenimiento y ocio, energía, turismo, educación, consumo, recursos humanos y medios de comunicación. Estos sectores, aunque no encajan en las categorías tradicionales del estudio, representan ámbitos altamente expuestos a dinámicas de digitalización y riesgos crecientes en privacidad y ciberseguridad. Junto a ellos, mantienen un peso relevante la Administración Pública y los Servicios Financieros, mientras que Sanitario, Tecnología, Industria y Logística completan una distribución equilibrada para la comparación del nivel de madurez RGPD entre sectores heterogéneos.

En conjunto, la distribución sectorial confirma que **el estudio incorpora una muestra equilibrada**, con presencia sólida de sectores regulados y altamente dependientes de la información, junto con otros en pleno proceso de transformación digital. Esta amplitud permite interpretar la madurez RGPD con una perspectiva comparada entre entornos de distinta presión normativa, capacidad organizativa y nivel de exposición a amenazas de ciberseguridad.

Ilustración 3: **Sector de actividad de la compañía**



03

Estado de la situación - Gobierno de la Privacidad

3.1.

Tipo de DPO y alcance geográfico de la función

La inmensa mayoría de las organizaciones participantes en el Observatorio cuentan con un Delegado de Protección de Datos interno, siendo menos del 5% aquellas que cuentan con un DPO externalizado. Este aumento de la internalización con respecto a años anteriores evidencia la creciente preocupación que las empresas tienen en torno a la Privacidad y Protección de Datos, prefiriendo internalizar la figura del DPO para hacer frente a los retos del cumplimiento normativo y consolidándose así la importancia que tiene esta función dentro de las compañías.

Entre las que disponen de un Delegado de Protección de Datos dentro de la organización, **en torno al 60% se encuentra dedicado en exclusiva a Privacidad y Protección de Datos, frente a un 40% que estaría asumido dentro de otras Áreas existentes de la compañía,** constatándose que las funciones del DPO van más allá de las tradicionales en materia Privacidad y Protección de Datos, asumiendo por ejemplo, competencias en el cumplimiento del RIA dadas las sinergias evidentes con el cumplimiento del RGPD.

Ilustración 4: **Evolución del tipo de DPO nombrado**

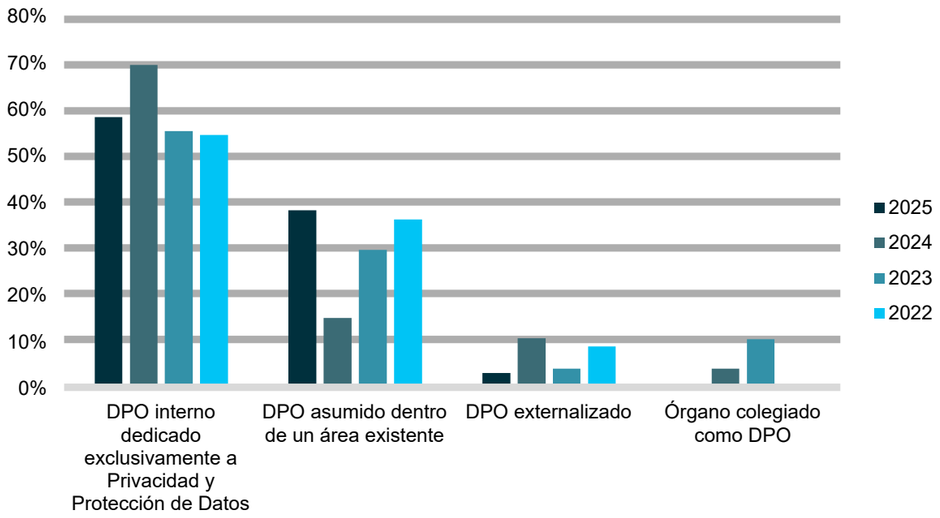
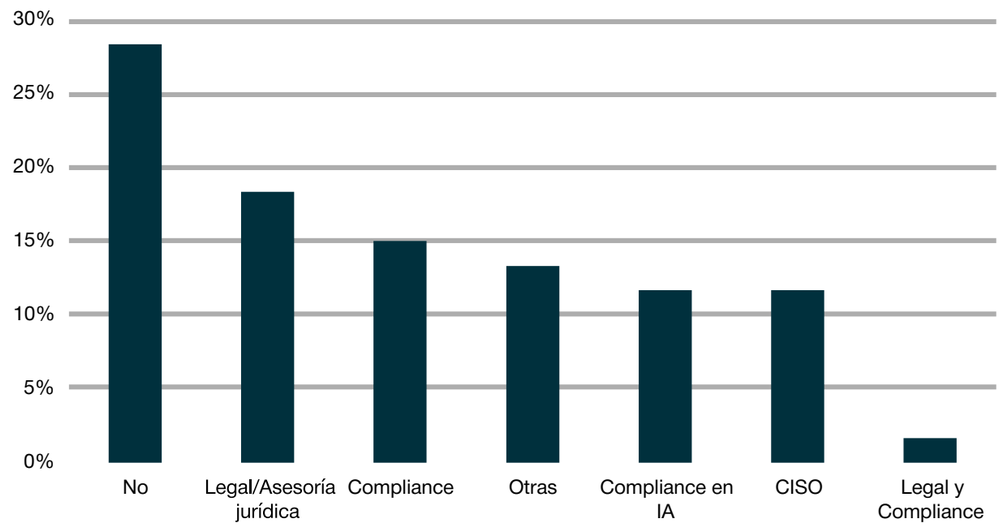


Ilustración 5: **Funciones adicionales a las de DPO**



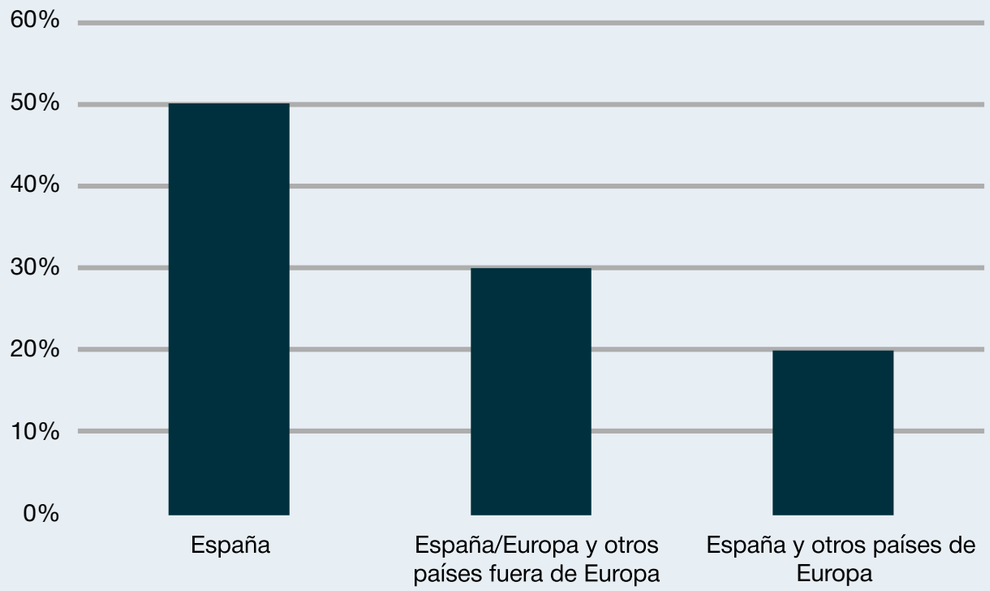
En este sentido, pese a que sigue predominando la figura del DPO que no compatibiliza su cargo con otras funciones (más del 25% así lo han declarado), este dato se ha visto reducido a la mitad con respecto a lo respondido años anteriores.

Entre las funciones con las que se compatibiliza, destaca la de Compliance en IA, siendo esta última una de las novedades con respecto a años anteriores. Estos resultados reafirman la preocupación de las organizaciones por el uso responsable de la Inteligencia Artificial y el complejo entorno normativo al que se enfrentan actualmente.

En cuanto al alcance territorial de las competencias del Delegado de Protección de Datos, en la mitad de los casos se limita al ámbito nacional, mientras que la otra mitad tendría un alcance internacional.

Este aumento de los DPO con alcance nacional viene motivado por la mayor participación de pequeñas y medianas empresas con presencia únicamente en España, combinado con esa complejidad del entorno normativo que requiere cada vez más de un alto nivel de especialización a nivel local, pudiendo estar optando así las organizaciones por figuras con un mayor nivel de conocimiento de la legislación nacional y menor alcance territorial.

Ilustración 6: **Alcance territorial de los DPOs**

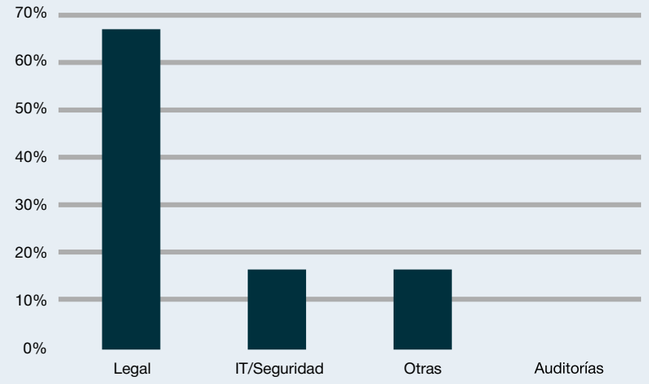


3.2.

Formación académica y certificaciones de los DPOs

La mayoría de los DPOs encuestados disponen de una formación jurídica (65%), consolidándose la tendencia de años anteriores, seguido de aquellos que cuentan con un perfil técnico entre los que destacan IT / Seguridad o algún tipo de ingeniería y, en menor medida, formación en Administración y Dirección de Empresas.

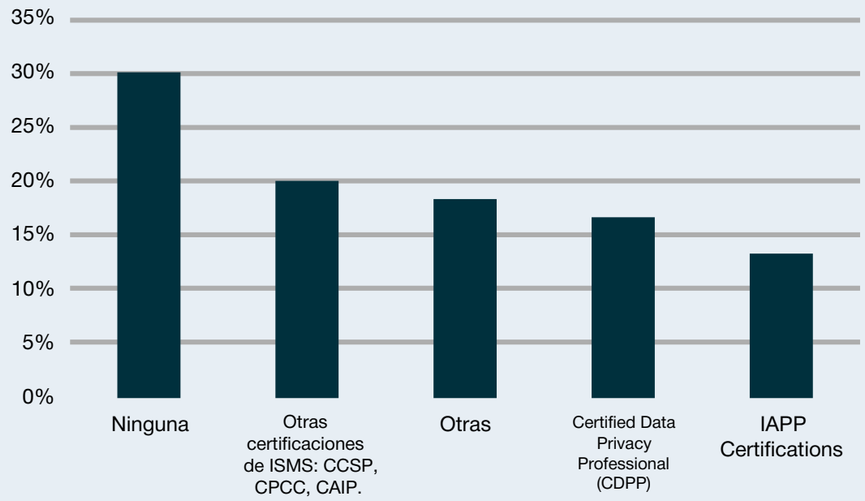
Ilustración 7: **Formación académica de los DPOs**



Entre las certificaciones con las que cuentan los Delegados de Protección de Datos, el CDPD conforme al esquema de la AEPD sigue siendo la más acreditada. Asimismo, se identifica un aumento en el número de encuestados que cuentan con otras certificaciones de ISMS Forum como el CCSP, CPCC, CAIP, etc., reflejo de esa evolución notoria en los roles y expertise de los DPOs que requiere de perfiles multidisciplinares con conocimientos legales, técnicos y éticos.

Por otro lado, se mantiene el porcentaje de DPOs que cuentan con otras certificaciones entre las que destacan CISA, CISM y estándares internacionales como ISO27001.

Ilustración 8: **Certificaciones profesionales de los DPOs**



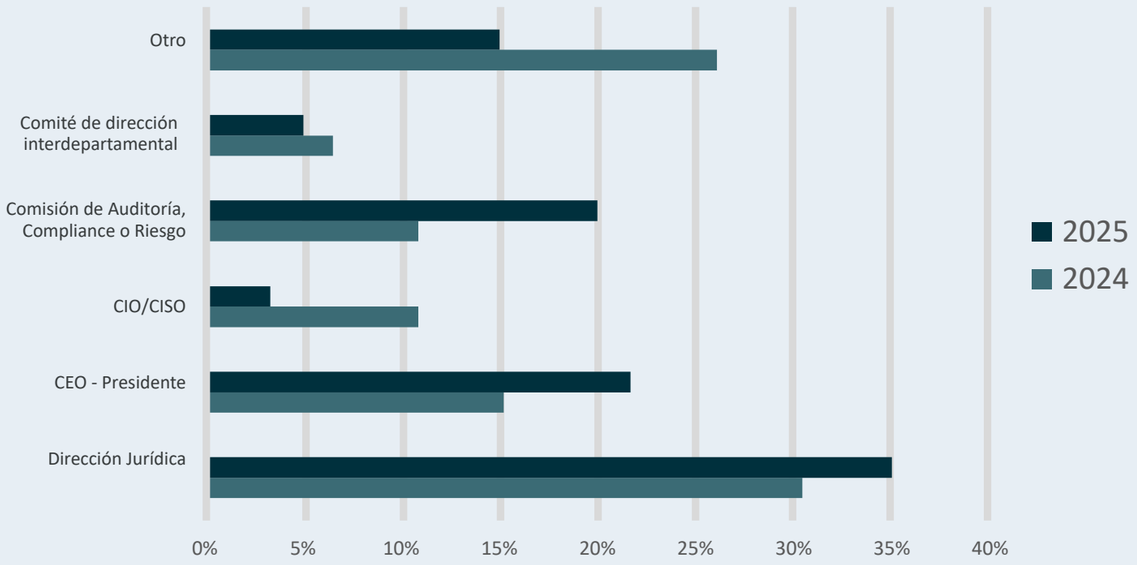
3.3.

Reportes

En torno al 35% de los Delegados de Protección de Datos reportan directamente a la Dirección de Asesoría Jurídica, pero destaca el aumento de los DPOs que reportan directamente al CEO o Consejo de Administración de sus organizaciones, reflejando cómo la Alta Dirección es cada vez más consciente de la importancia de la Privacidad y Protección de Datos.

Se incrementa también el número de aquellos que reportan a algún Comité de la organización (auditoría, riesgos o comités interdepartamentales, etc.), confirmándose la preocupación interna de las organizaciones por estas cuestiones.

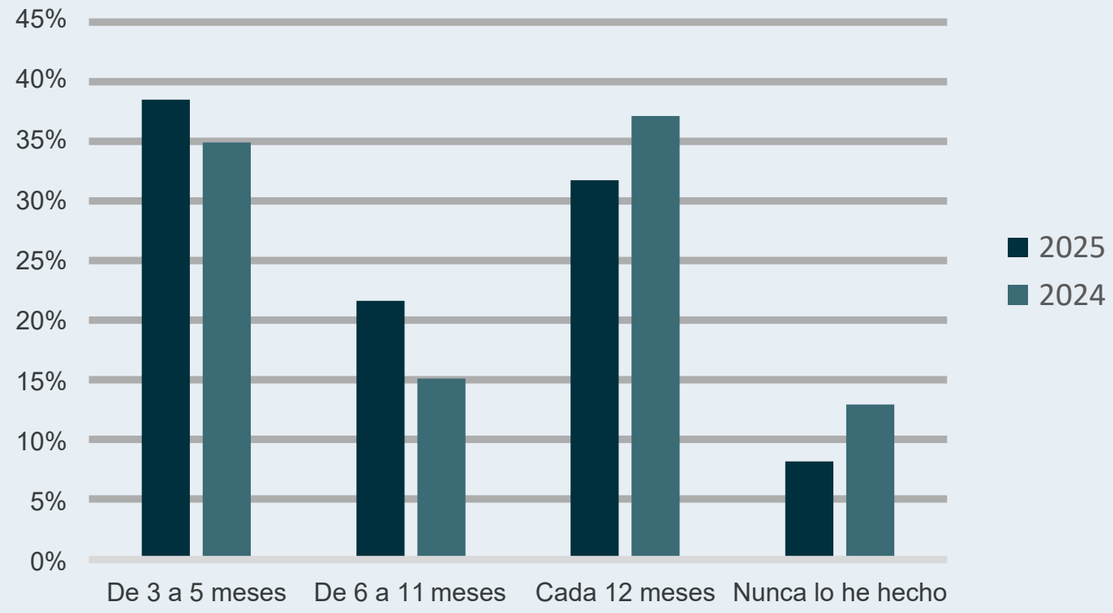
Ilustración 9: **Evolución del órgano al que se reporta dentro de la empresa**



En esta misma línea, se aprecia un incremento en la periodicidad de los reportes a la Alta Dirección fruto de esa preocupación, reduciéndose el número de compañías en las que se reportaba anualmente y aumentando las que lo hacen 2 o más veces al año, evidenciándose esa necesidad de llevar a cabo una supervisión continua como uno de los pilares de la responsabilidad proactiva de las empresas.

Adicionalmente, el porcentaje de empresas que nunca ha hecho un reporte se sitúa por debajo del 10%, siendo el dato más bajo en los últimos años y desprendiéndose cómo sigue evolucionando y aumentando el grado de madurez en la gobernanza del RGPD, ahora que se cumplen 10 años de la publicación del Reglamento.

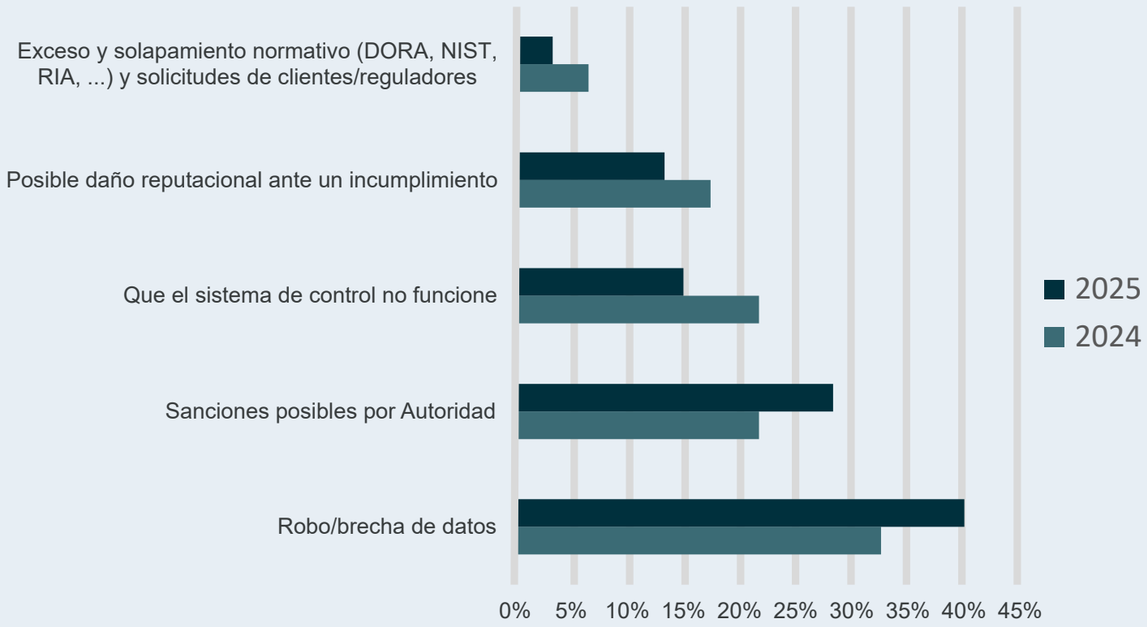
Ilustración 10: **Evolución de la periodicidad con la que se reporta a la Alta Dirección**



El análisis de las cuestiones que más preocupan de cara a los reportes a la Alta Dirección revela que **vuelven a crecer las brechas de datos y las sanciones de la Autoridad de Control.**

La irrupción de tecnologías como la Inteligencia Artificial democratiza esa capacidad de ataque sobre las empresas para intentar robar sus datos, conseguir las credenciales de sus clientes, etc., pudiendo estar al alcance de personas que no necesariamente tienen altos conocimientos técnicos. Sin duda, estos nuevos riesgos suponen un desafío para la Privacidad y Protección de Datos, que se refleja en las preocupaciones de las organizaciones.

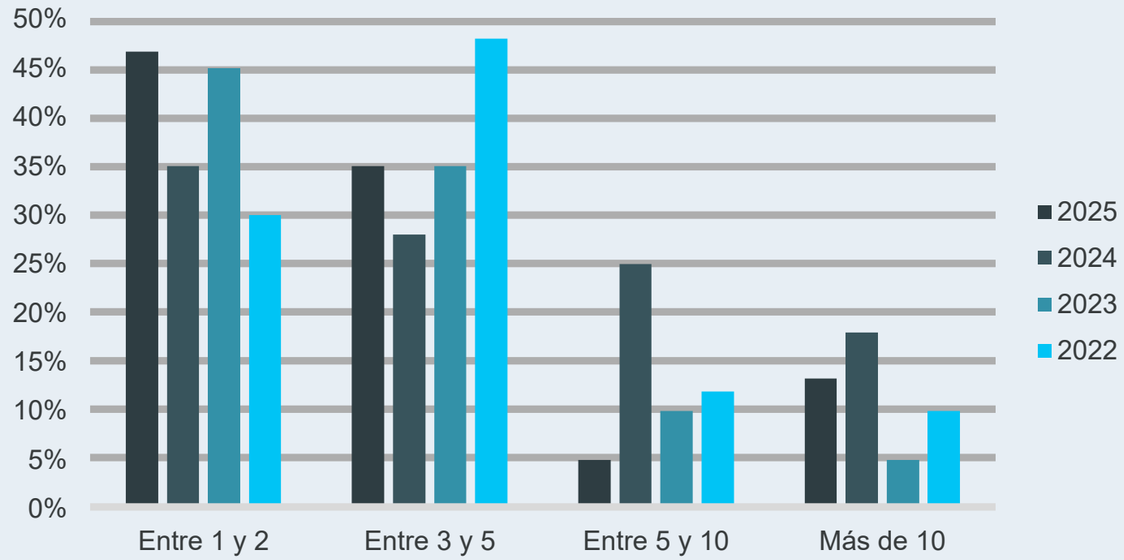
Ilustración 11: **Principales preocupaciones sobre los reportes a dirección**



3.4.

Equipos

Ilustración 12:
Evolución del tamaño de los equipos dedicados al cumplimiento del RGPD (2022–2025)



La evolución de 2022 a 2025 muestra un cambio significativo en cómo las organizaciones están configurando sus equipos de cumplimiento. **En 2025 aumenta el porcentaje de entidades que cuentan con 1–2 personas dedicadas al RGPD (aprox. 45%) y entre 3–5 personas (35%), consolidándose como el modelo predominante para cubrir las funciones esenciales del RGPD.**

Se ha reducido el porcentaje de organizaciones con equipos de más de 5 personas dedicados en exclusiva a Privacidad y Protección de Datos que, de nuevo, viene motivado por la mayor participación de empresas de pequeño y mediano tamaño.

No obstante, también podría ser un indicador de que los equipos que antes se dedicaban sólo al cumplimiento del RGPD ahora tengan que dedicar tiempo y recursos a otros aspectos como el gobierno y uso responsable de la IA dadas las sinergias entre el cumplimiento del RGPD y del RIA.

3.5.

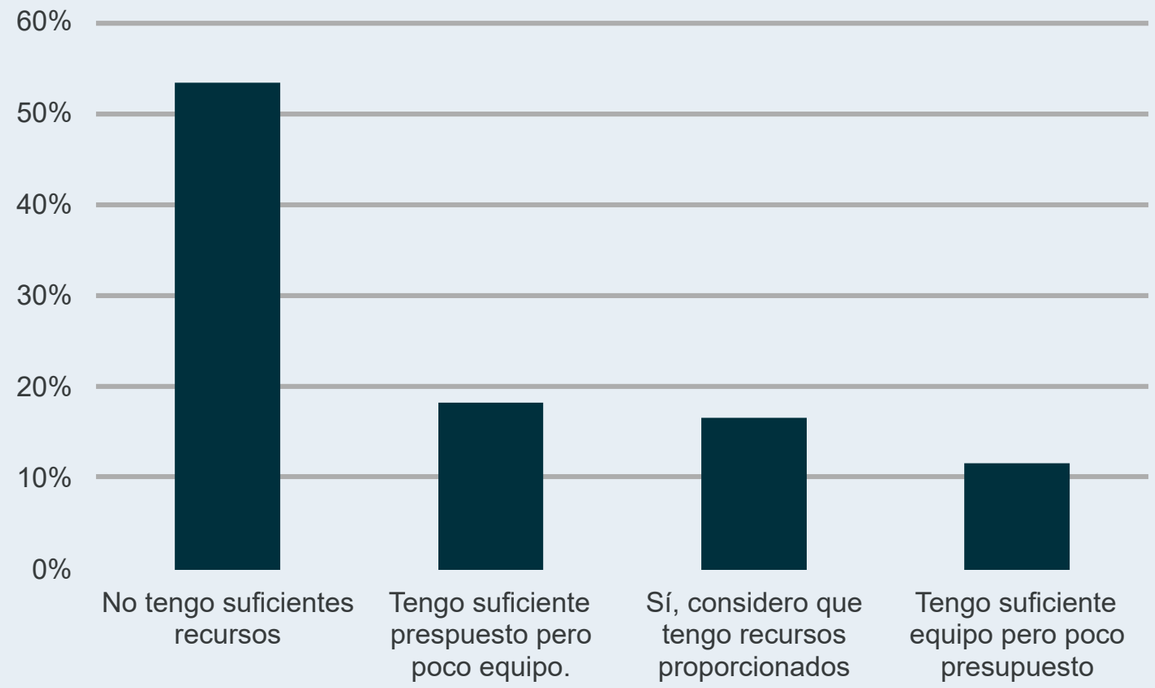
Evaluación de Obstáculos Internos y Actores Críticos en la Gestión del RGPD

Ante la pregunta a los Delegados de Protección de Datos de si cuentan con los recursos suficientes para el cumplimiento de sus obligaciones, **un 53% considera que no, siendo un aspecto limitante a la hora de afrontar una implementación efectiva de la normativa de Privacidad y Protección de Datos.**

Destaca el descenso considerable de las empresas que indican contar con recursos proporcionados al 17%, en comparación con el año 2024 en el que esta cifra se situaba por encima del 30%.

Estos datos reflejan que, pese a que las funciones y compatibilidad con otras funciones de los DPOs han aumentado, los recursos disponibles para hacer frente a esa nueva demanda no lo han hecho proporcionalmente, acarreando ese riesgo correspondiente de no poder cumplir con todas las obligaciones del cargo de Delegado de Protección de Datos.

Ilustración 13: **Percepción sobre la suficiencia de recursos**

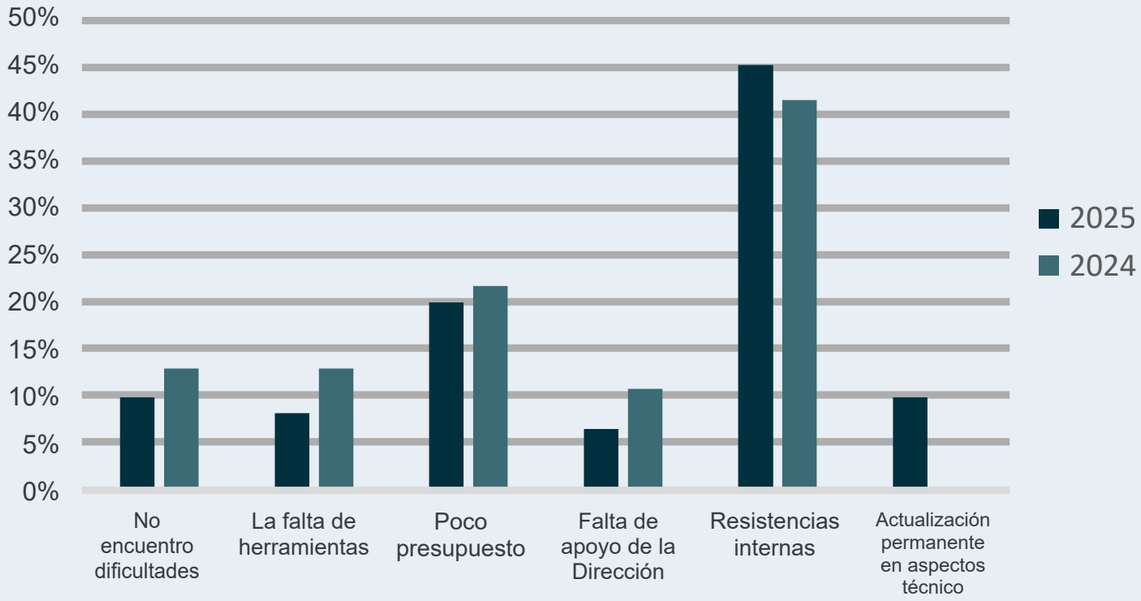


Analizando el detalle de aquellas dificultades que afrontan los DPOs en su día a día se materializa un año más como principal las resistencias internas, seguido de la falta de presupuesto, evidenciando la necesidad de seguir trabajando en esa adopción de una cultura de cumplimiento normativo en todos los niveles de la organización.

Como principal novedad de este año, el 10% de los encuestados hace referencia como principal dificultad a la necesidad permanente de estar al día con los aspectos y avances técnicos de las tecnologías emergentes y que, en muchas ocasiones, requieren de formación específica sin la cual no es posible identificar los riesgos en materia de Privacidad y Protección de Datos.

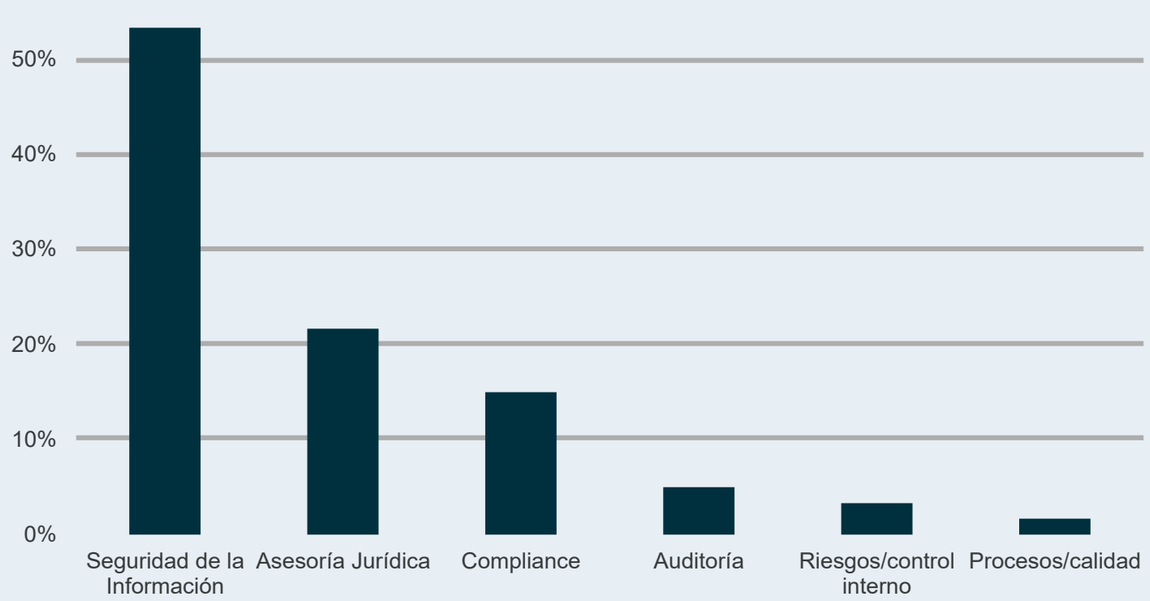
Por otro lado, se reduce casi a la mitad aquellos que indican que hay una falta de apoyo de la Dirección, situándose en un 7% en 2025, consolidándose el hecho de que los aspectos de privacidad están en el foco.

Ilustración 14: **Evolución de la principal dificultad que encuentran los DPOs para llevar a cabo su labor**



Por último, se ha analizado en 2025 qué áreas dentro de la organización son las que más se involucran en el cumplimiento del RGPD junto al DPO, **destacando notablemente con más de un 50% el área de Seguridad de la Información, seguido por Asesoría Jurídica y Compliance, con un 21% y 15% respectivamente.** Estos datos reflejan, cómo la evolución tecnológica y la necesaria evaluación de los riesgos requiere de la implantación de nuevas medidas técnicas y organizativas y procedimentales para garantizar la integridad, confidencialidad y disponibilidad de los datos dentro de las organizaciones, derivando en una estrecha relación entre las áreas de Seguridad y Privacidad.

Ilustración 15: **Áreas más involucradas en el cumplimiento del RGPD junto al DPO**



Otras áreas a las que hacen mención las empresas encuestadas como las más involucradas, aunque en menor medida, serían las de **control interno, auditoría y procesos.**

04

Modelo de madurez de cumplimiento RGPD

4.1.

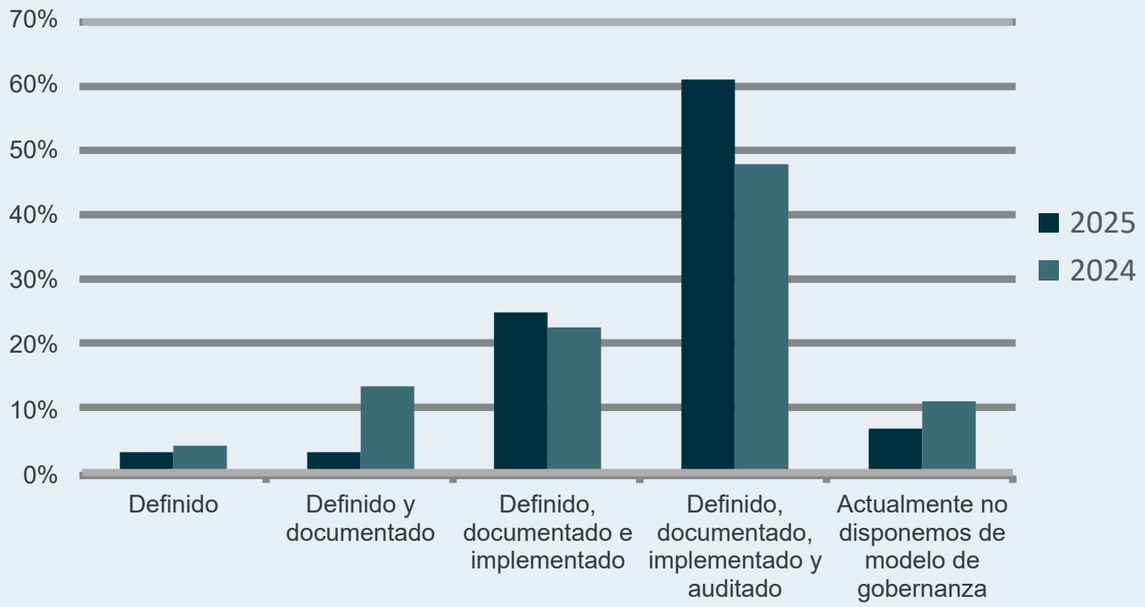
Nivel de Madurez del **Sistema de Gestión de Protección de Datos**

La madurez de un sistema de gestión de protección de datos refleja hasta qué punto una organización ha integrado de forma efectiva la privacidad en su cultura, sus procesos y su toma de decisiones. **Evaluar este grado de madurez permite identificar el nivel real de cumplimiento con el RGPD y otras normativas aplicables, medir la consistencia de las prácticas implantadas y detectar áreas de mejora para avanzar hacia un modelo más robusto y proactivo.** Con esta pregunta se busca conocer si la organización cuenta simplemente con medidas básicas y reactivas, o si, por el contrario, dispone de un enfoque estructurado, sistemático y orientado a la mejora continua en materia de protección de datos.

El análisis de las respuestas a la pregunta sobre el grado de madurez del sistema de gestión de protección de datos en las organizaciones participantes revela una clara tendencia hacia modelos avanzados y auditados. Estos resultados reflejan un grado de madurez elevado en la muestra, con una mayoría que ha superado la mera formalización documental y ha avanzado hacia la verificación y mejora continua mediante auditorías. Este dato es coherente con la alta proporción de organizaciones que afirman realizar auditorías periódicas en otras preguntas del estudio.

No obstante, la existencia de un grupo minoritario sin modelo de gobernanza constituye un riesgo estructural, ya que estas organizaciones carecen de los elementos básicos para garantizar la protección de datos de forma sistemática y sostenible. Para este segmento, se recomienda establecer unos mínimos de entrada (política, roles, inventario y ciclo de revisión) y un plan de implantación progresivo.

Ilustración 16: **Nivel de madurez del Sistema de Gestión de Protección de Datos**



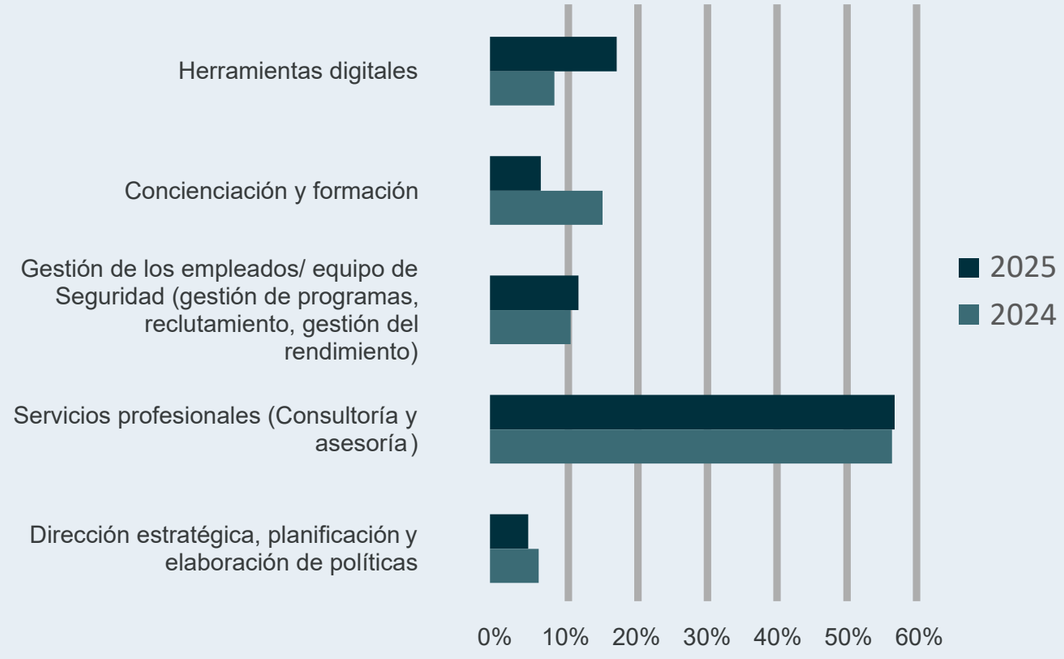
La comparación entre los datos de 2025 y 2024 muestra una evolución positiva en la madurez de los sistemas de gestión de protección de datos.

En 2025, el porcentaje de organizaciones con un sistema definido, documentado, implementado y auditado sube al 61%, frente al 48% del año anterior. También aumenta ligeramente el grupo que declara tener el sistema definido, documentado e implementado (25% en 2025 frente al 23% en 2024).

Por el contrario, disminuyen tanto los niveles intermedios (“definido” y “definido y documentado”) como el porcentaje de organizaciones que no disponen de modelo de gobernanza, que pasa del 11% al 7%.

Estos datos reflejan una consolidación de las prácticas avanzadas y una reducción de los grupos menos maduros, lo que indica una tendencia clara hacia la profesionalización y la mejora continua en la gestión de la privacidad. La auditoría y la revisión periódica se afianzan como elementos diferenciales, mientras que el riesgo asociado a la ausencia de modelo de gobernanza se reduce, aunque sigue presente en una minoría de organizaciones.

Ilustración 17: **Distribución presupuestaria por áreas de inversión estratégica**



4.2.

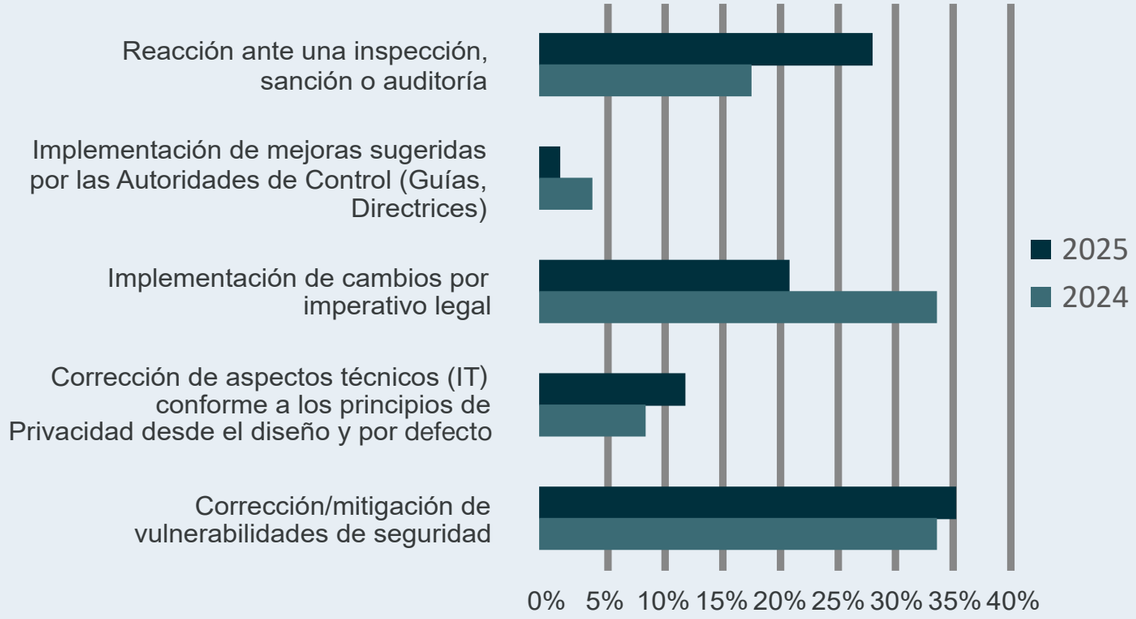
Asignación Presupuestaria y Priorización de Inversiones en Cumplimiento

La gestión del presupuesto en materia de Privacidad y Protección de Datos es un reflejo directo de las prioridades y el enfoque estratégico de las organizaciones ante los retos regulatorios y operativos.

Las preguntas 17 y 18 del cuestionario abordan, respectivamente, en qué actividades se concentra la mayor inversión económica y cómo se priorizan los recursos cuando surge una necesidad imprevista. Analizar estas cuestiones permite entender no solo dónde se sitúan los principales focos de gasto (como servicios profesionales, tecnología, formación o gestión interna), sino también cómo reaccionan las organizaciones ante situaciones de urgencia o cambios normativos inesperados.

Esta doble perspectiva ofrece una visión integral sobre la madurez presupuestaria y la capacidad de adaptación del sistema de cumplimiento en privacidad.

Ilustración 18:
Análisis comparativo de prioridades operativas frente a imprevistos presupuestarios



La lectura conjunta de ambas cuestiones revela una estrategia organizativa que combina la continuidad en la dependencia de servicios profesionales externos, motivada por esa falta de perfiles tan especializados en las organizaciones, con un refuerzo progresivo de la inversión en tecnología. El gasto preventivo y estructural, como la formación o la planificación estratégica, pierde protagonismo frente a la necesidad de dotarse de herramientas y capacidad de reacción ante riesgos inmediatos. Además, la creciente importancia de la respuesta a inspecciones y sanciones como prioridad presupuestaria refleja un entorno de cumplimiento cada vez más exigente, donde la exposición a la supervisión y el coste de su gestión se convierten en factores clave para la toma de decisiones.

Este enfoque pone de manifiesto que las organizaciones están adaptando sus prioridades para gestionar con mayor eficacia los incidentes y los nuevos requerimientos regulatorios (especialmente ante la llegada de tecnologías emergentes como la inteligencia artificial, que introduce riesgos que deben abordarse con rapidez). Aunque la tecnificación y la capacidad de respuesta aportan ventajas en resiliencia y adaptación, esto no implica una renuncia a la prevención o a la cultura interna de privacidad, ya que muchas actividades como la formación o la aplicación de privacy by design están cada vez más integradas en los procesos habituales.

Por tanto, el reto para los próximos años será encontrar un equilibrio entre la capacidad de respuesta ante riesgos emergentes y el refuerzo continuo de las competencias internas y la prevención (de modo que la gestión de la privacidad se mantenga integrada de forma estructural en la estrategia y los procesos de la organización).

4.3.

Automatización y Digitalización de Procesos de Cumplimiento

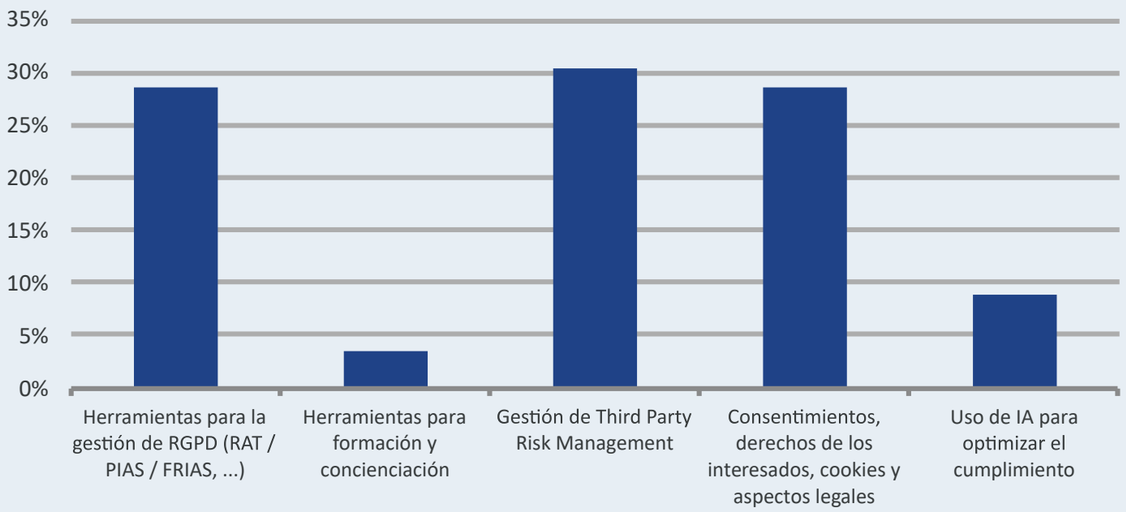
Los resultados muestran que las herramientas para la gestión de RGPD, la gestión de Third Party Risk Management y los consentimientos, derechos de los interesados, cookies y aspectos legales son las áreas de acción consideradas que requieren un mayor nivel de automatización mediante el uso de herramientas tecnológicas, con un porcentaje similar todas ellas.

Todo esto se deduce por el aumento de volumen de solicitudes de derechos de interesados y solicitudes/modificaciones de consentimientos que hacen necesaria un nivel considerable de automatización tecnológica en los procedimientos RGPD para poder dar cumplimiento en tiempo y forma.

De igual forma, el creciente uso por parte de las organizaciones de las cookies para obtener datos útiles, requiere una gestión automatizada para poder sacar conclusiones útiles y gestionar el volumen de información.

Por el contrario, las herramientas para formación y concienciación, y el uso de IA para optimizar el cumplimiento son consideradas como áreas de acción que requieren menor nivel de automatización mediante el uso de herramientas tecnológicas. A pesar de la importancia que está adquiriendo la IA en las entidades, podríamos entender que este bajo porcentaje se debe a la falta de madurez todavía de algunos de los procesos que se traduce en la imposibilidad de poder plantearse la aplicación de la IA en los mismos, así como la incipiente aparición de soluciones de IA para facilitar la labor de DPOs.

Ilustración 19: **Demandas de Digitalización y Automatización en Procesos Organizativos**



4.4.

Líneas de Acción con **Mayor Madurez en la Organización**

Gestión de los derechos y de la información figura en cabeza con 36%. Consideramos que este es el resultado del incremento en el último año del volumen de solicitudes de gestión de derechos por parte de los interesados y consecuente necesidad de las entidades de reforzar estos procedimientos para dar cumplimiento al gran volumen de solicitudes en tiempo y forma.

A continuación, figura el Registro de actividades de tratamiento, Procedimiento de Privacy By Design y la Firma de contratos de encargo de tratamiento con proveedores, líneas de acción que, desde la implementación de GDPR en España, resulta evidente que han sido objeto de mejora en las entidades de acuerdo con los criterios y guías que ha ido estableciendo la AEPD durante estos años, logrando actualmente un nivel de madurez superior al de hace unos años.

Ilustración 20: **Madurez Organizativa por Línea de Acción Implementada**

Concienciación y formación, Supervisión y accountability, Transferencias internacionales, Análisis de riesgos y evaluaciones de impacto son las líneas de acción consideradas con un menor nivel de madurez.

Resulta llamativo que figure el análisis de riesgos y evaluaciones de impactos, teniendo en cuenta el criterio de la AEPD y la importancia que otorga al hecho de que las entidades efectúen evaluaciones de impacto y análisis de riesgos antes de efectuar implementaciones. Asimismo, resulta sorprendentemente llamativo el porcentaje de 0,0% en las transferencias internacionales, dado que nos encontramos actualmente en un entorno globalizado en el que muchas entidades tienen proveedores tecnológicos en terceros países. Los resultados evidencian que estas áreas requieren mejoras para minimizar los riesgos.

4.5.

Áreas Organizativas Implicadas en la Ejecución del Cumplimiento

Los resultados muestran que el área de IT e Innovación, como el año pasado, tiene la mayor intervención en la implementación de las líneas de acción relacionadas con la protección de datos, con un 46%. Esto implica que para que los desarrollos de los procesos de las entidades puedan contar con las medidas técnicas necesarias para garantizar la privacidad, seguridad y, en general, el cumplimiento de la normativa de protección de datos resulta fundamental el papel de la tecnología.

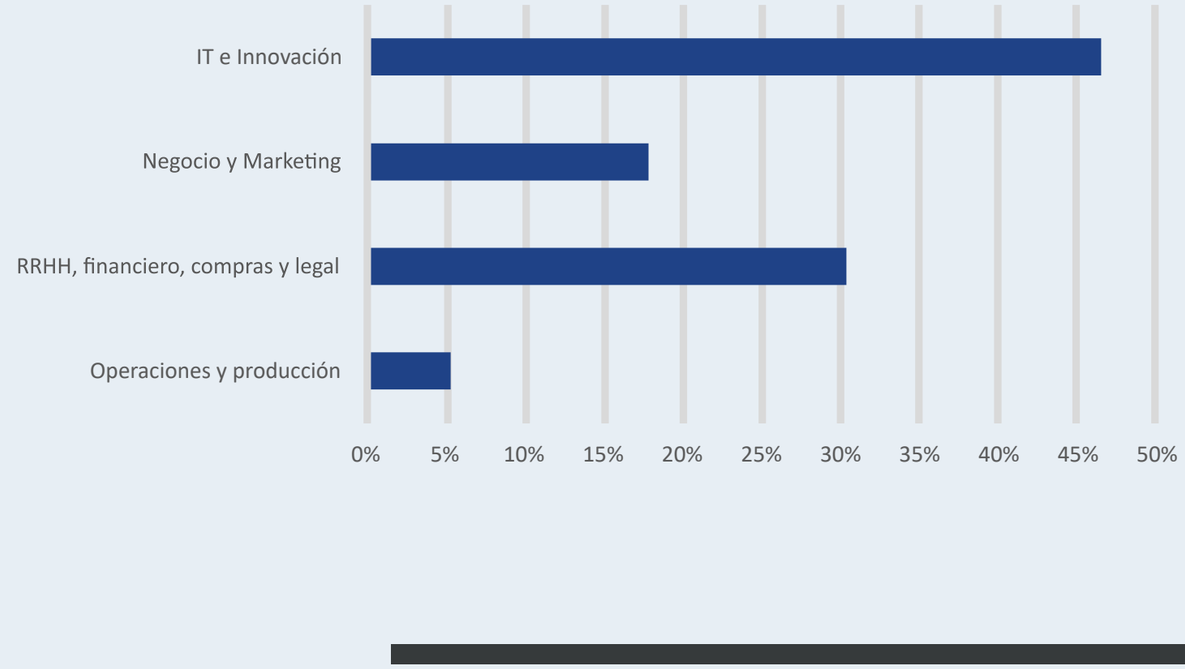
En este sentido, y dado, el incremento de volumen de las solicitudes de ejercicio de derechos GDPR, se confirma que las áreas que los gestionan tienden a buscar mejoras en sus procesos e implementar procedimientos que agilicen la gestión, necesitando la colaboración de las áreas de TI.

RRHH, financiero y legal, así como negocio y marketing, muestran un nivel moderado de involucración, obteniendo un porcentaje de 30%. En este punto, nos parece importante hacer mención específica al Departamento Legal, considerando que en muchas entidades el Departamento Legal interviene y lidera cada una de las líneas de acción recogidas en la pregunta anterior. Si bien el departamento de IT e Innovación es quien implementa técnicamente los desarrollos tecnológicos, el Departamento Legal interviene en todas las líneas de acción, bien sea directamente como una de sus funciones atribuidas expresamente, o bien desde una perspectiva de control para garantizar que las diferentes acciones/procedimientos de la compañía se encuentren en conformidad con la normativa de protección de datos.

En contrapartida, el Área de Operaciones continúa siendo el área de menos intervención decrementando el porcentaje respecto del año pasado y situándose en un 5%.

En cualquier caso, lo que resulta evidente es que estos resultados siguen mostrando la necesidad de una coordinación y colaboración entre las diferentes áreas de las compañías para la implementación y control de las diferentes líneas de acción en materia de protección de datos.

Ilustración 21:
Áreas con Mayor Nivel de Participación en la Ejecución de las Líneas de Acción

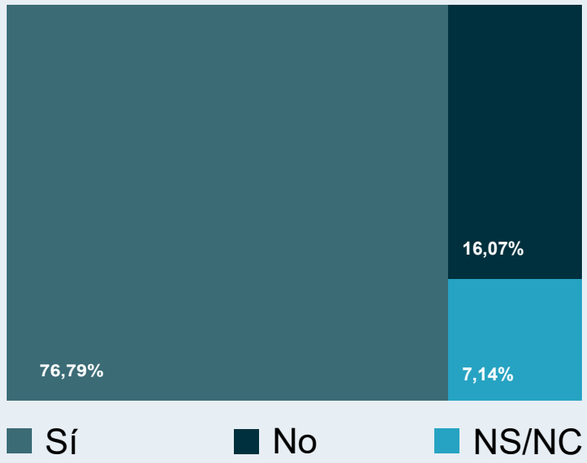


4.6.

Auditorías de Cumplimiento: Existencia, Alcance y Enfoque

La información recabada en el ejercicio 2025 evidencia la consolidación de la auditoría de protección de datos como una práctica habitual en las organizaciones, reflejando un grado de madurez significativo en la gestión del cumplimiento del RGPD. Tras el crecimiento sostenido observado en años anteriores, la ejecución formal de auditorías se mantiene en niveles elevados, lo que confirma su integración como elemento estructural del sistema de gobierno de la privacidad.

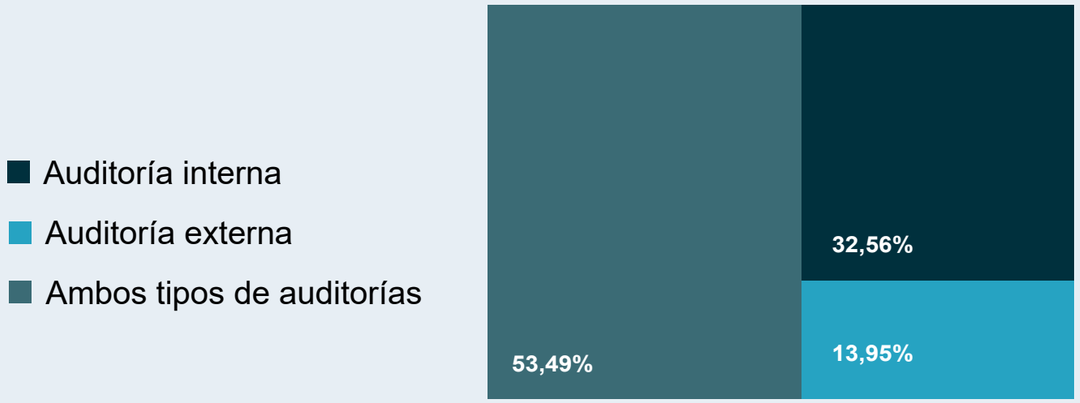
Ilustración 22:
Adopción de Procedimientos Formales de Auditoría en las Organizaciones



No obstante, se mantienen diferencias relevantes en función del sector de actividad y del tamaño de la organización. Los sectores más regulados y con mayor exposición al riesgo, como el financiero, tecnológico y sanitario, presentan una implantación más homogénea, mientras que en sectores menos regulados y en organizaciones de menor tamaño aún se identifican casos sin auditorías formalizadas. Este escenario pone de manifiesto que, pese al alto grado de implantación, persiste margen de mejora para lograr una adopción plenamente transversal.

El análisis del tipo de auditoría realizada en 2025 muestra la continuidad del modelo predominante en ejercicios anteriores, caracterizado por el predominio de la auditoría interna, complementada en un número significativo de casos por auditorías externas. Esta configuración confirma que la auditoría interna sigue siendo el principal mecanismo de control del cumplimiento del RGPD en la mayoría de las organizaciones.

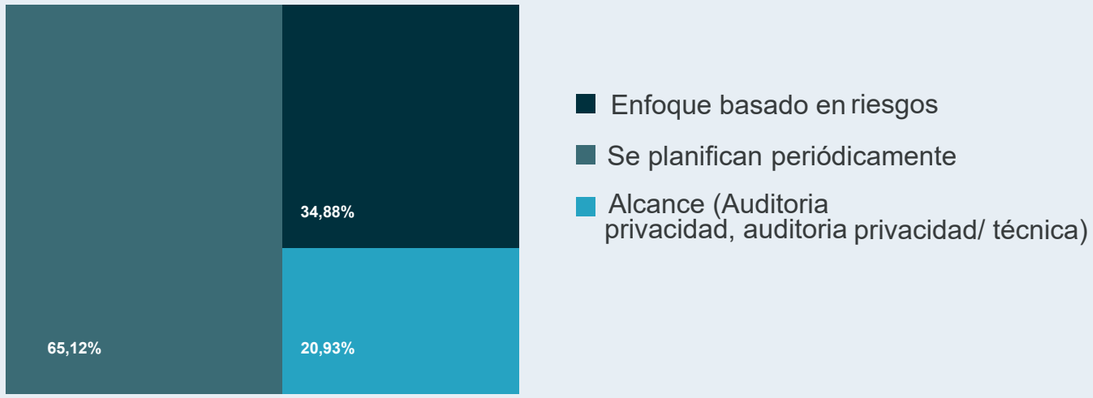
Ilustración 23:
Distribución de Tipos de Auditoría en Entidades que Ejecutan Procesos Formales



De manera coherente con la evolución documentada entre 2022 y 2024, la auditoría externa mantiene un papel complementario, especialmente en sectores más regulados, como el financiero, tecnológico y sanitario, donde responde a exigencias regulatorias, de certificación o de clientes. Asimismo, las auditorías externas continúan siendo menos frecuentes en empresas de menor tamaño, previsiblemente por limitaciones de recursos o menor necesidad de validaciones formales. En conjunto, el patrón observado refleja la estabilidad del modelo mixto, sin cambios estructurales relevantes.

El criterio aplicado para la ejecución de auditorías en 2025 mantiene una línea de continuidad con los ejercicios precedentes, situando la planificación periódica como el enfoque mayoritario. Este patrón confirma la adopción de un enfoque estructurado y sistemático del control del cumplimiento del RGPD, basado en ciclos regulares de revisión.

Ilustración 24:
Principios de Planificación y Alcance en los Procesos de Auditoría Organizacional



De forma consistente con los años anteriores, el enfoque basado en riesgos continúa teniendo una presencia minoritaria, concentrándose principalmente en sectores más regulados, como el financiero y el sanitario, así como en organizaciones de mayor tamaño. El criterio de auditoría por alcance específico se mantiene como una práctica complementaria, especialmente en grandes empresas. En términos generales, no se identifican cambios estructurales en los criterios de ejecución de auditorías respecto a ejercicios previos.

4.7.

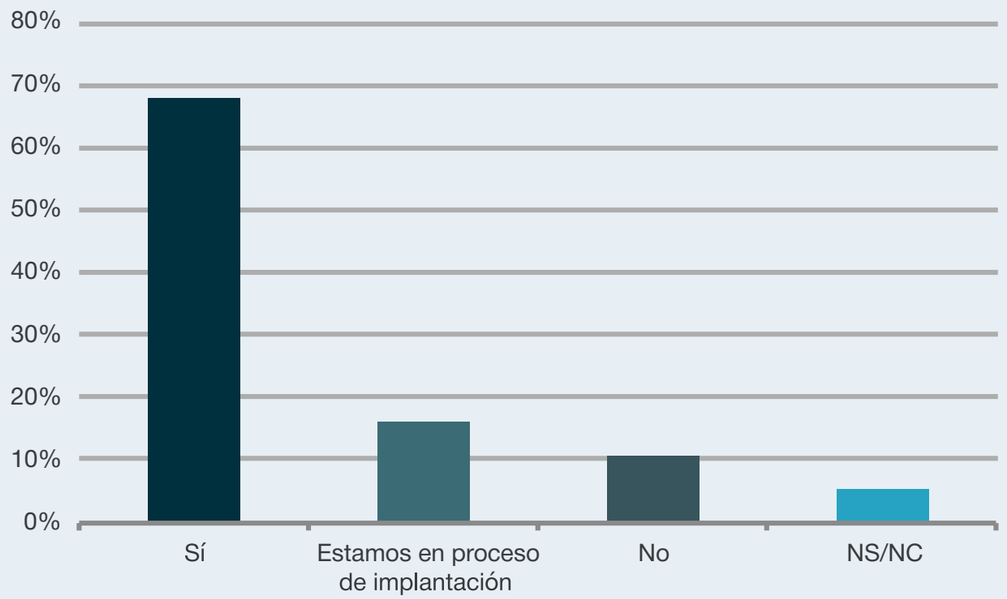
Gestión de Terceros y Diligencia Debida

En el ámbito de la diligencia debida en privacidad, los resultados correspondientes a 2025 ponen de relieve una evolución menos homogénea en comparación con otros mecanismos de control del RGPD. Si bien una parte significativa de las organizaciones declara disponer de procedimientos de diligencia debida antes de la firma de contratos de encargo, persiste un porcentaje relevante de entidades que se encuentran aún en proceso de implantación.

Esta situación es coherente con la evolución observada entre 2022 y 2024, en la que la adopción de estos procedimientos ha mostrado una mayor sensibilidad a factores organizativos, como la disponibilidad de recursos, la priorización interna o la integración de la diligencia debida en otros sistemas corporativos, lo que puede afectar a su visibilidad como proceso específico.

En conjunto, la diligencia debida continúa identificándose como uno de los principales ámbitos de mejora para avanzar hacia un modelo de madurez más consistente en la aplicación del RGPD.

Ilustración 25:
Implantación de Procedimientos de Evaluación de Terceros en Materia de Privacidad



05

Registro de indicadores
para análisis y benchmarking

5.1.

Inventario y Ciclo de Vida del Registro de Actividades de Tratamiento (RAT)

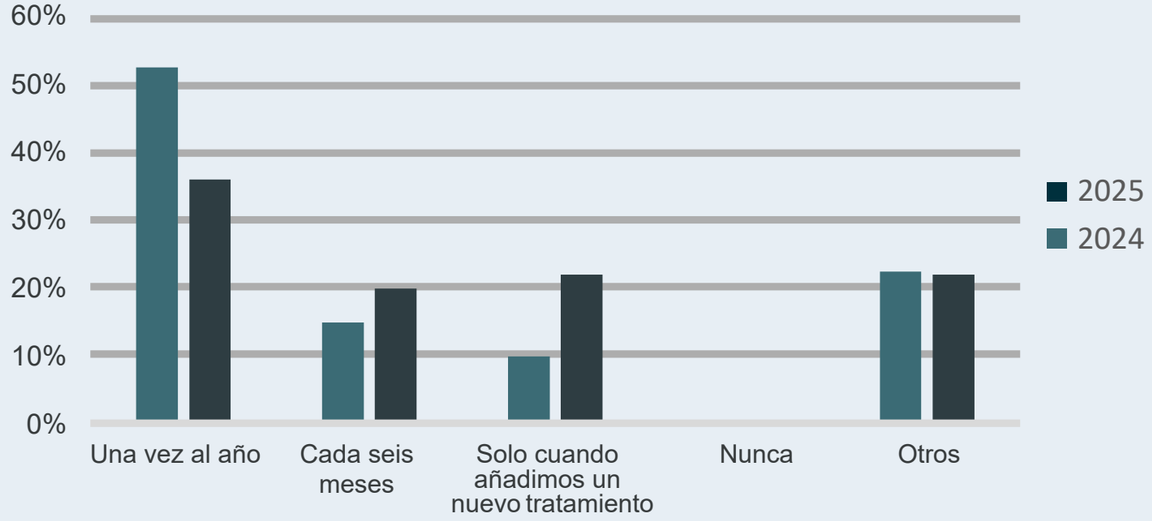
Ilustración 26: **Evolución del volumen de tratamientos de datos**

Comparando 2025 con el año anterior, observamos que el gráfico no experimenta grandes cambios en cuanto a la distribución de tratamientos que se encuentran registrados. Las mayores variaciones se encuentran en el tramo de 0 a 50 tratamientos, que al haber aumentado la muestra recogida en este año ha hecho que el porcentaje se reduzca, aun siendo la cantidad de tratamientos registrada similar en ambos ejercicios. El tramo de mayor cambio es el de 501 a 1000 tratamientos, donde se visualiza un aumento de 4.5 puntos, lo que nos lleva a pensar que las organizaciones tienden a registrar tratamientos de datos cada vez más especializados y menos generales lo que hace que el número de tratamientos aumente.

Las conclusiones que podemos obtener es que el grueso de la muestra se encuentra entre los 101 y 500 tratamientos registrados donde se ubican organizaciones de todos los sectores, pero con un predominio de las administraciones públicas. El 84% de los datos recogidos indican que las entidades no superan los 500 tratamientos registrados.

En cuanto a las organizaciones con mayor número de tratamientos registrados, los que tienen censados más de 1000 tratamientos obedecen a entidades con más de 5000 empleados enmarcadas en el sector de tecnología y comunicaciones y las que aportan entre 501 y 1000 tratamientos pertenecen mayoritariamente al sector financiero. Es de destacar que en ambos casos, los DPO de estas entidades con mayor número de tratamientos son internos y con una dedicación exclusiva y es en estos tramos en los que observamos un aumento más notable, luego podemos concluir que la tendencia en grandes entidades es a tener cada vez más tratamientos censados.

Ilustración 27:
Frecuencia de actualización del Registro de Actividades de Tratamiento (RAT)



La tendencia a la hora de actualizar el Registro de Actividades de Tratamiento (en adelante "RAT") nos indica que han aumentado las organizaciones que actualizan el RAT cada seis meses y que han disminuido las que lo ajustan de manera anual, lo que da a entender que la actualización es constante y se considera necesario llevar a cabo su actualización con más frecuencia para poder disponer de un RAT lo más actualizado posible, así mismo también han aumentado significativamente las entidades que lo actualizan cuando añaden un nuevo tratamiento, lo que nos lleva a pensar que la actualización del RAT es un tema que está presente en la dinámica de modificación de los proyectos de las organizaciones dado que cada vez que se añade un nuevo tratamiento se plantea la necesidad de actualizar el RAT.

5.2.

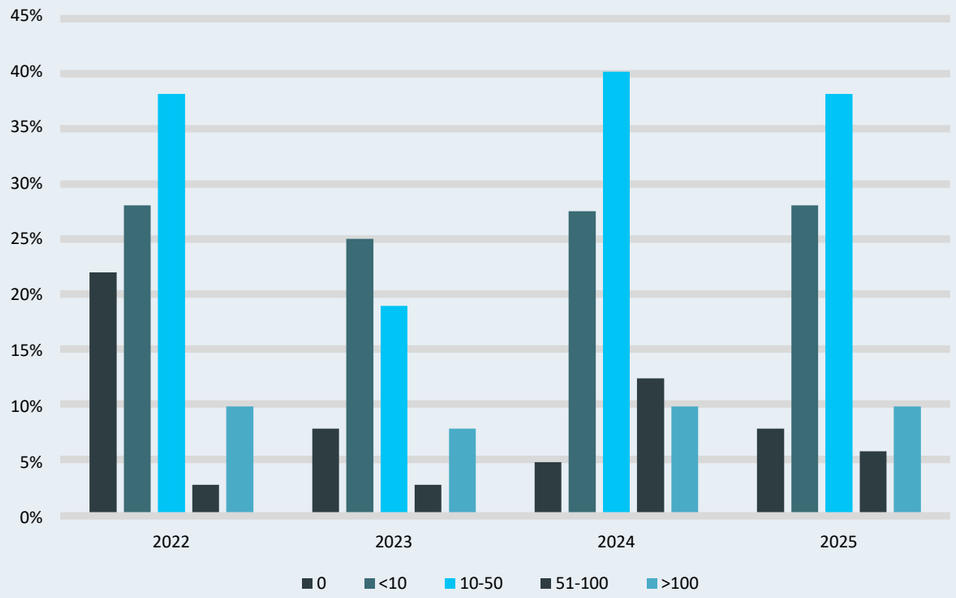
Evaluaciones de Impacto (EIPD/DPIA): Capacidad y Ritmo de Ejecución

Aunque las PIAs se han consolidado como una herramienta estructural del RGPD en las organizaciones, aún no se consideran un sistema integral de gestión del riesgo en materia de privacidad. Esto se refleja en las respuestas de las entidades, ya que solo un 4% identifica el análisis de riesgos y las evaluaciones de impacto como su área de mayor madurez.

El porcentaje de evaluaciones de impacto en organizaciones que no ha realizado ninguna PIA a lo largo de los años sigue siendo elevado, aunque menor, cuando comparamos con los resultados del tercer estudio de privacidad realizado en 2022. La ausencia de evaluaciones de impacto no significa ausencia de riesgos, sino falta de control sobre este riesgo.

Este resultado puede estar relacionado con una subestimación del riesgo por parte de las organizaciones, o con la realización de análisis informales en lugar de PIAs formalizados. Sin embargo, en el contexto tecnológico actual, resulta difícil justificar la inexistencia de tratamientos con alto nivel de riesgo.

Ilustración 28:
Análisis Comparativo del Número de PIAs Activos (2022–2025)



La ejecución de menos de 10 PIAs se mantiene estable a lo largo de los años, como se puede identificar en la gráfica.

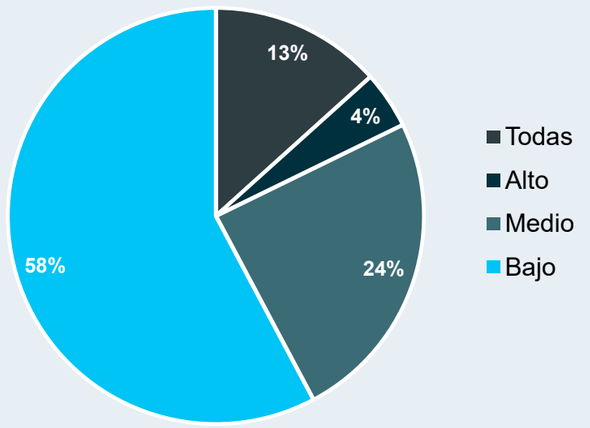
En 2024 se observa un pico significativo en el tramo de 51 a 100 PIAs, que ha vuelto a decaer en 2025, y también podemos observar picos en volúmenes altos, lo cual podría dar respuesta que el PIA es la herramienta clave para abordar o regularizar situaciones complejas.

El hecho de que tan solo un 10% de las organizaciones realicen más de 100 PIAs (dato que se mantiene estable con los años), pone de relieve que la DPIA sigue siendo percibida como costosa y compleja, a pesar de ser fundamental para demostrar la diligencia proactiva del responsable, y es uno de los instrumentos que puede ayudar a demostrarlo.

La evaluación de impacto es el instrumento que transforma el cumplimiento normativo en una gestión real del riesgo para los derechos y libertades fundamentales.

Nuevamente, siguiendo la tendencia de años anteriores, los sectores con más evaluaciones de impacto son el sector Sanitario junto con el de Servicios Financieros, por otro lado, los sectores que menos evaluaciones de impacto realizan son Administraciones públicas, Industria, construcción, retail y distribución.

En relación con la revisión anual de las evaluaciones de impacto, observamos que el 13% de las organizaciones ha actualizado todas sus PIAs, mientras que un 4% ha actualizado más del 75% de sus tratamientos.



Esto indica un nivel de madurez importante en aquellas organizaciones que consideran que las PIAs deben revisarse y actualizarse cuando sea necesario, y no ser documentos estáticos.

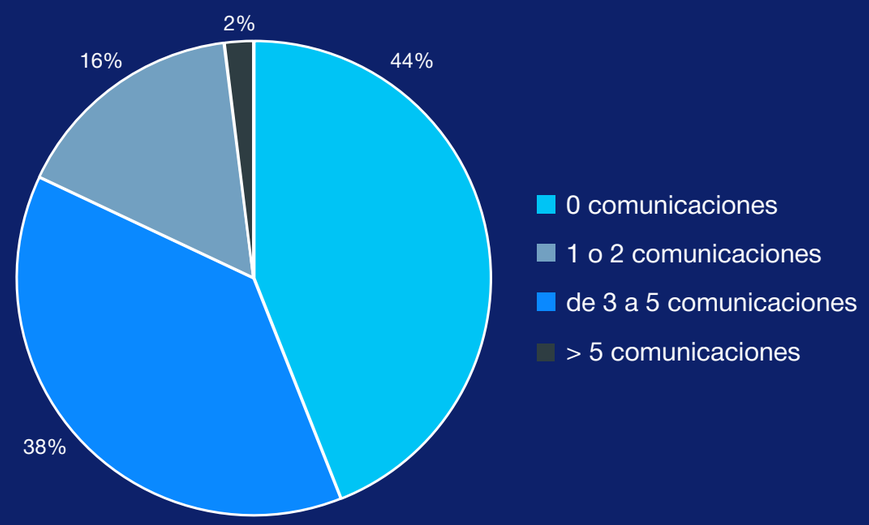
Además, el 24% de las organizaciones ha informado que ha actualizado al menos el 40% de sus evaluaciones de impacto durante este año.

Ilustración 29:
Distribución del Nivel de Riesgo de las PIAs Realizadas en 2025

5.3.

Gestión de **Incidentes y Notificaciones** a la AEPD

Ilustración 30:
Frecuencia de notificaciones de violaciones de datos personales remitidas a la AEPD



Según nos muestra la figura anterior, alrededor de la mitad de las organizaciones censadas en este ejercicio (44%) no han comunicado ninguna violación a la Agencia Española de Protección de Datos (en adelante AEPD) y un porcentaje muy elevado (38%) sólo han reportado una o dos comunicaciones durante el 2025, con lo que podemos concluir que en general hay muy pocas comunicaciones de violaciones a la AEPD, dado que el 82% de la muestra no ha comunicado más de 2 violaciones.

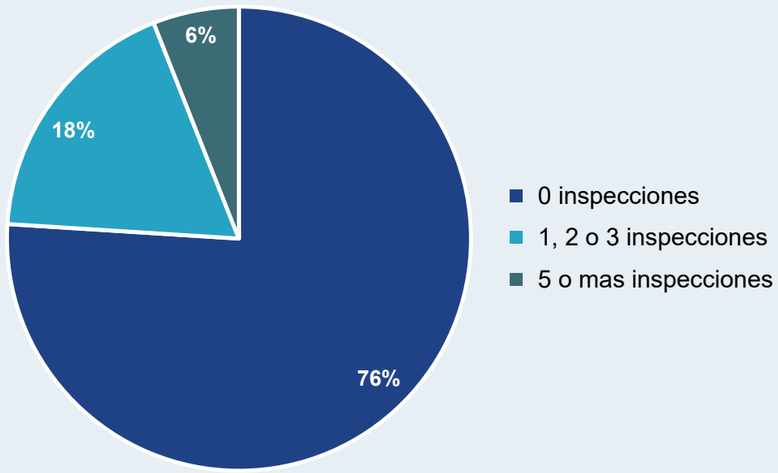
Los datos recogidos en este ejercicio son muy similares a los obtenidos el año anterior, salvo el tramo que refleja que un 2% de las organizaciones registradas en 2025 han comunicado más de 5 violaciones, valor que el año pasado no se dio en los resultados obtenidos.

Por ahondar en el detalle de las organizaciones que han declarado más de 5 violaciones, los sectores a los que pertenecen son: las Administraciones Públicas, Consumo y al sector sanitario.

Como conclusión, valorando la gráfica en su totalidad, se aprecia una baja notificación por parte de las organizaciones que puede estar respaldada por la reserva a notificar ante el miedo a posibles sanciones e inspecciones por parte de la Agencia o por un desconocimiento de los criterios que obligan a reportar.

También puede ser el fruto de una gestión exitosa de la seguridad de la entidad, pero en cualquier caso es recomendable que las organizaciones revisen sus procedimientos internos para asegurarse de que identifican y comunican correctamente las violaciones de datos cuando sea necesario.

Ilustración 31: **Distribución de inspecciones realizadas por la AEPD en las organizaciones encuestadas**



La información que otorga el gráfico anterior nos hace ver que el 76% de las organizaciones que han participado en esta encuesta no han recibido una inspección por parte de la AEPD en el ejercicio 2025, lo que teniendo en cuenta que la mayoría de las inspecciones se desencadenan por una reclamación o denuncia previa o por una detección de vulnerabilidades en los métodos de aplicación de seguridad tecnológica, nos puede llevar a pensar que las entidades censadas presentan un robusto diseño en protección de datos.

Cierto es que también existe un porcentaje mucho menor de inspecciones que se realizan desde la AEPD de manera aleatoria y que podrían enmarcarse en la figura del 18% y que responden a entidades del sector tecnológico.

En cuanto al 6% de entidades que han recibido cinco o más inspecciones, es probable que estos casos estén vinculados a actuaciones de seguimiento realizadas por la AEPD a organizaciones que previamente habían notificado alguna violación de datos.

El objetivo de estas revisiones adicionales suele ser verificar que las vulnerabilidades o deficiencias identificadas en incidentes anteriores han sido corregidas adecuadamente. De hecho, en la muestra analizada, este grupo coincide mayoritariamente con organizaciones que habían declarado violaciones de datos y que, posteriormente, fueron objeto de inspecciones sucesivas por parte de la Agencia.

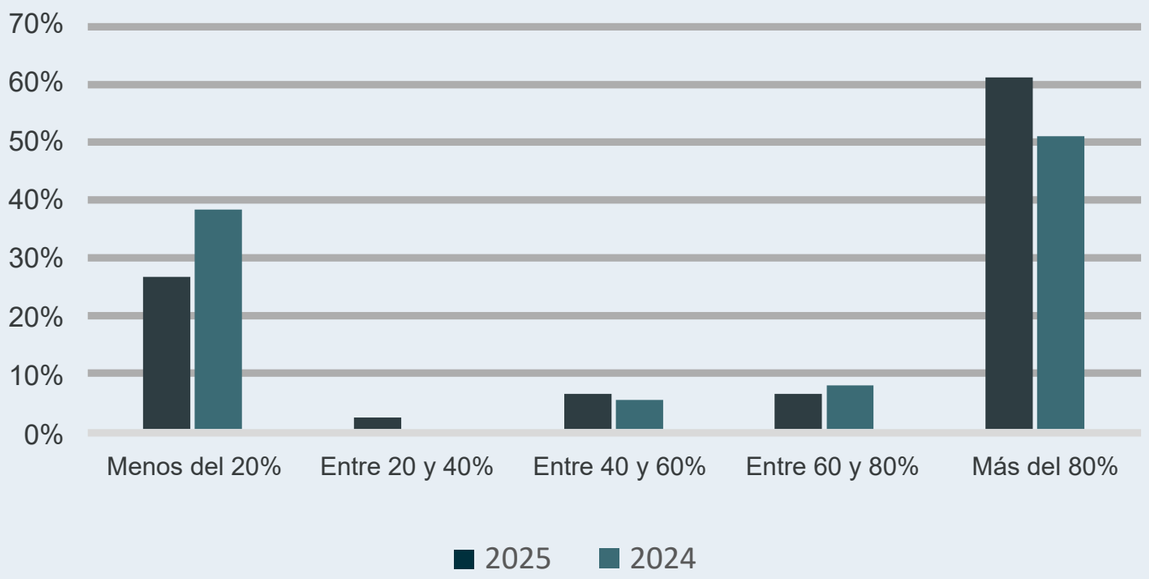
Como ya indicamos en el punto sobre violaciones, las entidades que se han visto revisadas por la AEPD en más de 5 ocasiones pertenecen a los sectores sanitario, de las administraciones públicas y consumo.

5.4.

Canal de Reclamaciones y Escalado Regulatorio

En la comparativa que se puede apreciar en la figura adjunta, llama la atención la variación en los tramos de los extremos, por un lado en el ejercicio 2025 han disminuido las organizaciones que sitúan en un 20% el éxito de su gestión de las reclamaciones que evitan que lleguen a ser una denuncia ante la AEPD y por otro lado han aumentado considerablemente aquellas organizaciones que sitúan su éxito en un 80%, lo que nos lleva a pensar que la labor de los DPO en este aspecto indica una gran capacidad de resolución interna y gestión efectiva de las reclamaciones con un alto incremento de éxitos en el último año, siempre impulsado y soportado desde las organizaciones implicadas.

Ilustración 32: **Proporción de reclamaciones gestionadas por el DPO que no derivan en denuncia ante la AEPD**



5.5.

Transferencias Internacionales: Mecanismos de Garantía y Adecuación

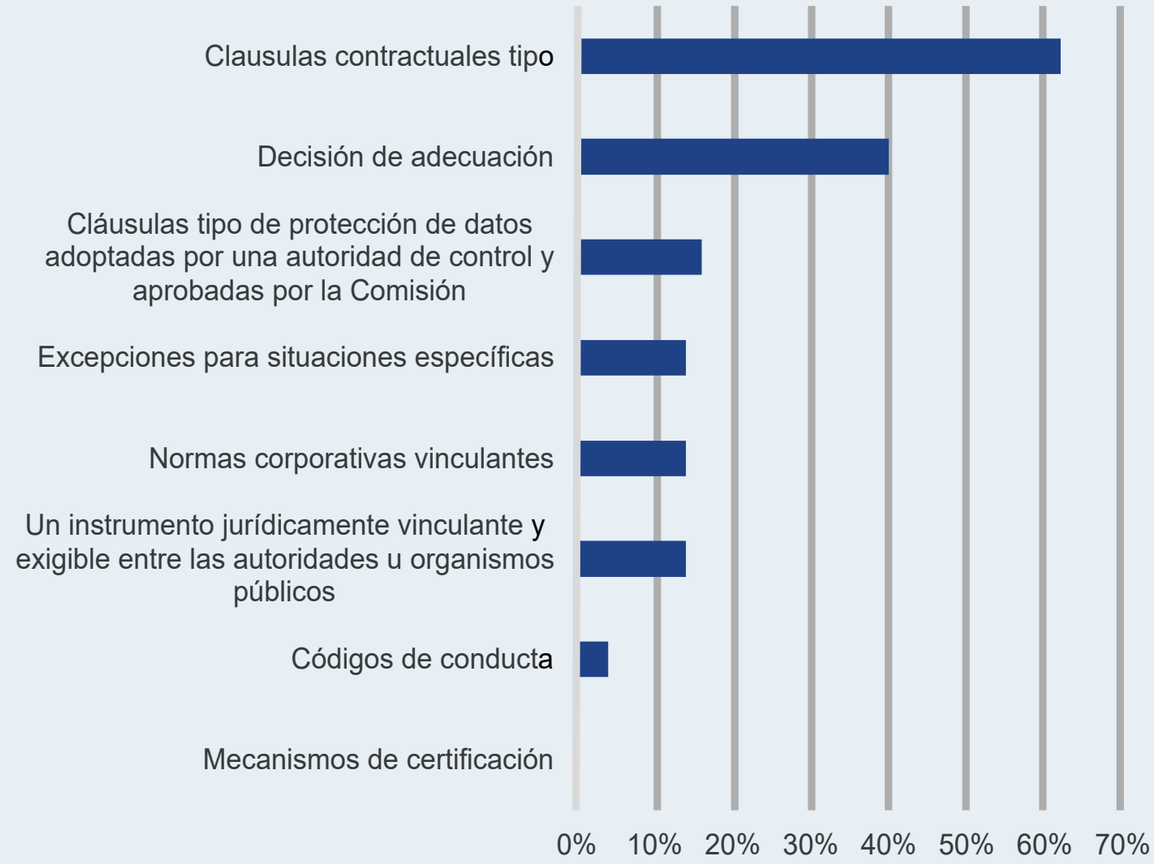
Según se puede identificar siguiendo los resultados de la encuesta, las organizaciones tienden a priorizar los mecanismos jurídicos disponibles, gestionando las transferencias internacionales desde una perspectiva contractual. Existe una clara preferencia por las Cláusulas Contractuales Tipo como principal solución, junto con un uso significativo de las decisiones de adecuación. Esto indica que muchas organizaciones optan por el mecanismo más conocido o por transferir datos personales a países considerados "seguros" según el RGPD, en busca de certeza jurídica. Aunque esto es positivo, no elimina la necesidad de controlar los flujos ni de realizar un análisis adicional, como una TIA complementaria.

El uso de las BCRS se sitúa en torno al 15%, y según las entidades que las emplean, parecen estar reservadas para grandes grupos multinacionales, con más de 20.000 empleados, pertenecientes a sectores como el Financiero, Tecnología y Telecomunicaciones, Industria y Energía.

Las excepciones reconocidas en el artículo 49 RGPD se utilizan en aproximadamente un 15% de los casos, lo que invita a reflexionar, ya que el RGPD las considera mecanismos residuales y no sistemáticos, debiendo se ser utilizadas de manera puntual.

Los datos reflejan un enfoque de cumplimiento formal, pero podemos ver que aún existe margen de mejora en la gestión del riesgo y la gobernanza efectiva de las transferencias internacionales.

Ilustración 33: **Mecanismos utilizados para regular las transferencias internacionales de datos personales en la organización**



5.6.

Certificación y Estándares de Cumplimiento

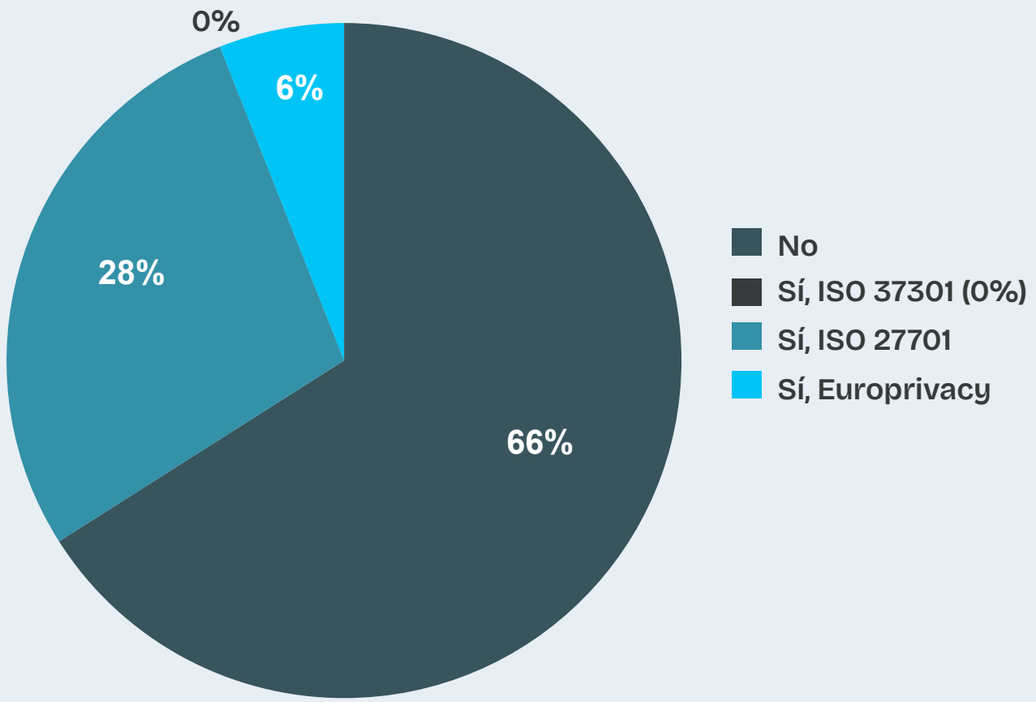
Las certificaciones en protección de datos siguen estando en una fase temprana, encontrándose principalmente asociadas a seguridad de la información más que a cumplimiento autónomo del RGPD, actualmente el 66% de las empresas encuestadas no utilizan mecanismos de certificación, lo que nos indica que no se perciben aún como una herramienta central de cumplimiento.

Existe un predominio de los esquemas en origen de ISO/IEC, a excepción de ISO/IEC 37301, desde la vertiente de la seguridad de la información (el 28% de los encuestados tienen la certificación ISO 27701). Cabe destacar que la ISO/IEC 27701 ha evolucionado y ahora se considera un estándar independiente, dejando de ser únicamente una extensión de la ISO/IEC 27001. Esto permite que las organizaciones implementen y certifiquen un Sistema de Gestión de la Información de Privacidad (SGIP) sin la obligación de poseer previamente una certificación de Sistema de Gestión de Seguridad de la Información (SGSI) bajo la ISO/IEC 27001.

Un 6% de los encuestados declaran utilizar Europrivacy™/®[1], el Sello Europeo de Protección de Datos conforme al artículo 42 RGPD, que se encuentra específicamente diseñado para evaluar la conformidad jurídica y técnica de las actividades de tratamiento y permite a los responsables y encargados del tratamiento demostrar la conformidad de sus procesos, productos y servicios con los efectos y beneficios legales de una certificación oficial del RGPD. El Sello se encuentra reconocido oficialmente por la UE (CEPD), el Espacio Económico Europeo (EEE), la Cooperación Europea para la Acreditación (EA) y las autoridades de protección de datos de 30 países, y se encuentra continuamente actualizado para alinearse con la evaluación normativa y jurisprudencial, algo que da respuesta al actual escenario de complejidad normativa al que nos enfrentamos.

Apostar por certificaciones conforme al art. 42 RGPD, conectadas directamente con el marco de supervisión, representa una oportunidad estratégica para reforzar la accountability, estandarizar criterios y aportar seguridad jurídica tanto a las organizaciones como a los interesados, haciendo de la privacidad un valor diferencial, en una sociedad cada vez más consciente del uso de sus datos personales.

Ilustración 34:
Adopción de mecanismos de certificación en materia de protección de datos



* No hubo nadie dentro de la muestra que seleccionase la opción **NO** a la pregunta **¿Se utilizan mecanismos de certificación en su organización?**

[1] Europrivacy es una marca registrada en varias jurisdicciones

06

Inteligencia Artificial

6.1.

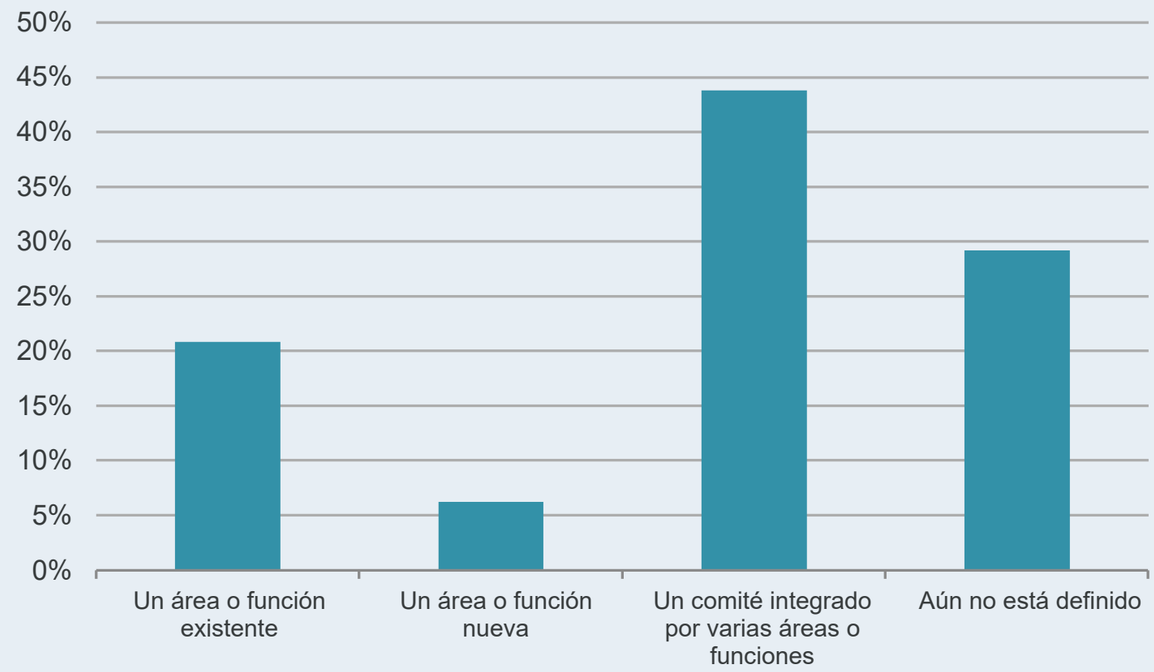
Modelo de Gobernanza y Asignación de Responsabilidades en IA

De las respuestas obtenidas, la mayoría ha atribuido la responsabilidad del cumplimiento del Reglamento IA (RIA) a un Comité integrado por varias áreas o de forma exclusiva a un área o función existente (44% y 21%, respectivamente). Esta atribución se debe al tipo de obligaciones que surgen de esta normativa, que combina obligaciones de carácter técnico, legal y ético, normalmente responsabilidad de áreas diferentes dentro de las organizaciones, poniendo de manifiesta esa necesidad de interrelación estrecha entre estas áreas para garantizar la responsabilidad del cumplimiento del RIA.

Respecto a las organizaciones que lo han atribuido a un área nueva (6 %), debería estar nutrida de profesionales que cuenten con conocimientos en gestión de riesgos y gobernanza en sectores tecnológicos. Aquí la diferencia entre un departamento nuevo dedicado en exclusiva a la gestión de esos sistemas y un comité o departamento existente es la posibilidad de dedicar más recursos en exclusiva a esta materia; lo que tiene todo el sentido en organizaciones cuyo núcleo de negocio sea eminentemente tecnológico.

Por último, las organizaciones que no lo han definido pueden ser bien porque su organización no desarrolla o implementa sistemas de IA o bien porque aún no se han adaptado a la nueva legislación y están valorando opciones. **En cualquier caso, de cara al año 2026 veremos un alineamiento de las organizaciones en este sentido.**

Ilustración 35: **Distribución de la Responsabilidad de Cumplimiento del Reglamento de Inteligencia Artificial**



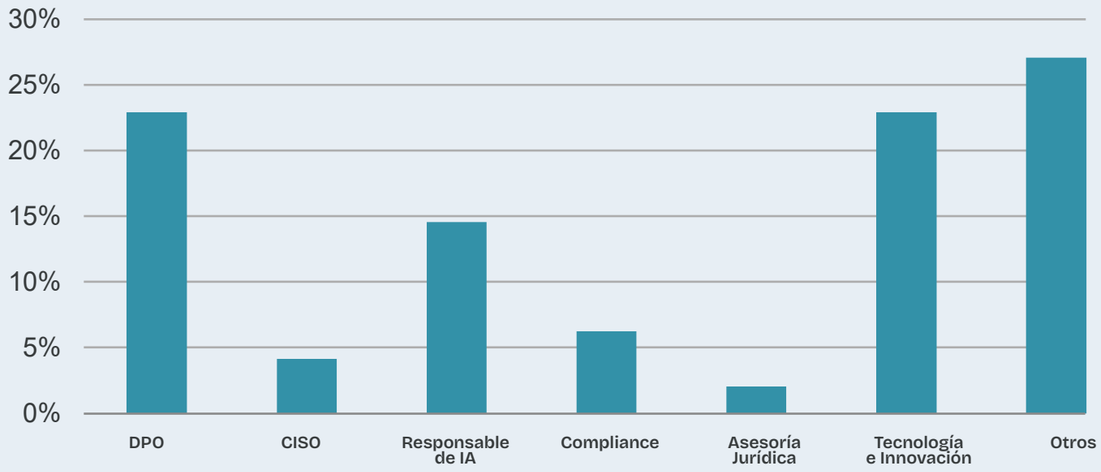
6.2.

Usos Estratégicos y Operativos de la IA en la Organización

Entrando en el detalle de la pregunta anterior, en los casos de atribución a áreas existentes observamos cómo hay una preminencia en la atribución al DPO, por su perfil de garante de la privacidad y las sinergias que hay entre el cumplimiento del RGPD y el RIA, y a las áreas de tecnología e innovación por el carácter técnico de esta nueva herramienta (22,92% de las respuestas en ambos casos). Asimismo, estos porcentajes son indicativos de que las posiciones indicadas, si bien son independientes en sus organizaciones, funcionalmente están integradas en otros departamentos.

No obstante, es destacable el porcentaje de otros (27,08%) lo que puede ser muestra de que los comités a quienes están atribuidas las responsabilidades del Reglamento de IA existían con anterioridad a su entrada en vigor y no se han creado específicamente para ello, como puede ocurrir con los comités de riesgos o de auditoría de las compañías.

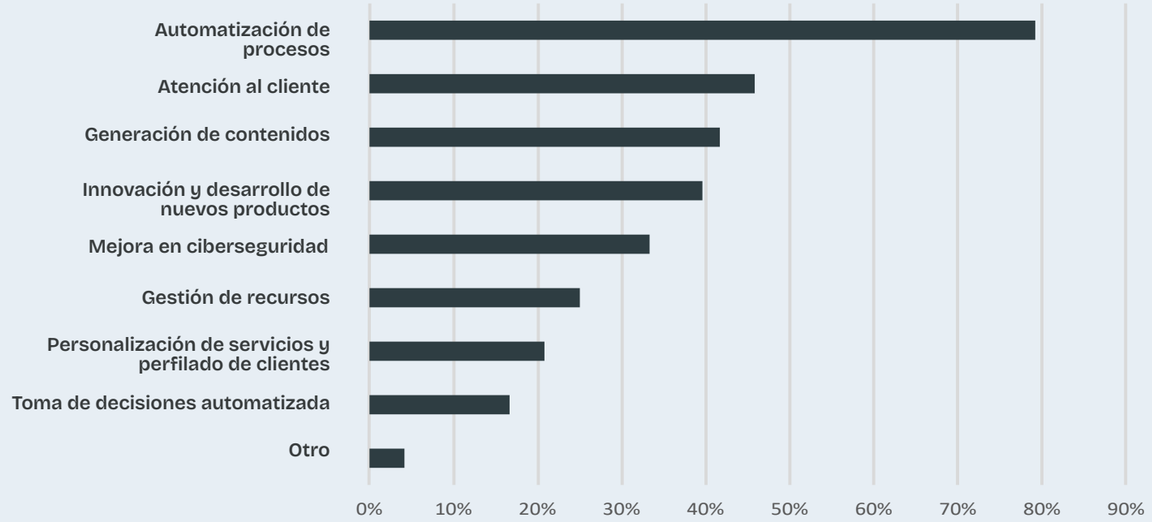
Ilustración 36: **Distribución de Responsabilidades de Cumplimiento de IA entre Funciones Existentes**



6.3.

Sistemas de Alto Riesgo: Presencia, Identificación y Funcionalidades Asociadas

Ilustración 37: **Distribución de los Principales Usos Organizativos de la Inteligencia Artificial**



La inmensa mayoría (79%) utiliza la IA para la automatización de procesos. Esto se debe a la rapidez con la que los modelos de IA procesan los datos, permitiendo crear flujos de información muy ágiles y replicando tareas humanas con mucha más velocidad.

Asimismo, su uso permite inferir y establecer patrones en los procesos de la organización que pudieran no ser conocidos por las mismas, permitiendo su análisis y corrección si así se cree necesario. Igualmente, la automatización de los procesos se asienta sobre la creencia de que lo realizado por una máquina presenta menos probabilidad de cometer errores que un humano, contribuyendo a la eficiencia de los procesos, aunque esto no sucede siempre. Es decir, no existirán errores en la ejecución automática de los procesos si su ejecución manual no los tenía. En caso contrario, únicamente supone replicar el error de forma más rápida al programarse el sistema con el error de origen.

De estos resultados, se observan los usos más comunes: la atención al cliente mediante chatbots, la generación de contenidos y la innovación y desarrollo de nuevos productos. Esto no deja de ser una automatización de los procesos creativos y de la atención a los usuarios, mediante la generalización de respuestas tipo o plantillas más personalizadas según la experiencia previa de quien utilice el sistema de IA. Para las organizaciones supone abrir la posibilidad a dedicar los recursos humanos a resolver aquellas incidencias o problemas que plantean los clientes más complejos, dejando las tareas rutinarias a los sistemas de IA.

Por último, entre los otros destaca el uso de IA para los trámites de recursos, abriendo su uso a temas más sensibles como la tramitación de reclamaciones y recursos jurídicos, tema en boga por las resoluciones recientes por el uso indebido de la IA en la redacción de los mismos.

6.4.

Riesgos, Desafíos y Retos Organizativos ante la Incorporación de la IA

Las respuestas ponen de manifiesto el uso de sistemas de IA ampliamente probados como puede ser chatbots o bien para la automatización de tareas o procesos rutinarios que implican un riesgo bajo. En los próximos meses, se verá si su uso sigue esta misma tendencia o las organizaciones se atreverán a implementar sistemas de IA de alto riesgo conforme se vaya observando su eficacia y la seguridad en su uso.

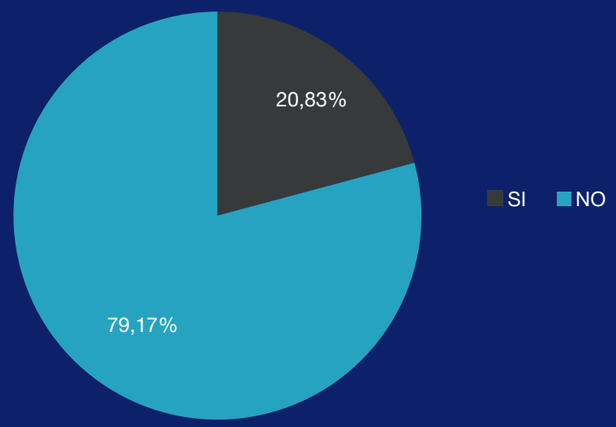
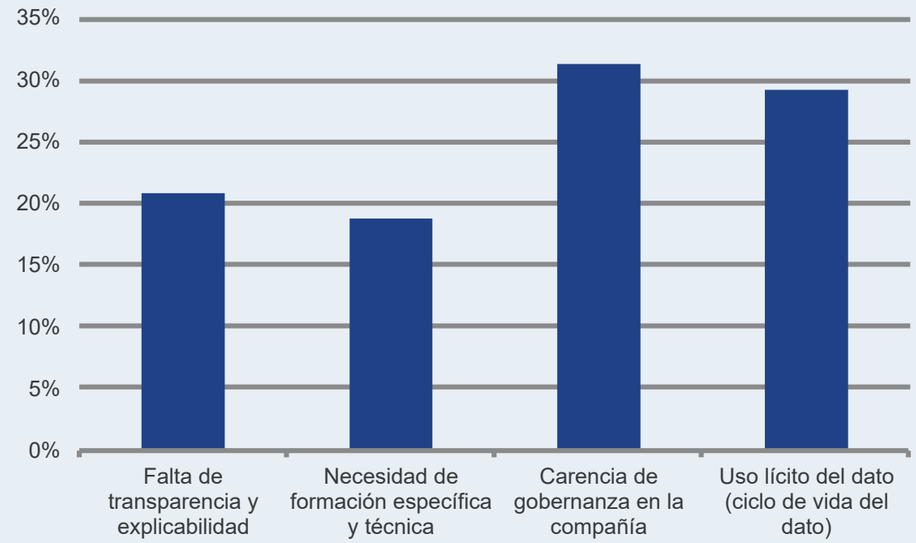


Ilustración 38:
Distribución de los Principales Usos Organizativos de la Inteligencia Artificial

De quienes han respondido que sí usan sistemas de IA de alto riesgo, los principales usos son en el sector de salud, para diagnóstico médico o para el establecimiento de precios dinámicos en los seguros de salud; o bien en el ámbito de los RR.HH. y de atención al cliente/usuario para la gestión de los empleados o la determinación de situaciones particulares que requieran de acciones específicas. Estas situaciones entran dentro de los casos de usos más probados, donde es relativamente más sencilla la detección de errores y su corrección por los humanos que están en el control de estas herramientas.

Ilustración 39: **Preocupación sobre principales riesgos de la IA en las organizaciones**



En este gráfico se observa que la preocupación sobre los principales riesgos es bastante equilibrada, destacando la falta de gobernanza en la compañía y la preocupación por el uso lícito del dato en todo su ciclo de vida. Los motivos principales son la novedad sobre la regulación en esta materia y la falta de resoluciones que establezcan un criterio administrativo o jurisprudencial sobre su uso legítimo.

Asimismo, la falta de transparencia y explicabilidad procede de la falta de compresión sobre el cálculo de los patrones ocultos y las predicciones que los sistemas de IA hacen, lo que requiere análisis y estudio para poder comprender su origen.

07

Reflexiones finales sobre la madurez del cumplimiento

El VII Estudio de Madurez en la Aplicación del RGPD muestra con claridad que los DPOs afrontan uno de los momentos más decisivos desde la entrada en vigor del Reglamento. La función ha evolucionado con rapidez y se va consolidando cada año, ya no es un rol estrictamente jurídico, sino un punto de conexión entre gobernanza, riesgos y tecnología. Seis de cada diez organizaciones declaran que cuentan hoy con un sistema de cumplimiento plenamente definido e implantado, lo cual supone un avance indiscutible. Pero **este progreso se produce en un escenario cada vez más exigente, en el que las obligaciones crecen y la tecnología avanza a un ritmo difícil de acompasar con los marcos de control actuales.** Aunque el papel del DPO ha ganado peso en la toma de decisiones y su profesionalización es evidente, la madurez formal no siempre se traduce en capacidad real para sostener el día a día del cumplimiento. Algunas de las carencias históricas se repiten, más de la mitad de los delegados declara no disponer de los recursos necesarios, las resistencias internas siguen presentes y aspectos centrales del RGPD, como las evaluaciones de impacto, la gestión de las transferencias internacionales o la supervisión de terceros, continúan mostrando debilidades llamativas para un marco normativo con una década de recorrido.

A ello se suma **la irrupción de la Inteligencia Artificial,** que **añade una presión inédita.** Se suman requisitos normativos y éticos a la implantación de sistemas y modelos de IA que son más recientes y menos aterrizados en la realidad de los modelos de cumplimiento de las organizaciones, y todo ello supone un reto importante en la definición de los modelos de gobernanza de IA. El DPO tendrá un rol muy importante en ese modelo que cada organización está definiendo.

Además, la convergencia del RGPD con el RIA, DORA o NIS2 obliga a los DPOs a comprender y gestionar riesgos tecnológicos que ya no pueden abordarse de manera única desde el derecho o desde el mundo ciber, sino de una manera mas holística. Las organizaciones están respondiendo con modelos de gobernanza más amplios, basados en comités que integran privacidad, riesgos, tecnología y legal. Sin embargo, siguen apareciendo zonas grises, la necesidad de asegurar el uso lícito del dato o la dificultad para supervisar el ciclo completo de la información ponen a prueba la madurez real de muchas compañías.

Al mismo tiempo, el volumen creciente de ejercicio de derechos, gestión de consentimientos, incidentes y requerimientos regulatorios ha llevado a un impulso claro hacia la automatización.

La transformación digital de la función del DPO se ha vuelto esencial para sostener la operativa del cumplimiento con los requisitos y volumétricas actuales. No obstante, mientras crece la inversión en herramientas tecnológicas, la formación y la cultura interna siguen relegadas a un segundo plano. Y sin esa base, las organizaciones corren el riesgo de quedarse en un modelo reactivo, incapaz de anticipar riesgos o de consolidar un enfoque verdaderamente preventivo.

El estudio muestra un ecosistema en transformación acelerada. Organizaciones con estructuras más maduras, sí, pero sometidas a una presión regulatoria sin precedentes; DPOs más visibles y con mayor peso estratégico, pero también más sobrecargados; y un marco tecnológico que obliga a rediseñar la gobernanza del dato.

El reto para 2026 será, por tanto, doble: convertir la madurez formal en madurez efectiva y capacitar a los DPO para atender a los riesgos digitales con más amplitud que propiamente el riesgo de privacidad, aportando más confianza de sus organizaciones hacia los stakeholders y mitigando los posibles riesgos de incumplimiento de las compañías.

dpi
DATA PRIVACY INSTITUTE

isms forum

VII

Estudio sobre el nivel de madurez en la aplicación de **Reglamento General de Protección de Datos**

Observatorio de la **Privacidad**