6º Estudio sobre el nivel de madurez en la aplicación del Reglamento General de Protección de Datos

Una iniciativa de:

isms forum

dpi
DATA PRIVACY INSTITUTE

Febrero 2025

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

OBSERVATORIO DE LA PRIVACIDAD

AUTORES

DIRECTOR	Carlos Alberto Sáiz
PARTICIPANTES	Cristina Köhler
	Edison Hernández-Suero
	Esmeralda Saracibar
	Ignacio Cagiga
	Jaime Requejo
	Josep Bardallo
	Araceli Moya
	Óscar López
	Xabier Alberdi
GESTIÓN DE PROYECTOS	Beatriz García
DISEÑO/MAQUETACIÓN	Marta Barroso

CONTENIDOS

Introducción

Objetivos del Observatorio de Privacidad

6ª Edición del Estudio

- La protección de datos sigue evolucionando en un entorno donde la digitalización y la regulación avanzan a un ritmo sin precedentes. Conscientes de este escenario, presentamos con gran entusiasmo la 6ª edición del Estudio del Observatorio de la Privacidad, desarrollado por el Data Privacy Institute de ISMS Forum.
- Este estudio anual se ha consolidado como una herramienta fundamental para analizar el estado de madurez en RGPD, identificar tendencias emergentes y proporcionar a los profesionales de la privacidad un marco de referencia que les permita fortalecer sus estrategias y anticiparse a los desafíos del futuro.

El valor de una evaluación continua

Año tras año, este informe no solo captura una fotografía del momento actual, sino que también marca la evolución del ecosistema de protección de datos, permitiendo:

· Detectar cambios en la función del Delegado de Protección de Datos (DPD), su rol estratégico dentro de las organizaciones y su nivel de influencia en la toma de decisiones.

· Comprender el impacto de nuevas normativas y regulaciones que afectan la gestión de la privacidad en empresas y Administraciones Públicas.

· Establecer métricas comparativas que ayuden a las organizaciones a evaluar su grado de cumplimiento en relación con sus pares.

· Facilitar la toma de decisiones basada en datos, aportando información clave para optimizar la asignación de recursos y mejorar la gestión de riesgos.

La privacidad ya no es solo una obligación regulatoria, sino un pilar esencial para la confianza digital y la sostenibilidad del negocio. Por ello, esta nueva edición busca servir como guía para que los profesionales del sector refuercen su impacto organizacional y promuevan una cultura de cumplimiento proactiva.

Una herramienta para el crecimiento del sector

El Estudio del Observatorio de la Privacidad es mucho más que un informe; es un punto de encuentro para la comunidad de privacidad. A través del análisis comparativo y la identificación de mejores prácticas, este informe permite a los profesionales:

1. Evaluar su posicionamiento y desempeño dentro del ecosistema de privacidad.

2. Detectar oportunidades de mejora en la implementación de estrategias de cumplimiento.

3. Optimizar la gestión de riesgos alineándose con estándares del sector.

4. Prepararse para los retos futuros, entendiendo las tendencias globales y regulatorias.

Agradecemos la participación de todos los profesionales que han contribuido con sus respuestas y reflexiones. Vuestra colaboración es clave para seguir fortaleciendo este análisis año tras año y, con ello, potenciar el papel de la privacidad como un motor de confianza y seguridad en el entorno digital.

Tipología de la muestra

La muestra de nuestro estudio en 2024 está compuesta mayoritariamente por grandes compañías. Más del 63% de las empresas encuestadas cuentan con más de 5.000 empleados, y de ellas, el 43,1% tiene más de 20.000 empleados. En contraste, un 18,97% de las empresas se encuentran en el rango de pequeñas y medianas empresas, con menos de 1.000 empleados.

Si bien la mayoría de las empresas encuestadas tienen entre 1.000 y 4.999 empleados (15,52%), se observa una representación significativa de compañías con más de 20.000 empleados, lo que permite obtener perspectivas desde distintas escalas operativas. Esta diversidad influye en el nivel de madurez en la aplicación del RGPD, dado que las empresas más grandes suelen disponer de mayores recursos y capacidades para cumplir con la normativa en comparación con las más pequeñas.Como conclusión de esta tercera gráfica, que se muestra bajo estas líneas, en lo que respecta al sector de operación, encontramos una diversidad notable. Los sectores más representados son Servicios Financieros y "otros", que juntos conforman más de la mitad de las respuestas. Esto sugiere que el estudio podría haber atraído a una proporción significativa de empresas del sector financiero, que históricamente han estado sujetas a regulaciones estrictas en materia de protección de datos. Sin embargo, también hay una presencia considerable de empresas en sectores como Industria, Construcción e Infraestructuras, Administración Pública y Logística y transporte, lo que indica que el RGPD es relevante en una amplia gama de industrias.

Por lo tanto, esta variedad de empresas participantes proporciona una base sólida para el estudio sobre el nivel de madurez en la aplicación del RGPD, ya que permite examinar cómo diferentes características empresariales pueden influir en la capacidad de las organizaciones para cumplir con las regulaciones de protección de datos.

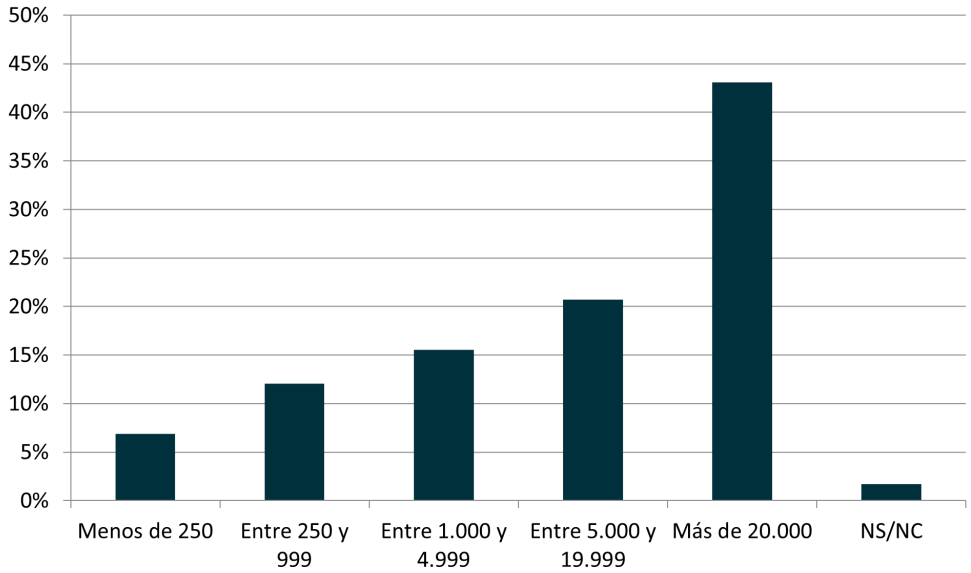

Ilustración 1: Tamaño de la compañía

En cuanto a los ingresos anuales de las empresas participantes, la distribución es igualmente variada. Un 18,97% de las empresas encuestadas reporta ingresos entre 5.000 y 10.000 millones de euros, mientras que un 17,24% supera los 10.000 millones de euros anuales. En el otro extremo, un 12,07% de las compañías reporta ingresos menores a 200 millones de euros. Esta heterogeneidad en la facturación es indicativa de una amplia gama de capacidades financieras, lo que puede influir en la implementación de medidas de cumplimiento del RGPD, como la contratación de personal especializado o la adopción de tecnologías avanzadas de protección de datos.

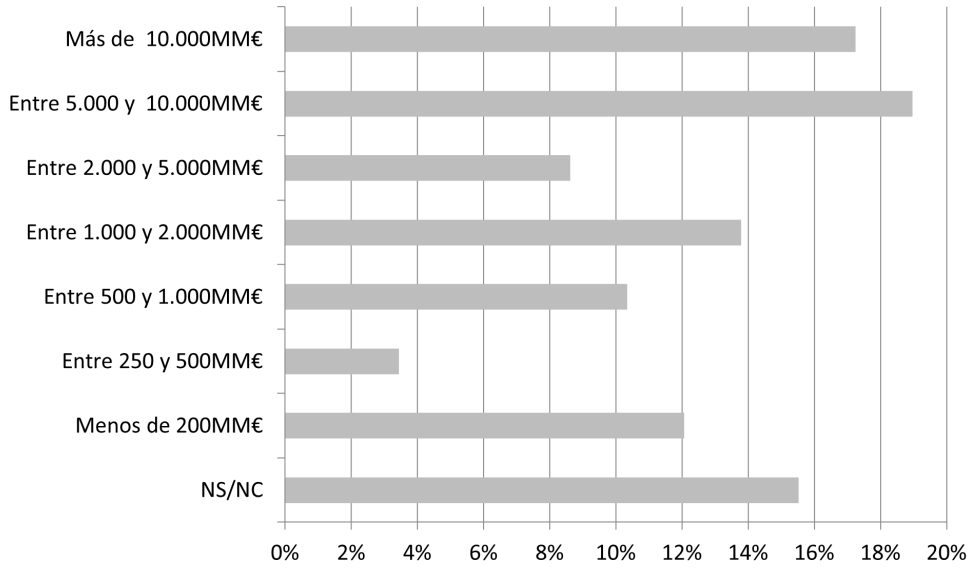

Ilustración 2: Facturación de la compañía

Ilustración 3: Sector de actividad de la compañía

Estado de situación -Gobierno de la Privacidad

Tipo de DPO y alcance geográfico de la función

La mayoría de las empresas españolas declaran disponer de un Delegado de Protección de Datos interno, principalmente dedicado de manera exclusiva a Privacidad y Protección de Datos y, en una menor proporción, compaginando tales tareas con otras dentro de la propia organización. Este alto porcentaje refleja la importancia que las grandes organizaciones otorgan a esta función, la cual ha evolucionado significativamente tras seis años de aplicación del RGPD.

Un 10% de las empresas encuestadas afirman disponer de un DPO externo, siendo minoritarias aquellas organizaciones que optan por un órgano colegiado que distribuya las funciones asignadas reglamentariamente al DPO entre diversas áreas de la compañía.

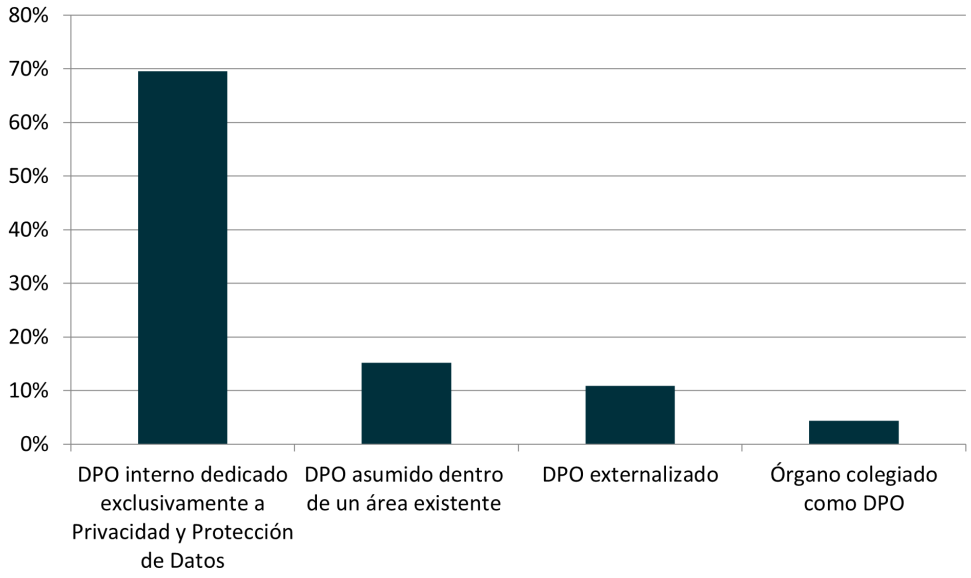

Ilustración 4: Tipo de DPO nombrado

En cuanto al alcance territorial de las competencias de esos DPO, los datos muestran un aumento de los DPO que asumen esta función a nivel global. Para el resto, sus competencias se limitan al ámbito nacional, mientras que un número menor de DPO desempeña esta función a nivel europeo.

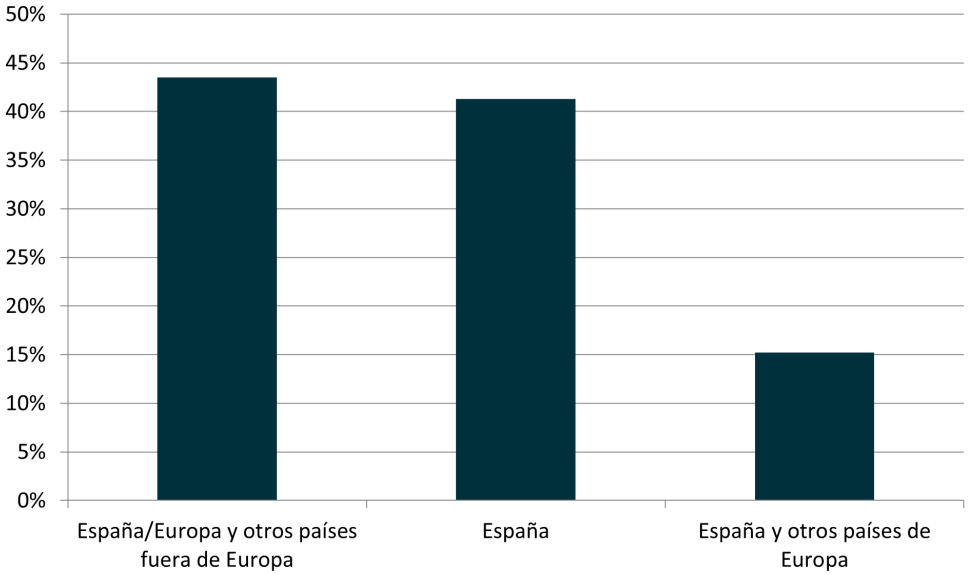

Ilustración 5: ¿Cuál es el alcance territorial de las competencias del DPO?

Compatibilidad con otras funciones

Más de la mitad de los DPOs dedican el total de su actividad a las funciones propias de esta figura, mientras que, el resto, lo compatibilizan con otras funciones y responsabilidades, entre las cuales destacan las referidas a Compliance, Ciberseguridad, Asesoría Jurídica o IA, siendo esta última una de las novedades de este año con respecto a los anteriores.

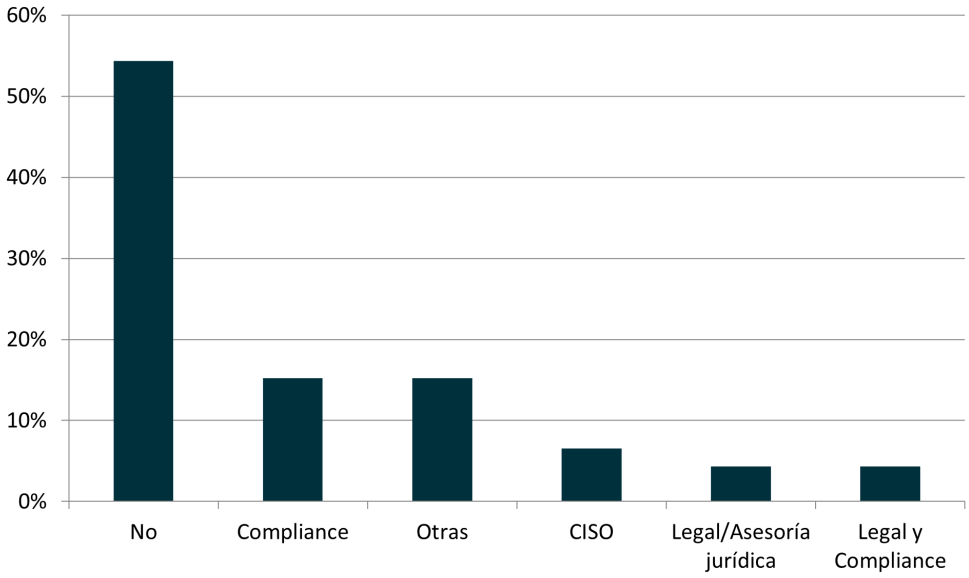

Ilustración 6: : ¿Compatibiliza su cargo de DPO con otras funciones?

Formación académica y certifiaciones de los DPOs

La mayoría de los DPOs encuestados disponen de formación jurídica (65%), seguida de los perfiles técnicos (24%) donde predominan la titulación en algún tipo de ingeniería. Un menor porcentaje tienen formación académica en Economía o Auditoría, mientras que alguno de ellos afirma tener formación combinada técnica y jurídica.

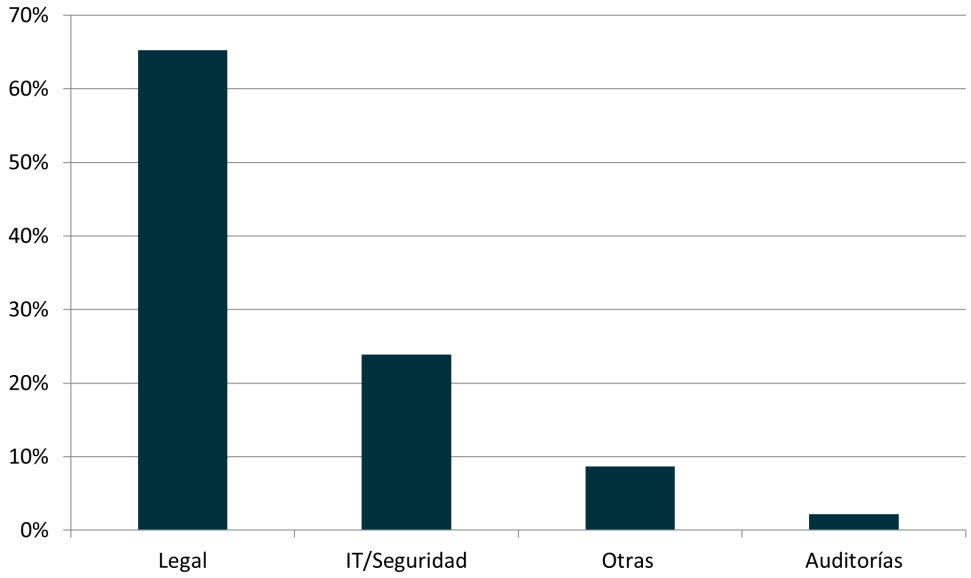

Ilustración 7: ¿Qué formación profesional posees?

Las certificaciones más acreditadas por los DPO son el CDPD conforme al esquema de la AEPD, el CDPP del ISMS Forum y la CIPP de la IAPP, disponiendo algunos de ellos de otras certificaciones como pudieran ser CISA o CISM de ISACA, CCSP, CPCC, CAIP del ISMS o en estándares internacionales ISOs, mayormente en 27001.

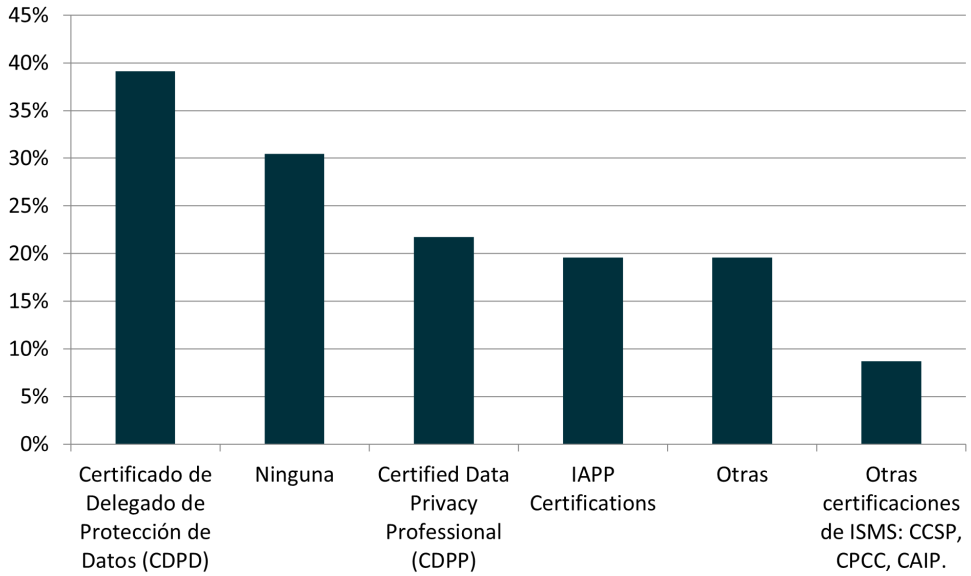

Ilustración 8: ¿Qué certificaciones profesionales mantiene activas?

Reportes

El mayor porcentaje de DPOs reportan directamente a la Dirección de Asesoría Jurídica y/o a la Secretaría del Consejo. El resto afirma reportar a distintos órganos, como son: el Comité de Compliance, Comité de Seguridad, CISO, Director General Corporativo, DPO de Grupo o al CCO. En algunos casos, el DPO reportan al CIO o al CEO-Presidente de la empresa.

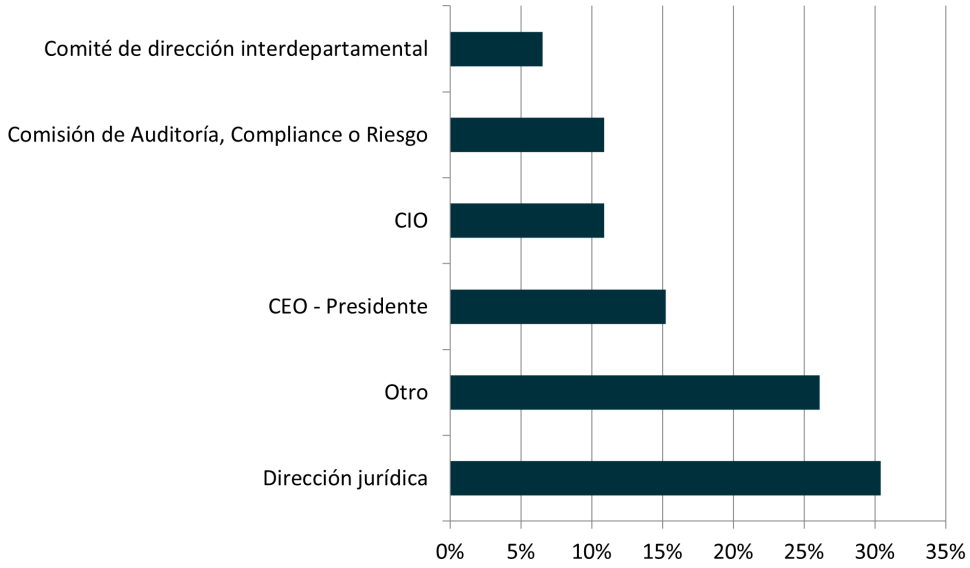

Ilustración 9: ¿A quién Reporta dentro de la empresa?

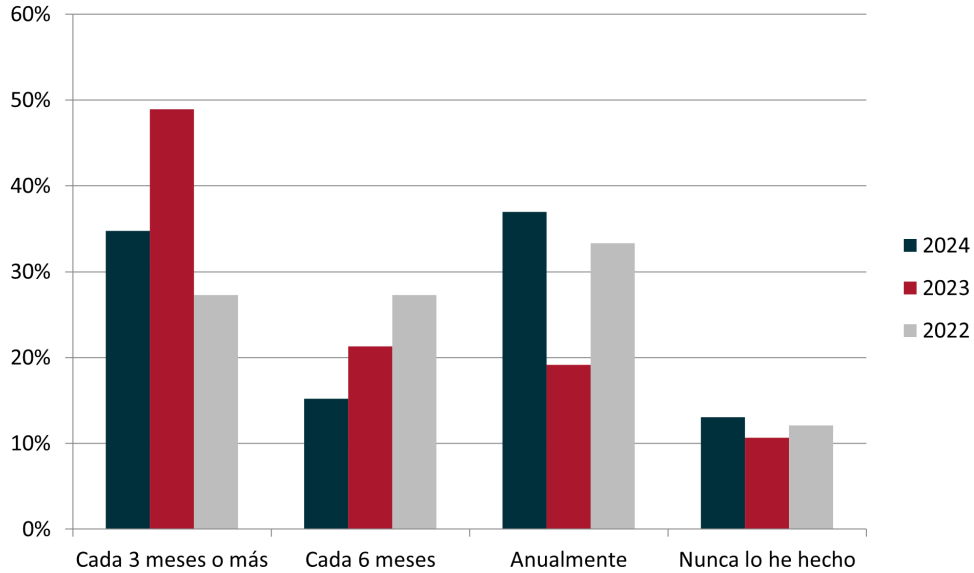

Ilustración 10: ¿Cada cuanto realiza un reporte formal al Management como DPO?

Se puede observar una tendencia a la reducción de reportes trimestrales y semestrales, con un aumento significativo de los reportes anuales, que en 2024 representan casi el 40%. Aunque esto puede indicar una madurez en la gobernanza del RGPD, también podría reflejar una menor supervisión continua. Además, un preocupante 13,04% de las organizaciones nunca ha realizado un reporte formal, lo que sugiere carencias en la implementación efectiva del cumplimiento normativo.

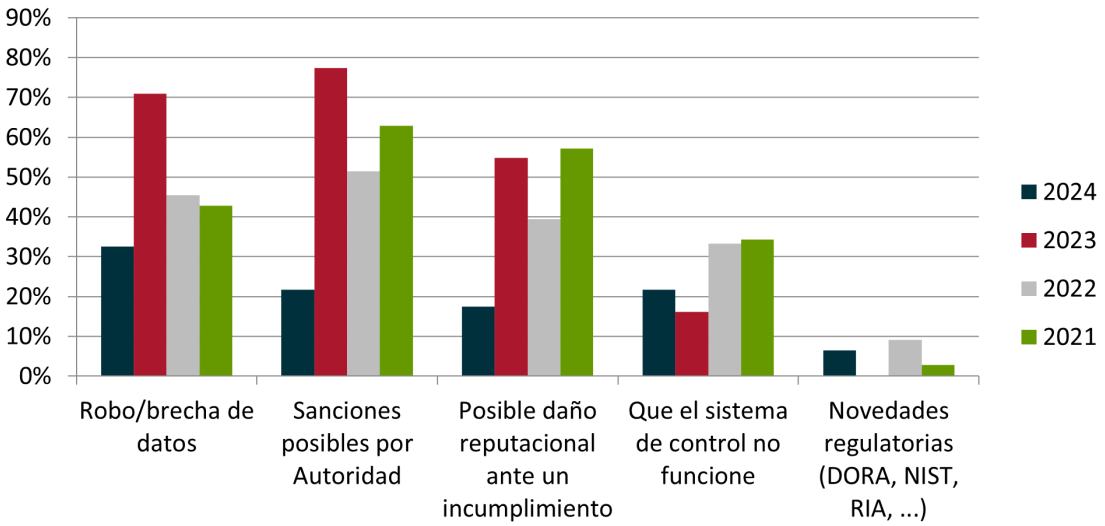

Ilustración 11: ¿Cuándo reportar hacia la Dirección, que es lo más le preocupa?

El análisis de las preocupaciones al reportar a la Dirección revela un cambio significativo en las prioridades de los DPO. La preocupación por brechas de datos y sanciones ha disminuido drásticamente en 2024 (32,61% y 21,74%, respectivamente) respecto a 2023, lo que sugiere mayor confianza en las medidas de seguridad y cumplimiento. El temor al daño reputacional también ha caído (17,39%), mientras que la preocupación por fallos en los sistemas de control ha crecido (21,74%), reflejando la creciente automatización del cumplimiento. Además, las novedades regulatorias (DORA, NIST, RIA) comienzan a ganar relevancia (6,52%). Estos cambios apuntan a una maduración en la gestión del RGPD, con un enfoque más estratégico y adaptativo frente a riesgos emergentes.

Equipos

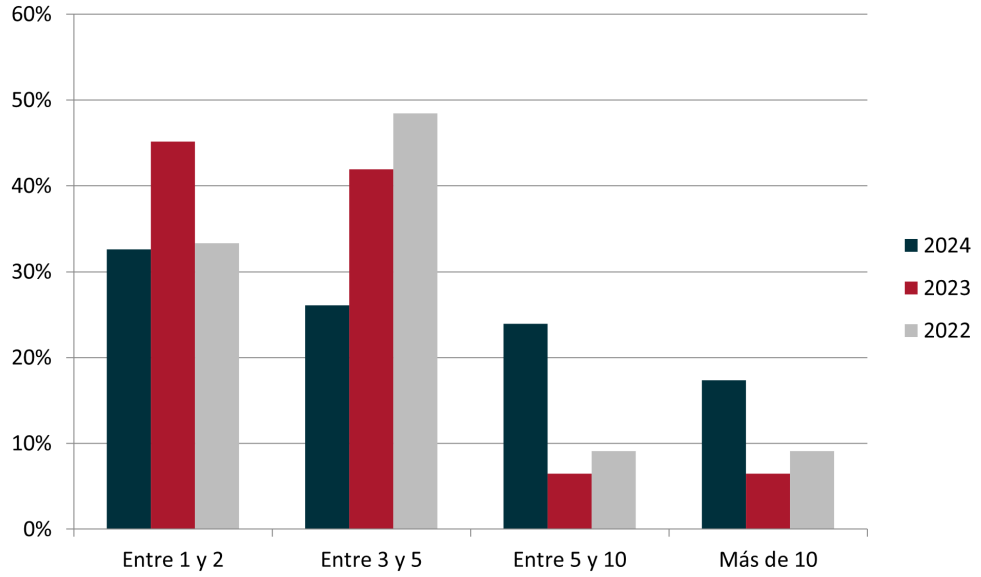

Ilustración 12: ¿Cuántas personas (incluyendo personal interno/externo) están dedicadas al cumplimiento continuo del RGPD?

El análisis muestra una evolución en la asignación de recursos al cumplimiento del RGPD en España. Se ha reducido el número de empresas con solo 1 o 2 personas dedicadas (del 45,16% en 2023 al 32,61% en 2024), mientras que ha crecido significativamente el porcentaje de organizaciones con equipos de 5 a 10 personas (del 6,45% al 23,91%) y más de 10 personas (del 6,45% al 17,39%). Esto indica una mayor madurez en la gestión del RGPD, con más empresas fortaleciendo sus equipos para afrontar los desafíos regulatorios y de protección de datos.

Dificultades y áreas de mejora

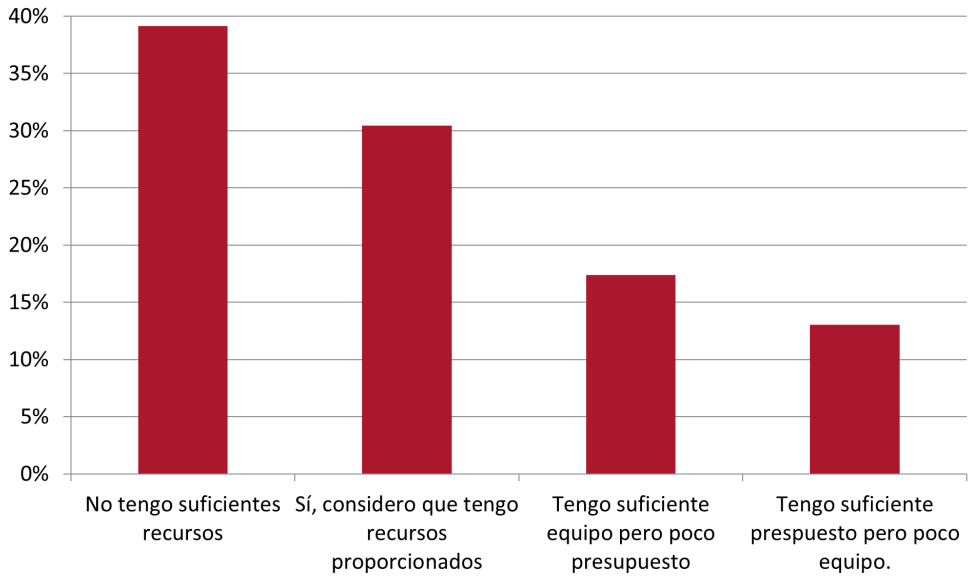

Ilustración 13: ¿Considero que tengo suficientes recursos para cumplir con mis obligaciones?

El análisis muestra que el 39,13% de los encuestados considera que no tiene suficientes recursos para cumplir con sus obligaciones en el RGPD, lo que indica una importante limitación en muchas organizaciones. Solo el 30,43% cree contar con recursos proporcionados, mientras que el resto enfrenta desequilibrios: un 17,39% tiene suficiente equipo, pero insuficiente presupuesto, y un 13,04% dispone de presupuesto pero con un equipo insuficiente. Estos datos reflejan que la falta de recursos ya sea económicos o humanos, sigue siendo un desafío clave en la implementación efectiva del RGPD

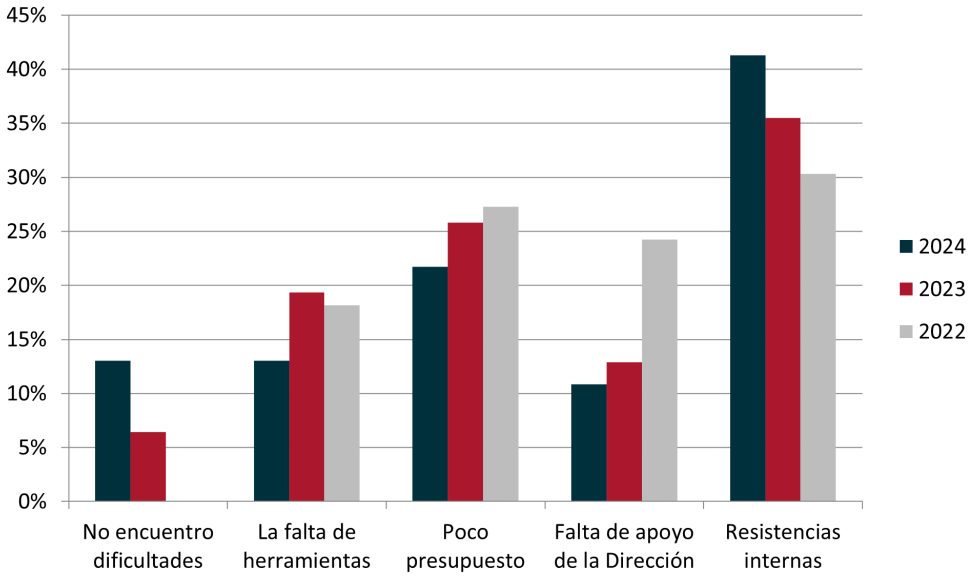

Ilustración 14: ¿Cuál es la principal dificultad que encuentra para llevar a cabo su labor?

El principal obstáculo para el cumplimiento del RGPD sigue siendo las resistencias internas, que han aumentado del 30,30% en 2022 al 41,30% en 2024, evidenciando dificultades en la adopción de medidas de protección de datos dentro de las organizaciones. La falta de presupuesto sigue siendo un desafío importante (21,74%), aunque en ligera disminución respecto a años anteriores. La falta de apoyo de la Dirección ha bajado significativamente (10,87%), lo que sugiere una mayor concienciación en niveles ejecutivos. La falta de herramientas también ha disminuido, mientras que el 13,04% de los encuestados afirma no encontrar dificultades, lo que puede indicar una mejora en la gestión del RGPD en algunas organizaciones.

Modelo de Madurez de Cumplimiento RGPD

Grado de madurez

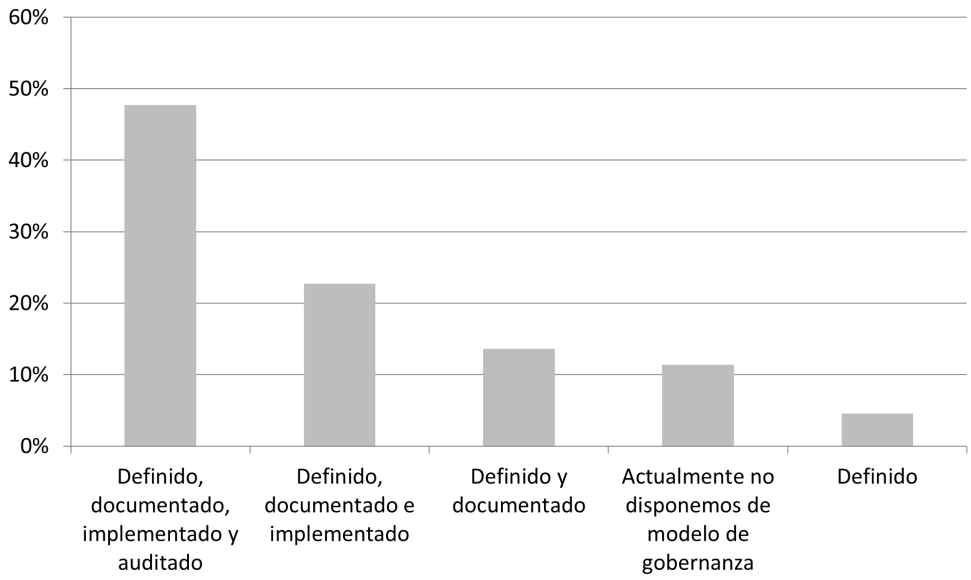

Ilustración 15: ¿cuál es el grado de madurez que tiene el sistema de gestión de protección de datos en su organización?

Las organizaciones grandes y reguladas (sector Financiero, Tecnológico y Sanitario) tienen mayor madurez en la gestión de la protección de datos.

Las empresas pequeñas y Administraciones Públicas presentan niveles más bajos de madurez, con SGPD documentados, pero no implementados ni auditados.

En términos generales, los resultados de 2024 son consistentes con los de 2023, aunque se observa un ligero avance en la implementación del SGPD en más organizaciones.

El grado de madurez del SGPD ha evolucionado ligeramente en 2024, con más empresas avanzando en la implementación, pero sin cambios significativos en la madurez total. Las empresas grandes y reguladas siguen liderando, mientras que las pequeñas y las Administraciones Públicas aún enfrentan desafíos.

Cruzando los datos con el tamaño de empresa por número de empleados se observa que las empresas que tienen un mayor grado de madurez son las más grandes. El 50 % de las empresas con mayor grado de madurez tienen más de 20.000 empleados.

Presupuesto

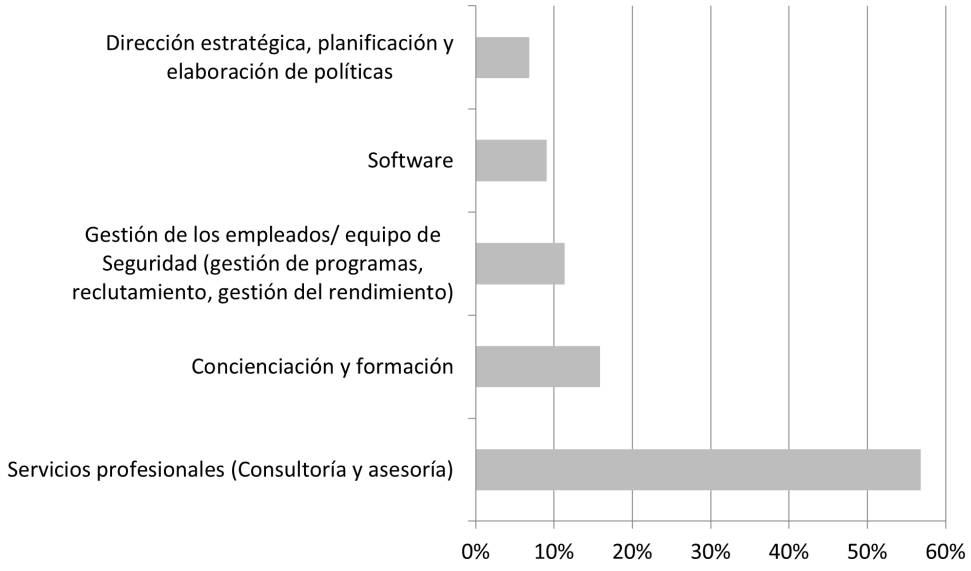

Ilustración 16: ¿Cuál es la actividad a la que se destina más presupuesto?

Servicios profesionales (Consultoría y asesoría) es la actividad con mayor inversión en varios sectores. Tanto en 2023 como en 2024, los sectores regulados han aumentado su dependencia de servicios profesionales, lo que sugiere un enfoque en adaptación normativa y cumplimiento.

Se presenta una aparente reducción del gasto en software en el sector Financiero. Esto podría indicar que la infraestructura tecnológica ya está implementada y que el enfoque ahora es en la gestión de riesgos y formación.

Mientras que en 2023 la prioridad era automatización, en 2024 las empresas tecnológicas parecen estar destinando más recursos a la gestión de la seguridad y empleados.

Concienciación y formación es una prioridad en empresas grandes, pero menos en empresas de tamaño mediano.

Gestión de empleados y seguridad tiene una mayor inversión en empresas medianas y grandes.

Software es una inversión clave para empresas grandes (entre 5.000 y 20.000 empleados).

Concienciación y formación recibe más presupuesto en Administración Pública.

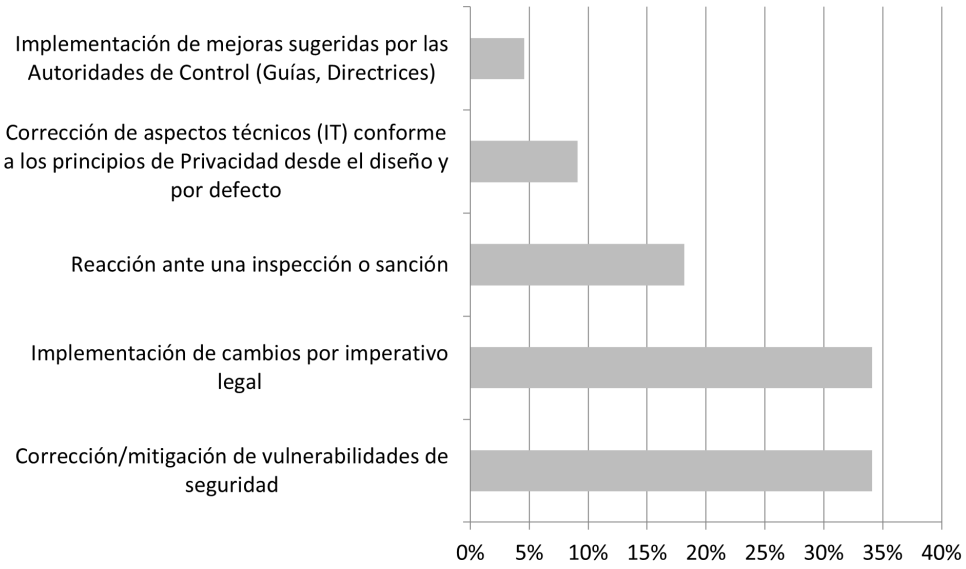

Ilustración 17: Ante una necesidad sobrevenida (no presupuestada)
y desde una perspectiva de gestión de costes, ¿cuál es el asunto más prioritario?

Se evidencia un empate en la máxima prioridad: Implementación de cambios por imperativo legal y Corrección/mitigación de vulnerabilidades de seguridad son los asuntos más prioritarios, mostrando incluso este último indicador un aumento respecto a 2023.

Alta prioridad en la respuesta regulatoria, siendo la reacción ante una inspección o sanción es también una de las principales preocupaciones.

Corrección de aspectos técnicos (IT) e Implementación de mejoras sugeridas por las Autoridades tienen menor peso, lo que sugiere que las empresas priorizan acciones obligatorias sobre iniciativas voluntarias (enfoque más reactivo

Madurez

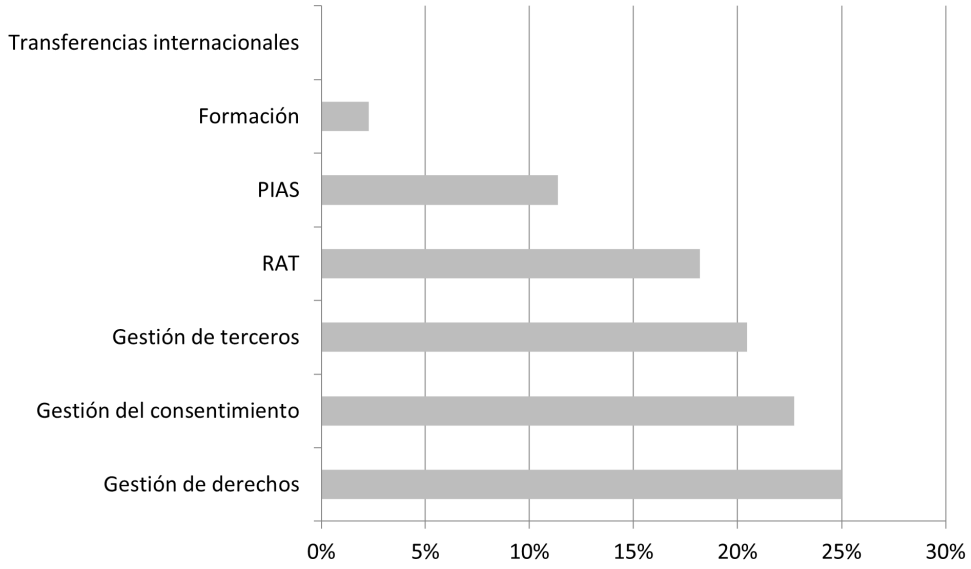

Ilustración 18: cuál es el área de acción en su organización que requiere un mayor nivel de automatización mediante el uso de herramientas tecnológicas

"Gestión de derechos" es el área de acción más mencionada, lo que sugiere una necesidad creciente de automatizar la gestión de solicitudes de derechos de los usuarios. "Gestión del consentimiento" sigue de cerca, reflejando la importancia de mejorar la administración del consentimiento en los tratamientos de datos. Ambas han subido en prioridad respecto a 2023.

Por su parte "Gestión de terceros" aparece como una necesidad relevante, indicando que la supervisión y cumplimiento con proveedores y socios sigue siendo un reto.

Para las empresas más grandes (+20.000 empleados) estas son las 3 áreas de acción con un mayor enfoque en automatización para manejar grandes volúmenes de datos y usuarios.

Empresas grandes (5.000 a 20.000 empleados), muestran un enfoque en RAT (Registro de Actividades de Tratamiento) y PIAs (Evaluaciones de Impacto en Protección de Datos), indicando una necesidad de mejorar la trazabilidad de sus procesos.

Las Empresas más pequeñas (<250 empleados): Enfocan la automatización en la gestión del consentimiento, lo que puede estar relacionado con la necesidad de simplificar el cumplimiento normativo sin contar con grandes equipos especializados.

En un análisis por sectores, observamos que Servicios Financieros muestra una mayor demanda en gestión de derechos y gestión de terceros, reflejando la importancia de cumplir con normativas estrictas y manejar proveedores de manera eficiente. Por su parte, el sector de Tecnología y Telecomunicaciones se enfoca más en la gestión del consentimiento y el RAT, lo que sugiere un esfuerzo en automatizar el manejo de datos personales en entornos digitales.

En el sector de la Industria y Construcción, la necesidad de automatización está más equilibrada entre varias áreas, pero con un ligero enfoque en gestión de terceros, probablemente por la complejidad de sus cadenas de suministro.

Ilustración 19: ¿cuál es la línea de acción que presenta un mayor nivel de madurez en su organización en cuanto a su implementación?

El "Registro de actividades de tratamiento" sigue siendo la línea con mayor madurez, creciendo en casi todos los sectores y tamaños de empresa.

El "Análisis de riesgos y evaluaciones de impacto" ha perdido prioridad, bajando en la mayoría de las categorías por sector y tamaño de empresa.

Las empresas grandes (+ 5.000 empleados) han seguido desarrollando su madurez en gestión de contratos, mientras que las medianas y pequeñas han reducido su foco en esta área.

En el sector Tecnológico ha crecido el enfoque en "Privacy by Design", lo que sugiere que este sector está priorizando integrar la privacidad en el diseño de sus productos y servicios.

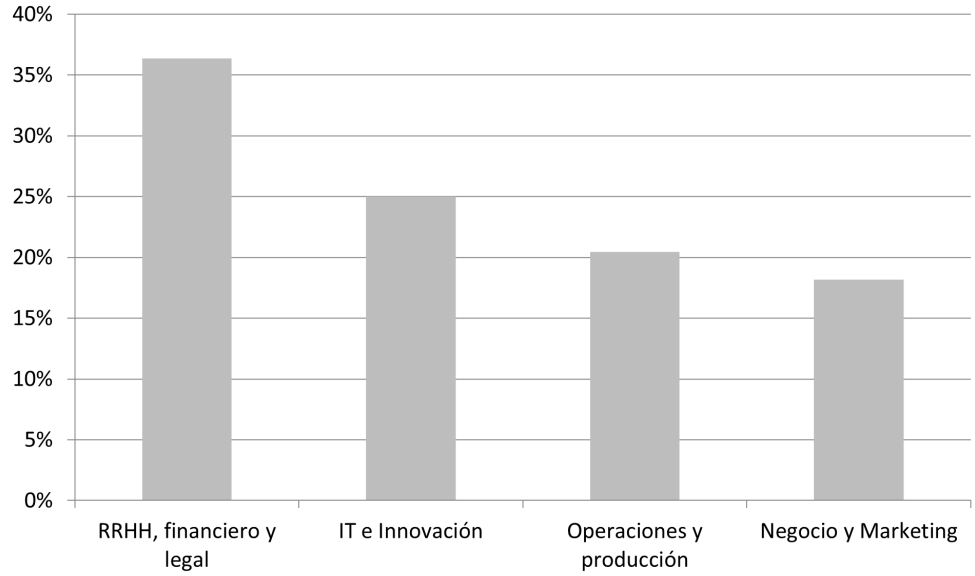

Ilustración 20: ¿Cuál es el área con mayor grado de intervención/participación en la implementación de las anteriores líneas de acción?

"RRHH, financiero y legal" siguen siendo las principales áreas de intervención en la implementación de políticas de privacidad, especialmente en empresas grandes y sectores regulados como Financiero y Administración Pública.

El papel de IT e Innovación se mantiene fuerte, pero con una ligera reducción en 2024, lo que podría indicar que las organizaciones están estabilizando sus procesos tecnológicos en privacidad.

Negocio y Marketing está aumentando su nivel de intervención, lo que sugiere una mayor preocupación por integrar la privacidad en estrategias comerciales.

Las empresas grandes involucran más a las áreas de tecnología y marketing para cumplir con el RGPD, mientras que las pequeñas priorizan procesos operativos y de producción.

Auditorías

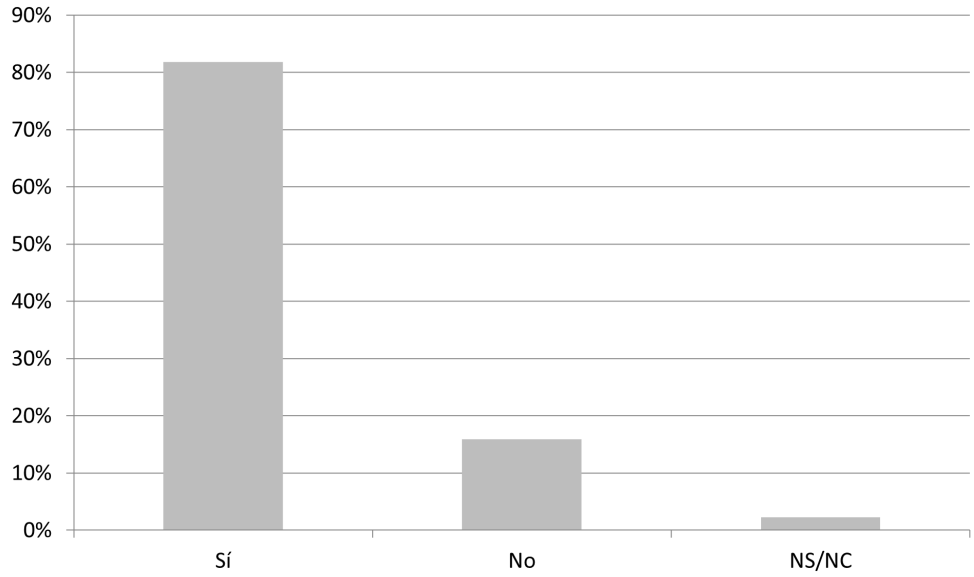

Ilustración 21 : ¿Están ejecutando auditorias formalmente en su organización?

Más organizaciones están implementando auditorías en 2024 en comparación con 2023, pero el cambio es leve.

Las grandes empresas y el sector Financiero lideran la adopción de auditorías, mientras que las empresas más pequeñas y la Administración Pública aún muestran casos sin formalizar auditorías.

El sector Tecnológico y Financiero muestran mejoras continuas en la implementación de auditorías, lo que refleja el impacto de la regulación creciente en estas industrias.

En lo que respecta al sector de Industria y Construcción, evidencia mayor variabilidad, con algunas organizaciones implementando auditorías y otras todavía sin formalizarlas.

Por último, el sector de la Administración Pública, aún existen respuestas negativas, lo que podría deberse a diferencias en la implementación de auditorías en distintos organismos.

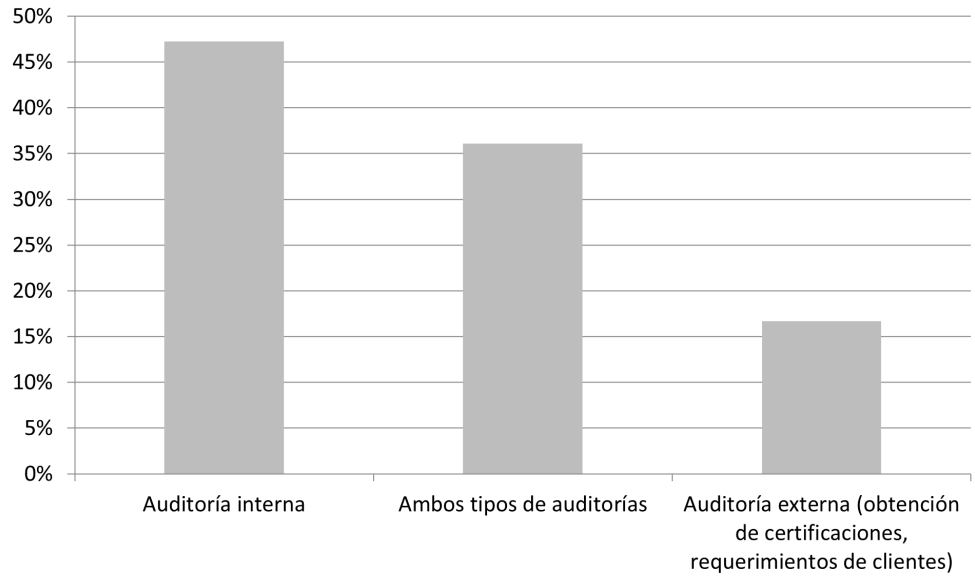

Ilustración 22: ¿Qué tipo de auditoría se realiza?

Las auditorías internas siguen siendo la opción más utilizada en todos los sectores y tamaños de empresa, pero su uso ha disminuido ligeramente en favor de auditorías combinadas.

Las auditorías externas son menos comunes en empresas pequeñas, lo que puede estar relacionado con restricciones de recursos o menor necesidad de certificaciones.

Los sectores Financieros y Tecnológicos tienen una mayor tendencia a utilizar auditorías combinadas, reflejando requisitos regulatorios y de clientes.

Las auditorías internas siguen siendo la opción más utilizada en todos los sectores y tamaños de empresa, pero su uso ha disminuido ligeramente en favor de auditorías combinadas.

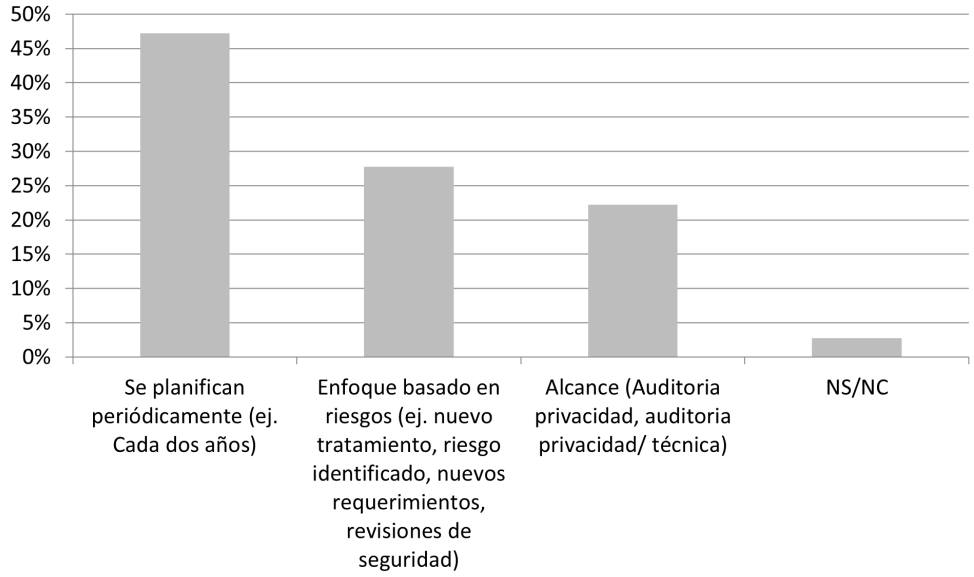

Ilustración 23: ¿Qué criterio se sigue para la ejecución de las auditorias?

La mayoría de las organizaciones planifican sus auditorías periódicamente (por ejemplo, cada dos años), lo que indica un enfoque estructurado en la supervisión del cumplimiento, manteniendo la tendencia del 2023, marcando una tendencia estable en la planificación regular de auditorías.

Por el contrario, un 17% de las organizaciones siguen un enfoque basado en riesgos, lo que podría sugerir que las auditorías se activan en función de cambios significativos en los tratamientos de datos o incidentes.

El criterio de alcance específico también se mantiene, en torno al 14%, principalmente entre las grandes empresas, lo que podría indicar una mayor personalización en sus procesos de control.

Los sectores Financiero y Sanitario están adoptando más auditorías basadas en riesgos, lo que sugiere una mayor sensibilidad a cambios normativos y eventos críticos.

Las empresas más pequeñas siguen dependiendo más de auditorías planificadas, con menos flexibilidad en la adaptación a riesgos emergentes.

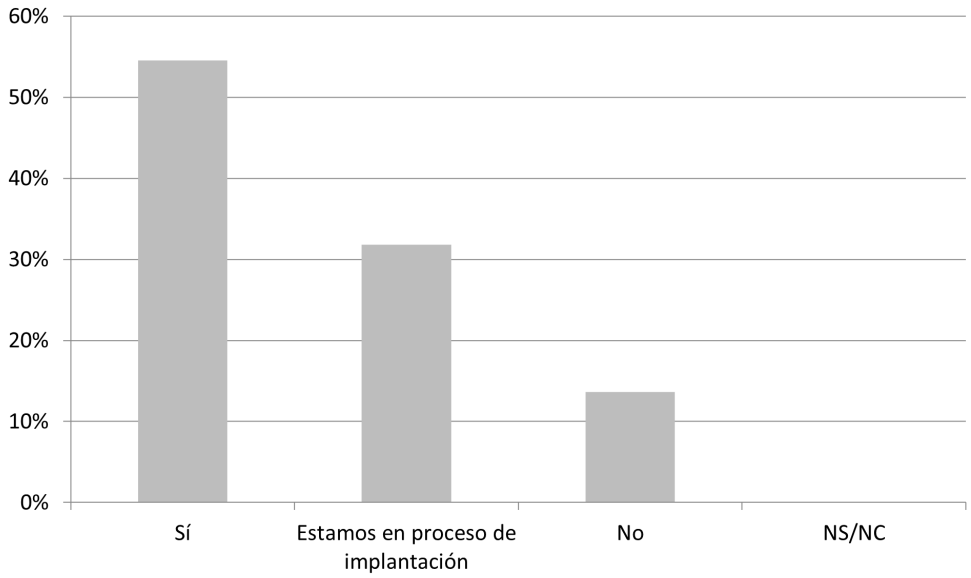

Ilustración 24: ¿Se tiene un procedimiento de diligencia debida de privacidad antes de la gestión o firma de los contratos de encargo?

Aunque muchas empresas siguen teniendo procedimientos de diligencia debida en privacidad en la contratación de encargados de tratamiento, los datos de 2024 sugieren una desaceleración en la adopción y un leve retroceso en la madurez del cumplimiento en comparación con 2023, lo que podría representar un riesgo de cumplimiento si las empresas no fortalecen sus prácticas de diligencia debida en privacidad.

Esta tendencia podría ser explicada por distintas razones, entre las cuales encontramos:

(i) dificultades enfrentadas por empresas para finalizar los procesos de implantación iniciados en 2023,

(ii) "despriorización" del cumplimiento por reasignación de recursos a otras áreas,

(iii) cambio en las entidades participantes del estudio, o

(iv) integración del procedimiento formal de diligencia debida en otros sistemas, lo que lleva a una percepción de que "no existe" un procedimiento específico.

Registro de indicadores para análisis y benchmarking

Número de tratamientos de datos identificados

A diferencia del año pasado, los datos de 2024 revelan que se han identificado más tratamientos de datos que en comparación con otros años anteriores. Esto puede deberse a varios factores, entre los que puede incluirse el uso de nuevas tecnologías, como puede ser la IA.

La mayoría de las organizaciones gestionan un número moderado de tratamientos. El 37,50% de las organizaciones tienen entre 101 y 500 tratamientos, lo que indica que este es el rango más común, aunque más de la mitad de las organizaciones (52,5%) registran menos de 100 tratamientos.

Coincide que más del 50% (21/40) de los participantes, consideran a su vez, que la línea de acción que presenta un mayor nivel de madurez en su organización en cuanto a su implementación es el registro de actividades de tratamiento.

Solo el 7,5% de las organizaciones gestionan entre 501 y 1000 tratamientos. Apenas el 2,5% superan los 1000 tratamientos, y estas organizaciones pertenecen principalmente a sectores como telecomunicaciones y tecnología.

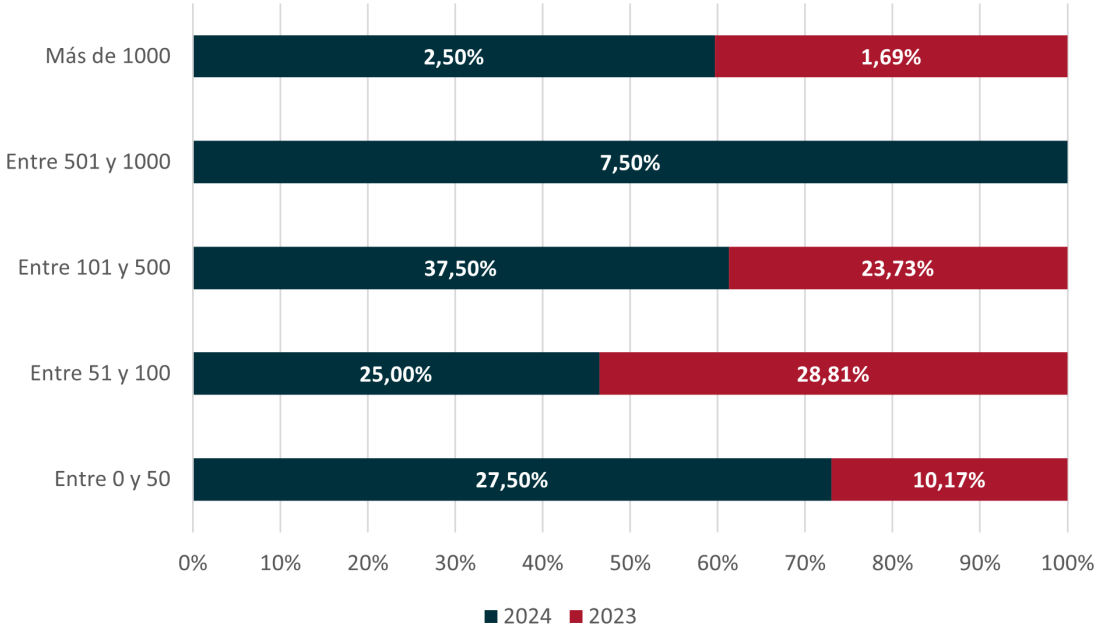

Ilustración 25:¿Qué número de tratamientos de datos tiene registrados?

RAT y PIAs

En la encuesta del año pasado se incluyó como nueva pregunta la frecuencia de actualización del Registro de Actividades del Tratamiento (RAT), obteniendo como conclusión principal que todas las empresas lo actualizan, y que más de un tercio (33,3%) lo hace una vez al año o menos, sin que se evidencien diferencias entre sectores o tamaños de empresa.

Los datos de este año sugieren que la actualización anual del RAT es la práctica más extendida (52,5%). Si bien el RGPD no establece una periodicidad específica, esta frecuencia podría no ser suficiente en organizaciones con modificaciones frecuentes en el tratamiento de datos personales.

El 15% de los entrevistados actualiza el RAT cada seis meses, lo que demuestra un mayor compromiso con la actualización periódica. Por otro lado, solo un 10% lo actualiza únicamente cuando se añade un nuevo tratamiento, lo que puede ser insuficiente si no se revisan los tratamientos existentes o se modifican las condiciones de aquellos ya implementados en la organización.

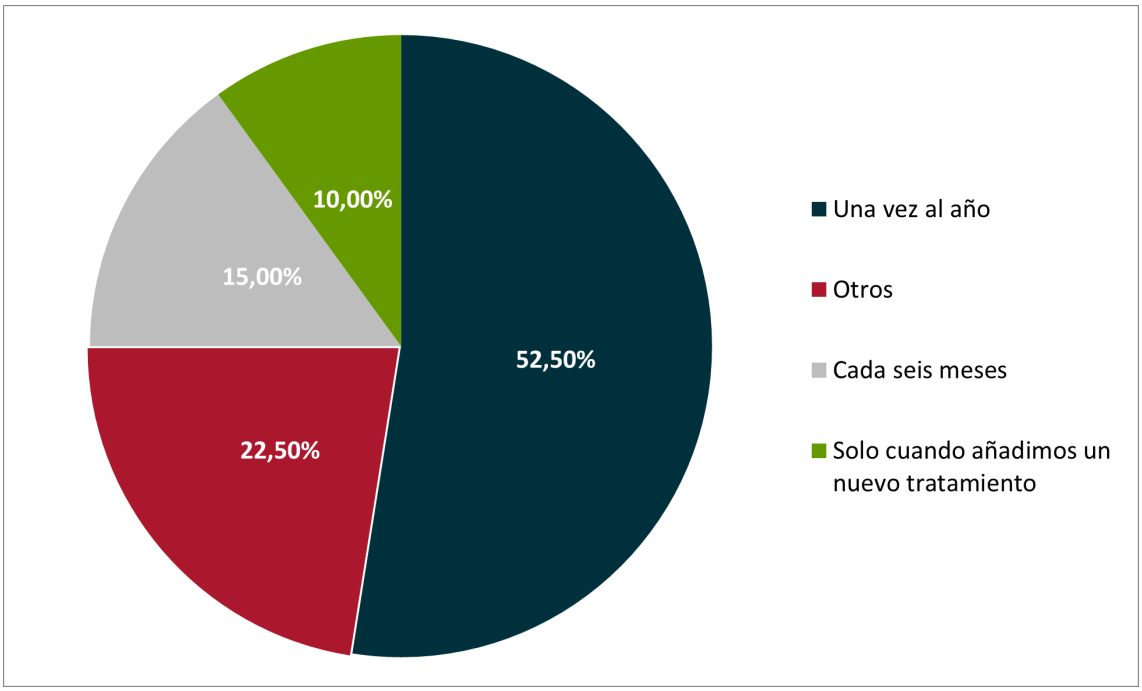

Ilustración 26: Cada cuánto actualizas el RAT

La mayoría de las organizaciones (67,5%) tiene entre 10 y 100 PIAs en vigor, lo que indica que las evaluaciones de impacto son una práctica establecida en una parte significativa de las organizaciones. Un 27,5% de organizaciones ha realizado menos de 10 PIAs, lo que puede deberse, entre otros factores, a que manejan un número reducido de tratamientos de alto riesgo o a que no han identificado correctamente cuándo son obligatorias estas evaluaciones.

El número de empresas que no ha realizado ninguna PIA sigue disminuyendo, situándose en un 5% (frente al 8% en 2023 y al 22% en 2022). Nuevamente, los sectores con más evaluaciones de impacto son el sector Sanitario junto con el de Servicios Financieros.

A pesar de que muchas organizaciones han implementado una gestión avanzada de las evaluaciones de impacto, todavía existe un porcentaje significativo de empresas con baja adopción o sin control adecuado sobre estas evaluaciones (5%). Esto subraya la necesidad de aumentar la sensibilización y establecer procesos que permitan identificar y gestionar los riesgos asociados al tratamiento de datos personales.

De las organizaciones encuestadas, únicamente un 10% ha realizado más de 50 PIAs en 2024, alineándose con aquellas que ya tenían más de 50 PIAs en vigor. Esto sugiere que estas organizaciones probablemente disponen de un proceso más maduro y estructurado para gestionar evaluaciones de impacto. El sector que más PIAs modificó el último año fue el educativo y el de telecomunicaciones.

Tan solo un pequeño porcentaje de organizaciones ha actualizado la totalidad de sus PIAs durante el último año, lo que refleja que la revisión integral sigue siendo un reto para muchas empresas.

Aunque algunas organizaciones han mantenido un enfoque constante en la realización de PIAs, los resultados indican que la mayoría realiza evaluaciones limitadas o no tiene claridad sobre ellas. Esto pone de manifiesto la necesidad de una mayor concienciación, formación y metodologías claras para asegurar que los PIAs se lleven a cabo cuando sean requeridos por el RGPD.

Reclamaciones, violaciones e inspecciones

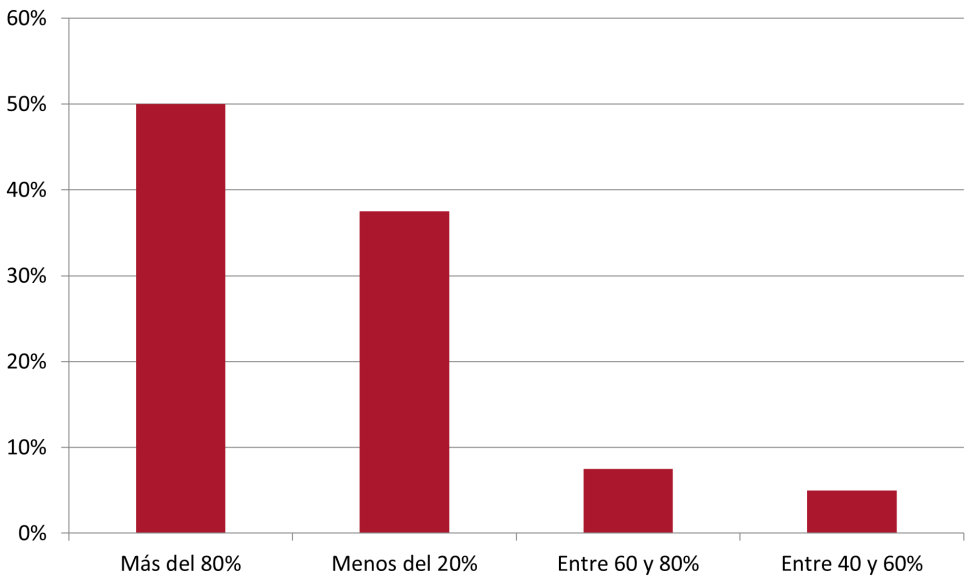

Ilustración 27 : De las reclamaciones que gestionas como DPO, ¿cuántas no acaban como denuncia a la AEPD?

Las organizaciones que han desarrollado procesos efectivos para la atención de solicitudes de reclamaciones consiguen resolver la mayoría sin que se conviertan en denuncias ante la AEPD. El 50% de los DPO logran gestionar más del 80% de las reclamaciones sin que lleguen a denuncia ante la AEPD, lo cual indica una gran capacidad de resolución interna y gestión efectiva de las reclamaciones.

Sin embargo, un porcentaje significativo de empresas aún enfrenta dificultades para gestionar estas reclamaciones de manera interna, lo que puede identificar un área de mejora clave en términos de cumplimiento y gestión de riesgos. Según los resultados de la encuesta, el 37,5% de los DPO solo logra evitar denuncias en menos del 20% de los casos, lo que sugiere dificultades en la resolución temprana de la reclamación realizada.

Según los resultados de la encuesta el 42% de las organizaciones nunca ha notificado una violación de datos a la AEPD. El 37,5% ha reportado menos de 3 incidentes, lo que sugiere que la mayoría de las empresas apenas ha tenido que gestionar este tipo de reportes. Solo un 15% ha informado menos de 5 violaciones, lo que sigue siendo una cifra baja en términos generales.

Se puede identificar como posible razón ante la baja notificación la falta de conocimiento o reticencia a notificar por miedo a sanciones o desactualización de los criterios que obligan a reportar. Aplicando tal vez algunas organizaciones criterios restrictivos para considerar un incidente como una violación de datos que deba comunicarse.

Aunque la baja cantidad de notificaciones puede reflejar una gestión efectiva de la seguridad, es necesario estar en alerta ante un riesgo de falta de notificación. Es recomendable que las organizaciones revisen sus procedimientos internos para asegurarse de que identifican y comunican correctamente las violaciones de datos cuando sea necesario.

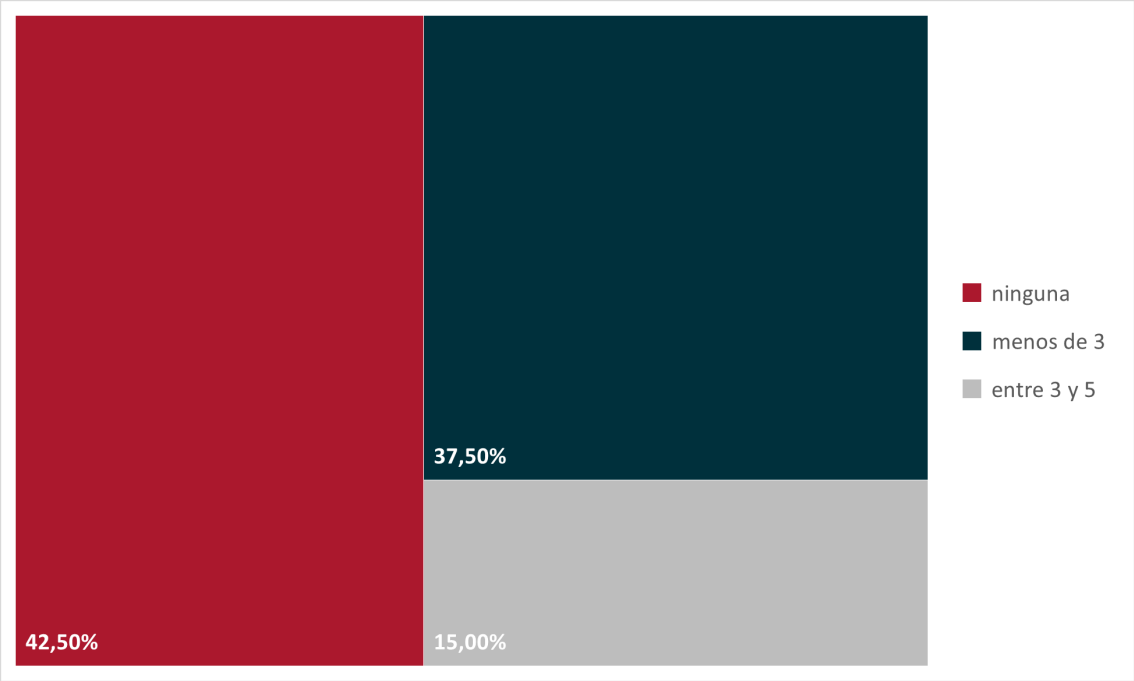

Ilustración 28: Número de violaciones de datos que ha comunicado a la AEPD.

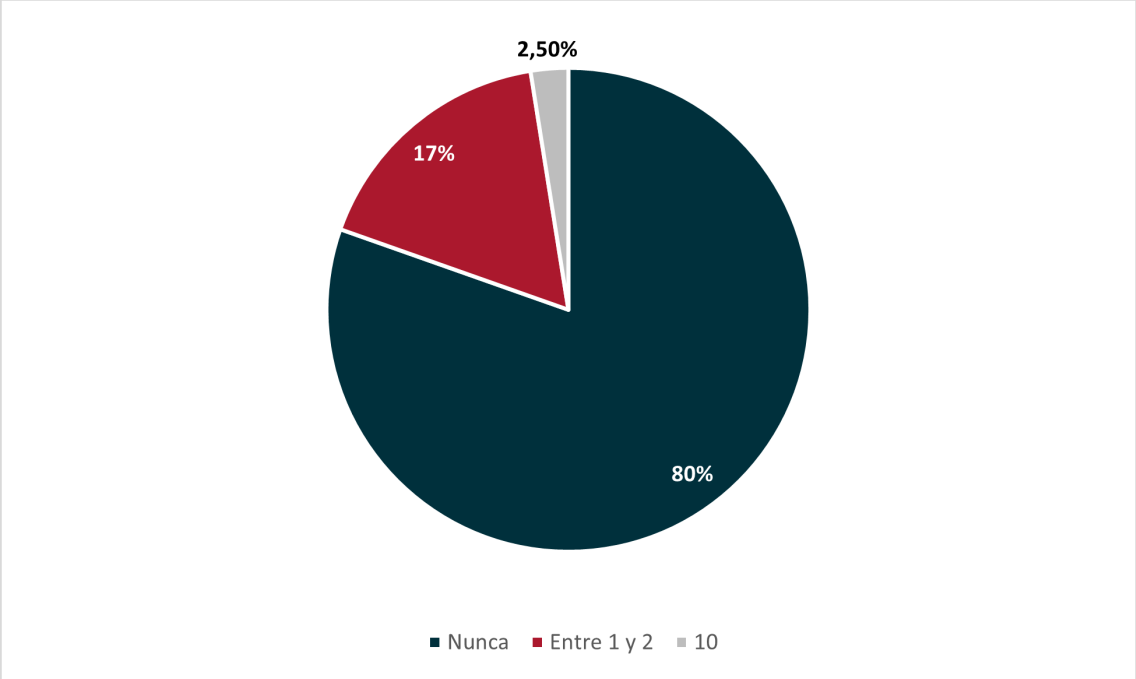

Ilustración 29 : Número de inspecciones que ha tenido

El 80% de los encuestados responden que nunca han tenido una inspección, volviendo a niveles de 2022 (84%), en comparación con los resultados de 2023, donde el 54,24% de las organizaciones indicaba que no tuvieron inspecciones.

De aquellos que han tenido una inspección, la mayoría pertenece al sector salud, seguido por los sectores financiero y de logística y transporte en proporciones menores pero similares. Solo un pequeño porcentaje (aproximadamente 2,5%) correspondiente al sector salud ha reportado hasta 10 inspecciones, siendo el mayor número identificado hasta la fecha.

Es necesario tener en cuenta que la AEPD también actúa tras denuncias o reclamaciones realizadas por los interesados, por lo que un bajo número de inspecciones no significa que las organizaciones estén exentas de sanciones. A pesar de esta baja probabilidad, las organizaciones deben mantener una gestión proactiva de cumplimiento para evitar sanciones.

Inteligencia Artificial

Impacto del Reglamento Europeo de IA en las Empresas

Con la reciente entrada en vigor del Reglamento Europeo de Inteligencia Artificial, el 1 de agosto de 2024, y con los primeros plazos de adecuación ya corriendo, las empresas han iniciado su proceso de adaptación a marchas forzadas.

Este nuevo marco regulatorio supone un hito clave en la protección de los derechos de las personas frente al uso de sistemas de Inteligencia Artificial. Muchas de las obligaciones que impone están estrechamente vinculadas a los modelos de cumplimiento y control en privacidad, como son el análisis de riesgos, la implementación de medidas de mitigación, la gestión de incidentes, y la formación de empleados. A ello debemos sumar que muchos de los casos de uso, entrenamiento de algoritmos e integración de sistemas IA están íntimamente relacionados con el tratamiento de datos personales.

En este contexto, y dada la importancia creciente de la IA en el cumplimiento normativo, seguimos planteándonos preguntas sobre la aplicación práctica del Reglamento de IA y su impacto en las organizaciones, lo que se refleja en las encuestas que realizamos.

Gobernanza y Responsabilidad en el Cumplimiento del Reglamento de IA

Dado que el cumplimiento del Reglamento de IA requiere una gobernanza clara, resulta clave definir sobre quién recae la responsabilidad de su implementación en las empresas.

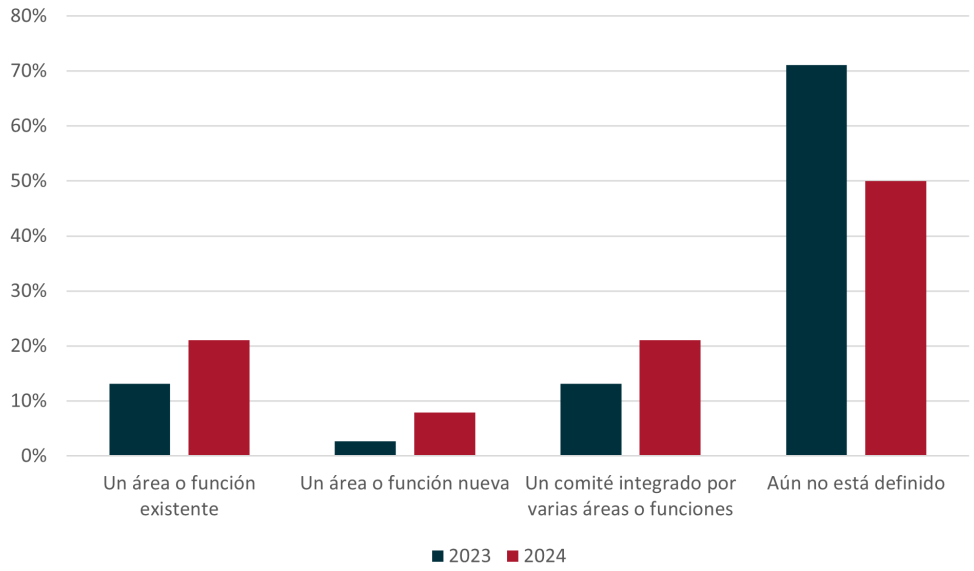

Ilustración 31: ¿Sobre quién recae la responsabilidad de cumplimiento del Reglamento de IA?

Un año después de que nos hiciéramos esta misma pregunta por primera vez, y con el Reglamento de IA ya en vigor, podemos ver que el grado de madurez de las compañías en cuanto al gobierno de sus iniciativas de IA ha tenido una mejora considerable.

El 50% de los encuestados, frente al 71% que contestó lo mismo en 2023, indica que su compañía aún no se ha planteado sobre quién debe recaer la responsabilidad de cumplimiento del nuevo Reglamento de IA.

Esta falta de planificación podría indicar una falta de conciencia sobre las implicaciones regulatorias de la IA o una falta de iniciativas proactivas para abordarlas, sobre todo teniendo en cuenta que el reglamento establece diferentes fechas de cumplimiento para la aplicación de sus disposiciones, y que algunas de estas ya están vencidas, como es la prohibición de aquellas prácticas relacionadas con la IA que se consideran de riesgo inaceptable por vulnerar derechos fundamentales y valores de la Unión Europea.

Dentro del 50% restante, donde se encuentran los encuestados que sí se han planteado sobre quién recae la responsabilidad del cumplimiento del Reglamento de IA, hay diversidad de opiniones: Un 21% de los encuestados ha considerado que lo más adecuado es que un área o función ya existente fuera quien debía heredar dicha responsabilidad, otro 21% considera que la responsabilidad debía ser compartida en un comité que integra a varias áreas o funciones; mientras que tan solo un 8% de los encuestados cree que debía crearse una función nueva para heredar estas responsabilidades.

Estos datos reflejan que, aunque las empresas han avanzado en la reflexión sobre la gobernanza de la IA, aún queda camino por recorrer para consolidar estructuras de cumplimiento sólidas y alineadas con las exigencias del Reglamento. Con los plazos de adecuación en marcha, la necesidad de definir responsabilidades y estrategias claras se vuelve más urgente que nunca.

Análisis de Responsabilidad en Empresas

Tras identificar la necesidad de definir una estructura de gobernanza, exploramos a qué áreas dentro de las organizaciones se les ha asignado la responsabilidad del cumplimiento del Reglamento.

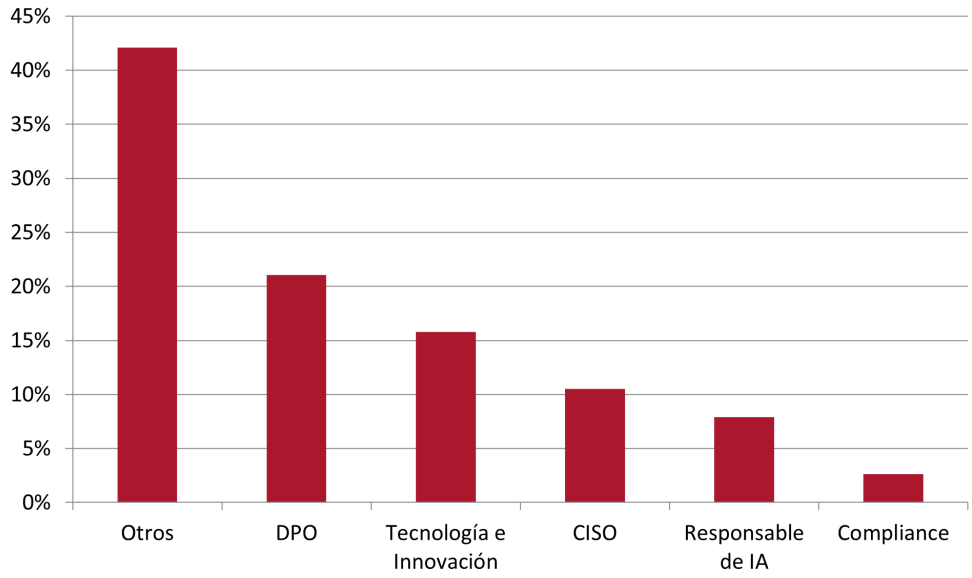

Ilustración 32: En caso de asignarse a un área o función existente, ¿Cuál es?

En línea con la pregunta anterior y, ahondando un poco más en la cuestión de qué área o función debería ser la que herede la responsabilidad del cumplimiento del nuevo Reglamento de IA, vemos que hay una opción que se destaca de las demás, y que se consolida como destacada comparando los resultados de la encuesta de 2024, con los de 2023.

Los resultados sugieren una diversidad en la posible asignación de responsabilidades para el cumplimiento del Reglamento de Inteligencia Artificial (IA) dentro de las compañías. El DPO (21,06%) y el CISO (10.53%) se mantienen como las opciones que la mayoría de las empresas encuestadas han elegido para heredar la responsabilidad del cumplimiento del reglamento, lo que destaca la importancia de la privacidad y la seguridad en la implementación de IA, y las sinergias que este nuevo reglamento puede tener con GDPR, y los procesos de Privacy by design y Security by Design.

Vemos también cómo se considera una opción viable el trasladar estas responsabilidades a las funciones y equipos más técnicos, y que más cerca están del propio desarrollo de estas soluciones de IA, como pueden ser el Responsable de IA (7,89%), o el área de Tecnología e Innovación (15,79%), lo que refleja la necesidad de abordar los aspectos éticos y regulatorios de la IA desde las fases de diseño de la solución técnica.

Por último, se aprecia que la opción "Otros" sigue siendo escogida por un gran número de encuestados (42,11%), lo que indica una variedad de enfoques organizativos para cumplir con estos nuevos requerimientos regulatorios por parte del Reglamento de IA en la efectiva implantación de un sistema de cumplimiento y gestión de riesgos

Apliación de la IA en las Empresas

Más allá del cumplimiento normativo, es relevante conocer para qué están utilizando las empresas la inteligencia artificial y qué aplicaciones tienen más presencia en el entorno corporativo.

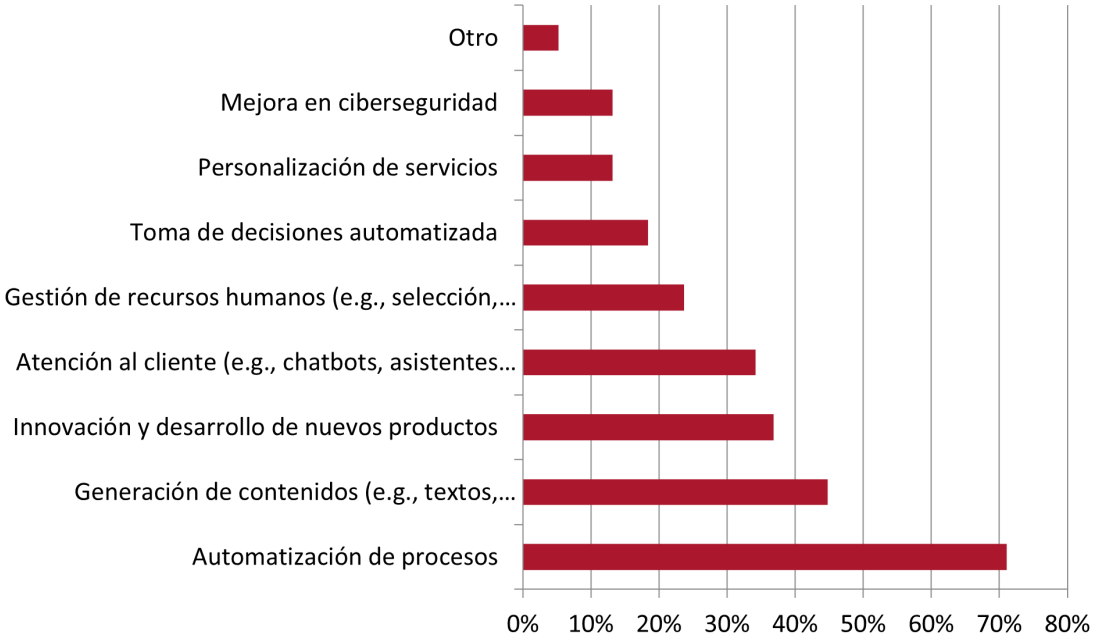

Ilustración 33 : ¿Para qué fines principales utiliza IA su organización?

La inteligencia artificial se ha convertido en una herramienta clave en la estrategia de muchas organizaciones, pero su aplicación varía ampliamente según el sector, la madurez tecnológica y las necesidades específicas de cada empresa. Para comprender mejor cómo las compañías están aprovechando la IA, hemos preguntado a los encuestados en qué ámbitos y con qué finalidades la están utilizando. Los resultados nos permiten no solo identificar las tendencias actuales, sino también analizar cómo ha evolucionado el uso de la IA en comparación con años anteriores.

Se observa que la opción más seleccionada por los encuestados ha sido la de Automatización de procesos, con un 71,05%, lo que refleja que las empresas siguen viendo en la IA una herramienta clave para mejorar la eficiencia operativa, reducir costos y optimizar tareas repetitivas. Este dato sugiere que, aunque la IA está ganando terreno en ámbitos más estratégicos, su principal aplicación sigue estando en la optimización de procesos internos ya existentes.

Más allá de la automatización de procesos, la segunda finalidad más mencionada por los encuestados es la Generación de contenidos (44,74%), lo que evidencia el creciente uso de modelos de IA generativa en la creación de textos, imágenes y vídeos. Le sigue en tercer lugar Innovación y desarrollo de nuevos productos (36,84%), lo que indica que muchas empresas ya están explorando la IA como un motor de transformación y diferenciación en el mercado; y en cuarto lugar, con un 34,21%, se encuentra la Atención al cliente, donde chatbots y asistentes virtuales están consolidándose como soluciones clave para mejorar la experiencia del usuario y optimizar la gestión de consultas.

A medida que las empresas maduren en la adopción de soluciones con IA y, sobre todo, en la adopción del Reglamento, es previsible que los fines para los que esta se use continúen diversificándose, impulsando nuevos modelos de negocio y redefiniendo la manera en que operan.

Clasificación de los Sistemas de IA según Reglamento

Dado que la regulación europea clasifica los sistemas de IA en función de su nivel de riesgo, es fundamental comprender cómo las empresas encuestadas han categorizado sus soluciones.

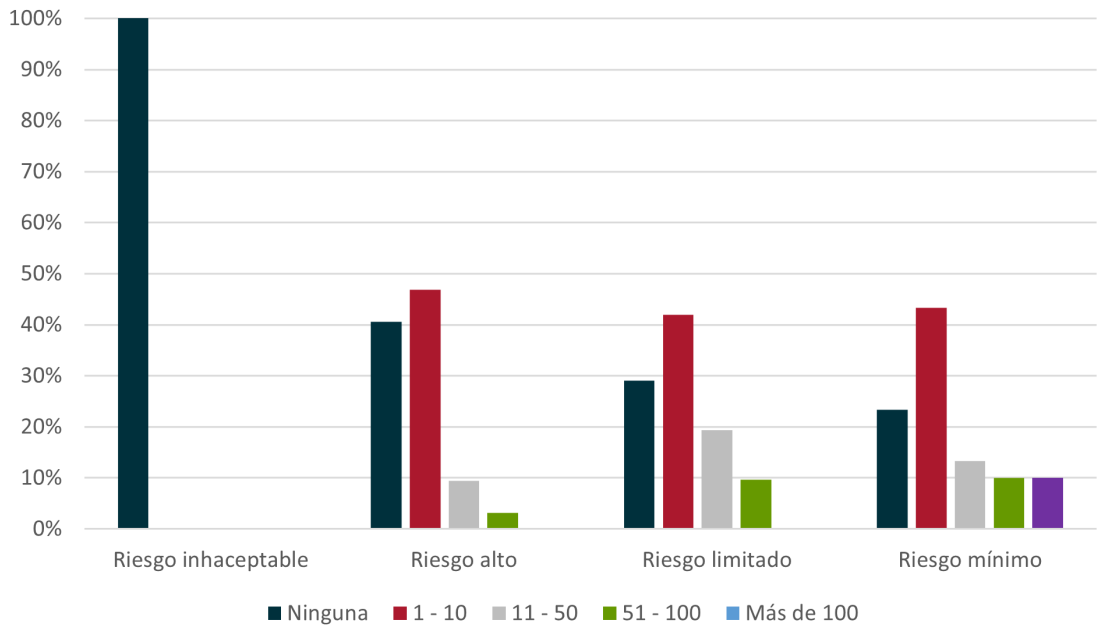

Ilustración 34 : ¿Con qué nivel de riesgo del Reglamento de IA (RIA) se clasifican los sistemas de IA presentes en su organización?

El Reglamento Europeo de IA clasifica los sistemas de inteligencia artificial en diferentes niveles de riesgo, estableciendo requisitos proporcionales a su impacto potencial en los derechos y libertades de las personas. Para entender cómo las empresas están gestionando esta clasificación, hemos preguntado a los encuestados cuántos sistemas de IA tienen en funcionamiento y en qué categorías de riesgo encajan según la normativa. Este análisis nos permite identificar el grado de exposición de las compañías a las obligaciones regulatorias y evaluar su nivel de preparación para cumplir con los requisitos asociados a cada tipo de sistema.

Como se aprecia, tras sus correspondientes análisis, ninguno de los encuestados dice estar utilizando o desarrollando sistemas de IA que puedan encuadrarse dentro de las prácticas que el Reglamento entiende como prohibidas. El gráfico revela que la mayoría de las compañías encuestadas tienen un volumen significativo de sistemas de IA clasificados en las categorías de menor nivel de riesgo, como 'Riesgo Alto', 'Riesgo Medio' y 'Riesgo Limitado'.

A medida que el nivel de riesgo disminuye, vemos como también disminuye el número de encuestados que afirman que su compañía no dispone sistemas de IA encuadrados en esa categoría de riesgo, o de que sean menos de una decena de sistemas de IA: En Sistemas de Riesgo Alto, ese valor agregado alcanza el 87,51%, en sistemas de Riesgo limitado, el 70,97%; y en sistemas de Riesgo mínimo, el 66,66%

Este patrón sugiere que las empresas están adoptando enfoques más cautelosos en su implementación de IA, priorizando soluciones que, aunque innovadoras, se consideran de bajo impacto en términos regulatorios.

Merece la pena destacar que entre las empresas que afirman disponer de un alto volumen de sistemas de IA clasificados como de Riesgo Alto, en su mayoría pertenecen al sector sanitario. Este resultado es coherente con el papel que juega la IA en este ámbito, donde su aplicación en diagnósticos, tratamientos y gestión de datos clínicos implica un impacto directo en la seguridad y los derechos de las personas. Dado que el Reglamento Europeo de IA impone requisitos estrictos para estos sistemas, las compañías del sector salud se enfrentan a mayores desafíos de cumplimiento y gobernanza tecnológica.

Conclusiones

En conclusión, la nueva regulación de la IA establece un marco normativo crucial para garantizar que el uso de estas tecnologías respete los derechos fundamentales de las personas, complementando las disposiciones del RGPD. A pesar de que ambas normativas abordan diferentes aspectos del cumplimiento, su interrelación es evidente, especialmente en lo que respecta al tratamiento de datos personales en sistemas de IA. Las empresas deben adaptarse a esta dualidad normativa, implementando políticas de gobernanza que aseguren tanto la privacidad como la seguridad en el uso de la IA desde el diseño. Este desafío, aunque complejo, ofrece una oportunidad clave para las organizaciones de fortalecer sus estructuras de cumplimiento y avanzar hacia un uso responsable y ético de la inteligencia artificial.

Resumen Ejecutivo

Desde el DPI de ISMS Forum llevamos estudiando y apoyando la figura del DPO desde hace muchos años y fomentando las mejores prácticas de cumplimiento en privacidad para todas las organizaciones.

El Observatorio y estas encuestas nos ayudan a valorar la evolución de las compañías respecto al cumplimiento en privacidad, así como la evolución del DPO a lo largo del tiempo, reflejando hitos conseguidos, niveles de madurez alcanzados, así como retos, preocupaciones y problemas a los que damos visibilidad.

Podemos anunciar como principales conclusiones:

1. Posición Estratégica y nivel de madurez:

La figura de DPO se va consolidando dentro de las organizaciones, respecto a su nivel de autonomía y su nivel de report a la Dirección. Sigue siendo importante la preparación de los DPO, su formación y certificaciones profesionales.

Los sistemas de cumplimiento en privacidad están madurando, están definidos, implantados y auditados en muchos casos, y se mantiene como punto importante la colaboración interdepartamental (Ciberseguridad, Asesoría jurídica, Compliance, etc.) para abordar de manera integral las cuestiones de privacidad.

Se sigue una senda importante de automatización de diversas tareas y líneas de actividad de los DPO, y destaca la necesidad de operativizar con tecnología tareas como la gestión de derechos, la realización de PIAs, la gestión de riesgo de terceros (diligencia debida y encargados de tratamiento) o la realización periódica de auditorías.

2. Retos y necesidades:

Los datos siguen revelando otra vez una necesidad significativa de asignación de recursos y equipo de trabajo, subrayando la importancia de una inversión adecuada en este ámbito no solo para equipo interno sino también para asesores externos, formación, herramientas, etc.

Asimismo, se pone de relieve la necesidad de trabajar y mejorar en respuesta regulatoria ante incidentes y nuevas normas, mantener un adecuado sistema de auditorías, así como el trabajo para vencer las resistencias internas.

3. Desafíos Emergentes:

Podemos destacar algunos desafíos emergentes, como la adaptación a nuevas regulaciones y la gestión de incidentes de seguridad, que están en el centro de las preocupaciones de los profesionales de privacidad y de los responsables de los que dependen.

Con la llegada del Reglamento de IA y entrada en aplicación, se nota que las compañías comienzan a diseñar modelo de gobernanza, aunque aún quedan muchas que les falta comenzar a definir. Los DPOs y los CISOs destacan como el rol más habitual para liderar la implantación y cumplimiento regulatorio de los nuevos requisitos del Reglamento de IA, dejando ver las sinergias entre los nuevos requisitos normativos y los sistemas de cybercompliance y RGPD.

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

OBSERVATORIO DE LA PRIVACIDAD

www.ismsforum.es
info@ismsforum.es
(+34) 915 63 50 62

Una iniciativa de

isms forum

dpi DATA PRIVACY INSTITUTE