www.ismsforum.es

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

OBSERVATORIO DE LA PRIVACIDAD

Una iniciativa de

isms forum

dpi DATA PRIVACY INSTITUTE

Febrero 2024

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	Alberto Lopez
	Cristina Köhler
	Edison Hernández-Suero
	Ignacio Cagiga
	Jaime Requejo
	Josep Bardallo
	Laura Elia Caballero
	Óscar López
	Xabier Alberdi
GESTIÓN DE PROYECTOS	Beatriz García González
DISEÑO/MAQUETACIÓN	Cynthia Rica Gómez

CONTENIDOS

Introducción

Objetivos del Observatorio de Privacidad

Presentamos con enorme entusiasmo y gratitud la 5ª edición del Estudio del Observatorio de la Privacidad desarrollado por el Data Privacy Institute de la Asociación ISMS Forum. Los resultados que se plasman en este informe final son resultado de una Encuesta dirigida y contestada por los Delegados de Protección de Datos de diferentes organizaciones en nuestro país.

Los objetivos del Observatorio de la Privacidad son:

- Convertirse en una plataforma para el análisis del nivel de madurez de cumplimiento en el ámbito de la protección de datos.
- Revelar las tendencias y los retos que comparten los Delegados de Protección de Datos de entidades públicas y privadas.
- Generar métricas e indicadores en nuestro país que permitan la realización de análisis comparativos e informes de benchmarking en la función de protección de datos.
- Colaborar y establecer relaciones de interlocución con instituciones y reguladores.

La Encuesta y el Estudio

Esta iniciativa ha sido diseñada con el objetivo de arrojar luz sobre los roles cruciales desempeñados por los expertos en privacidad dentro de las organizaciones y ofrecer un análisis exhaustivo de las dinámicas actuales en el ámbito de la protección de datos.

En el transcurso de esta encuesta, hemos recopilado información valiosa que arroja luz sobre aspectos clave de la función de Delegado de Protección de Datos. Los resultados no solo proporcionan una instantánea detallada de la posición actual de los DPD en las empresas, sino que también destacan las tendencias emergentes y los desafíos que enfrentan en el panorama dinámico de la privacidad.

Agradecemos sinceramente la participación activa de todos los encuestados, cuyas respuestas han sido fundamentales para la creación de este informe exhaustivo. Continuaremos trabajando juntos en los próximos años para fortalecer la comunidad de profesionales de privacidad y contribuir al avance de la protección de datos en el ámbito de empresas y Administraciones Públicas.

Este informe no solo sirve como un testimonio de las tendencias actuales en la gestión de la privacidad, sino que también proporciona a los líderes empresariales y a los profesionales de privacidad una herramienta valiosa para evaluar y mejorar sus prácticas. Al comprender las complejidades y desafíos que enfrenta la comunidad de privacidad, estamos mejor equipados para avanzar hacia un futuro donde la protección de datos sea una prioridad compartida.

Utilidad del Estudio

Uno de los aspectos más destacados de este informe es su utilidad como herramienta de benchmarking para profesionales de privacidad y Delegados de Protección de Datos (DPD). La comparación de prácticas, posiciones y desafíos dentro de nuestra comunidad ofrece a cada profesional la oportunidad de evaluar su desempeño en relación con sus pares en diversas empresas y organizaciones. Este enfoque comparativo no solo fomenta la transparencia, sino que también proporciona beneficios significativos a nivel individual y organizacional.

En este sentido, el Estudio pretende aportar los siguientes beneficios:

- Identificación de Mejores Prácticas: Al analizar las respuestas de profesionales en roles similares, cada encuestado tiene la oportunidad de identificar y adoptar las mejores prácticas utilizadas por líderes de la industria.
- Evaluación de Posicionamiento: El benchmarking permite a los profesionales evaluar su posición en la jerarquía organizativa y comprender cómo se comparan en términos de responsabilidades y nivel de influencia en comparación con otros colegas.
- Optimización de Recursos: Al conocer las asignaciones de recursos en otras empresas, los profesionales pueden abogar por inversiones más efectivas y estratégicas en sus propios programas de privacidad.
- Preparación para Desafíos Futuros: La identificación de desafíos compartidos por profesionales en roles similares permite una preparación proactiva para los cambios y desafíos que puedan surgir en el futuro.

Este enfoque de benchmarking no solo sirve como una herramienta de autoevaluación, sino que también fomenta la colaboración y el intercambio de conocimientos entre profesionales. Al conocer las experiencias y enfoques de otros, la comunidad de privacidad puede crecer colectivamente y enfrentar los desafíos de manera más efectiva.

Al revisar este informe, alentamos a cada profesional a reflexionar sobre cómo sus prácticas y enfoques se comparan con las tendencias identificadas. Os invitamos a utilizar esta información como un trampolín para mejorar continuamente y contribuir al desarrollo de estándares más elevados en la gestión de la privacidad.

Estudio sobre el nivel de madurez en la aplicación del RGPD

Conforme a lo que dispone el Reglamento General de Protección de Datos (RGPD), la rápida evolución de la tecnología requiere de un marco sólido y coherente que proteja el tratamiento de datos personales realizado dentro de la Unión Europea, dada la importancia de generar confianza para permitir el desarrollo eficaz de la economía digital.

Para lograr este objetivo, dicha norma establece un modelo de cumplimiento basado en la prevención y gestión del riesgo derivado del tratamiento de información personal, exigiendo la aplicación de medidas jurídicas, técnicas y organizativas adecuadas con las que poder acreditar el correcto cumplimiento de las obligaciones que la norma impone al responsable y al encargado del tratamiento, en su caso.

Esta es la premisa con la que ISMS Forum puso a disposición del mercado una herramienta de evaluación a través del primer indicador nacional de madurez en protección de datos personales con el que las organizaciones puedan determinar el nivel de riesgo que mantienen en comparación con la media establecida.

Tipología de la muestra

La muestra de nuestro estudio está formada en su mayoría por grandes compañías. Las empresas más representativas cuentan con más de 1.000 empleados (más del 75%) y entre ellas, más del 28% cuentan con más de 20.000 empleados. Tan solo el 21% son pequeñas y medianas empresas.

Por lo tanto, aunque la mayoría de las empresas encuestadas tienen entre 1.000 y 4.999 empleados, también hay una proporción considerable de empresas con más de 20.000 empleados. Esta diversidad en el tamaño de las empresas sugiere que se han obtenido perspectivas desde diferentes escalas operativas, y esto, a su vez, influye en el nivel de madurez en la aplicación del RGPD. Aunque se verá más adelante, es probable que las empresas más grandes tengan recursos y capacidades diferentes para implementar y cumplir con los requisitos del RGPD en comparación con las más pequeñas.

Del mismo modo son organizaciones con grandes volúmenes de facturación, más del 52% de las encuestas corresponden a empresas con facturaciones anuales superiores a 1.000 millones de euros, y dentro de este grupo, cerca de un 17% cuenta con una facturación superior a 10.000 millones de euros.

Por esto mismo, en cuanto a los ingresos anuales totales de las empresas encuestadas, se observa una distribución variada en los diferentes rangos de ingresos. Desde empresas con menos de 200 millones de euros en ingresos anuales hasta aquellas con más de 10.000 millones de euros. Este espectro es indicativo de una amplia gama de capacidades financieras entre las empresas participantes. Las empresas con mayores ingresos pueden tener más recursos disponibles para invertir en medidas de cumplimiento del RGPD, como la contratación de personal especializado o la implementación de tecnologías avanzadas de protección de datos.

En cuento a los sectores más representativos de la muestra, destaca, por encima de todos, el sector financiero, con un 25% del total, el doble que los dos siguientes que serían Industria, Construcción e Infraestructuras y Administraciones Públicas, en ese orden.

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.

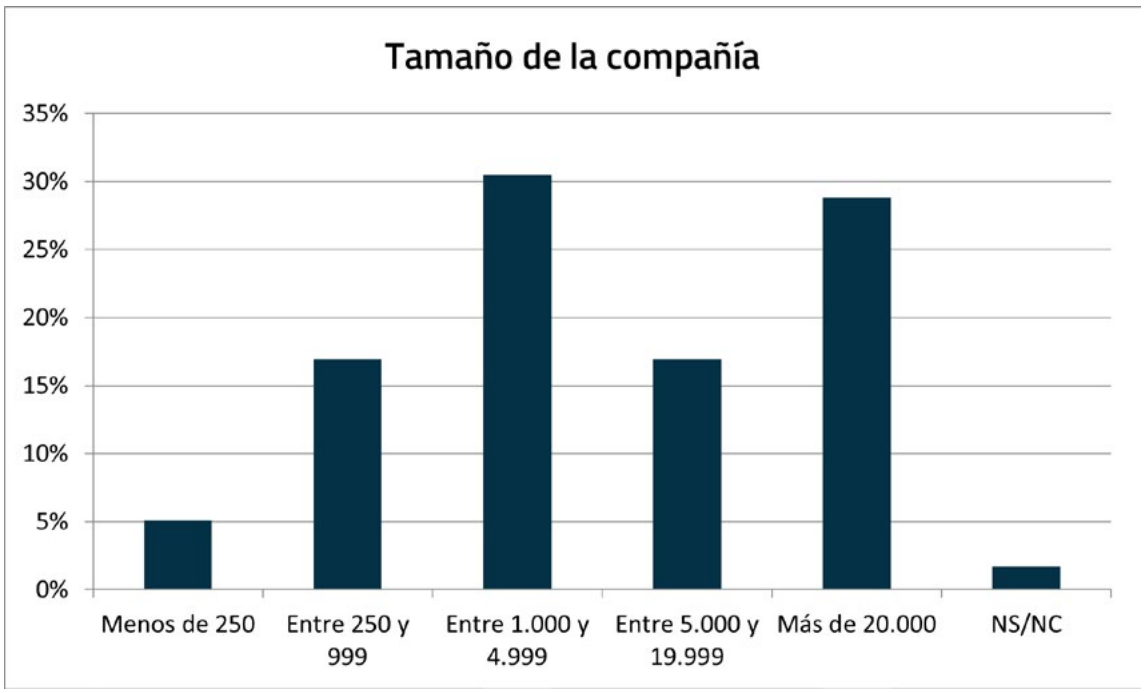

Ilustración 2: Facturación de la compañía

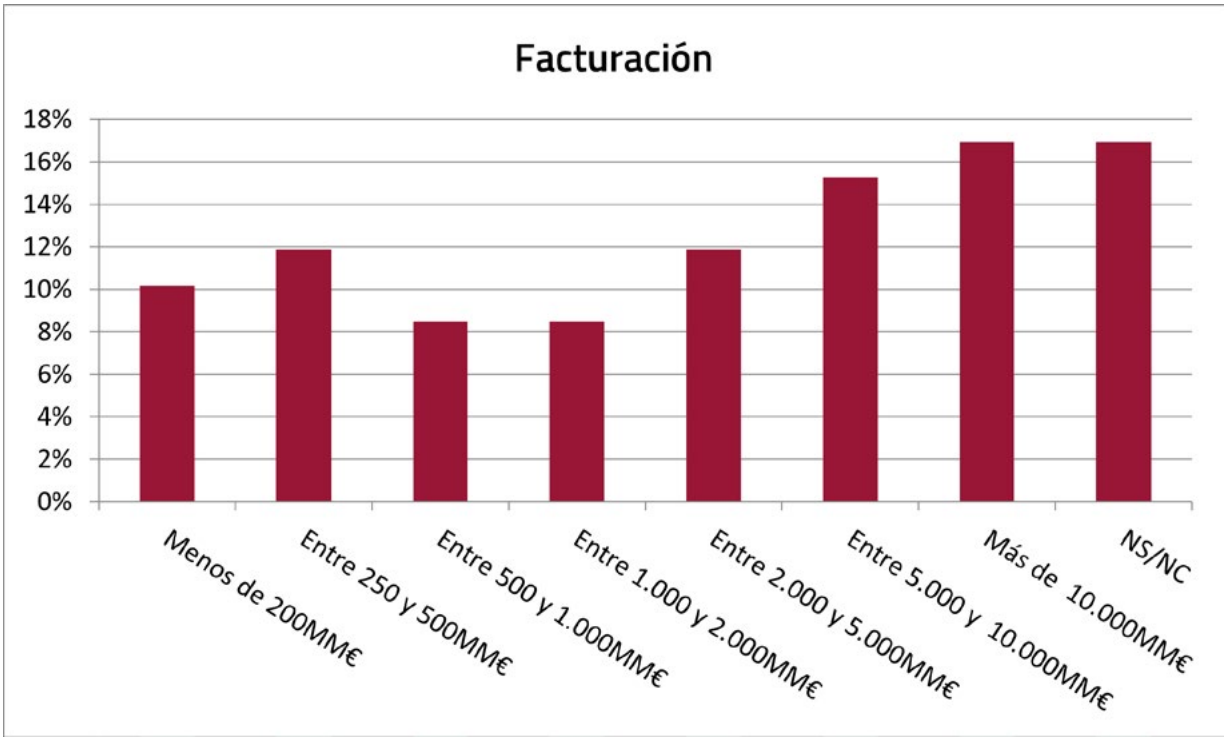

Ilustración 2: Facturación de la compañía

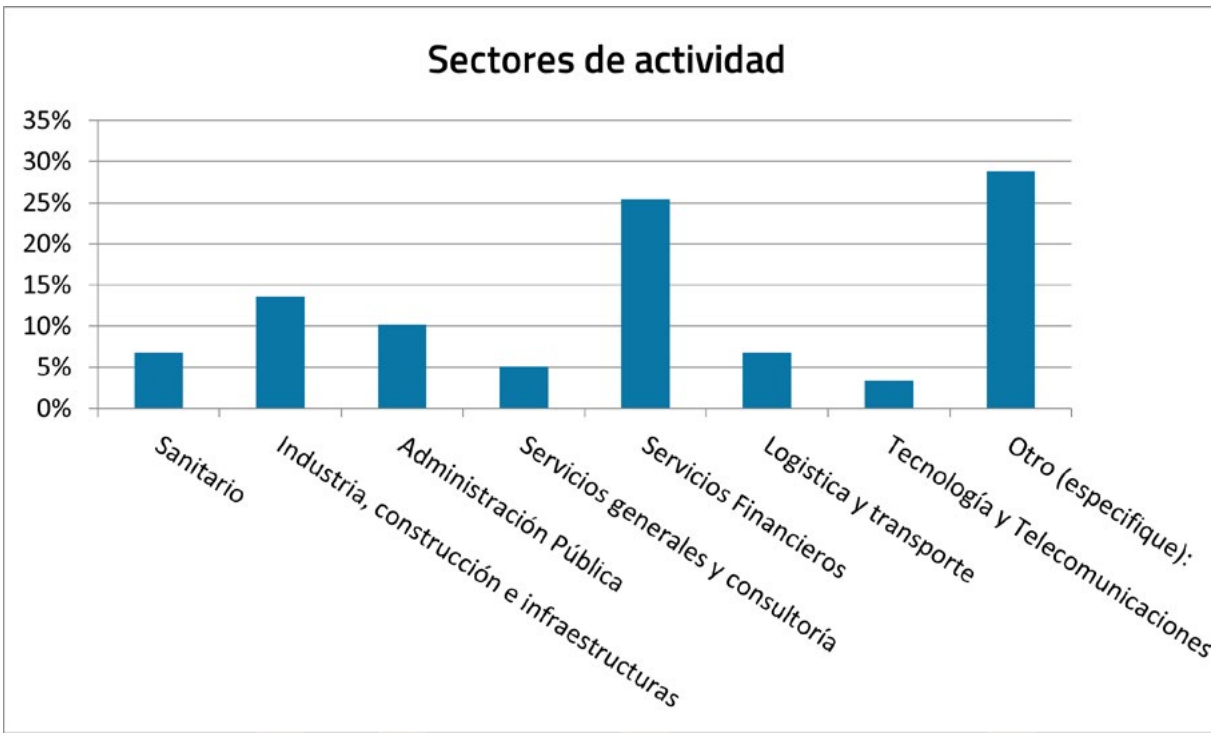

Ilustración 3: Sector de actividad de la compañía

Estado de situación -Gobierno de la Privacidad

Tipo de DPO y alcance geográfico de la función

En relación con el tipo de DPO nombrado en las empresas entrevistadas, durante este año continua la tendencia que veíamos en años anteriores donde el DPO tenía una función en exclusividad de protección de datos, y se identificaba como un área independiente de las ya existentes en las compañías. Como se puede apreciar en el gráfico actual de 2023, su externalización ha disminuido y la opción del Órgano Colegiado ha vuelto a emerger en comparación con el año anterior.

En relación con el tipo de DPO nombrado en las empresas entrevistadas, la predominancia (55.32%) de DPOs internos dedicados exclusivamente a Privacidad y Protección de Datos refleja un compromiso firme con el cumplimiento del RGPD por parte de las empresas, con tendencia ascendente desde 2021. Es decir, hay una asignación específica de recursos para garantizar la conformidad normativa. Sin embargo, la presencia significativa (29.79%) de DPO asumidos dentro de áreas existentes sugiere una integración progresiva de la función de protección de datos en la estructura organizativa. La elección del 10.64% de órganos colegiados como DPO o la externalización del rol (4.26%) también revela diferentes enfoques para abordar los requisitos del RGPD, posiblemente influenciados por consideraciones de recursos, arquitectura organizativa y/o estrategias de gestión del riesgo de privacidad en cada caso.

En definitiva, estos resultados indican una variedad de enfoques adoptados por las empresas para cumplir con los requisitos de protección de datos, reflejando su diversidad y la adaptación a las necesidades específicas de cada organización.

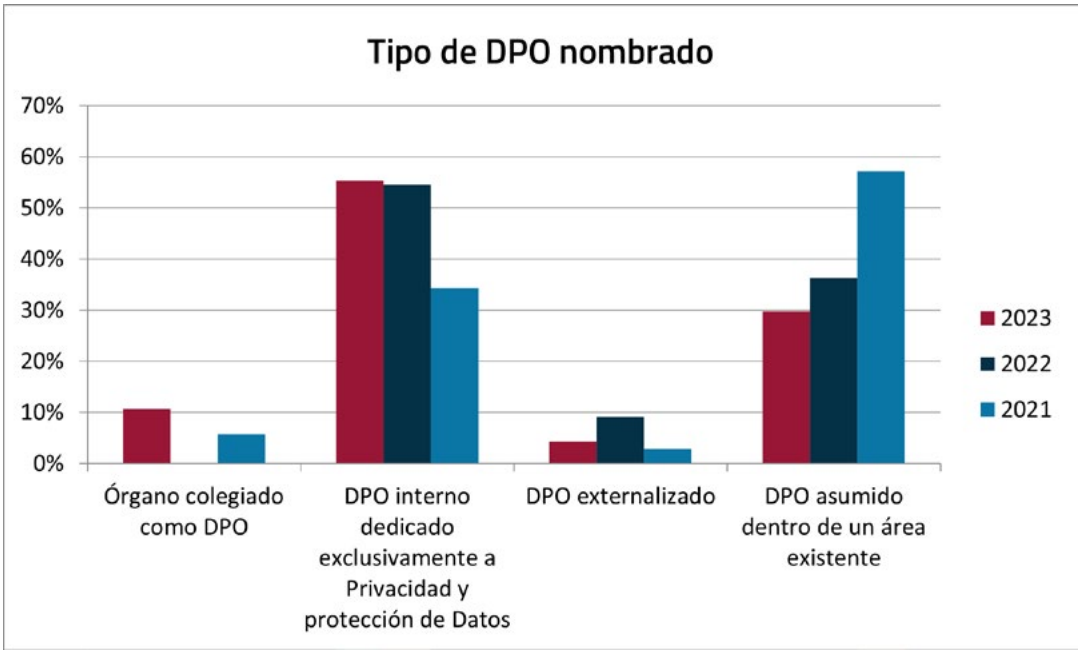

Ilustración 4: Tipo de DPO nombrado

Respecto a la compatibilidad del cargo con otras funciones, se mantiene la tendencia de años anteriores. Cerca de la mitad (46.81%) de los DPOs no compatibilizan su cargo con otras funciones, lo que sugiere una dedicación exclusiva a la protección de datos. Sin embargo, un porcentaje significativo asume responsabilidades adicionales, especialmente en áreas como Compliance (17.02%), Legal/Asesoría jurídica (17.02%) y CISO (21.28%), lo que podría afectar su capacidad para priorizar efectivamente las tareas de privacidad. El 6.38% restante ejerce funciones adicionales no especificadas, lo que indica una variedad de roles combinados que podrían influir en la eficacia de la gestión de la privacidad.

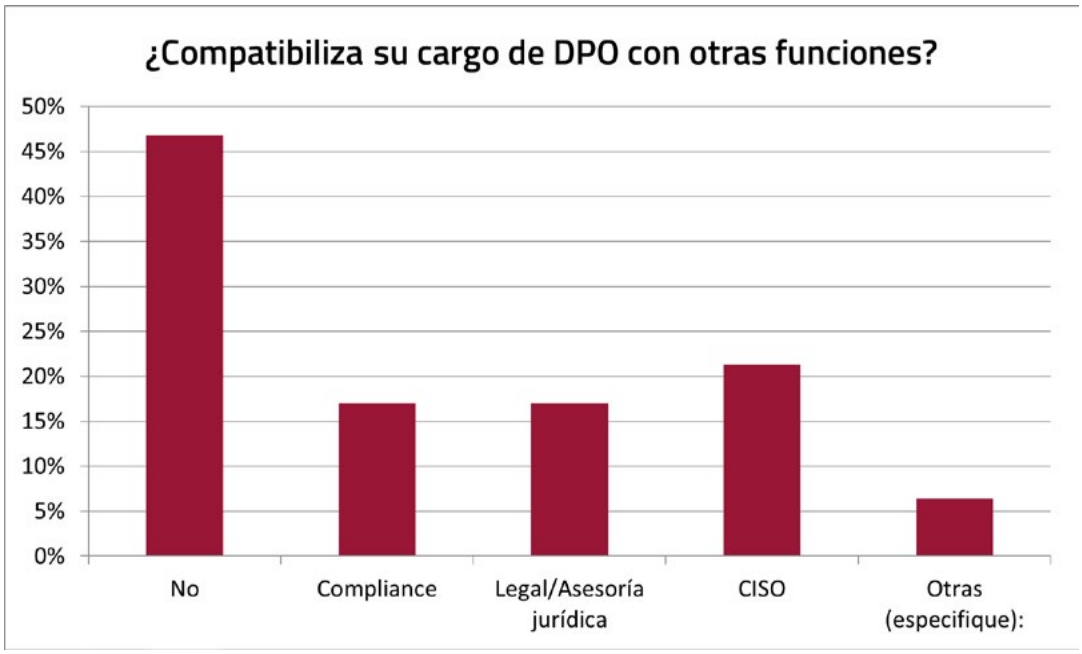

Ilustración 5: Compatibilidad del cargo de DPO

En relación con el alcance territorial de su competencia, la mayoría de los DPOs (63,83%) tienen un alcance exclusivamente en el ámbito nacional (en comparación con el año anterior que era un 84%). Esto sugiere un enfoque local en la gestión de la privacidad Sin embargo, un porcentaje significativo (21.28%) también abarca otros países europeos, mientras que una minoría (14.89%) se extiende más allá de Europa, reflejando una diversidad en el alcance geográfico de las competencias del DPO.

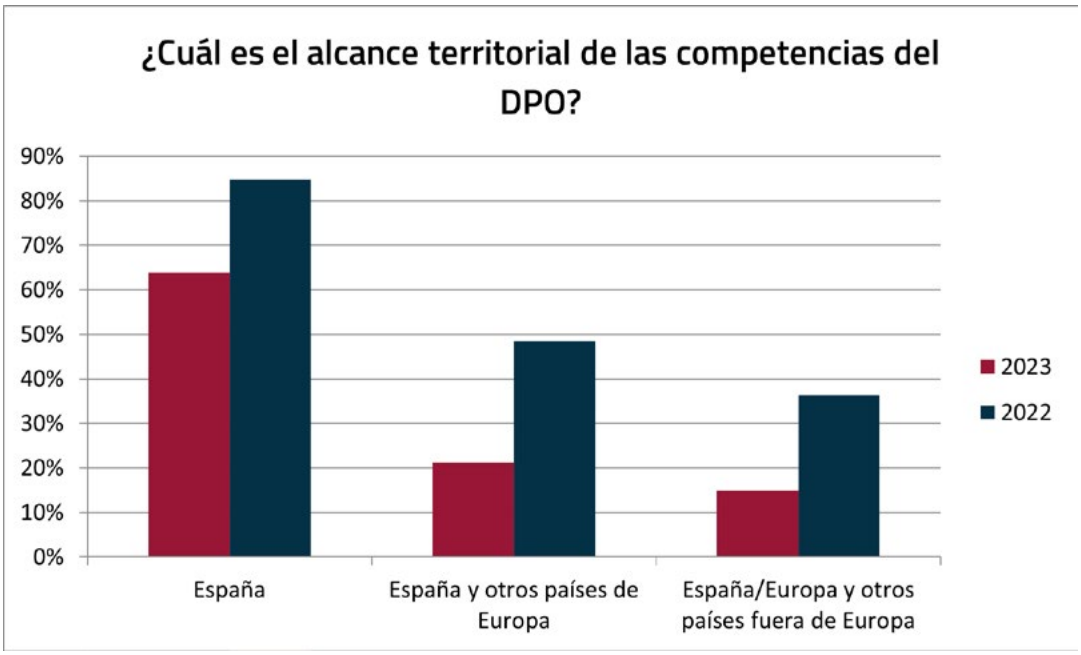

Ilustración 6: Alcance territorial del DPO

Formación académica y certificaciones de los DPOs

La mayoría de los DPOs poseen formación legal (55.32%), lo que subraya la importancia de la comprensión jurídica en la gestión de la privacidad. Sin embargo, un porcentaje considerable tiene experiencia en IT/Seguridad (27.66%), lo que puede reflejar también la necesidad de conocimientos técnicos en la protección de datos. La presencia de otras formaciones específicas (14.89%) indica una diversidad de habilidades que pueden complementar la función del DPO, lo que sugiere la importancia de una perspectiva multidisciplinaria en la gestión de la privacidad.

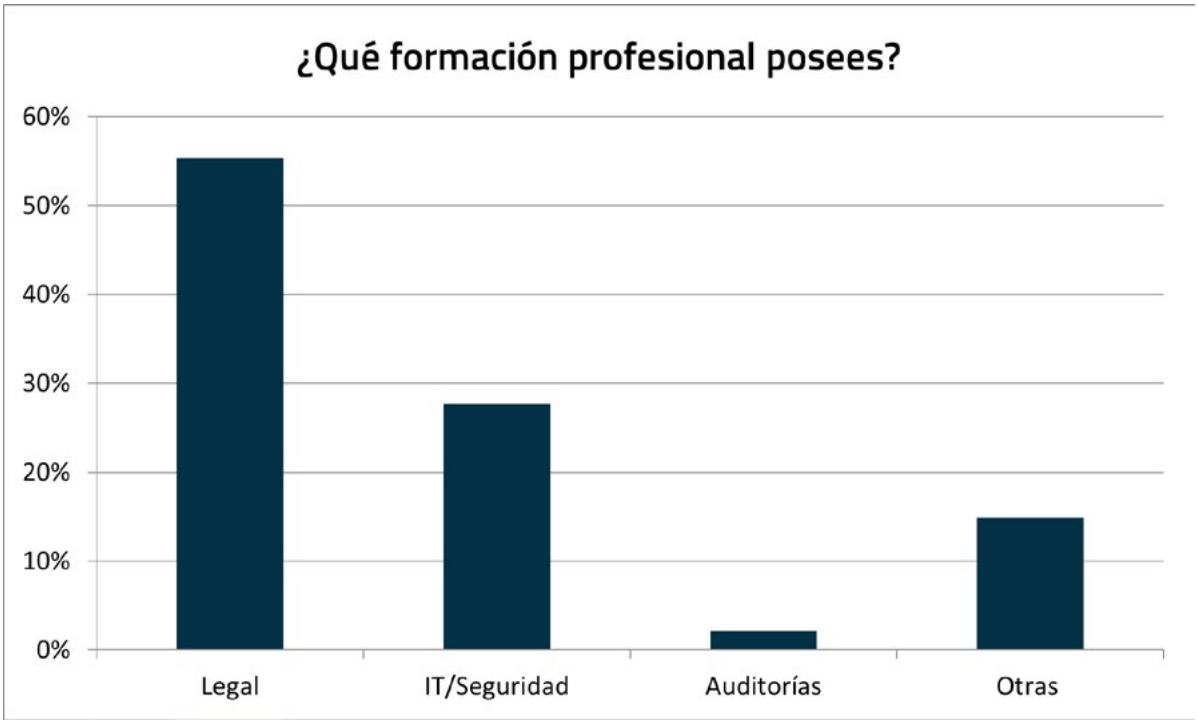

Ilustración 7: Formación del DPO

El número de certificados en CDPD sigue superando a los certificados en CDPP como en años anteriores. En otras certificaciones se incluyen principalmente CISA, CISM y CRISC junto con la ISO 27001, tendencia que se mantiene con los años. Cabe destacar que el 30% de los participantes no dispone de ninguna certificación relacionada con la función de DPO.

Es decir, entrando en detalle, una proporción significativa (38.30%) de los DPOs no mantiene ninguna certificación activa, lo que podría indicar una brecha en la capacitación formal en protección de datos. Sin embargo, el Certificado de Delegado de Protección de Datos (CDPD) es ampliamente mantenido (36.17%), destacando la relevancia y la adopción de esta certificación en el campo de la privacidad. Además, la presencia de otras certificaciones específicas (23.40%), como Certified Data Privacy Professional (CDPP) e IAPP Certifications, sugiere una búsqueda de competencias adicionales en el área de la privacidad y la seguridad de la información.

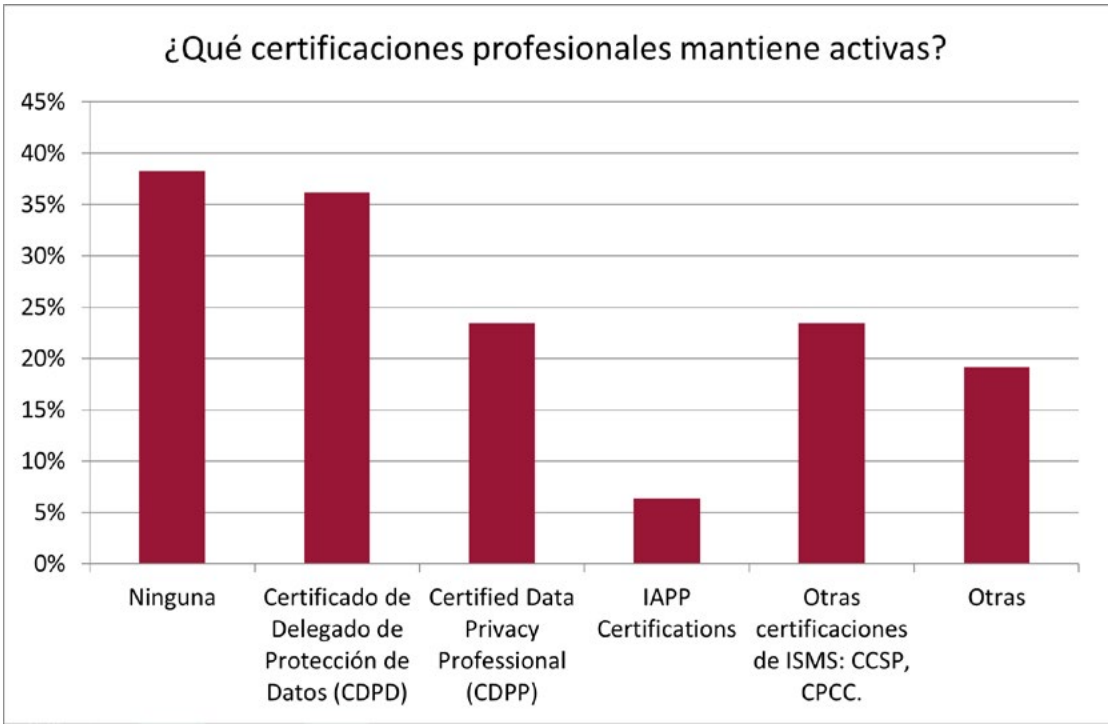

Ilustración 8: Certificaciones activas

Reportes

La Dirección Jurídica ha sido la opción más extendida como destinatario de los reportes realizados por la función de protección de datos este año. En la serie histórica de los últimos tres años esta sigue siendo también la opción más elegida. No obstante, no se trata de la estructura mayoritaria en términos absolutos (29'79%). Con cerca de un 24% se consolida y aumenta respecto a años anteriores la opción de reporte a la alta dirección (CEO - Presidente). Esto evidencia la alta relevancia de la protección de datos en los niveles superiores de la empresa.

También ha aumentado a un 13% el reporte al CIO. Las opciones que están teniendo un descenso, respecto al 2021, son la de reporte al Comité de Dirección Interdepartamental y a la Comisión de Auditoría y Compliance (14.89%), resaltando la importancia del cumplimiento normativo en la supervisión de la privacidad. La diversidad de otras opciones (14.89%) sugiere una variedad de estructuras organizativas para la supervisión de la privacidad, lo que puede influir en la efectividad y la autonomía del DPO en su función. Esta distribución de responsabilidades subraya la necesidad de una coordinación estrecha entre las funciones de privacidad y los órganos de dirección y supervisión de la empresa.

Ilustración 9: Reportes

Combinando los datos con el tipo de empresa por cantidad de empleados se observa que la elección para corporaciones globales (más de 1000 empleados) es la de reportar a la Dirección Jurídica, mientras que en las empresas de gran escala (entre 250 y 999 trabajadores) se ha establecido reportar a una Comisión de Auditoría y Compliance. En las empresas de menos de 250 empleados las empresas eligen en igual proporción entre reportar al CEO-Presidente y a la Dirección Jurídica.

Pormenorizando los resultados, la mayoría de los DPOs realizan informes formales al Management cada 3 meses o más (48.94%), lo que sugiere una comunicación regular y periódica sobre asuntos de privacidad. Sin embargo, un porcentaje considerable opta por informes menos frecuentes, con un 21.28% y un 19.15% que lo hacen cada 6 meses y anualmente, respectivamente. Además, un 10.64% nunca ha realizado un reporte formal, lo que podría indicar una brecha en la comunicación sobre asuntos de privacidad con la dirección. Estos hallazgos resaltan la importancia de establecer procesos de informes regulares para garantizar una supervisión adecuada y una toma de decisiones informada en materia de protección de datos.

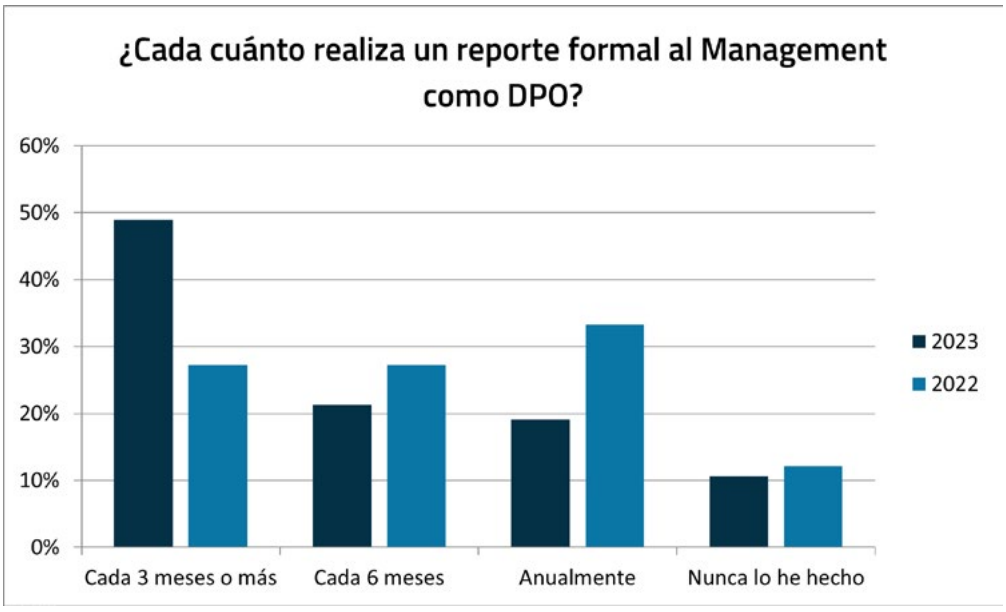

Ilustración 10: Temporalidad del reporte

Combinando los datos con el tamaño de empresa por número de personas empleadas, se aprecia que en las corporaciones globales se mantienen la tendencia de reportar cada 3 meses. En las empresas a gran escala se prefiere realizar un reporte anual, mientras que en las de menos de 250 empleados han obtenido el mismo porcentaje, para el reporte, el realizarlo cada 3 meses y cada 6 meses.

Realizando el mismo ejercicio con los sectores empresariales se observa que el 50% de los participantes relacionados con la Administración Pública nunca realizan reportes a sus superiores, y los que sí lo hacen llevan a cabo esta tarea anualmente. El sector sanitario, servicios financieros y el sector de seguros coinciden con reportar trimestralmente con rangos entre el 50% y 80% para cada sector, respectivamente.

Para finalizar con el apartado de reportes emitidos por el DPO, se muestran los resultados, comparados desde el 2021, donde cada participante ha podido elegir, entre las opciones propuestas, la que más le preocupa.

Entrando en detalle, los resultados muestran que, al reportar a la Dirección, las mayores preocupaciones del DPO son las posibles sanciones por parte de las autoridades (74.47%) y el riesgo de robo o brecha de datos (72.34%). Estas cifras reflejan una sólida conciencia sobre las graves implicaciones legales y financieras de incumplir con el RGPD. Además, casi el 60% de los encuestados están preocupados por el posible daño reputacional ante un incumplimiento, lo que subraya la importancia de proteger la imagen y la confianza de la empresa. Sin embargo, una proporción menor (23.40%) también expresa preocupación por el funcionamiento efectivo del sistema de control, lo que indica la necesidad de una vigilancia constante y la mejora continua de las medidas de seguridad y cumplimiento.

Ilustración 11: Preocupaciones de los reportes a la dirección

Equipos

Respecto al año anterior, se ha aumentado significativamente la respuesta que indica equipos de una o dos personas. En términos generales, los equipos dedicados a la protección de datos son más reducidos este año, comparados con las respuestas del año anterior.

Los resultados sugieren que la mayoría de las empresas tienen una dedicación moderada al cumplimiento continuo del RGPD, con entre 1 y 5 personas (83.98%) asignadas a esta tarea. Sin embargo, un pequeño porcentaje (16.02%) de empresas tienen más de 5 personas dedicadas, lo que podría indicar una mayor complejidad en la gestión del cumplimiento normativo. Esta distribución sugiere que muchas empresas optan por equipos pequeños pero efectivos para abordar los desafíos del RGPD, mientras que unas pocas asignan recursos significativos adicionales para garantizar un cumplimiento exhaustivo y continuo.

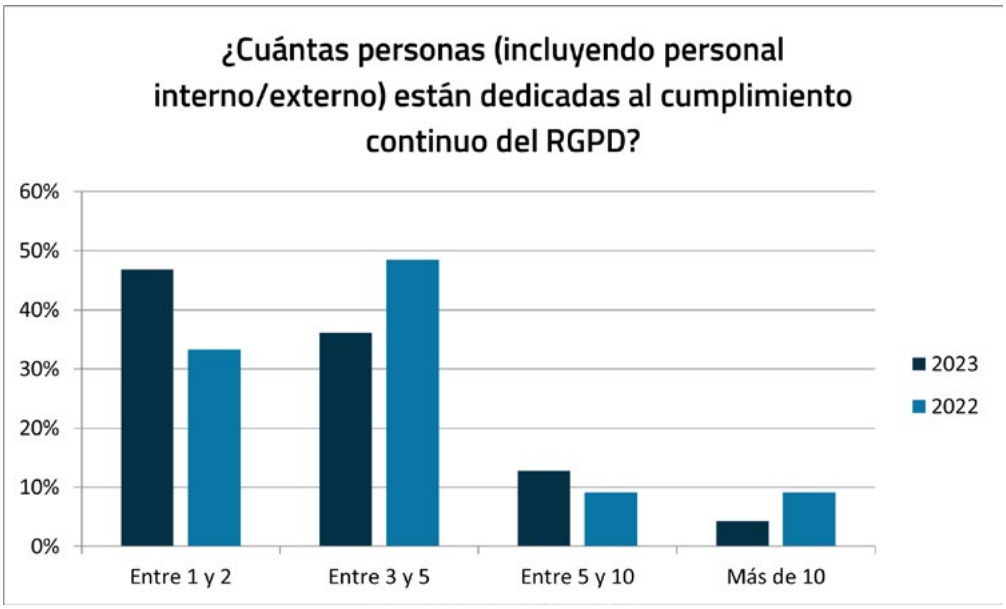

Ilustración 12: Personal dedicado al cumplimiento del RGPD

Al analizar las empresas por su tamaño, notamos que los equipos más grandes se encuentran en las corporaciones de alcance global, mientras que la opción de contar con un equipo reducido está presente en el resto de los tipos de empresas.

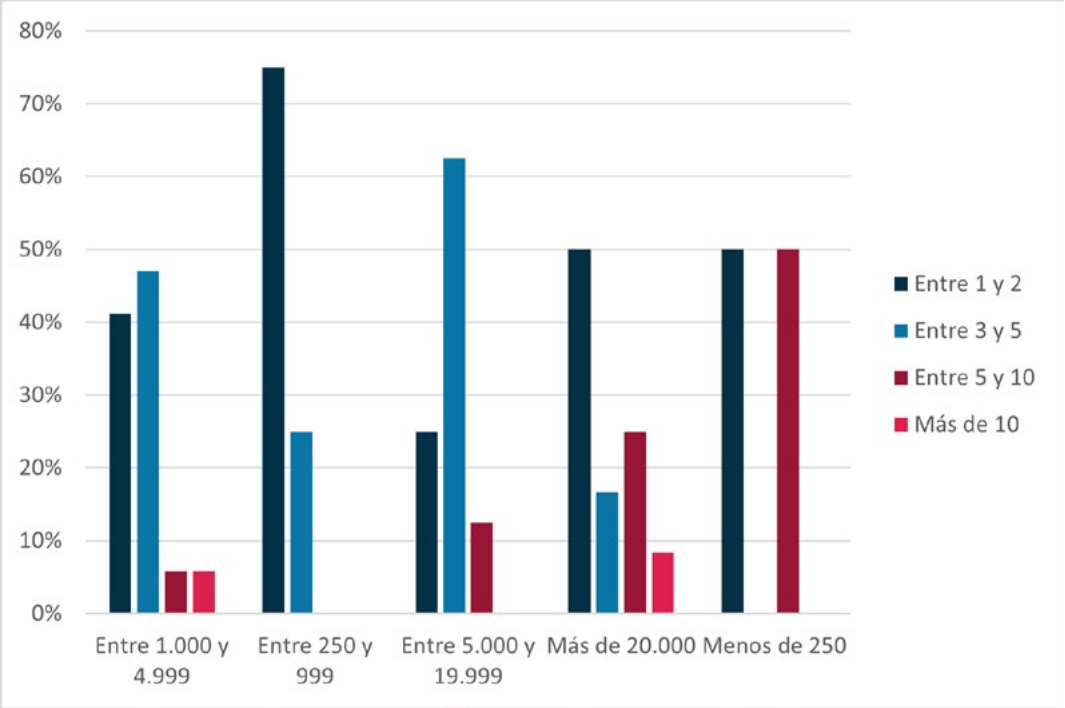

Ilustración 13: Personal dedicado en función del tamaño de empresa

Respecto a las dificultades que encuentran las funciones de protección de datos, en este año 2023, en cuanto a las motivaciones, destaca por encima de los demás las resistencias provenientes desde dentro de la misma corporación. Se reducen las demás opciones siendo la más significativa la falta de apoyo por la dirección. La reducción de este indicador podría señalar un mayor compromiso desde los órganos de dirección. Hay que destacar que en 2023 un 10% de los participantes no encuentran ninguna resistencia en el desarrollo de su actividad.

Por lo tanto, estos resultados sugieren que, si bien algunos enfrentan desafíos técnicos y financieros, la oposición interna y la falta de apoyo de la dirección son obstáculos significativos en la implementación efectiva del RGPD. La resistencia interna puede reflejar la necesidad de una mayor concienciación y colaboración dentro de la organización, mientras que la falta de recursos puede limitar la capacidad de los DPOs para implementar medidas de cumplimiento. Esta combinación de desafíos destaca la importancia de abordar tanto los aspectos técnicos como los culturales en la gestión de la privacidad.

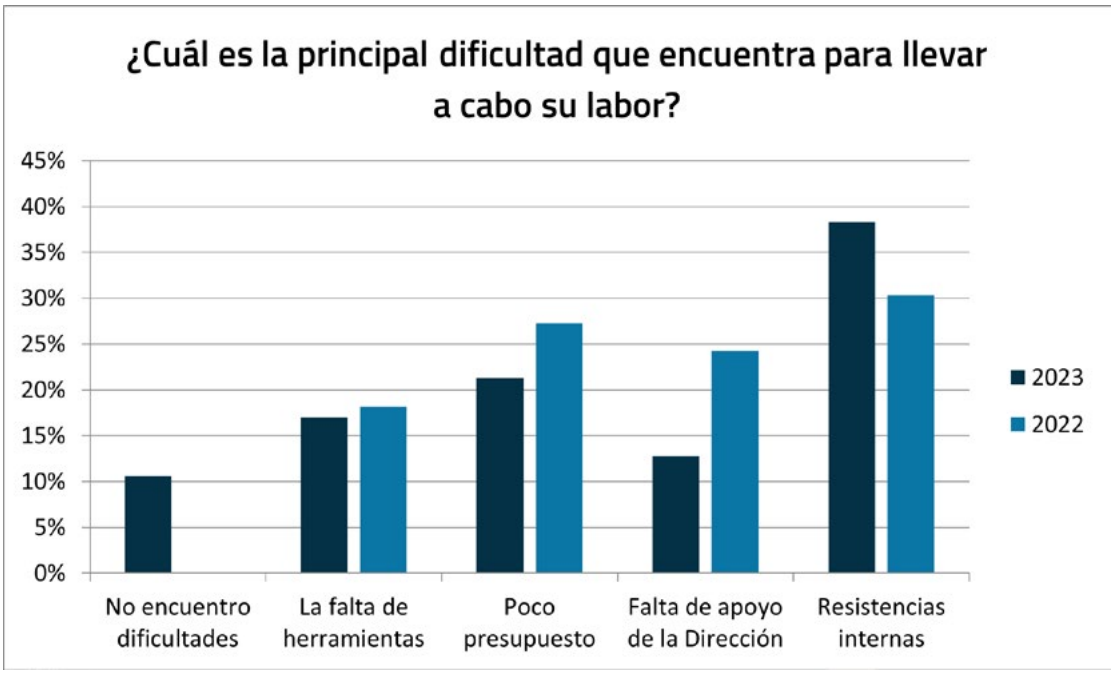

Ilustración 14: Dificultad del DPO

Combinando los datos con el tamaño de empresa por número de empleados, se observa que en las compañías con menos de 250 solo se seleccionen por partes iguales la falta de presupuesto y la falta de herramientas. Respecto de las grandes corporaciones la opción más seleccionada es la resistencia interna.

Por último, los participantes han tenido la ocasión de indicar cuáles son las áreas que más colaboran con la tarea de protección de datos, donde destaca la función de Seguridad de la Información como departamento más involucrado. Entre todos los departamentos, también se mantienen por encima de los demás, por su nivel de involucración, las áreas legales y las de compliance. Por el contrario, se percibe una menor implicación de los departamentos de procesos y auditoría.

Esto sugiere una fuerte integración entre el DPO y las áreas de seguridad de la información y asesoría jurídica, reflejando la importancia de la protección de datos desde una perspectiva técnica y legal. Además, la implicación de áreas como compliance y auditoría muestra un enfoque holístico hacia el cumplimiento normativo. Sin embargo, la menor participación de áreas como procesos/calidad y riesgos/control interno podría indicar oportunidades para una mayor colaboración en la gestión de la privacidad dentro de la organización.

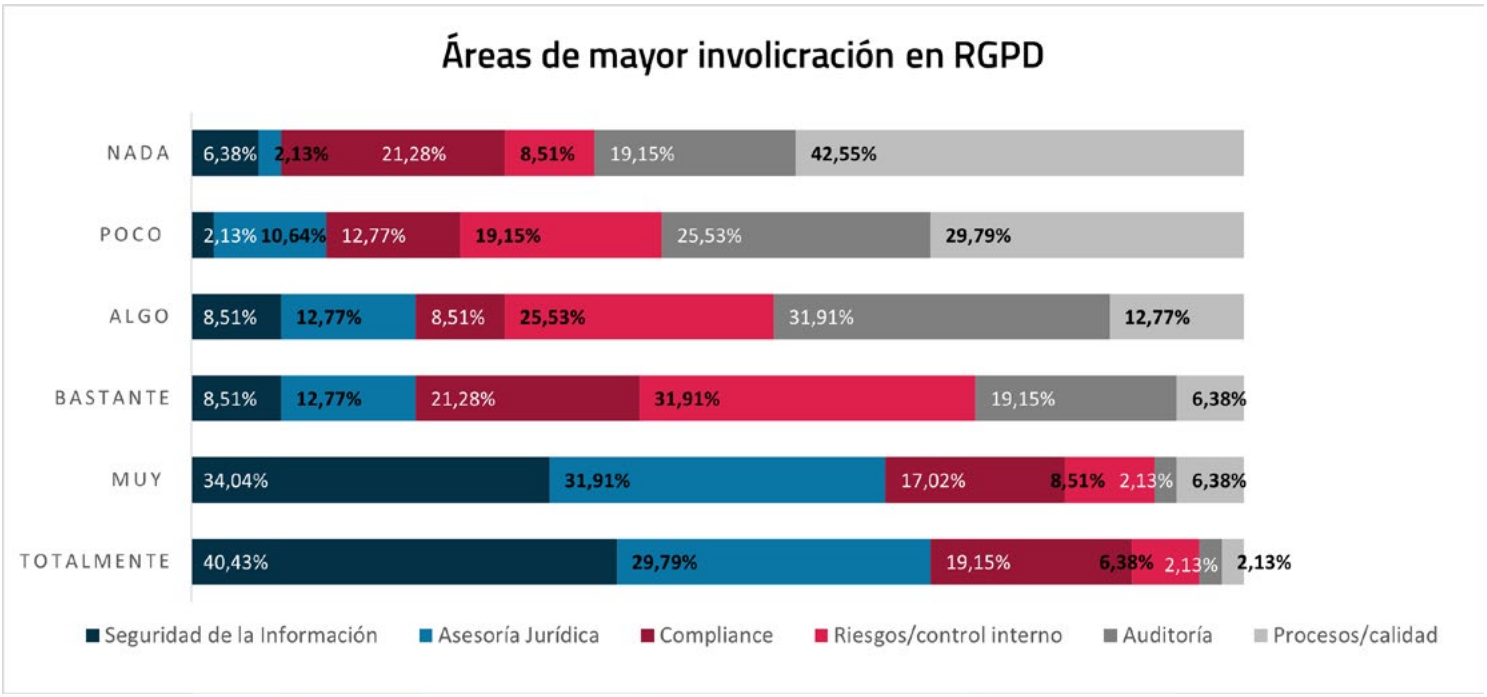

Ilustración 15: Áreas de mayor involucración en RGPD

Modelo de Madurez de Cumplimiento RGPD

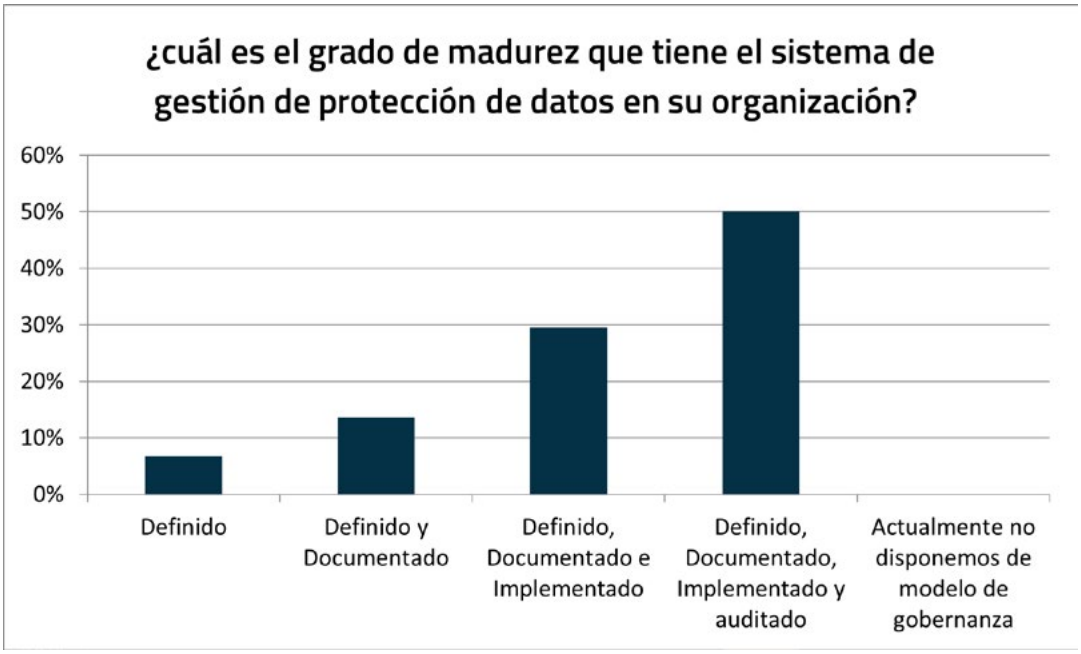

Ilustración 16: Grado de madurez del Sistema de Gestión de Protección de Datos

Resulta destacable que todas las entidades afirman contar con un modelo de gestión de la privacidad en su organización. De éstas, la mitad asegura disponer de un sistema de gestión con un muy alto grado de madurez.

Las entidades que han declarado disponer de un Sistema de Gestión de Protección de Datos de madurez mínimo (20,46%), se corresponde en gran medida con entidades con un menor volumen de ingresos. Destaca la madurez del sector financiero, sanitario y tecnológicas.

Es destacable también que el sector Administraciones Públicas sigue por debajo de la empresa privada en nivel de adecuación, situándose todavía en un "definido y documentado" pero ninguna en estadio "auditado".

Por ello, los resultados sugieren que la mayoría de las organizaciones tienen un nivel significativo de madurez en sus sistemas de gestión de protección de datos, con un 50% que informa haber definido, documentado, implementado y auditado su sistema. Esto indica un compromiso sólido con el cumplimiento del RGPD y una infraestructura establecida para gestionar la privacidad de manera efectiva. Sin embargo, también es alentador ver que un porcentaje considerable (29.55%) ha progresado hasta la etapa de implementación. Esto sugiere una evolución continua hacia la mejora de las prácticas de protección de datos en las organizaciones encuestadas.

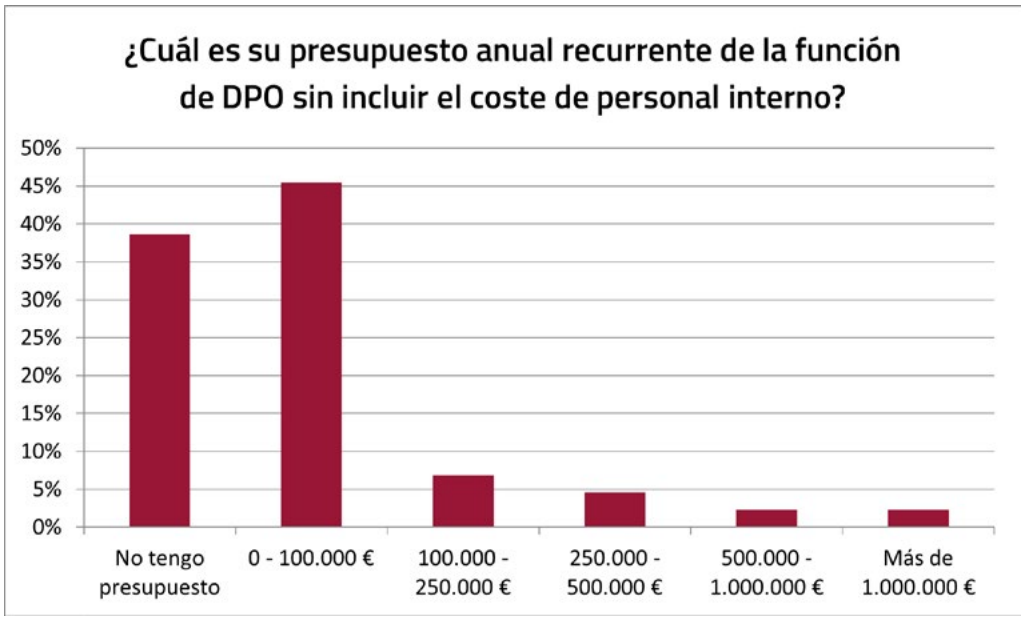

Ilustración 17: Presupuesto anual recurrente de la función de DPO (excl. coste de personal interno)

La inmensa mayoría de entidades (84,09%) declara no contar con presupuesto (38,64%) o disponer de un presupuesto inferior a los 100.000€ (45,45%) destinado a la gestión de la función de DPO. Esta tendencia se mantiene respecto a los Estudios realizados en 2021 y 2022. Llama la atención que las limitaciones de presupuesto mostradas lo son, independientemente del tamaño de las organizaciones (grandes empresas y empresas grandes).

Si analizamos los resultados por sector de actividad económica, observamos que aquellas entidades que afirman contar con un presupuesto superior a los 100.000€, incluso mayor a 1.000.000€, pertenecen mayoritariamente al Sector Financiero.

Aun cuando el RGPD requiere a los Responsables y Encargados dotar los DPD con los recursos necesarios para el desempeño de sus funciones, la falta de asignación de recursos es un reclamo constante entre los DPD, no solo en España, sino en el resto de la UE, tal y como lo muestra el Segundo Informe sobre las Conclusiones de la Segunda Acción de Ejecución Coordinada de las Autoridades de Control (2023), respecto a la designación y cargo de los DPD.

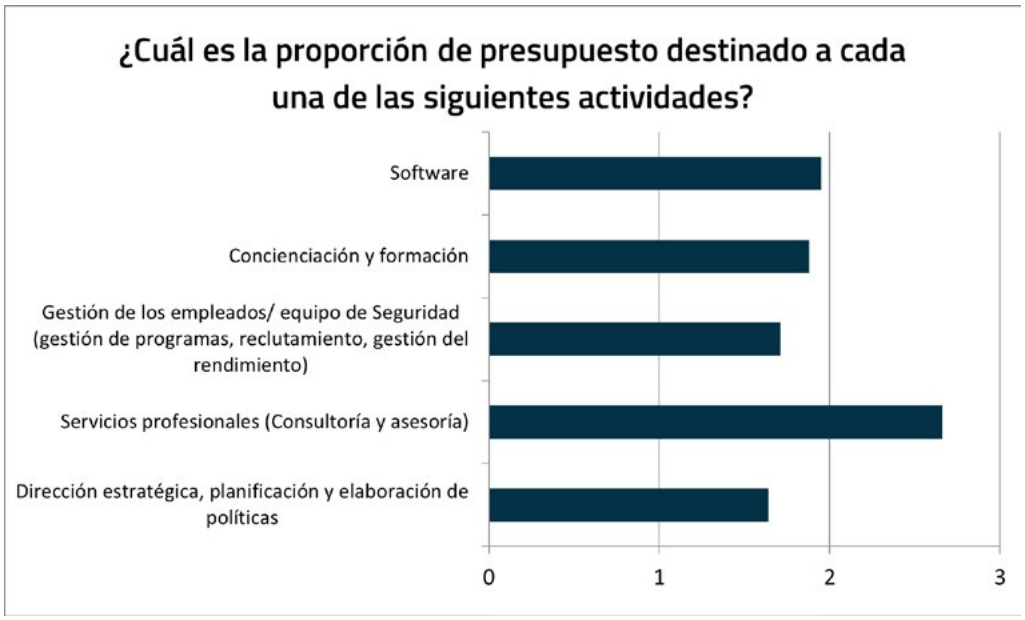

Ilustración 18: Presupuestos actividades

A diferencia del Estudio del año 2022, observamos una nivelación del gasto entre las distintas actividades. El presupuesto destinado a Software y Gestión de empleados y equipos de seguridad se reduce respecto a las otras actividades, a diferencia del Estudio previo donde fueron las mayores destinatarias de inversión.

La proporción de presupuesto que ha aumentado de forma notoria respecto al ejercicio 2022 ha sido el destinado a los Servicios Profesionales (consultoría y asesoría), lo que podría interpretarse como una respuesta o reacción de los Responsables y Encargados para comprender el alcance las novedades legislativas, así como de los cambios en las directrices y criterios de los reguladores y Autoridades de Control, y enfrentarse a la respectiva implementación.

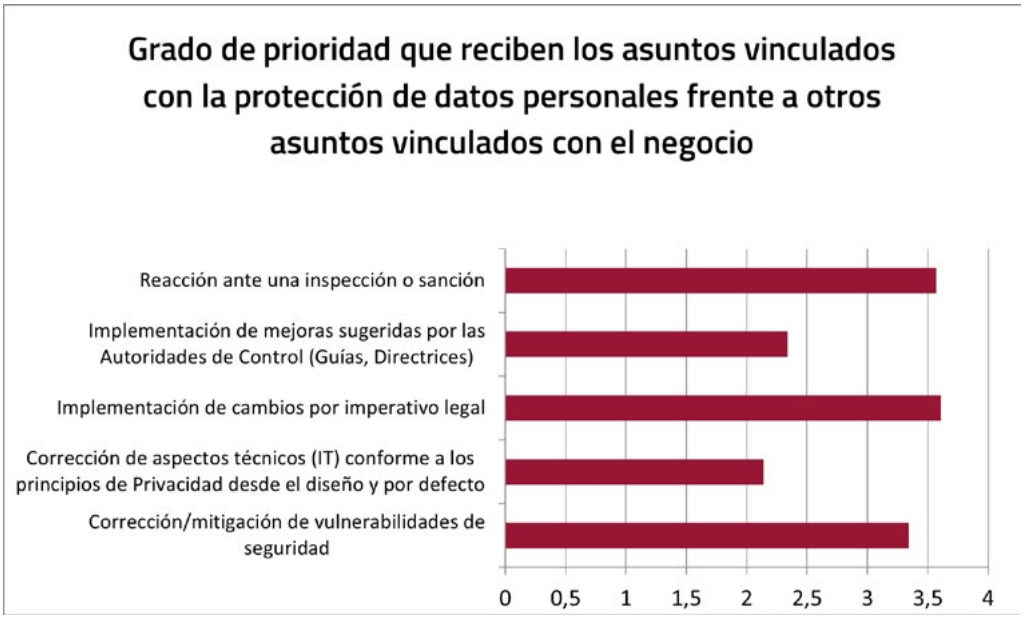

Ilustración 19: Prioridad de asuntos vinculados con la protección de datos

Al analizar las prioridades en la gestión de asuntos vinculados con la protección de datos, se observa cómo se prioriza el gasto en acciones reactivas, frente a acciones preventivas. Como asunto de mayor prioridad se encuentra el gasto asociado a la "Implementación de cambios por imperativo legal", seguido muy de cerca por la "Reacción ante una inspección o sanción" y la "Corrección/ de vulnerabilidades de seguridad". Por el contrario, los asuntos donde se invierte en menor cantidad son en los asuntos relacionados con la "Implementación de las recomendaciones que proponen las Autoridades de Control a través de sus Guías y Directrices" y, por último, aquellos asuntos vinculados al Privacy by Design y el Privacy by Default.

Esta muestra resulta consistente con la ausencia (o bajo importe) de un presupuesto anual recurrente destinado a la función del DPD.

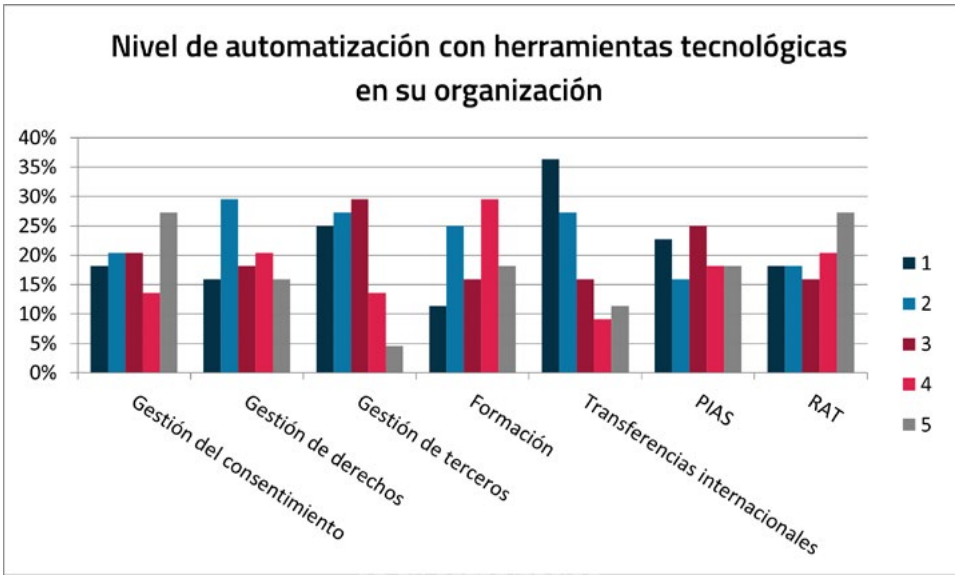

Ilustración 20: Nivel de automatización con herramientas

En relación con la automatización de procesos mediante el uso de herramientas tecnológicas, los resultados evidencian como la Formación y la gestión del RAT (registro de actividades de tratamiento) son los procesos más automatizados, seguido de cerca por la Gestión de Consentimientos. En el extremo opuesto, se ubica la Gestión de Terceros y las Transferencias Internacionales, manteniendo la tendencia mostrada en los resultados de los Estudios de los años 2021 y 2022. La Gestión de Derechos y la gestión de las PIAS (Procedimientos de Evaluación de Impacto en la Protección de Datos), si bien no se encuentran entre las 2 actividades más automatizadas, los resultados muestran un nivel de automatización considerable.

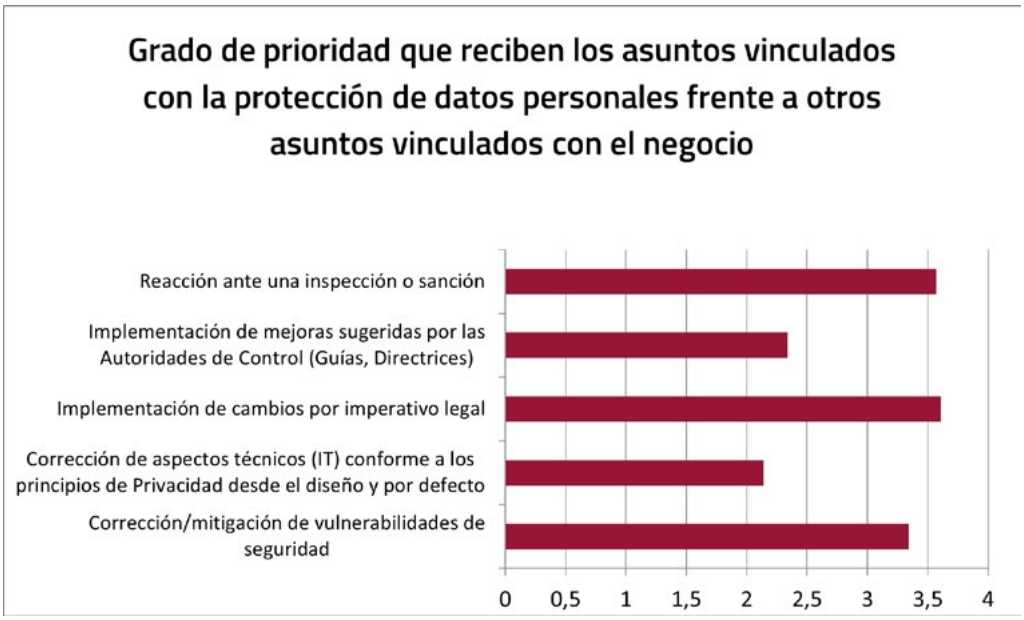

Ilustración 21: Líneas de acción en base a su estado de madurez en cuanto a la implantación en su organización.

No hay cambios relevantes frente al estudio del año pasado, 2022. El Registro de Tratamientos, las bases legítimas y la firma de contratos siguen en cabeza con revisiones sistemáticas mientras que el proceso de alerta temprana o PrivacyByDesign y la monitorización no terminan de despegar. Tampoco el apartado de Transferencias Internacionales cuyo riesgo frente al 2022 se ha suavizado con la aprobación del nuevo Data Privacy Framework con EEUU.

Entrando en detalle, pormenorizando cada media (weighted average), Los resultados revelan que la mayoría de las líneas de acción han progresado significativamente en su estado de madurez en cuanto a la implantación en las organizaciones. Por ejemplo, el análisis de riesgos y los PIAs muestran una distribución equilibrada a lo largo de los diferentes estados de madurez, lo que sugiere una atención adecuada a la gestión proactiva de riesgos y la evaluación del impacto en la protección de datos. Además, la firma de contratos y DPAs muestra una alta proporción en los estados más avanzados de ejecución y revisión de procedimientos, indicando una sólida implementación en esta área crítica. Sin embargo, áreas como las bases legítimas y la transferencia de datos aún tienen margen para mejorar en la revisión de la eficacia de los procedimientos implantados y la generación de planes de corrección o mejora.

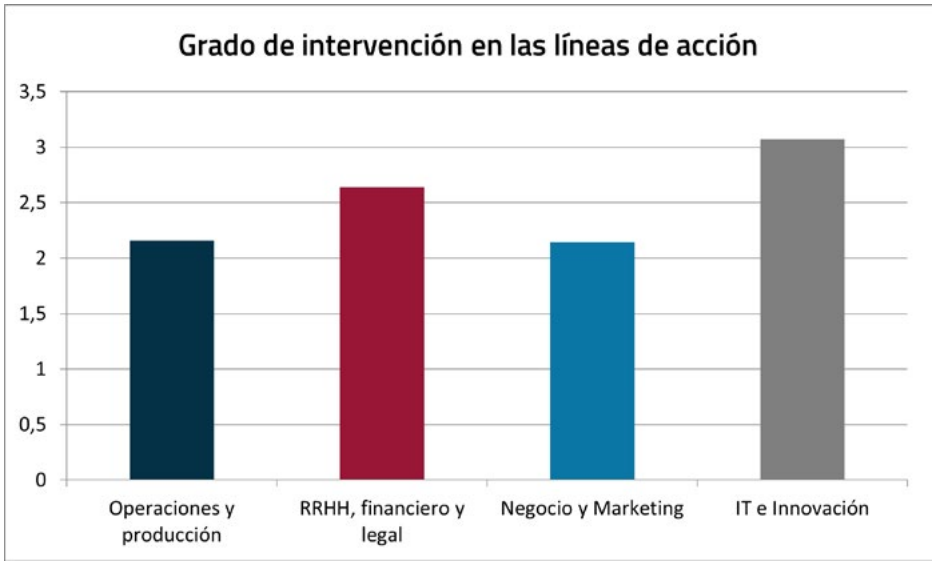

Ilustración 22: Grado de intervención en las líneas de acción

Los resultados indican que el área de IT e Innovación, como en años anteriores, tiene la mayor intervención en la implementación de las líneas de acción relacionadas con la protección de datos, con un 45.45% en el nivel de mayor involucración (valor 1). Esto sugiere una comprensión de la importancia de la tecnología en la gestión de la privacidad y una fuerte colaboración en la implementación de medidas técnicas y soluciones innovadoras. Por otro lado, RRHH, financiero y legal, así como negocio y marketing, muestran un nivel moderado de involucración, mientras que operaciones y producción tienen la menor intervención. Estos resultados resaltan la necesidad de una colaboración interdisciplinaria para garantizar una implementación efectiva de medidas de protección de datos en toda la organización.

Ilustración 23: Ejecución de auditorías

Este apartado sigue aumentando. Frente al año 2022 teníamos un 63% de respuestas afirmativas, y en este año 2023 ya superamos el umbral del 75%. Esto indica un compromiso significativo con la evaluación y mejora continua de los procesos y procedimientos relacionados con la privacidad de los datos.

Esto, a su vez, no presenta cambios importantes es el perfil de las auditorías, donde el 50% optan por un modelo mixto de internas y externas, si bien predominan las internas. Las externas están relegadas a sectores más regulados como Sanitarios o Financiero, por requisitos de otros reguladores o captación de clientes que lo están en sus países, multinacionales, etc.

La realización de auditorías forma parte de las mejores prácticas en materia de cumplimiento del RGPD y demuestra un enfoque proactivo hacia la garantía de la conformidad normativa y la protección de la información personal. Sin embargo, es importante que el 22.73% restante considere la posibilidad de implementar auditorías en sus prácticas de gestión de protección de datos para fortalecer aún más su enfoque de cumplimiento y gestión de riesgos.

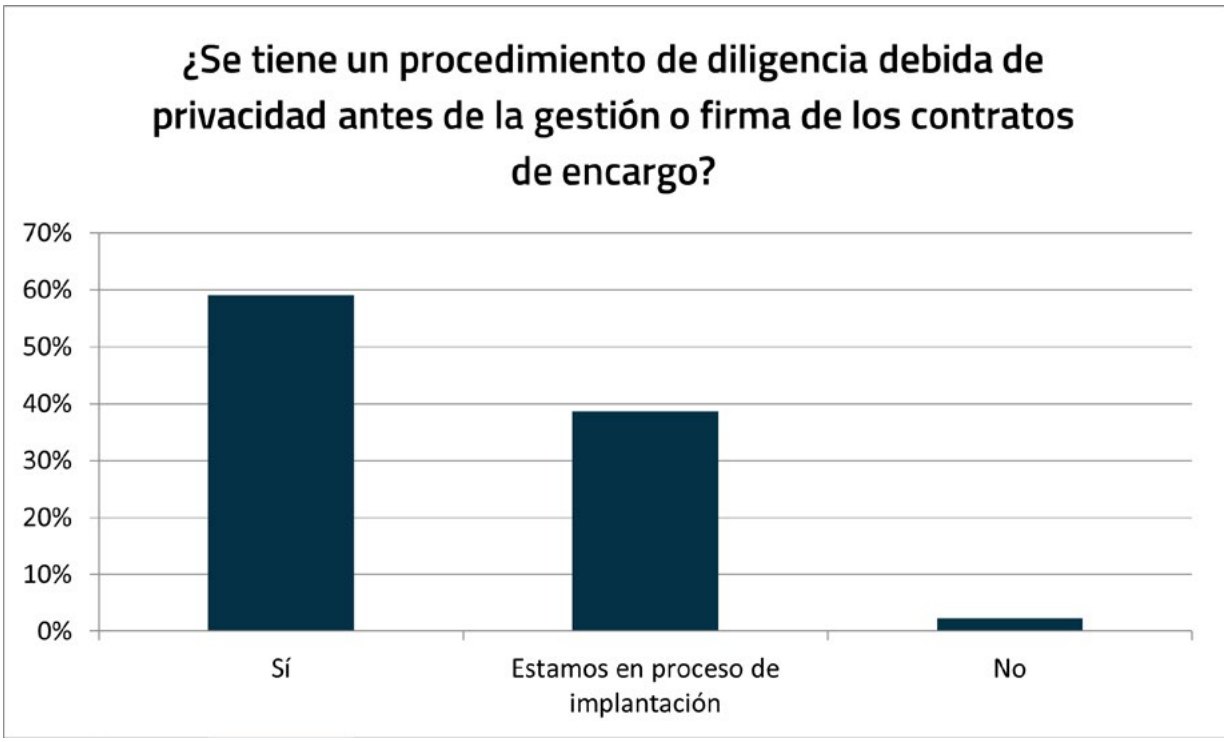

Ilustración 24: Procedimiento de diligencia

Hay una ligera evolución positiva en el bloque de las compañías que ya están en proceso de implantación de procesos de diligencia antes de la contratación, (59.09%) esto sugiere que obedece a una mayor automatización en los procesos de compras, incorporando en la cadena del proceso la parte de cuestionarios y aprobación por las áreas de Privacidad para seguir con la compra. Esto refleja un enfoque proactivo hacia la protección de datos al considerar cuidadosamente los aspectos de privacidad antes de comprometerse con terceros. Además, el 38.64% de las organizaciones están en proceso de implantación, lo que sugiere un reconocimiento de la importancia de este procedimiento y un compromiso con su implementación en el futuro cercano. Sin embargo, es alentador ver que solo un pequeño porcentaje (2.27%) indica no tener este procedimiento establecido, lo que sugiere una conciencia generalizada sobre la importancia de la diligencia debida en la protección de datos en el contexto de los contratos de encargo.

Registro de indicadores para análisis y benchmarking

Número de tratamientos de datos identificados

Al igual que en el año pasado, en este 2023 podemos identificar que las empresas con mayor número de empleados son las que más tratamientos de datos han identificado y mantienen actualizados en el RAT, teniendo una media de entre 50 y 100 tratamientos.

Los valores identificados son similares a los del 2022, siendo los sectores de Industria, construcción e infraestructura y financiero los que más tratamientos manejan.

Un análisis más profundo sugiere que la mayoría de las organizaciones encuestadas tienen un número moderado de tratamientos de datos registrados, con el 28.81% entre 51 y 100 y el 23.73% entre 101 y 500. Esto indica una diversidad de operaciones de procesamiento de datos, que podrían abarcar desde pequeñas hasta medianas cantidades de información personal. Es interesante observar que un 10.17% tiene entre 0 y 50 tratamientos registrados, lo que podría indicar organizaciones más pequeñas o menos complejas en términos de gestión de datos. Sorprendentemente, el 1.69% reporta tener más de 1000 tratamientos, lo que sugiere una escala significativa de operaciones de procesamiento de datos en estas organizaciones.

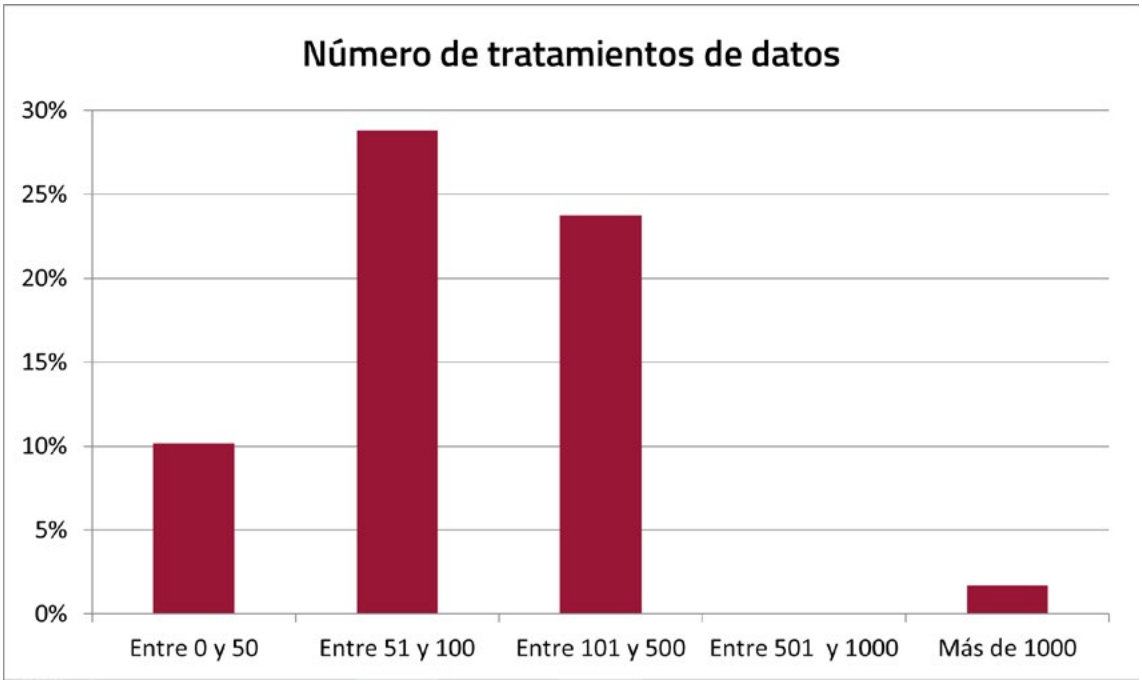

Ilustración 25: Número de Tratamiento de datos registrados

Cada cuando se actualizar el RAT

En la encuesta de este año 2023 se incluyó una nueva pregunta sobre la frecuencia de actualización del Registro de Actividades del tratamiento (RAT), obteniendo las conclusiones principales de que todas las empresas actualizan el RAT, y que más del 33 % lo hace una vez al año o menos, sin que se evidencien diferencias entre sectores o tamaño de empresa.

Entrando en detalle, los resultados sugieren y reflejan una variedad de prácticas en la actualización del Registro de Actividades de Tratamiento (RAT). Mientras que un 23.73% lo actualiza una vez al año y un 10.17% cada seis meses, un sorprendente 16.95% solo lo actualiza cuando se añade un nuevo tratamiento, lo que puede indicar una falta de atención continua a la gestión de datos. Es alentador ver que ningún encuestado indicó nunca actualizar el RAT, lo que sugiere un reconocimiento generalizado de la importancia de mantener este registro. Sin embargo, el 13.56% reporta "otros" métodos de actualización, lo que podría reflejar una variedad de enfoques en la gestión y actualización de esta importante herramienta de cumplimiento del RGPD.

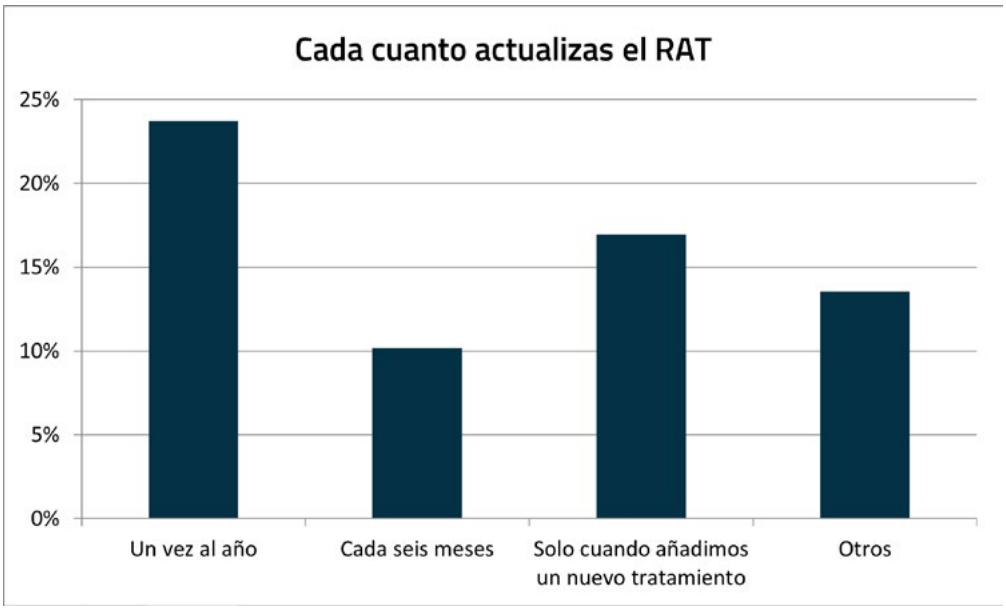

Ilustración 26: Temporalidad con la que se actualiza el RAT

Número de PIAs realizados

Los números de Evaluaciones de Impacto realizados por las empresas que se encuentran actualmente en vigor son similares a los encontrados en las anteriores encuestas, donde el 25% ha realizado hasta 10 PIAs y el 19% entre 51 y 100.

El número de empresas que no ha realizado ninguna PIA sí que baja hasta un 8% (en el 2022 fueron un 22%), y los sectores con más Evaluaciones de Impacto es el sector Sanitario junto con los de Servicios Financieros.

Un análisis en detalle revela que la mayoría de las organizaciones encuestadas tienen realizado un número moderado de Evaluaciones de Impacto en la Protección de Datos (PIAs), con un 25% que ha realizado entre 1 y 10, y un 19% entre 11 y 50. Esto sugiere un nivel de atención a la gestión de riesgos de privacidad, con una cantidad significativa de organizaciones que han realizado múltiples evaluaciones para abordar los posibles impactos en la privacidad de los datos. Sin embargo, es preocupante que un 8% no haya realizado ningún PIA, lo que podría indicar una falta de conciencia sobre la importancia de esta herramienta para evaluar y mitigar los riesgos para la privacidad. Además, otro 8% reporta haber realizado más de 100 PIAs, lo que podría indicar una escala significativa de operaciones de procesamiento de datos y un enfoque proactivo hacia la gestión de riesgos de privacidad.

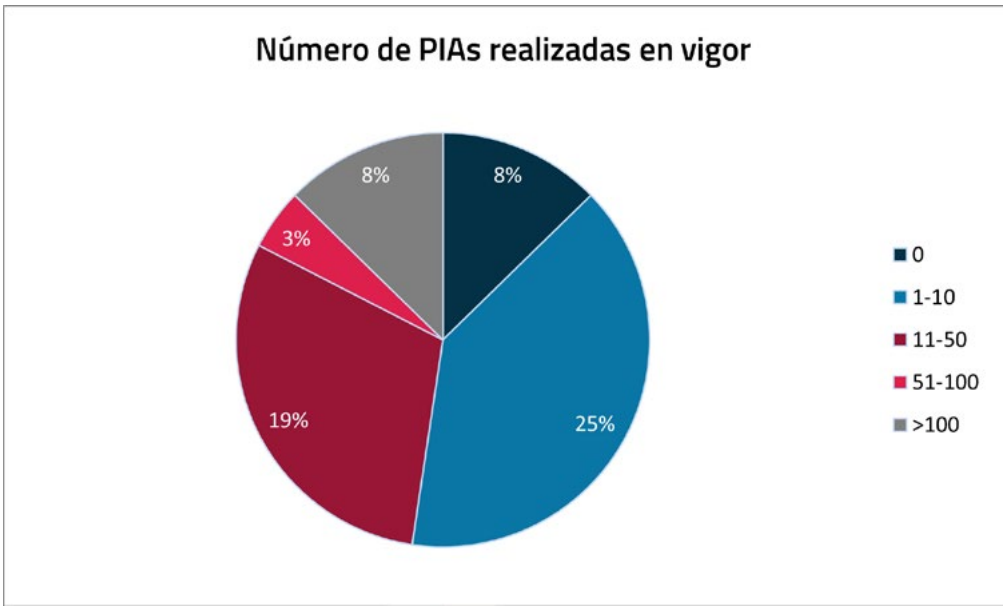

Ilustración 27: PIAs realizadas en vigor

¿Cuántas de esas PIAs fueron realizadas en 2023?

De las PIAs en vigor en las empresas consultadas, se analizó cuáles de ellas han sido modificadas o creadas el último año para tener un indicador de la variabilidad anual de los tratamientos de alto riesgo en las empresas.

El sector que más PIAs modificó el último año fue el sector Financiero, existiendo un 14% de las empresas que han respondido a la encuesta que no han modificado ninguna PIA durante este 2023.

Por lo tanto, los resultados muestran que la mayoría de las organizaciones (39%) realizaron entre 1 y 10 Evaluaciones de Impacto en la Protección de Datos (PIAs) durante 2023, lo que indica un nivel considerable de atención a la gestión de riesgos de privacidad durante ese año. Sin embargo, es preocupante que un 14% de las organizaciones no hayan realizado ninguna PIA durante ese período, lo que sugiere una falta de atención o recursos dedicados a la evaluación y mitigación de los riesgos para la privacidad. Además, solo un pequeño porcentaje de organizaciones (2%) realizó más de 100 PIAs en 2023, lo que podría indicar una escala significativa de operaciones de procesamiento de datos y un enfoque proactivo hacia la gestión de riesgos de privacidad en estas organizaciones.

Ilustración 28: PIAs realizadas en 2023

Porcentaje de proveedores con los cuales se ha actualizado el contrato de encargo del tratamiento previo al 25 de mayo de 2022

En Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales, se establecía que los contratos de encargado del tratamiento suscritos antes del 25 de mayo del 2018 al amparo del artículo 12 de la LOPD 15/199, mantendrían su vigencia hasta el vencimiento señalado, y si se pactaban indefinidamente, hasta el 25 de mayo de 2022.

En la encuesta de este año se ha podido apreciar cómo un 26% ha actualizado más del 80% de sus contratos (produciéndose una bajada con respecto al 35% del año anterior).

Los resultados, por lo tanto, concluyen que una parte significativa de las organizaciones ha actualizado los contratos de encargo de tratamiento con la mayoría de sus proveedores antes del 25 de mayo de 2022, con un 25.42% que ha actualizado más del 80% de los contratos. Esto sugiere un esfuerzo proactivo por cumplir con los requisitos del GDPR y garantizar la conformidad con las regulaciones de protección de datos. Sin embargo, también es notable que un porcentaje significativo de organizaciones (10.17%) haya actualizado menos del 20% de los contratos, lo que podría indicar un desafío en la gestión de la relación con los proveedores en términos de cumplimiento de la privacidad de datos.

Ilustración 29: Porcentaje de proveedores con los que se ha actualizado el contrato de encargo de tratamiento

Número de violaciones de datos comunicadas a la AEPD

El Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, (RGPD) establece en su artículo 33 la obligación de notificar las brechas de los datos personales que puedan suponer un riesgo para los derechos y libertades de las personas físicas a la Autoridad de Control competente.

En el caso de España, la Autoridad de Control a la que hay que notificar es la Agencia Española de Protección de Datos (AEPD), tanto para el sector privado como para el público, excepción de los organismos públicos de las Comunidades Autónomas donde exista Autoridad de Control Autonómica.

Los resultados sugieren que la mayoría de las organizaciones encuestadas (32.20%, inferior al año anterior -45%-) no han experimentado ninguna violación de datos que hayan comunicado a la Agencia Española de Protección de Datos (AEPD), lo que indica un buen nivel de gestión de seguridad de la información. Sin embargo, es preocupante ver que un porcentaje considerable de organizaciones ha experimentado al menos una violación de datos, con un 10.17% que ha comunicado una violación y un 6.78% que ha comunicado más de cuatro. Esto resalta la importancia de mantener robustos sistemas de seguridad de la información y procedimientos de respuesta a incidentes para proteger la privacidad de los datos y cumplir con las regulaciones de protección de datos.

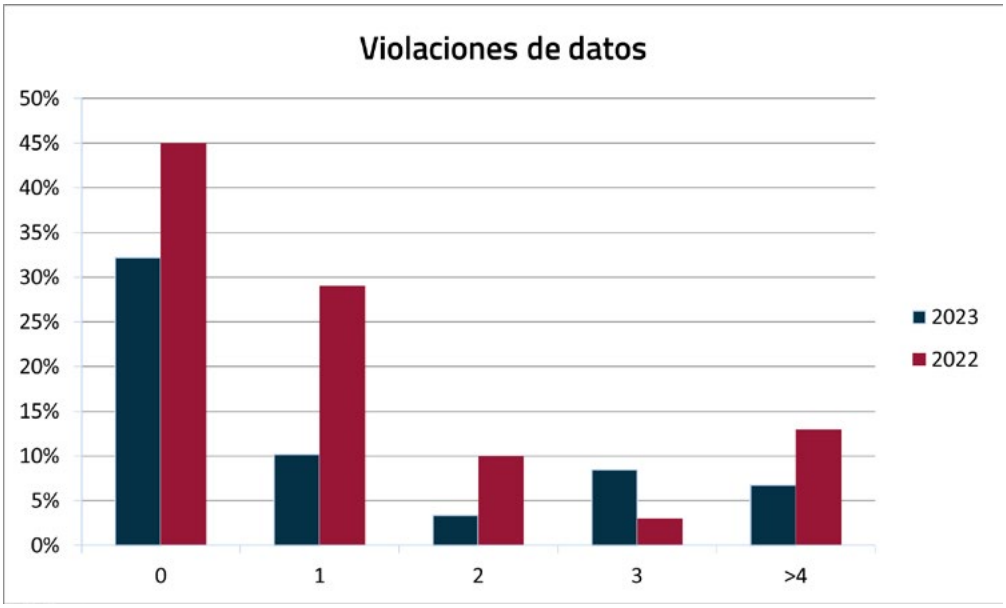

Ilustración 30: Violaciones de datos comunicadas

Número de inspecciones que ha tenido

En las Potestades de investigación y planes de auditoría preventivas reconocidas a la Agencia Española de Protección de datos, se encuentra la actividad de investigación. De esta manera, entre otros, podrá recabar información precisa para el cumplimiento de sus funciones, realizar inspecciones, requerir la exhibición o el envío de los documentos y datos.

Los resultados indican una disminución significativa en el número de inspecciones realizadas en 2023 en comparación con 2022. El 54.24% de las organizaciones no tuvieron inspecciones en 2023, en contraste con el 84% en 2022. Además, solo un pequeño porcentaje de organizaciones experimentaron una inspección en 2023, con un 5.08% en comparación con el 10% en 2022. Estos hallazgos podrían indicar una reducción en la actividad de supervisión por parte de las autoridades de protección de datos en el año 2023.

Los sectores que más señalan haber tenido inspecciones son los Servicios Financieros y Sanitario.

Ilustración 31: Número de inspecciones

Número de contratos de Encargado de tratamiento

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, inclusive en formato electrónico. En cualquier caso, ya se trate de un acuerdo o de otro acto jurídico, su contenido debe reunir los requisitos establecidos en el RGPD.

Los resultados revelan una distribución diversa en cuanto al número de Contratos de Encargo/Proveedores entre las organizaciones encuestadas. Un pequeño porcentaje (1.69%) no tiene ningún contrato registrado, lo que podría indicar que estas organizaciones no externalizan procesos que involucren el tratamiento de datos personales. Sin embargo, la mayoría de las organizaciones (alrededor del 60%) tienen entre 1 y 500 contratos, lo que sugiere una variedad en la escala de operaciones y en la complejidad de las relaciones con los proveedores. Es importante que estas organizaciones gestionen eficazmente estos contratos para garantizar el cumplimiento normativo y la protección de los datos personales conforme a las regulaciones aplicables.

Lo sectores que más contratos de Encargado de Tratamiento gestionan son los de logística y del sector Financiero.

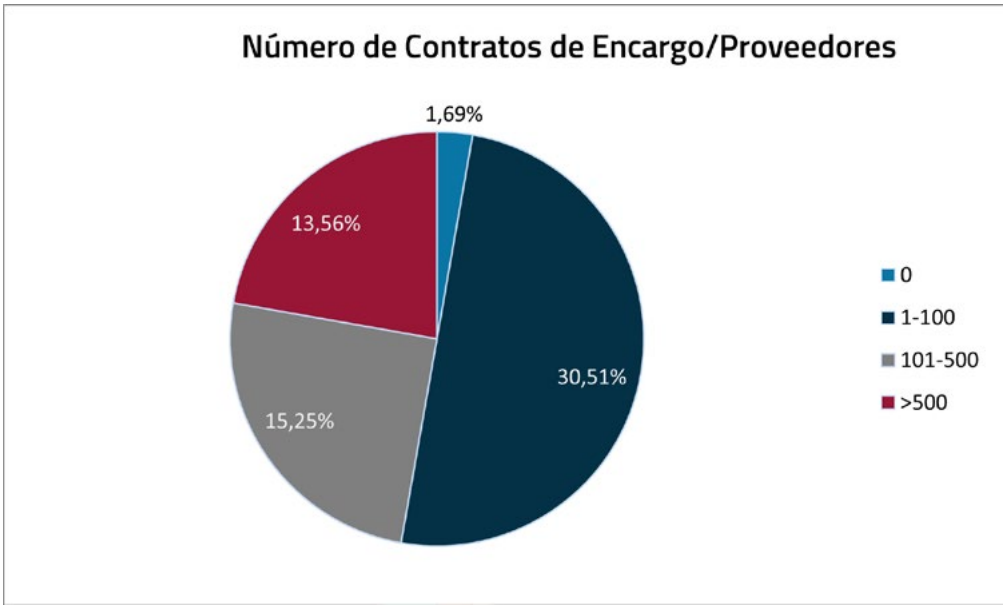

Ilustración 32: Número de contratos de Encargado/Proveedores

Inteligencia Artificial

La inminente aprobación del Reglamento Europeo de IA supone un hito muy importante en defensa de los derechos de las personas ante el uso de sistemas con Inteligencia Artificial, y a su vez establece un nuevo marco regulatorio que las empresas deben cumplir. Muchas de esas nuevas obligaciones están muy vinculadas a modelos similares a los de cumplimiento y control en privacidad (análisis de riesgos, inventario de sistemas IA, implantación de medidas, formación a empleados, gestión de incidentes, etc.). 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. A pesar de que el nuevo Reglamento de IA no regula una figura del estilo "DPO" como sí hace el RGPD, las compañías están trabajando en modelos de gobernanza de la IA, donde los Delegados de protección de datos tendrán un papel fundamental y en muchos casos protagonista. Por todo ello, hemos incluido este año en la encuesta algunas preguntas relativas al fenómeno de la IA y el nuevo Reglamento.

Análisis de impacto del futuro Reglamento de IA

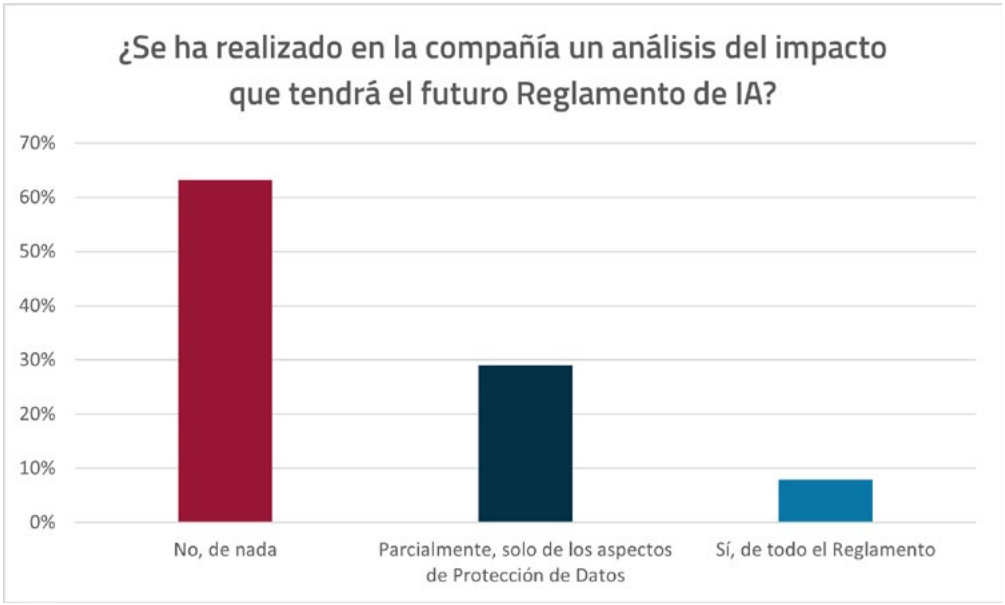

Ilustración 33: Análisis de impacto del futuro Reglamento de IA

El 63% de los encuestados (casi dos tercios) afirma no haber realizado aún ningún tipo de análisis de impacto del futuro reglamento de IA en su compañía. Esto puede indicar una falta de preparación para los cambios regulatorios y las implicaciones de la IA en términos de protección de datos. Mientras que, el 37% restante de los encuestados si habría realizado algún tipo de análisis de impacto, aunque con ligeras apreciaciones: un 29% de ellos habría realizado un análisis de impacto del Reglamento, pero solo en materia de Protección de Datos; y, el 8% restante habría hecho un análisis de impacto completo, sin limitarse a las implicaciones que podría tener únicamente para Protección de Datos.

Responsabilidad del futuro Reglamento de IA

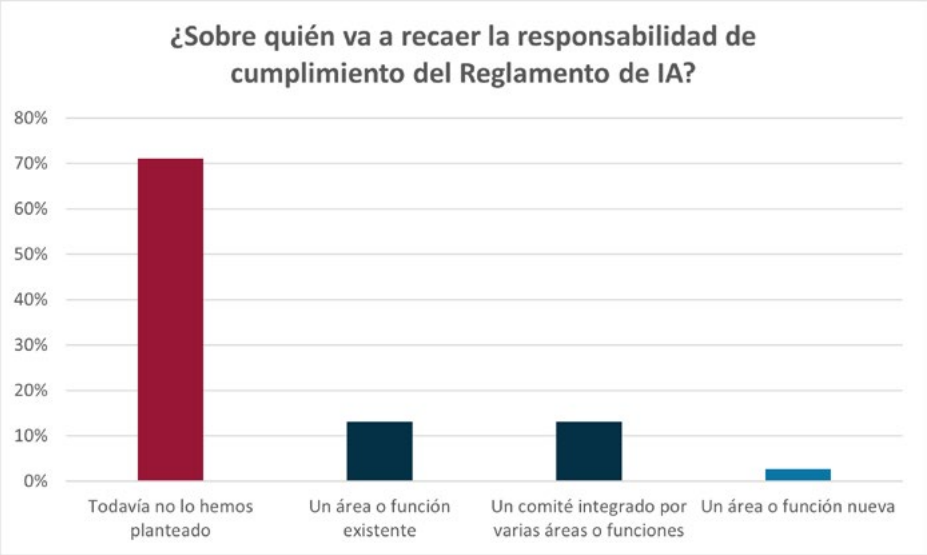

Ilustración 34: Responsabilidad del Reglamente de IA

Un 71% de los encuestados 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.

Dentro del 29% restante, donde se encuentran los encuestados que sí se han planteado dicha cuestión, hay diversidad de opiniones: Un 13% de los encuestados cree que lo más adecuado sería que un área o función ya existente sea quien herede dicha responsabilidad, otro 13% considera que la responsabilidad debería ser compartida en un comité que integre a varias áreas o funciones; mientras que tan solo un 3% de los encuestados cree que debería crearse una función nueva para heredar estas responsabilidades.

Será importante para estas compañías evaluar y desarrollar estrategias para cumplir con las regulaciones de IA de manera efectiva en el futuro.

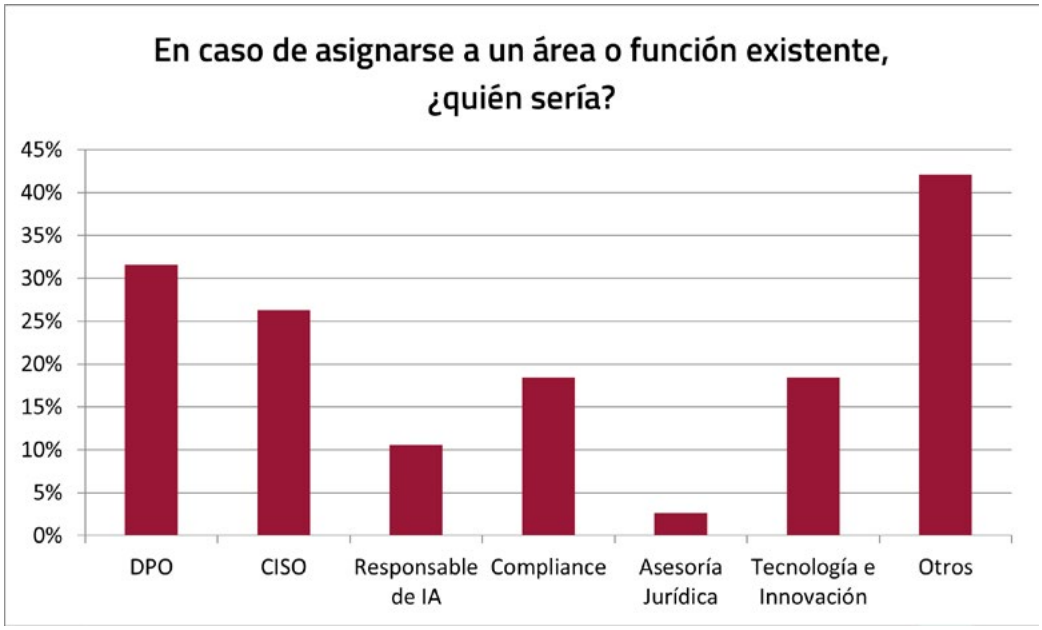

Ilustración 35: Áreas a las que se le asignaría la responsabilidad de IA

En línea con la pregunta anterior y, ahondando un poco más en la cuestión de qué área o función debería ser la que heredara la responsabilidad del cumplimiento del nuevo Reglamento de IA, vemos que hay una opción que se destaca de las demás.

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 (31.58%) y el CISO (26.32%) son las opciones más comunes, lo que destaca la importancia de la privacidad y la seguridad en la implementación de IA.

También se considera una opción relevante nombrar una función específica como Responsable de IA (10.53%) y al área de Compliance (18.42%), lo que refleja la necesidad de abordar los aspectos éticos y regulatorios de la IA.

También arroja un resultado amplio la opción "Otros", 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

Acciones de concienciación sobre el futuro Reglamento de IA

En línea con las respuestas de la primera pregunta de este bloque, donde se aprecia una sensación de desentendimiento con el nuevo Reglamento de IA, casi la mitad de los encuestados afirma no haber tomado concienciación en su compañía. Esto refleja una posible falta de atención o entendimiento sobre las implicaciones y requisitos del Reglamento de IA.

En el lado opuesto, entre los encuestados que, si han realizado ya alguna acción de concienciación, un 21 % lo habría abordado directamente en el Comité de Dirección; un 10 % habría limitado estas acciones formativas a comités intermedios; y, finalmente, otro 10 % habría extendido las acciones formativas a la totalidad de la plantilla, mediante noticias, infografías, y otras píldoras formativas.

Estas iniciativas demuestran un nivel de concienciación sobre la importancia de la preparación para el Reglamento de IA en la alta dirección y en niveles jerárquicos intermedios. Será crucial para las compañías sin acciones aún considerar implementar programas de concienciación y formación para garantizar una preparación adecuada para las regulaciones futuras.

Ilustración 36: Acciones de concienciación sobre el futuro Reglamento de IA

Resumen Ejecutivo

Desde el DPI de ISMS Forum llevamos estudiando y apoyando la figura del DPO desde hace muchos años. El Observatorio y estas encuestas nos ayudan a valorar la evolución de esta función 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:

Los DPO van ocupando poco a poco posiciones más estratégicas dentro de las organizaciones, destacando su importancia en la toma de decisiones relacionadas con la privacidad y la protección de datos.

Se va consolidando la figura con mayor autonomía respecto a otras áreas y funciones complementarias. Existe un mejor nivel de report a la Dirección y se realiza con mayor frecuencia que en años anteriores. 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 maduran también verticales de trabajo como la gestión de riesgo de terceros (diligencia debida y encargados de tratamiento).

2. Retos y necesidades:

Los datos revelan 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 la implantación de los procedimientos de privacy by design, así como de 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.

Este año es muy significativa la llegada del Reglamento de IA, sobre el que aún las compañías tienen mucho que hacer en cuanto a formación y diseño de modelo de gobernanza, pero hay que destacar que los DPO están bien posicionados para ser la función que lidere la implantación y cumplimiento regulatorio de los nuevos requisitos de esta norma.

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