El rol del DPO en las empresas

KPMG. Make the Difference.

2025

kpmg.es

Introducción

Ser **Delegado de Protección de Datos o DPO** por sus siglas en inglés, no es (ni ha sido) tarea fácil. El incremento de los requisitos regulatorios, así como la interconexión y globalidad de las empresas exigen a los responsables de privacidad un mayor conocimiento normativo y sectorial que les permita responder a los diferentes requisitos de privacidad que se pueden encontrar en los países en los que operan. A ello se suma el avance acelerado de las nuevas tecnologías, como la IA y la transformación digital, que exige, por un lado, la involucración del DPO y la de sus equipos en las iniciativas y en el diseño de los proyectos desde su concepción, y por otro la actualización continua de las capacidades y las competencias en estas materias.

Y todo ello en un contexto en el que los ciudadanos son cada vez más conscientes de sus derechos: solicitan y exigen más información sobre sus datos y se preocupan por su privacidad. El informe *"Responsible data use at a crossroads: European citizen´s perspective on privacy"* de KPMG ponía de manifiesto que el **75% de los ciudadanos españoles encuestados tenían mayor conciencia conscientes sobre la privacidad que 5 años atrás**. La promoción del cumplimiento regulatorio, las campañas de concienciación dentro y fuera de las empresas y otros aspectos relacionados con los medios de información y actualidad, explicarían este fenómeno.

Como consecuencia, el **DPO está adquiriendo una mayor relevancia dentro de las estructuras corporativas**, con un papel fundamental en la generación de confianza; es la persona encargada de impulsar la protección de datos dentro de las compañías en las que los datos es uno de los activos de mayor valor.

Desde KPMG, nos hemos propuesto **analizar en este informe cómo está evolucionando la figura del DPO en España y Europa**, poniendo el foco en aspectos como su posición dentro de la estructura de la organización, su involucración en el diseño de proyectos y procesos de las compañías, las funciones que desempeña, o los equipos y la tecnología con los que trabaja. Asimismo, hemos comparado la realidad de este perfil profesional en España con la de sus homólogos europeos.

Las conclusiones del informe se han extraído de una **encuesta realizada a 50 empresas** que operan en **países de la Unión Europea**, donde aplica el Reglamento General de Protección de Datos (RGPD).

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

¿Cómo se abordan los objetivos y las estrategias?

La relación entre privacidad y seguridad en las organizaciones

En un momento en la que digitalización se ha integrado en la vida de los ciudadanos, tanto en el ámbito profesional como en el personal, los datos personales se consolidan como uno de los principales activos de las compañías. Si un análisis avanzado de estos datos permite ofrecer productos y servicios que respondan a las necesidades del consumidor y generar así nuevas oportunidades de negocio, también es cierto que una brecha de seguridad que exponga esta información puede suponer un impacto para la reputación de la organización, y más importante aún, en la seguridad de los interesados (clientes, empleados, terceras partes…. etc.). Por ello **los equipos de privacidad y seguridad han de colaborar estrechamente**.

El 54% de los encuestados señala que como DPO trabaja de manera cercana con el CISO y el departamento de seguridad, realizando revisiones periódicas para alinear tanto estrategias como objetivos. En estas organizaciones, **la privacidad y la seguridad se entienden como disciplinas interrelacionadas, que trabajan conjuntamente en la mitigación de los riesgos**.

No obstante, el porcentaje de organizaciones en las que la colaboración entre ambas áreas es ocasional es elevado (46%).

En estos casos, se priorizan los aspectos más operativos de la función de privacidad.

En España, en comparación con otros países, se observa un mayor porcentaje de empresas en las que el DPO colabora de forma estrecha con el CISO, especialmente en aquellas que operan en varios mercados. De este modo, en estas organizaciones, se produce una **alineación estratégica entre las funciones DPO – CISO, dando como resultado una práctica más sólida en protección de datos, y un enfoque integral en la gestión de riesgos y cumplimiento normativo**.

En los tiempos actuales nadie cuestiona que la privacidad y la ciberseguridad van de la mano y, los profesionales de la privacidad, necesitan apoyarse en las áreas enfocadas a aplicar medidas de seguridad en los sistemas ya que cada día integran tecnologías más complejas.

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

¿Existe involucración real del DPO? ¿Es suficiente y visible?

El DPO tiene como una de sus principales funciones asegurar el cumplimiento normativo y actúa como enlace entre empresas, reguladores y derechos individuales. Pero ¿es su participación efectiva para garantizar la integración de principios de privacidad y seguridad en los procesos empresariales?

De acuerdo con los datos de la encuesta, **la alta dirección de las empresas, de los DPO en España está activamente involucrada en la gestión de la protección de datos**, en comparación con un 10% de los DPO europeos. Esto subraya la importancia de que **el compromiso con la privacidad debe emanar de los niveles más altos de la empresa, promoviendo una cultura de responsabilidad en la protección de datos personales a través de un liderazgo visible**.

Según la encuesta, el 65% de los DPO europeos identifica tiene una involucración moderada, participando en algunas de las decisiones clave de la compañía, cifras que son muy similares a las de los DPO españoles (60%). Únicamente un 16% de los DPO europeos indica que no tienen visibilidad o esta es mínima, cifra que es menor en el caso de los nacionales (10%).

Sin embargo, aún queda camino por recorrer para aumentar la involucración. Los resultados muestran que solo el 24% de los DPO encuestados participa desde el inicio en nuevos proyectos tecnológicos, un 35% es notificado, pero no participa activamente, y más del 40% se involucra una vez iniciado el despliegue. Además, un 16% indica que no existen procedimientos formales para su participación.

La involucración del DPO desde el inicio de los proyectos y oportunidades estratégicas es clave para construir este tipo de decisiones teniendo en cuenta la privacidad, aumentando la sensibilización y promoviendo una cultura empresarial.

¿Dónde se encuentran las resistencias internas?

El DPO tiene como una de sus principales funciones asegurar el cumplimiento normativo y la protección de datos en las organizaciones. Para ser efectivo, **necesita colaborar estrechamente con todas las áreas internas de la empresa**.

El departamento **donde se encuentran los mayores retos o resistencias es Marketing, seguido de las áreas de Operaciones, y recursos humanos**.

Un 32% de los encuestados realiza reuniones periódicas con los diferentes equipos de proyecto para conocer las nuevas iniciativas de la compañía, mientras que un 25% identifica que son los departamentos quienes les involucran directamente, a través de mecanismos internos.

Un 25% de las personas que han respondido a esta encuesta, coinciden en que, falta en ocasiones, una colaboración estructurada, ya que en algunos casos estas se producen por solicitudes ad hoc, lo cual refleja un enfoque reactivo en lugar de proactivo en la gestión de la privacidad, y no les permite anticiparse a las necesidades.

Es importante integrar la privacidad como objetivo principal de negocio que implique a todas las áreas y no sólo cuando surgen necesidades inmediatas.

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

¿Cómo se mide y reporta la privacidad?

Aunque el 70% de los encuestados reporta al más alto nivel de la organización, un porcentaje significativo reporta al CISO o al departamento de seguridad (13%) y existe un mínimo porcentaje que reporta a otros roles (Cumplimiento, Legal o Riesgos principalmente). Esto nos muestra que en algunas organizaciones la privacidad se integra como parte de estas áreas funcionales, y esta dependencia podría repercutir en la capacidad del DPO o responsable de privacidad, en su caso, de actuar con independencia en el ejercicio de sus funciones, como requiere la normativa.

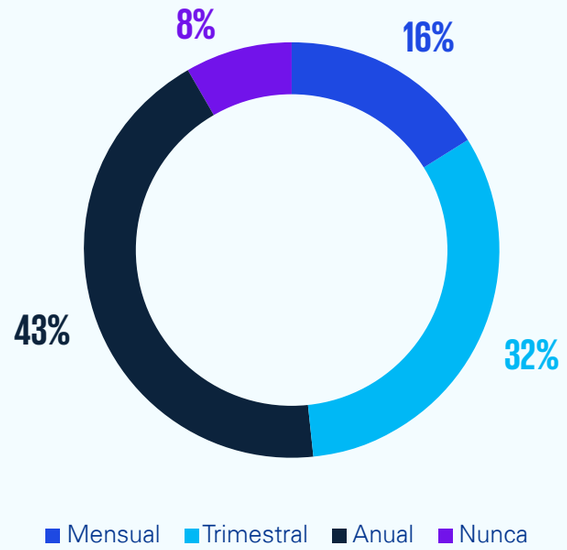
Es recomendable que el reporte a la alta dirección sea prioritario para garantizar tanto la independencia del DPO, como la alineación estratégica de la privacidad con los objetivos de la compañía.

En relación con la frecuencia, más del 90% reporta al menos una vez al año, siguiendo lo dispuesto en el RDGD. Se intercalan varios tipos de frecuencia, un 43% únicamente realiza reportes con carácter anual, lo cual puede significar que desde la alta dirección se considera suficiente recibir actualizaciones de forma puntual, teniendo por tanto una percepción de que el DPO y la privacidad tiene poco impacto estratégico.

Un segundo grupo (12%) reporta trimestralmente. Se ha identificado en estos casos que se tratan de compañías que tienen un alcance internacional, permitiendo monitorizar frecuentemente el estado de la protección de datos, siendo un tema estratégico y de impacto en el crecimiento.

Tener un reporte más frecuente que el anual, permite a nuestros DPO involucrar activamente a la alta dirección. La implantación de procesos mensuales o trimestrales de reporte crea estructuras que integran la privacidad en la estrategia empresarial. En el caso de los DPO españoles, el reporte anual es el mayoritario (60%), seguido del mensual (30%).

¿Con qué frecuencia se realiza el reporta a la alta dirección?



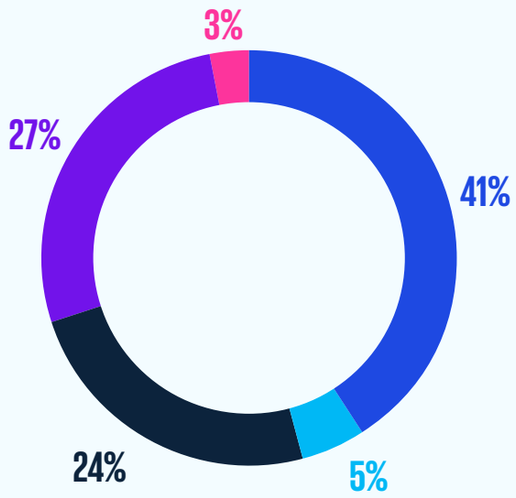
Si bien muchas empresas intentan alinearse con los estándares de cumplimiento, la falta de métricas efectivas y reportes frecuentes a la alta dirección limita el impacto estratégico del DPO.

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

Indicadores de éxito: ¿qué se mide?

La monitorización y la evaluación de la madurez del programa de privacidad parece que sigue siendo una asignatura pendiente en algunas de las compañías. Nos encontramos con un panorama con una diversidad significativa. Aunque más del 40% de las **organizaciones ha desarrollado un enfoque que permite medir su programa** según estándares internos adaptados a sus necesidades, aún muchas organizaciones tienen **pendiente trabajar en definir sus métricas y finalmente implantarlas**. El 24% se encuentra trabajando en su implementación, y un 27% no dispone de métricas que permitan medir de manera efectiva el resto del programa. No disponer de métricas para medir la efectividad del programa implantado puede repercutir en mayores dificultades a la hora de solicitar un mayor presupuesto o recursos para la función, así como demostrar el valor que tiene la privacidad en la organización. **Las métricas y su seguimiento permiten también establecer objetivos de privacidad de conformidad a los datos, y a la realidad que afronta cada compañía.**

¿Qué métricas se utilizan para medir el éxito del programa de privacidad?



- Indicadores clave de rendimiento (KPI) basados en un marco de control interno que abarca ámbitos como la gestión de derechos, la gestión de la violación de datos personales, etc.
- Actualización del registro de actividades
- Se está trabajando en implementar indicadores
- No existen parámetros normalizados para medir el programa de privacidad
- Auditorías externas

¿Las necesidades de privacidad se encuentra cubiertas?

Mas de la mitad de los encuestados considera que dispone de un equipo con los participantes suficientes para ejecutar su trabajo (57%), pero acusa la carencia de otro tipo de recursos o encuentra limitaciones en algunas áreas, frente a un 22% que señala que no dispone de las personas necesarias en su equipo para la gestión de privacidad.

Esto puede indicarnos que, **aunque las compañías están invirtiendo recursos en privacidad, no llegan a cubrir las necesidades que actualmente demandan y pueden suponer un desafío para el cumplimiento efectivo o la consecución de los objetivos marcados.**

Tan sólo un 19% de los DPO indica que el presupuesto que recibe es suficiente para cumplir con las obligaciones que tiene asignadas por su rol y en los equipos. Según la información facilitada, estas organizaciones a su vez, realiza los reportes a la alta dirección con mayor frecuencia, y la medición de su programa de privacidad se basa en métricas construidas e implementadas desde sus propios marcos de control normativo.

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

Tecnología y privacidad: ¿Cuáles son las herramientas detrás de la gestión?

Se ha identificado un **uso extendido de las herramientas** más conocidos de **ofimática** (36%), lo cual puede hacernos pensar que no se está utilizando la tecnología como un factor estratégico en la gestión de la privacidad. Uno de los riesgos que podemos identificar en este caso son las limitaciones en términos de escalabilidad, seguridad, y en algunos casos eficiencia.

Un 22% de los DPO encuestados identifica que han **desarrollado sus propias aplicaciones** internas para la gestión de la privacidad, afrontando así los desafíos que plantean este tipo de desarrollos, como puede ser que, si se realizan de manera aislada puede generar falta de integración con otros procesos de la compañía, generando duplicidades.

Si bien es cierto que en ambos casos, se combina su uso con herramientas de terceros especializadas en privacidad.

Se ha observado en algunas organizaciones, un porcentaje significativo de los DPO (36%) que ha optado por el **uso de herramientas especializadas para gestionar la privacidad**. Un porcentaje menor (10%) de este grupo, prefiere centralizar sus esfuerzos utilizando exclusivamente una herramienta proporcionada por un proveedor.

La clave en este punto es facilitar la gestión de aquellas tareas documentales que son esenciales para cumplir con los deberes de ***accountability***, permitiendo dedicar tiempo y recursos a actividades donde es necesario aunar fuerzas al requerir una mayor colaboración entre áreas. Se asegura así que los nuevos productos que las empresas quieren lanzar o nuevos servicios tienen presente la privacidad como un factor diferencial.

Hay que **tener en cuenta los objetivos y metas de cada compañía para decidir si es conveniente unificar los procesos a través de soluciones más integradas que optimicen la gestión del cumplimiento**.

El 46% de los encuestados coincide en que el **cumplimiento regulatorio es la pieza clave a tener en cuenta a la hora de escoger una herramienta** para gestionar la privacidad, seguido muy de cerca de la usabilidad por parte del equipo y la gestión del propio programa, lo que supone que la herramienta permita recoger varios procesos de privacidad.

Encabezan las prioridades de los DPOs españoles la usabilidad para los equipos y la propia gestión del programa de privacidad.

Las prioridades de los DPOs españoles (Top 5)

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

La agenda del DPO

La actividad que consume más tiempo en el reloj del DPO es la **gestión del programa de privacidad y la comprobación de su efectividad**, seguidas de un **trabajo continuo para garantizar su alineamiento con los objetivos estratégicos de la compañía**. El día a día del DPO se complementa con resolución de consultas, respuestas a peticiones por parte de los equipos que demandan asesoramiento y acciones destinadas a la formación y sensibilización. Los DPO tienen más que presente el compromiso continuo con la privacidad a través de las actividades de *Accountability*, dedicando gran parte de su tiempo a la revisión de contratos, gestión de terceros y procesos de *privacy by design* a través de la involucración en nuevos proyectos o iniciativas.

Para mejorar la protección de datos y la privacidad, es crucial integrar la privacidad en la estrategia empresarial y considerar la implementación de herramientas tecnológicas más avanzadas y procesos estructurados que faciliten una colaboración proactiva y eficiente entre diferentes áreas de la organización.

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

¿Quién hace qué y cuándo?

Segun los resultados de esta encuesta, el 72% de las oficinas de privacidad de los encuestados se componen de un equipo que tiene entre **5 y 10 miembros o FTE**. También hemos obtenido como resultado, que el 48% de los encuestados DPO **llevan en su posición más de 5 años**.

En el panorama nacional, el tamaño de la oficina es más reducido, con carácter general. El 70% de los equipos está formado por menos de 5 empleados. Sin embargo independientemente del alcance territorial, el 81% de los DPO ha respondido que su **presupuesto no es suficiente o no es acorde** o no cubre al 100% la demanda de su función.

El 72% de las oficinas de privacidad se componen de entre

5 y 10 miembros

El 48% de los DPO llevan en su posición

+ 5 años

El 81% de los DPO considera que su

presupuesto

no es suficiente o no es acorde

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

¿Quiénes forman parte de la oficina del DPO?

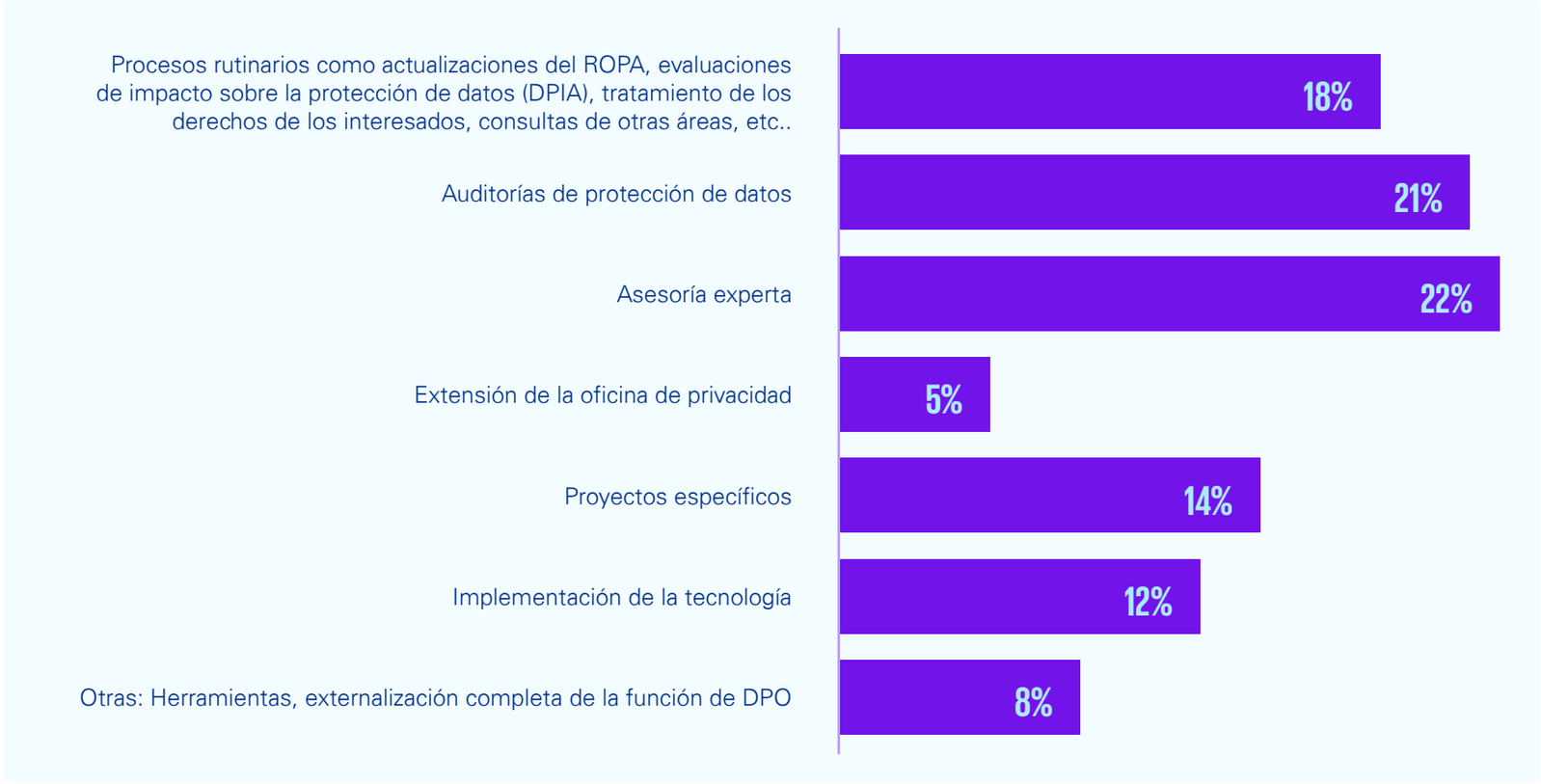
Como identificábamos anteriormente, con carácter general un 70% de los encuestados indica que dispone de **equipos reducidos** para la gestión de la privacidad (<5 miembros), en estos casos se podrían enfrentar dificultades para abordar la creciente complejidad de la privacidad, especialmente en **organizaciones más grandes o que operan en múltiples jurisdicciones**.

Los **equipos**, son **multidisciplinares** y más del 55% de los perfiles responde a profesionales especializados en privacidad y protección de datos. Con los especialistas en *Compliance* (26%) e ingenieros (10%) crean equilibrio entre habilidades técnicas, legales y de cumplimiento.

En España, la actividad que con mayor frecuencia externalizan los **DPO son las auditorías de protección de datos**, suelen buscar servicios de asesoramiento para cuestiones concretas y específicas, y delegan parte del día a día de la oficina, también conocido como *Business as Usual* (BAU por sus siglas en inglés).

Los equipos son multidisciplinares, equilibrando así las competencias técnicas, organizativas y de cumplimiento necesarias para abordar con eficacia las tareas.

En relación con los servicios externalizados por parte del Oficina, se reparten de la siguiente manera:



© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

¿Cómo se abordan algunas obligaciones?

Sobre las distintas obligaciones que existen en la oficina, veremos cómo se afrontan las **principales tareas** para dar respuesta a los requisitos normativos:

Registro de actividades del tratamiento

Sobre la **actualización del RAT** o registro de actividades del tratamiento y quién se encarga de esta función, el 37% manifiesta que es una actividad que tiene delegada a negocio. Por su parte el 63% de los DPO indica que se realiza directamente entre las áreas que tienen asignadas las tareas de protección de datos, a veces con entidad propia y en otras ocasiones circunscritas en determinadas áreas departamentales, que principalmente suelen ser *Compliance* o Legal.

Evaluaciones de impacto sobre la protección de datos (EIPD, PIA)

En la **ejecución de las evaluaciones de impacto sobre la protección de datos (EIPD) o PIA** por sus siglas en inglés, hemos encontrado cierta disparidad en las respuestas. Mientras el 48%de los encuestados afirma que las realiza el DPO y el personal dedicado de su oficina, el 52% comparte que se gestionan por diversas áreas como riesgos, negocio, seguridad u otros.

Gestión de incidentes

Según la encuesta, la **gestión de incidentes** con afectación a datos personales suele ser una tarea compartida entre TI, seguridad, negocio y DPO en el 65% de los casos y solo en el 35% se gestionan y lideran directamente por DPO siendo este quien lleva la iniciativa.

En España el 50% de los DPO colabora con los equipos de IT y un 30% señala que existen en la organización equipos especializados en la gestión de incidentes que reportan directamente al DPO.

Medidas de seguridad

Al respecto de las **medidas de seguridad**, hemos encontrado que en casi en el 60% de los casos las medidas de seguridad son delegadas al área de Seguridad de la Información con limitada supervisión por parte del DPO o de su oficina.

Retención, borrado y expurgo de información

El establecimiento de **políticas internas para la retención, borrado y expurgo** de información en su mayoría son realizadas por el DPO y su función en colaboración con las áreas de negocio, opción que marca el 60% de los encuestados). El 30% comparte que en su organización las definen las áreas de negocio con la involucración del DPO en los casos requeridos y un 10% señala que las impulsan áreas terceras que no llegan a involucrar a DPO.

KPMG

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

Responsabilidad proactiva

Aunque las auditorías ya no son obligatorias, parte de la gestión de la **responsabilidad proactiva**, o el establecimiento de medidas técnicas y organizativas para asegurar y garantizar el cumplimiento normativo, se puede materializar en actividades entre las cuales se pueden encontrar la evaluación o auditoría del programa de privacidad. A este respecto solo el 18% de los DPO cuenta con un equipo interno o externo dedicado a realizar auditorías de cumplimiento normativo. El 38% de los encuestados indica que se realizan internamente desde su oficina y el 43% se apoya en otros departamentos, como auditoría interna.

Más de la mitad de los DPO encuestados confía en la **concienciación y las campañas de sensibilización** para comunicar los cambios en las políticas de privacidad y protección de datos (54%), un 27% delega en los responsables de cada área este papel, tras efectuar la comunicación, mientras que un porcentaje pequeño pero reseñable (19%), sólo realiza comunicaciones en caso concretos y específicos.

Es fundamental que el DPO involucre a terceros departamentos en la ejecución de tareas como por ejemplo la actualización del registro de actividades, la ejecución de las EIPD o la gestión de los derechos de protección de datos.

No olvidemos que tal y como cita el artículo 39 del RGPD, las **funciones del DPO pasan por informar, asesorar y supervisar el cumplimiento**. Si bien, este artículo no manifiesta que sea directamente el DPO quien deba ejecutar las EIPD, completar los RAT o dar respuesta a los derechos que solicitan los interesados.

Mientras que en Europa la preocupación se iguala entre la falta de presupuesto y la colaboración de otras áreas, en España el 78% de los DPO considera que la falta de involucración de terceras áreas es un reto que hay que abordar.

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

La percepción de los DPO sobre las oportunidades y retos de su función

Las necesidades de nuestros DPO pivotan en dos direcciones, casi el 50% demanda **aumentar su participación en las decisiones estratégicas** de la organización, un 43 % de los DPO reclaman un mayor reconocimiento del valor que aporta la función de privacidad y protección de datos en la gestión de riesgos. Un 8% indica que necesitarían **acceso a mejores recursos tecnológicos** para el desempeño de su trabajo. Los datos son similares entre los DPOs españoles y europeos.

En España

11% reclama falta de recursos

11% contesta estar al día con regulaciones y novedades de tecnología emergente

78% dificultades involucrando a terceros departamentos en privacidad

En Europa

40% reclama falta de recursos

20% contesta estar al día con regulaciones y novedades de tecnología emergente

40% dificultades involucrando a terceros departamentos en privacidad

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

Formación continua y transversal

La constante publicación de noticias de privacidad o novedades regulatorias hacen necesaria la **actualización y puesta al día** de la función del DPO. Este argumento se apoya en los resultados de la encuesta en los que se identificó que el 54% de los DPO se forma de manera continua y participa en foros y grupos de relevancia en la materia de privacidad y protección de datos. Sin embargo, ponemos de manifiesto que el otro 46% reconocía no hacerlo o hacerlo ocasionalmente.

Las exigencias informativas y normativas demandan que los profesionales de la privacidad se mantengan al día y compartan con sus semejantes sus preocupaciones creando así grupos de trabajo que permitan hacer fuerza en sector.

Innovación y estrategia

Es interesante poner de manifiesto que tanto en España como en el resto de los países europeos la percepción del 60% de los encuestados es que deberían estar involucrados en **decisiones con un tinte más estratégico** demandando por tanto una mayor **involucración en este tipo de proyectos desde el inicio y no de manera accidental o accesoria**, como manifiesta alguno de los participantes en este estudio.

Sobre la **autopercepción de la función del DPO en términos de innovación** y evolución, el 35% está actualmente involucrando la **tecnología** en sus procesos, mientras que el 37% espera hacerlo, aunque no ha empezado. El 27% restante por el momento no ha implementado, ni considera hacer cambios significativos en el corto plazo porque se encuentran **inmersos en mejora de la madurez de sus procesos de cara a poder preparar estos para una posible automatización**.

En relación a la **implementación de nuevas tecnologías como parte de la estrategia**, un 70% de los DPO españoles ya se encuentran integrando nuevas herramientas para gestionar *big data* e IA, frente a un 30% que aún no han implementado nada debido a que se encuentran trabajando activamente en cumplir por el momento con la normativa de privacidad.

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

Conclusiones

Incremento de la visibilidad del DPO en las decisiones más estratégicas

El rol del DPO ha ganado **mayor visibilidad y participación en las decisiones estratégicas** de las organizaciones. Este cambio es esencial, ya que permite que la privacidad y la protección de datos sean consideradas desde las primeras etapas de cualquier proyecto, lo que fortalece la gestión de riesgos y el cumplimiento normativo.

Colaboración entre áreas como CISO, DPO, IT, etc.

Se ha identificado que la **colaboración entre las áreas** de seguridad de la información (CISO), protección de datos (DPO) y tecnologías de la información (IT) es **fundamental para una función efectiva del DPO**. Esta cooperación asegura que la privacidad y la protección de datos se aborden de manera integral, **permitiendo una respuesta más eficiente a los desafíos y mitigando los riesgos asociados**. Pero es necesario también tener en cuenta al resto de áreas de las compañías.

Recursos insuficientes para la demanda cada día más creciente

La creciente demanda de privacidad y protección de datos por parte de los ciudadanos ha puesto de manifiesto la **insuficiencia de recursos** con la que cuentan muchos DPO. Es crucial que las **organizaciones asignen los recursos necesarios para que los DPO puedan innovar, formar a sus equipos y mejorar continuamente los programas de privacidad para cumplir con las expectativas regulatorias y de los usuarios**.

Metodología

Informe basado en una encuesta realizada a los DPO o responsables de privacidad de 50 empresas europeas de diferentes sectores (sector financiero, *retail*, industria, educación, energía o tecnología) en el último trimestre del año 2024.

Los porcentajes de los gráficos pueden no sumar 100 por efecto del redondeo de los decimales.

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

Contactos

Javier Aznar
Socio de Riesgo Tecnológico, Ciberseguridad y Privacidad KPMG en España
jaznar@kpmg.es

Ángela Manceñido
Manager de Riesgo Tecnológico, Ciberseguridad y Privacidad KPMG en España
amancenido@kpmg.es

María Cristina Köhler
Manager de Riesgo Tecnológico, Ciberseguridad y Privacidad KPMG en España
mariacristinakohler@kpmg.es

kpmg.es

© 2025 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

KPMG y el logotipo de KPMG son marcas registradas de KPMG International Limited, sociedad inglesa limitada por garantía.

La información aquí contenida es de carácter general y no va dirigida a facilitar los datos o circunstancias concretas de personas o entidades. Si bien procuramos que la información que ofrecemos sea exacta y actual, no podemos garantizar que siga siéndolo en el futuro o en el momento en que se tenga acceso a la misma. Por tal motivo, cualquier iniciativa que pueda tomarse utilizando tal información como referencia, debe ir precedida de una exhaustiva verificación de su realidad y exactitud, así como del pertinente asesoramiento profesional.