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

Fecha publicación

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

OBSERVATORIO DE LA PRIVACIDAD

AUTORES

PARTICIPANTES	Carlos Alberto Sáiz Peña
	Leyre Duo Navarro
	María Cristina Köhler García
	Nora García Portillo
	Xabier Alberdi Oyanguren
GESTIÓN DE PROYECTOS	Beatriz García González
DISEÑO/MAQUETACIÓN	Cynthia Rica Gómez

CONTENIDOS

Introducción

Objetivos del Observatorio de Privacidad

- Convertirse en una plataforma para el análisis del nivel de madurez de cumplimiento en el ámbito de la protección de datos.
- Generar indicadores nacionales sobre esta materia en empresas y entidades privadas y públicas.
- Generar métricas y referencias nacionales.
- Colaborar y establecer relaciones de interlocución con instituciones y reguladores.

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 que se lleve a cabo en la Unión Europea, a la vista de la importancia de generar la confianza que permita a la economía digital desarrollarse de manera eficaz.

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.

Sobre el Estudio

El presente estudio sobre el nivel de madurez en la aplicación del Reglamento General de Protección de Datos es la tercera edición del análisis que establece el Observatorio de la Privacidad de ISMS Forum con la finalidad de aportar información sobre el estado de la técnica en esta materia, así como para facilitar información de utilidad para empresas y profesionales a través de la generación de un indicador anual que permita, de un lado, interpretar de una mejor manera la evolución interanual de los riesgos que amenazan a la protección de los datos personales y, de otro lado, poner esta información en relación con otros factores relevantes a estos efectos.

El documento, realizado por ISMS Forum, se basa en la información facilitada por una muestra de Delegados de Protección de Datos que desempeñan sus labores en el ámbito territorial nacional, tanto en empresas multinacionales como nacionales.

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 y entre ellas, más del 34% cuentan con más de 20.000 empleados. Tan solo el 10% son pequeñas y medianas empresas. Cabría esperar un aumento de la participación de estas empresas en los próximos ejercicios una vez aprobado el proyecto de Ley "reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción".

Del mismo modo son organizaciones con grandes volúmenes de facturación, más del 36% de las encuestas corresponden a empresas con facturaciones anuales superiores a 10.000 millones de euros.

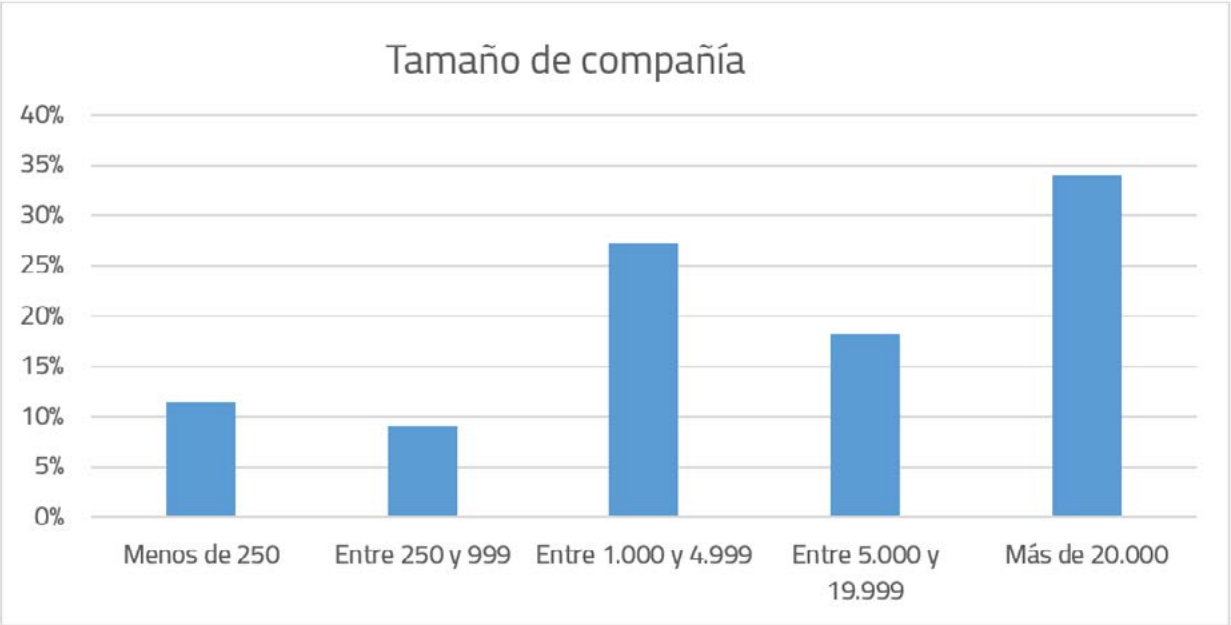

Ilustración 1: Tamaño de las compañías de la muestra

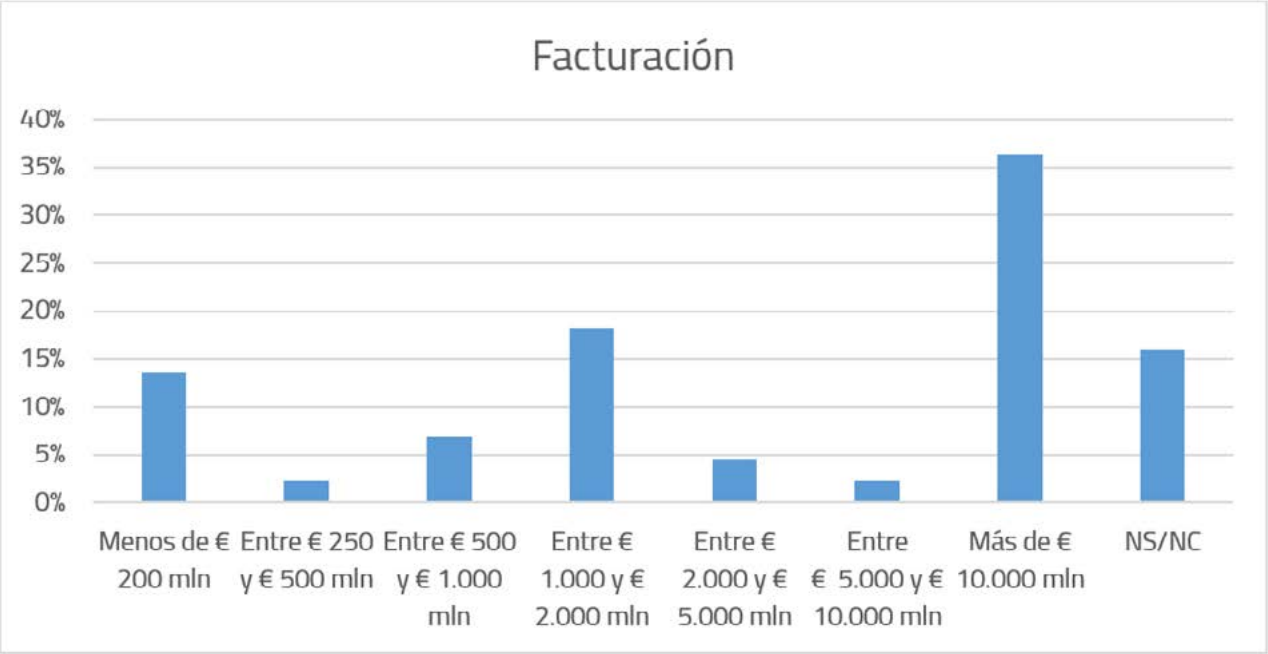

Ilustración 2: Facturación de las compañías de la muestra

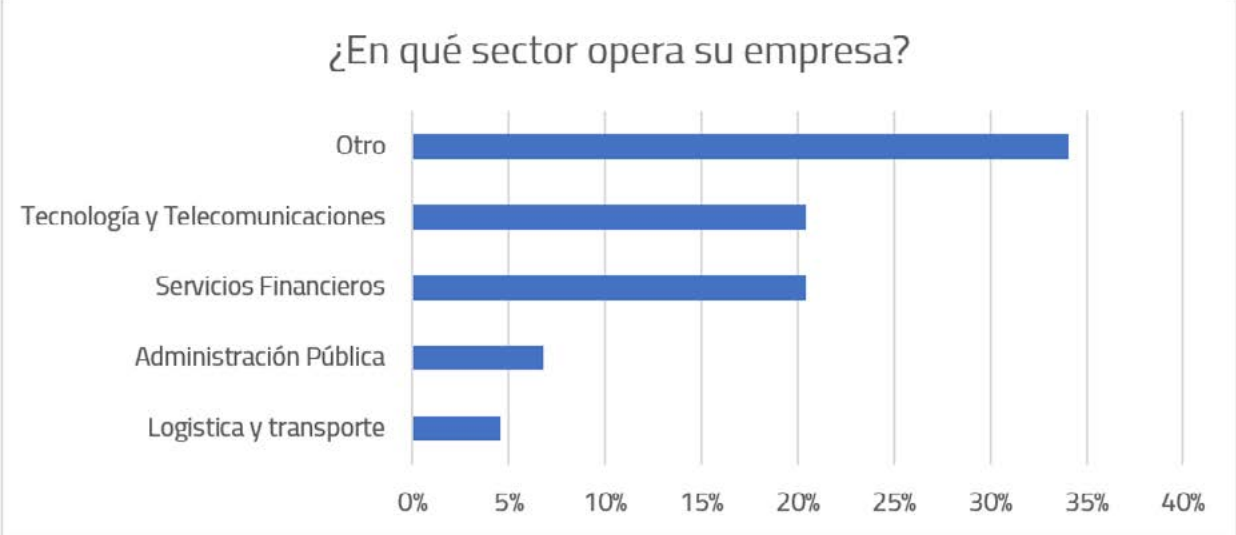

Ilustración 3: Sector de las compañías de la muestra

Estado de situación - Gobierno de la Privacidad

Tipo de DPO y alcance geográfico de la función

En cuanto a tipología de DPO, este año el formato de "función exclusiva de protección de datos" ha superado al de "DPO asumido dentro de un área existente", ganando la función más autonomía.

El 36% de los participantes compatibilizan la función de DPO con cumplimiento, legal o ciberseguridad principalmente.

En comparación con el año anterior, esta opción de función exclusiva ha aumentado en 20 puntos porcentuales. La externalización del DPO también ha aumentado en un 6% y la opción del comité interdepartamental ha desaparecido.

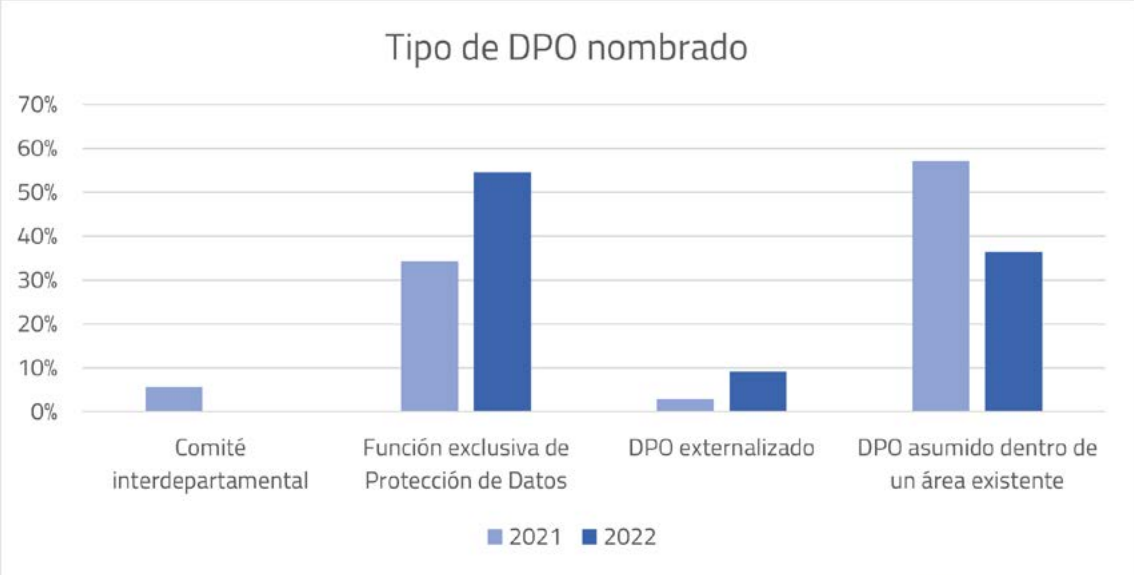

Ilustración 4: Tipo de DPO

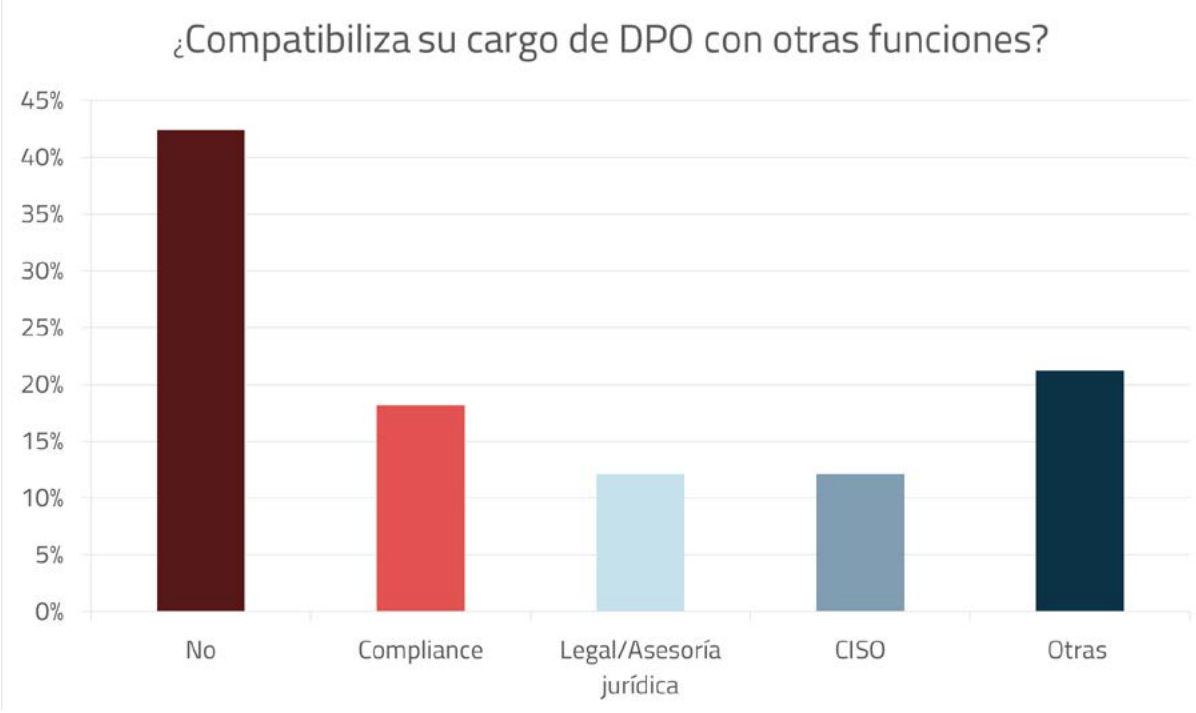

Ilustración 5: Funciones aparte de las de DPO

Un 44% de los encuestados desarrolla sus funciones solo en España, mientras que la mitad de los encuestados tienen un alcance europeo. Un 32% de los participantes se hacen cargo de la protección de datos en un ámbito nacional, europeo y también fuera del continente.

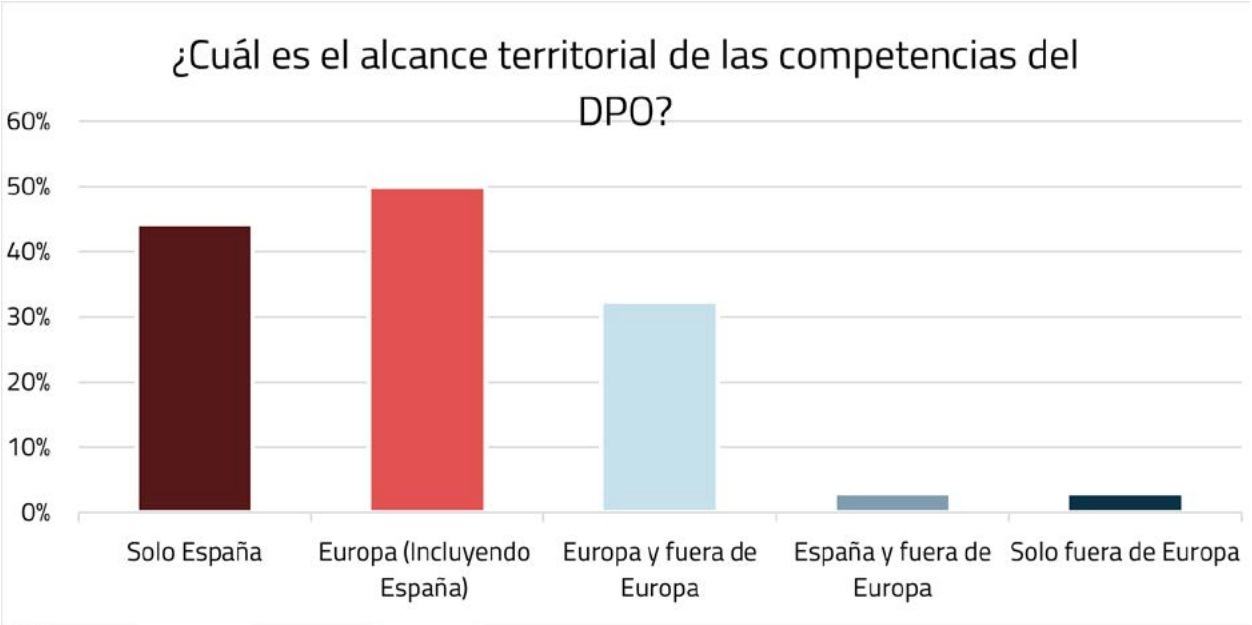

Ilustración 6: Alcance territorial de las funciones del DPO

Formación académica y certificaciones de los DPOs

La mitad de los DPOs disponen de estudios en Derecho. El 30% están formados en IT y seguridad de la información. El resto de encuestados pertenecen a las áreas de ingeniería, ADE y auditoría.

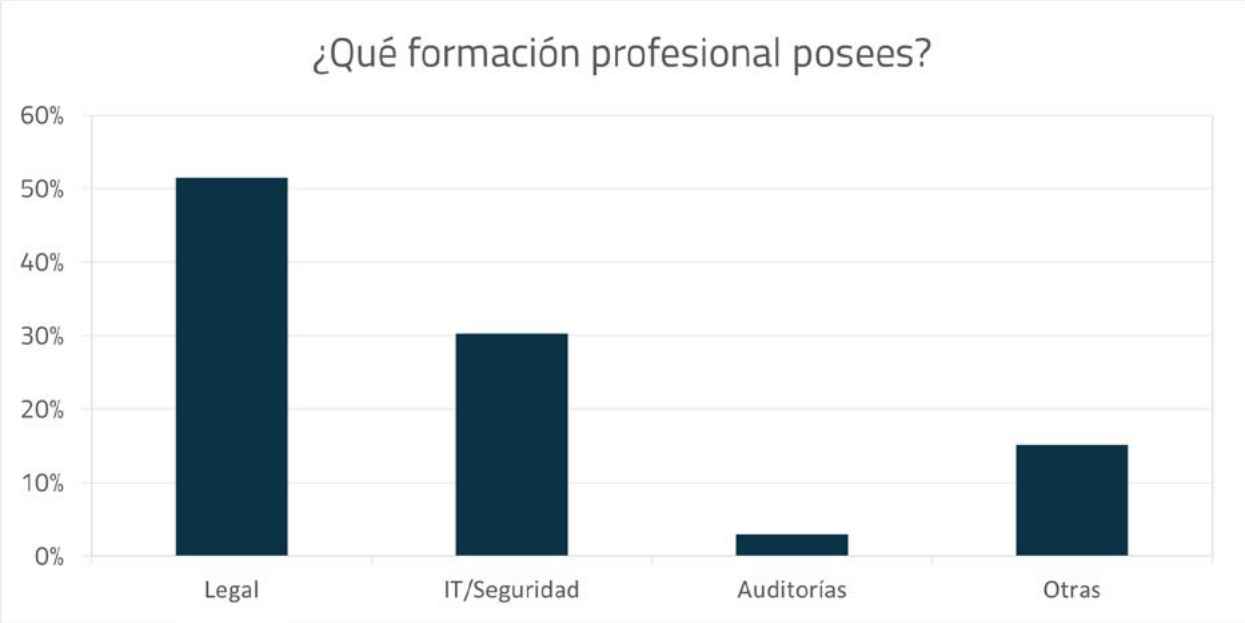

Ilustración 7: Formación del DPO

El número de certificados en CDPD supera a los certificados en CDPP en 10%. Lo que supone un cambio de tendencia respecto a años anteriores donde la certificación en CDPD se movía por debajo o al mismo nivel que la de CDPP.

En Otras Certificaciones se incluyen principalmente CISM y CISA, tendencia que se mantiene con los años.

Cabe destacar que el 40% de los participantes no dispone de ninguna certificación relacionada con la función de DPO.

Ilustración 8: Certificaciones del DPO

Reportes

Las áreas a las que generalmente reporta el DPO se reparten entre la función Legal, Compliance y la alta dirección. En este sentido se aprecia un leve descenso en la tendencia en el reporte a Legal a favor de Compliance.

Entre las otras opciones planteadas por los encuestados a la hora de dirigir sus reportes, destacan las funciones de CISO y opciones mixtas que incluyen a varios departamentos conjuntamente o por separado.

Ilustración 9: Reporte del DPO

Las principales preocupaciones a la hora de reportar son las sanciones y los daños reputacionales, seguidos por las brechas de seguridad y debilidades en el sistema de control. La tendencia en comparación con el año anterior se mantiene en cuanto a los cuatro temas ofrecidos, no obstante, surgen nuevas preocupaciones como son la dificultad en llegar a los objetivos, falta de medidas de seguridad adecuadas y necesidad de aumentar el compromiso de la dirección.

Ilustración 10: Preocupación del informe del DPO

La frecuencia de reporte está repartida relativamente a iguales partes entre anual, semestral y trimestral, aunque la opción más elegida ha sido la del reporte anual. Se destaca que un 12% no realiza ningún tipo de reportes al management.

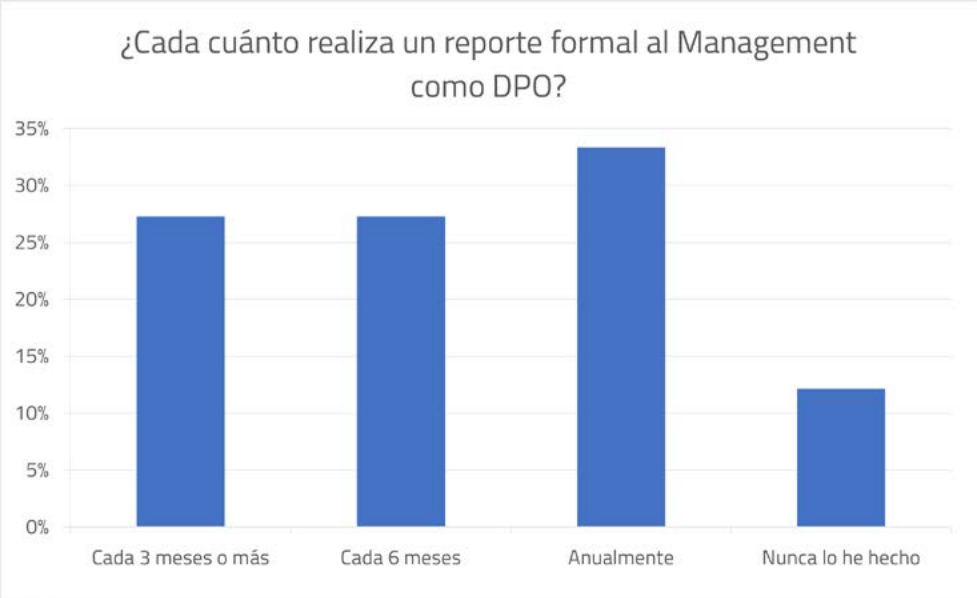

Ilustración 11: Temporalidad de reporte del DPO

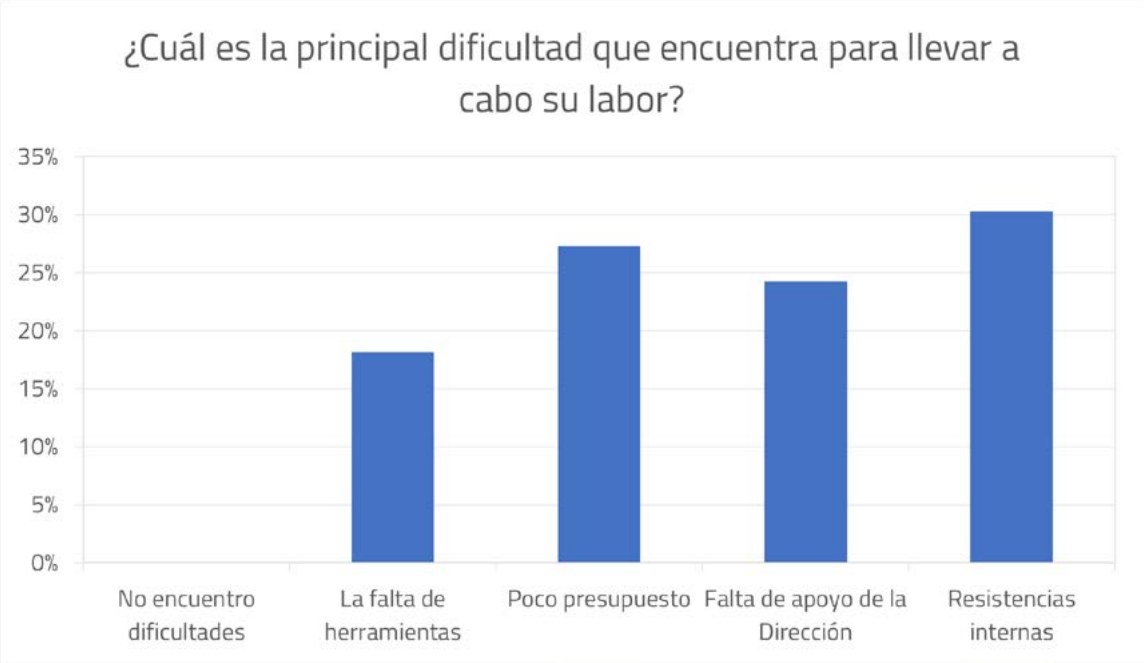

Ilustración 12: Dificultades del DPO

Ningún encuestado considera que no hay dificultades a la hora de llevar a cabo su función. Entre las principales dificultades destaca la resistencia de otras áreas, seguido por un presupuesto insuficiente, falta de apoyo por la dirección y necesidad de mejores herramientas. Revela la necesidad de seguir generando una cultura de privacidad y de implantar procedimientos eficaces de Privacy by Design.

Equipos

Los equipos en la mayoría de los casos son medianos y pequeños. Aproximadamente el 80% de los encuestados trabajan en equipos inferiores a 5 personas. Solo se encuentran equipos medianos y grandes en empresas de más de 20.000 empleados. El equipo más común para todos los tamaños de empresa es de entre 3 y 5 componentes.

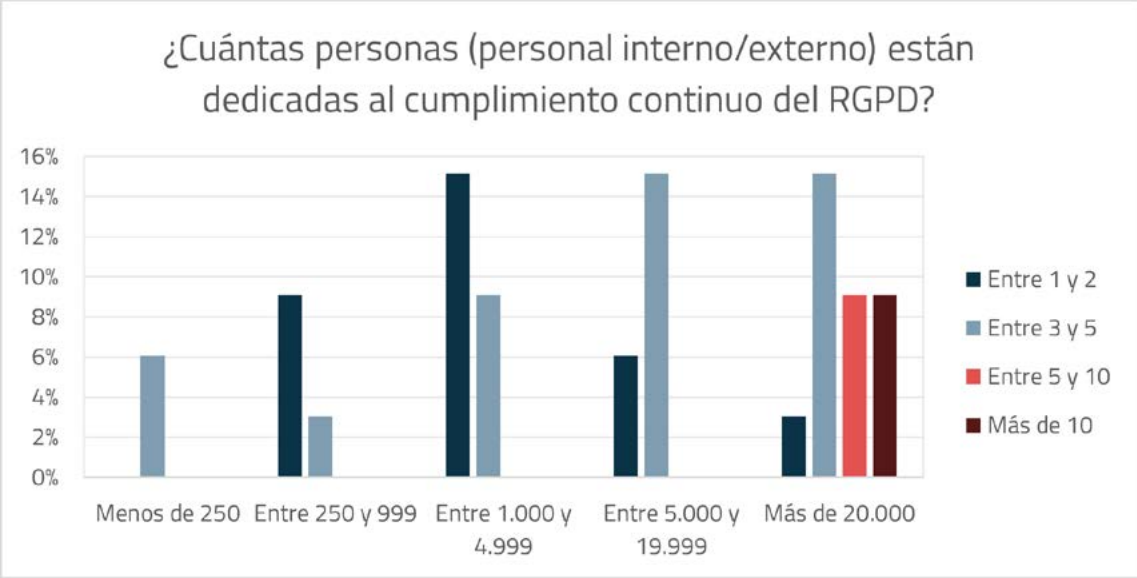

Ilustración 13: Plantilla dedicada al cumplimiento del RGPD

En cuanto a las áreas de la empresa que más colaboran con el DPO destaca claramente el área de seguridad de la información con la mayor intensidad de involucración y el departamento de Procesos/calidad como el menos involucrado. Los aliados naturales del DPO además del mencionado, siguen siendo Asesoría Jurídica, Compliance y Auditoría.

Ilustración 14: Áreas involucradas en el cumplimiento del RGPD

Modelo de madurez de cumplimiento RGPD

Presupuesto en RGPD

Cuando nos referimos al presupuesto anual recurrente de la función de DPO (sin incluir el coste del personal interno), podemos ver que el 33% no tiene un presupuesto definido, frente al 49% que lo tiene hasta un tope de 100.000 €. Si comparamos estos datos con lo respondido en la encuesta del 2021, vemos que ha variado ligeramente y se dedica algo menos de presupuesto. En cambio, el presupuesto insuficiente era uno de los mayores obstáculos del DPO conforme a una pregunta anterior.

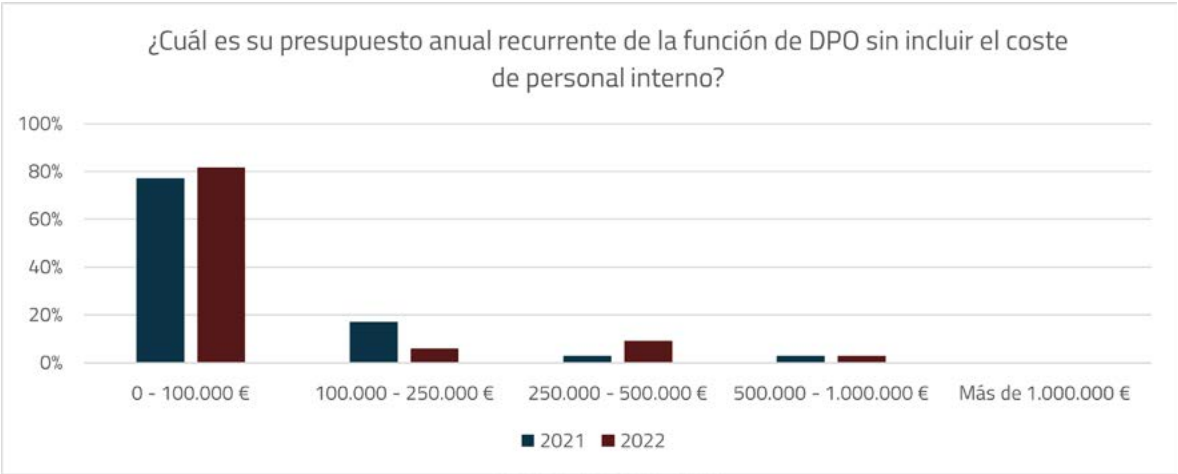

Ilustración 15: Presupuestos anuales

Ilustración 16: Presupuestos por actividad

Al analizar el presupuesto por actividades, vemos que en primer lugar se encuentra la concienciación y formación y la dirección estratégica, planificación y elaboración de políticas. En mitad de la tabla, nos encontramos la inversión en software y la gestión de los empleados y equipos de seguridad. La partida a la que menor presupuesto se dedica es el gasto en los servicios profesionales.

Modelo de cumplimiento de RGPD

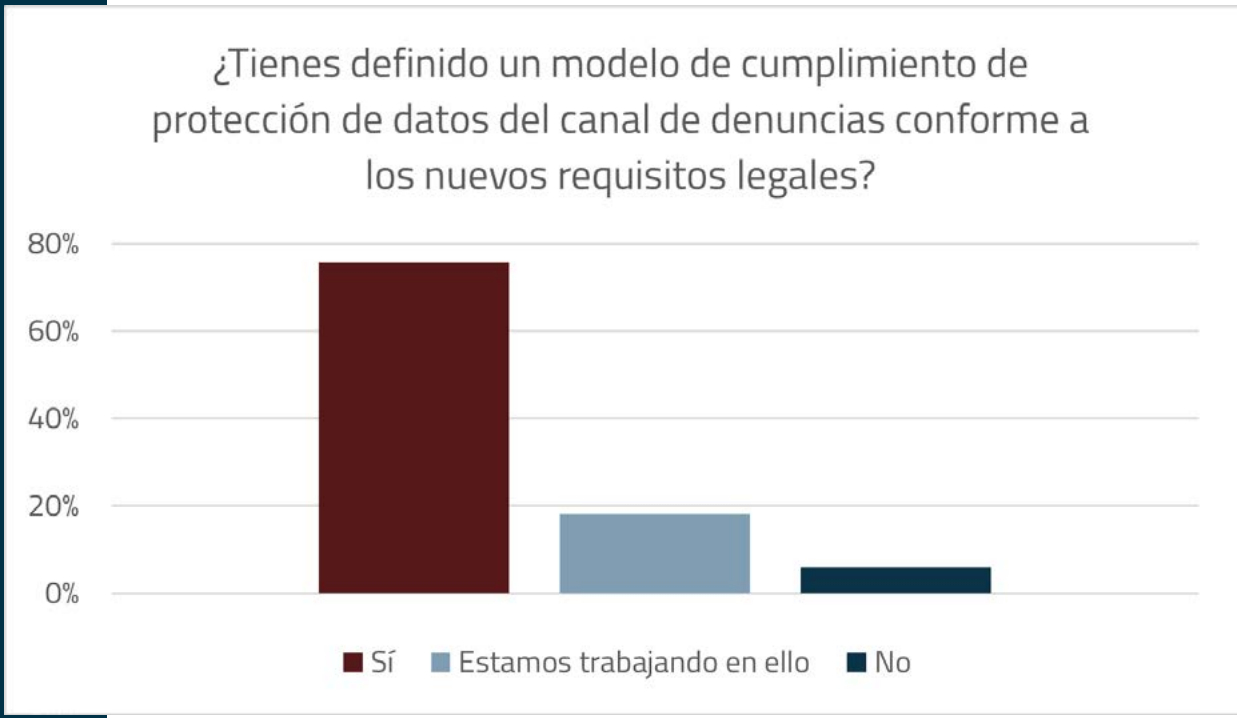

Ilustración 17: Modelo de cumplimiento de protección de datos del canal de denuncias

El 76% tienen definido un modelo de cumplimiento de protección de datos del canal de denuncias conforme a los nuevos requisitos legales. El 18% está trabajando en ello y sólo el 6% está pendiente de la adecuación. Hay que considerar que los encuestados son DPO de entidades medianas y grandes que ya tienen canales de denuncia. Con la futura nueva ley de protección de denunciantes, habrá muchas empresas que implantarán desde cero un canal de denuncia y los correspondientes procedimientos de protección de datos ligados a su utilización.

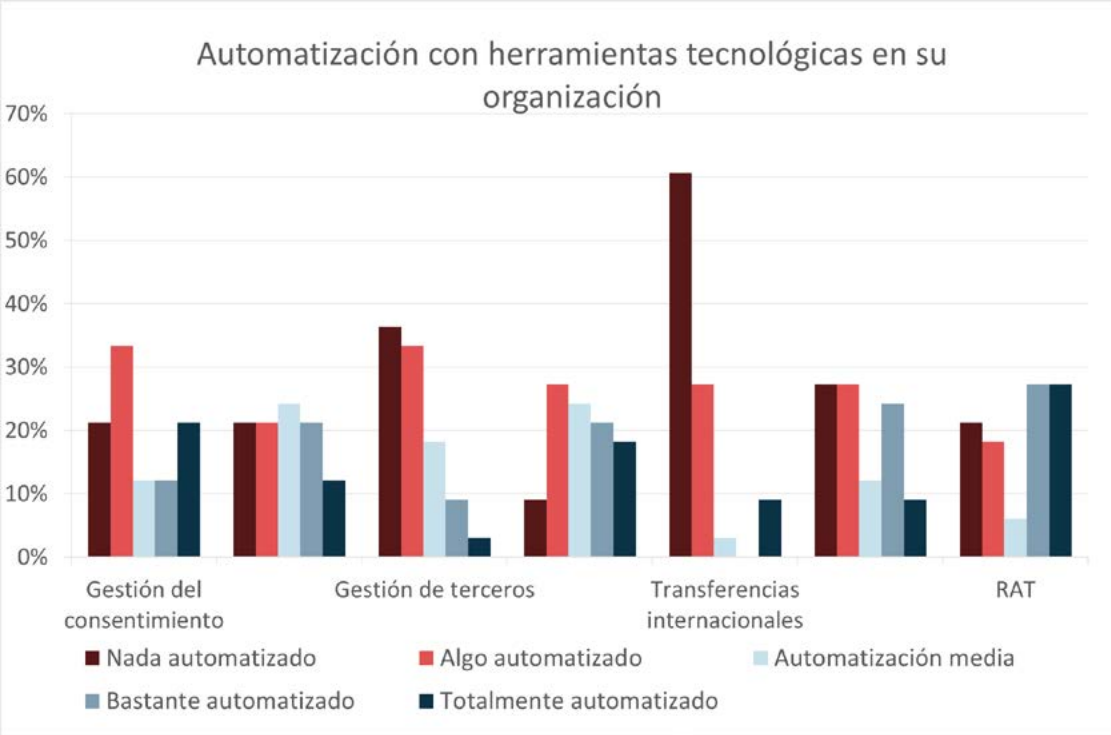

Ilustración 18: Nivel de automatización de herramientas

Si hablamos sobre el uso de herramientas tecnológicas para la gestión de las distintas líneas de acción podemos ver que sigue siendo la elaboración de los PIAs y el RAT, los más automatizados, seguido de la gestión de terceros y la gestión de derechos. Por el contrario, la gestión de las transferencias internacionales continúa siendo la menos automatizada.

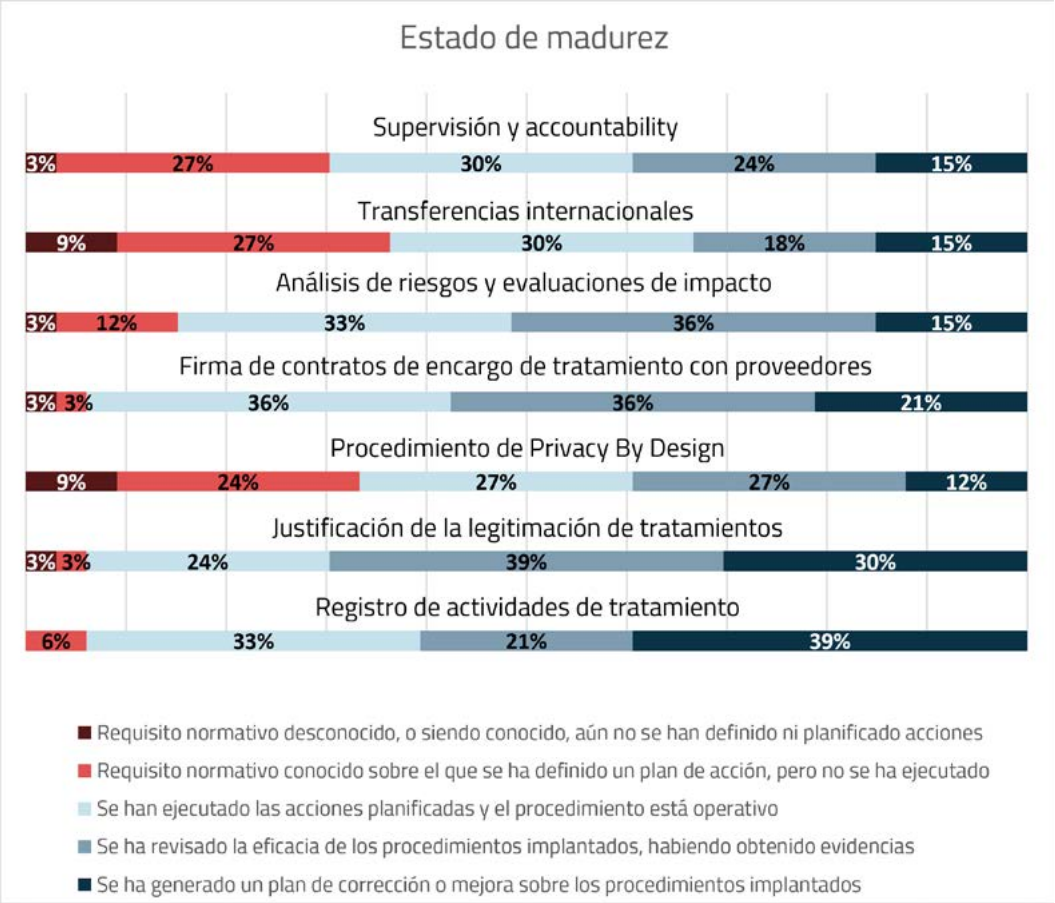

Ilustración 19: Estado de Madurez

En relación con el nivel de madurez de las organizaciones conforme las distintas líneas de acción, el Registro de actividades, la legitimación de tratamientos y los análisis de riesgos y evaluaciones de impacto se encuentran en la fase de plan de corrección y mejoras sobre los procedimientos implantados o en revisión de la eficacia de los procedimientos implantados.

Los procedimientos de Privacy by Design, las transferencias internacionales y la accountability están en fase de definir un plan de acción, pero sin ejecutar todavía.

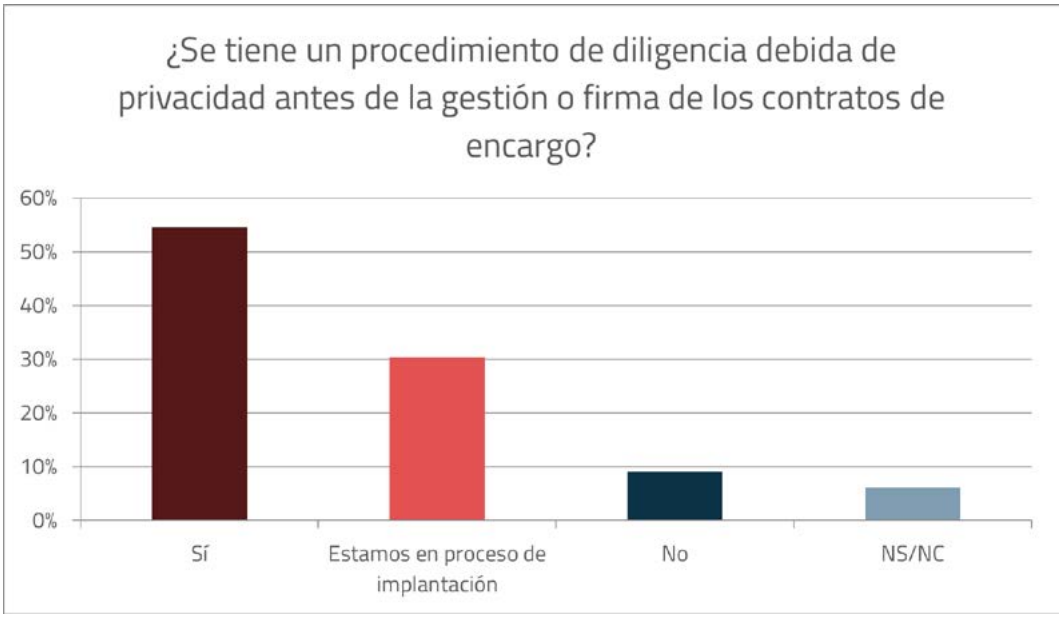

Ilustración 20: Procedimiento de diligencias de privacidad

Ilustración 21: Auditorias

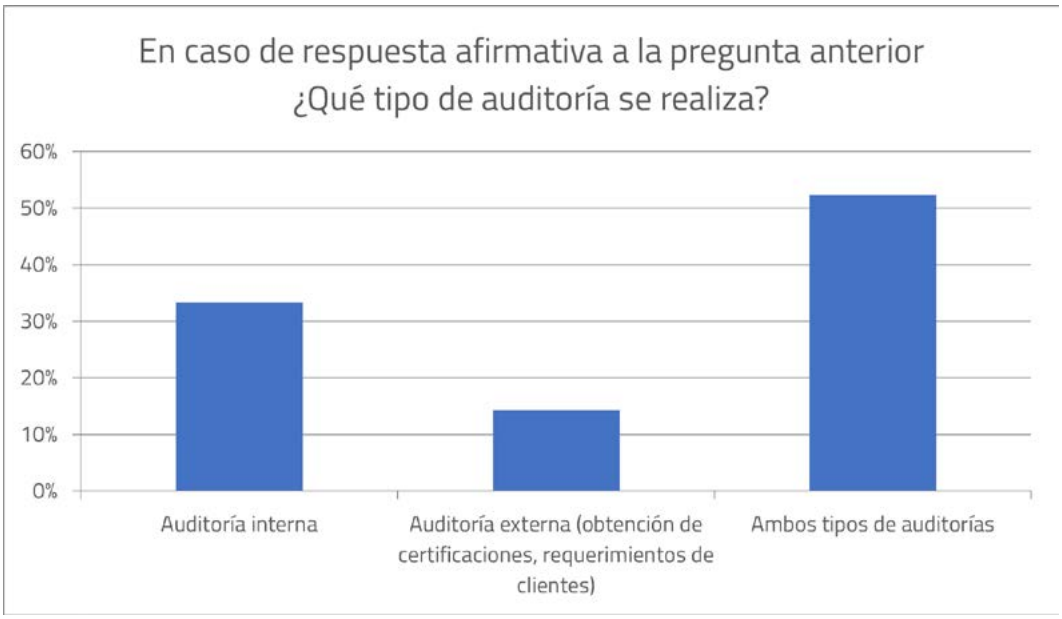

Ilustración 22: Tipos de auditorias

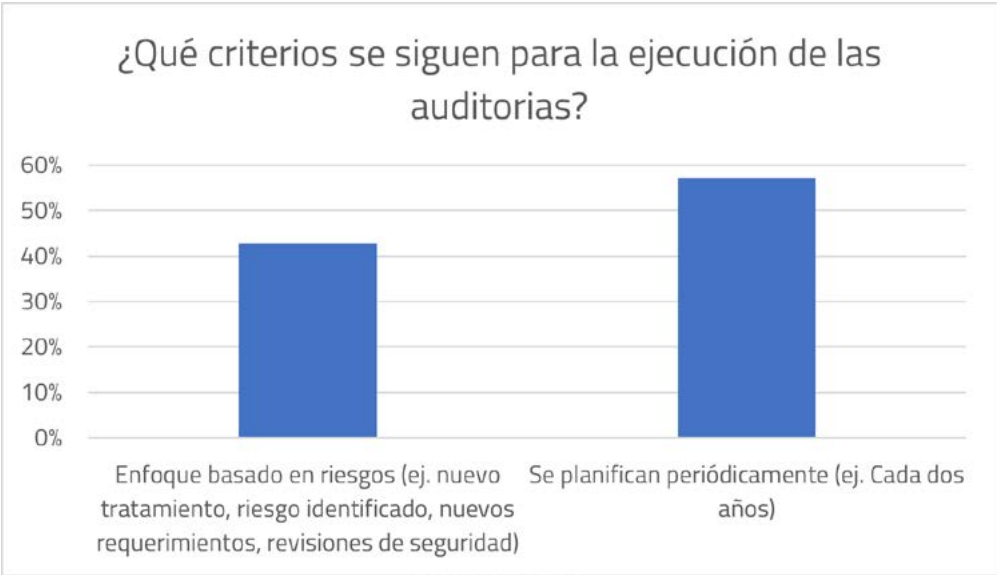

Ilustración 23: Criterios para la ejecución de auditorias

Cuando hemos preguntado sobre el procedimiento de diligencia debida de privacidad antes de la gestión o firma de los contratos de encargo, aproximadamente el 55% de las respuestas declara tenerlo frente a un 30% que ha respondido que está en proceso de implantación.

Registro de indicadores para análisis y benchmarking

Número de tratamientos de datos identificados

La obligación de mantenimiento del registro de actividades se establece a partir de los 250 trabajadores, a estos efectos, podemos identificar que las empresas con mayor número de empleados correlativamente han identificado más tratamientos de datos.

Según los datos obtenidos, los sectores que más registros de tratamientos han realizado son Servicios Financieros, seguido de logística y transporte y otros (energía, educación, juego, entretenimiento, ...).

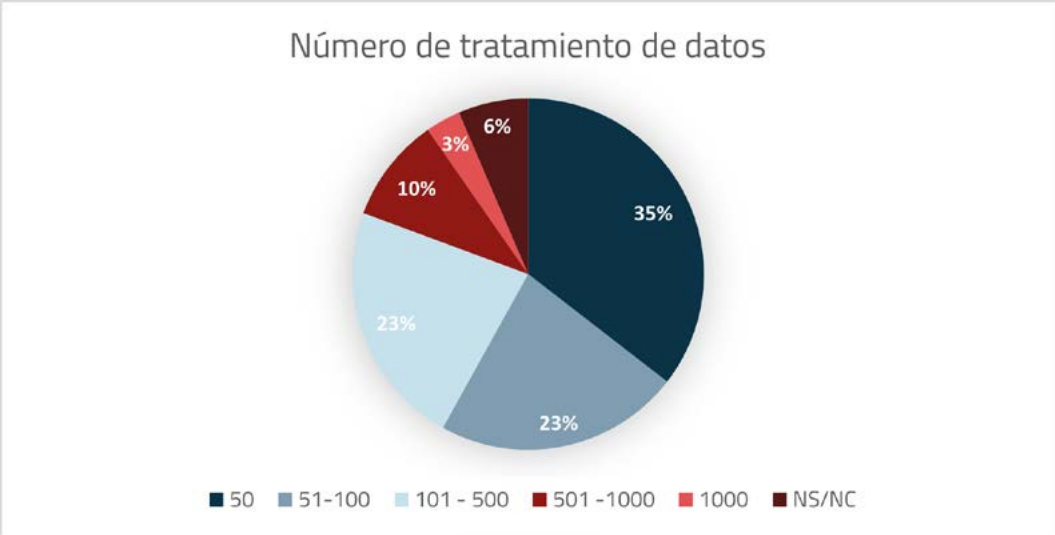

Ilustración 24: Número de tratamiento de datos

La media se sitúa entre los 50 y los 100 tratamientos. La diferencia de número de tratamientos por debajo y por encima de la media es destacable.

Número de PIAs realizados

Las Evaluaciones de impacto nos permiten conocer los riesgos que para los derechos y libertades de las personas físicas pueden tener las operaciones de tratamiento que entrañen un alto riesgo.

Según los datos obtenidos, al igual que respecto al número de tratamientos los sectores que más Evaluaciones de Impacto han realizado son por Servicios Financieros, seguido de logística y transporte y otros (energía, educación, juego, entretenimiento…).

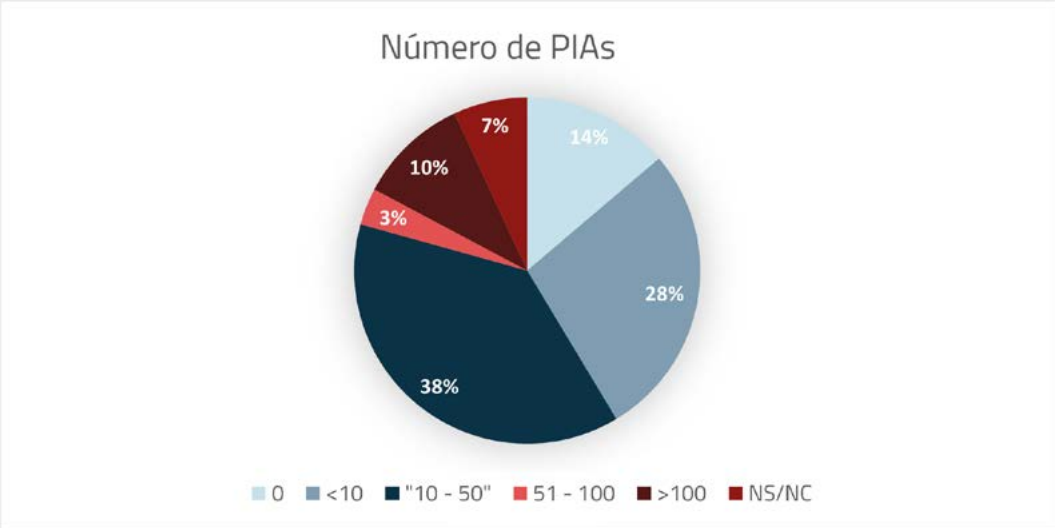

Ilustración 25: Número de Pías

El 14% de responsables de tratamiento no ha realizado ninguna Evaluación de Impacto, el 28% ha realizado hasta 10 PIA, el 38% entre 10 a 50 PIA, el 3% entre 51 a 100 y el 10% más de 100 PIA. Los datos son similares al año anterior.

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

La Disposición transitoria quinta de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establecía que los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo del artículo 12 de la LOPD 15/1999, mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Un 35% de los encuestados ha actualizado más del 80 % de sus contratos con ET durante este año, lo cual significa un cumplimiento importante de este aspecto.

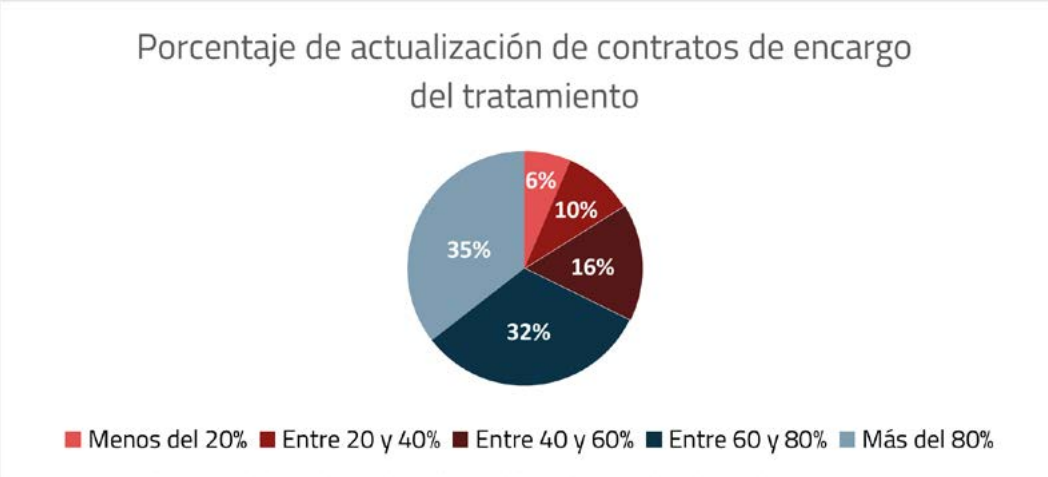

Ilustración 26: Contratos de encargado de Tratamiento

Número de violaciones de datos comunicadas a la AEPD

Cuando se produce una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, salvo que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la brecha debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella. Se requiere así, de un proceso maduro que permita en el tiempo adecuado facilitar la información necesaria, que, entre otras, debe incluir: la naturaleza de la violación, las categorías de datos e interesados afectados, junto con las medidas adoptadas.

De todos los sectores encuestados, Industria, Construcción e Infraestructuras, Tecnología y Telecomunicaciones y Servicios Financieros indican haber reportado un 63% sobre el porcentaje total de las respuestas ante las violaciones de seguridad de datos a la Agencia Española.

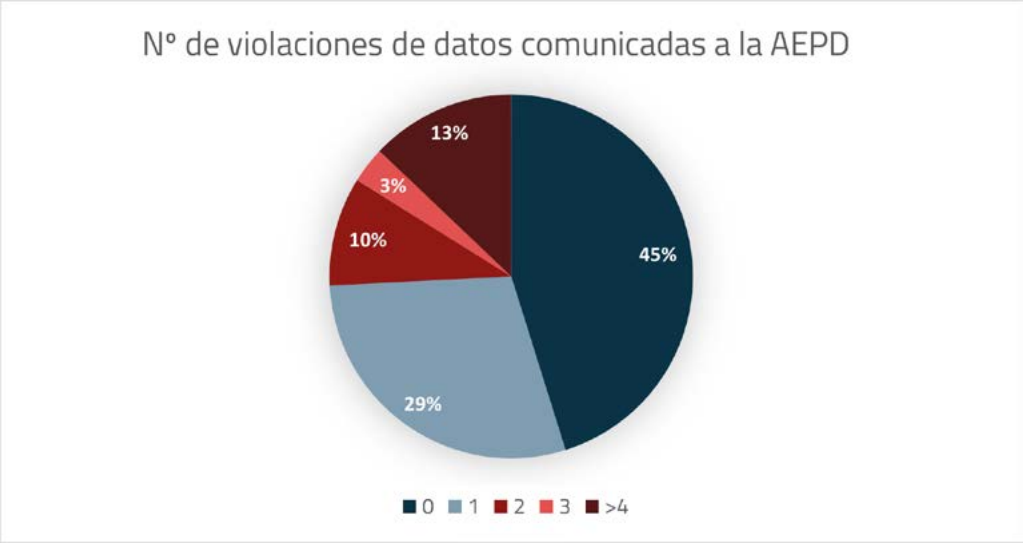

Ilustración 27: Número de violaciones de datos

Número de inspecciones 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.

Servicios Financieros es el sector que más inspecciones de la Autoridad de Control ha tenido entre los encuestados. Revisando los datos de la memoria anual de la AEPD, este sector también se encuentra dentro del top 6 de sectores según importe global de multas, y junto con Telecomunicaciones, han sido los sectores que han recibido las multas más cuantiosas.

El 84% de los responsables de tratamiento señalan que no ha tenido ningún tipo de inspección por parte de la Autoridad de Control.

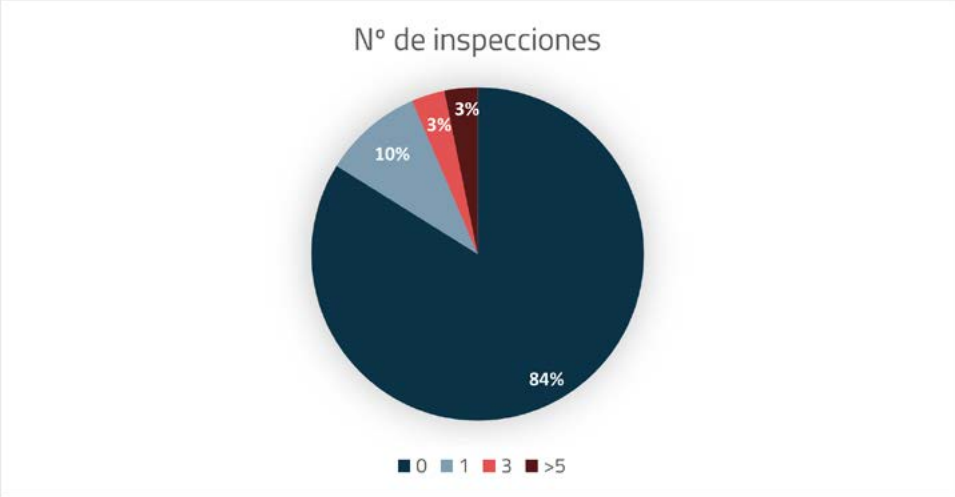

Ilustración 28: Número de inspecciones

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

@ISMSForum
ISMS Forum

Una iniciativa de

isms forum

dpi DATA PRIVACY INSTITUTE