Pridatect

Estudio europeo sobre protección de datos en el sector salud, 2020.

Contenidos

01. Escenario actual

Dentro del **sector de la salud** se trabaja con **datos personales de clientes o pacientes que deben estar especialmente protegidos,** puesto que un tratamiento inadecuado puede suponer que se ponga en riesgo la intimidad de las personas.

Precisamente, desde la entrada en vigor del **RGPD,** se ha puesto de manifiesto la obligación de asegurar a las personas el derecho a saber cómo van a ser tratados sus datos, qué información se recoge, y de igual manera, también se ha regulado la forma en la que una empresa debe tratar dichos datos. Hay que tener en cuenta que el RGPD impone una obligación que responsabiliza legalmente a las empresas a garantizar la protección de los datos personales y a establecer un protocolo para procesar, tratar o eliminar cualquier dato personal, con importantes sanciones económicas que castiguen su incumplimiento.

El RGPD afecta a cualquier profesional o centro del sector de la salud y a empresas que traten datos relativos a la salud de las personas. Además, hay que añadir que el RGPD considera como datos especialmente sensibles aquellos relativos a la salud de las personas, por lo que hay que darles un tratamiento especial.

En la actualidad, existen muchas empresas digitales, múltiples servicios y aplicaciones que tratan datos de salud, y que como en cualquier otro caso, están sujetas a la necesidad de proteger todos los datos personales con los que trabajan. Esto unido al incremento de soluciones tecnológicas que se están empleando actualmente para controlar la seguridad desde que se estableció la crisis sanitaria derivada de la pandemia del Covid 19, hace que exista un amplio flujo de datos relativos a la salud que pueden suponer un riesgo en lo referente a protección de datos.

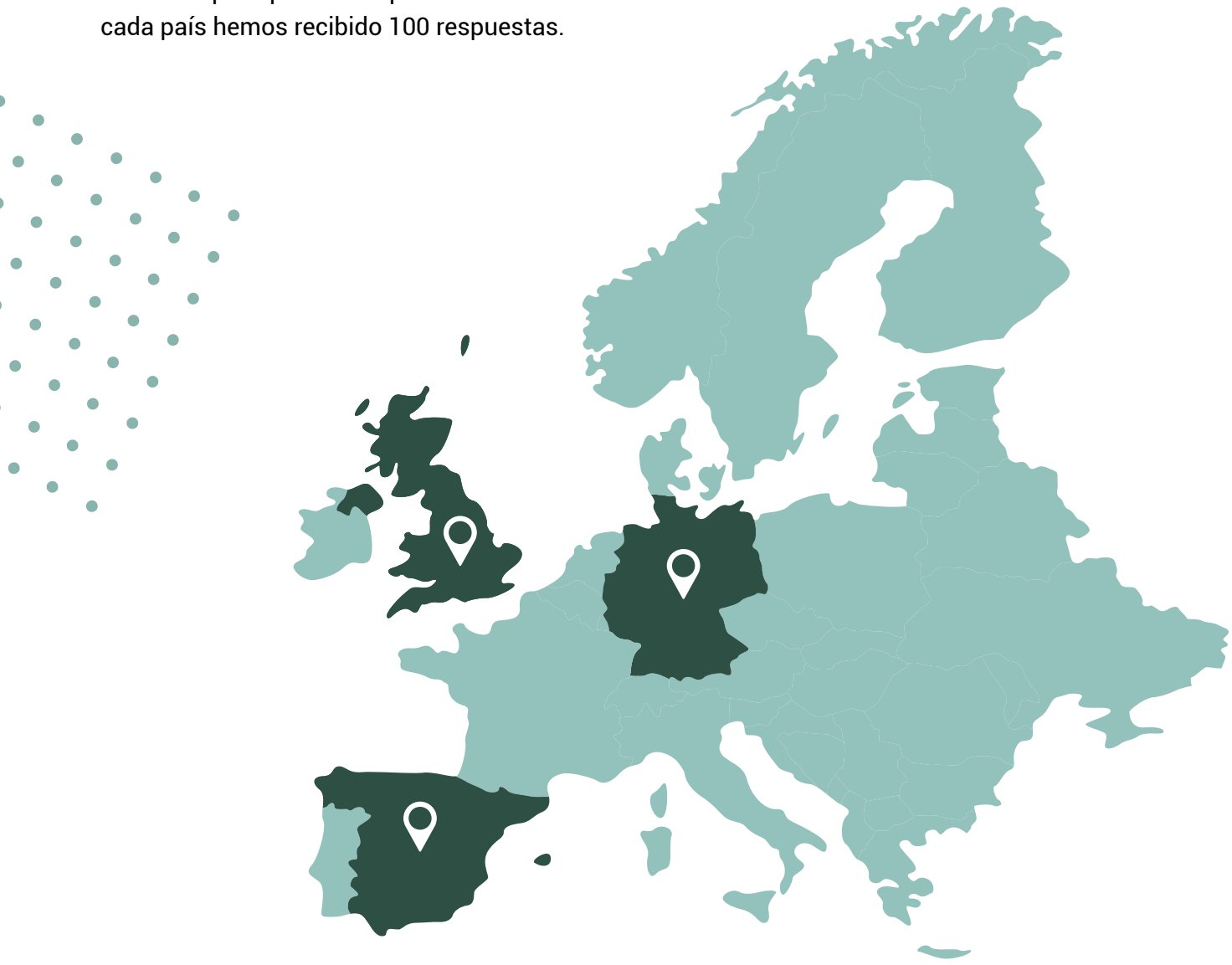
Cumplir con todos los **requerimientos del RGPD** no siempre es una tarea sencilla, sin embargo, cuando están en juego los derechos de las personas y esto puede afectar notablemente a la reputación de una organización, crece la urgencia e importancia de tomarse en serio la protección de los datos.

En este estudio hemos querido analizar hasta qué punto las empresas del ámbito de la salud son conscientes de la importancia de la protección de datos, así como el nivel de conocimiento de las necesidades implicadas o la obligación de establecer las medidas adecuadas.

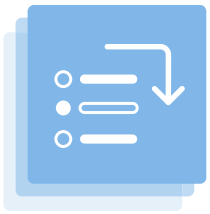
02. Metodología

Con el fin de conocer la situación de cumplimiento actual y proporcionar buenas prácticas para las organizaciones e investigaciones en auge, durante el mes de **Mayo de 2020 hemos encuestado a CEOs y managers de 300 organizaciones del sector salud y farmacéuticas de España, UK y Alemania** para poder completar este estudio. De cada país hemos recibido 100 respuestas.

En este estudio analizaremos particularmente los **resultados obtenidos en España** y, cuando hagamos referencia a ello, a los **datos a nivel Europeo.**



03. ¿Qué hacen las organizaciones del sector salud respecto a la protección de datos?



A. Percepción de cumplimiento del RGPD:

Analizamos el nivel de importancia que las empresas y centros del ámbito de la salud le dan a la protección de datos.

B. Recogida y tratamiento de datos personales:

Estudiamos el nivel de cumplimiento del RGPD a la hora de informar a pacientes y clientes o de establecer los acuerdos de consentimiento y confidencialidad necesarios al compartir datos.

C. Políticas y medidas de seguridad implementadas en organizaciones:

Averiguamos si se están tomando las pautas y protocolos recomendados para llevar un proceso que asegure la protección de los datos personales y de salud con los que se trabajan.

A. Percepción de cumplimiento del RGPD

Pregunta 1

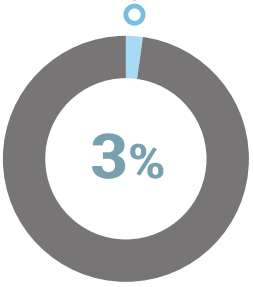
En una escala de 1 a 5, ¿hasta qué punto es importante la protección de datos en tu organización?

Con el avance de la digitalización y la creación de redes en el cuidado de la salud, los médicos, hospitales, compañías farmacéuticas y muchos otros proveedores de servicios vinculados a la salud, **están cada vez más obligados a lidiar con los problemas de protección y seguridad de datos**. El RGPD clasifica los datos de salud en la categoría de datos particularmente sensibles, y esto hace inevitable que requieran una protección especial.

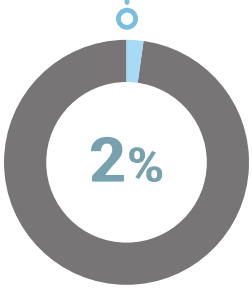
¿Son las organizaciones conscientes de ello?

Los resultados de nuestra encuesta muestran claramente que, aunque el 3% de las organizaciones no conceden importancia a la protección de datos, un 77% de las organizaciones del sector de la salud consideran que la protección de datos es “muy importante”.

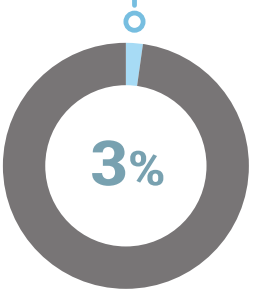
No es importante



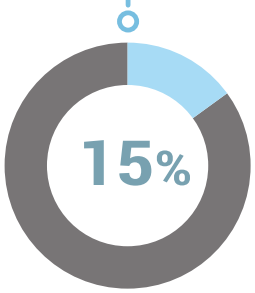
Poco importante



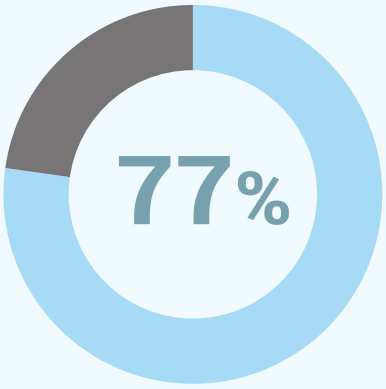
Indiferente



Importante

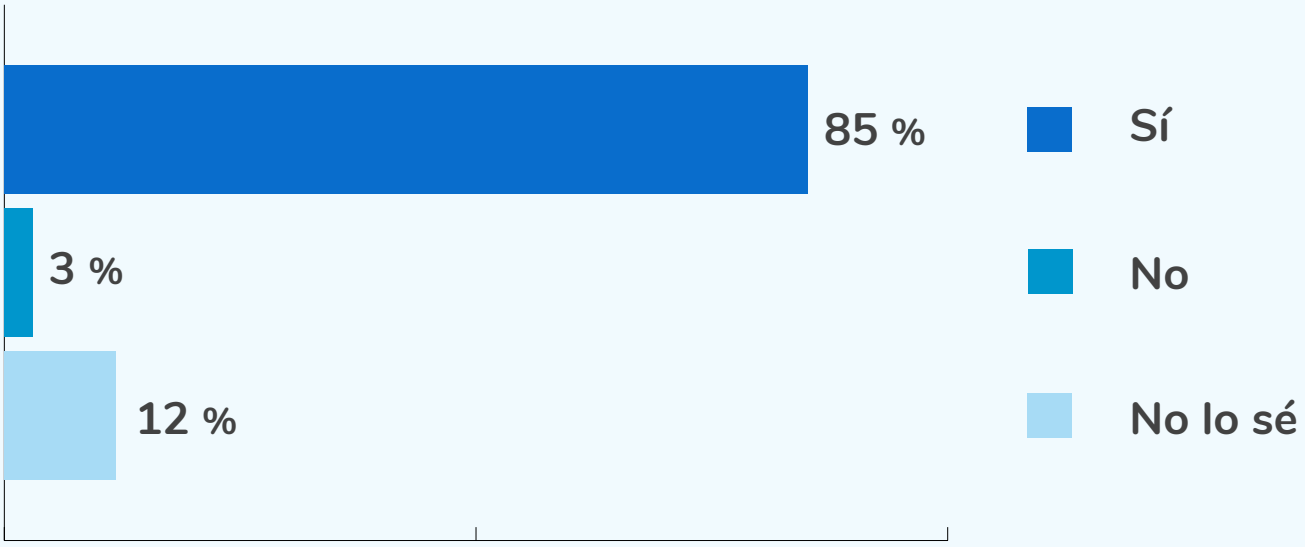


Muy importante



Pregunta 2

¿Tu organización reúne los requerimientos para cumplir con el RGPD?



Cumplir con el RGPD es sinónimo a ofrecer la mayor garantía en cuanto a protección de datos para los clientes, usuarios de un servicio o pacientes, sumado a la tranquilidad para la empresa y para los profesionales que tratan esos datos, de saber que no van a poner en riesgo los datos de ningún paciente, que han tomado las medidas adecuadas para saber actuar en el caso de sufrir alguna pérdida y de tener un protocolo de actuación para cada situación que pueda darse, aparte de salvaguardarse en cuanto a lo que sanciones por incumplimiento se refiere.

Hay que dar una serie de **pasos para garantizar el cumplimiento,** que pasan por contar con un DPO si fuese necesario, realizar evaluaciones de riesgos, evaluaciones de impacto, identificar posibles brechas de seguridad y tener tanto medidas preventivas como un protocolo para gestionarlas. Pasando al ámbito digital, si se cuenta con una web o con servicios que se ofrezcan a través de apps, información que se haga llegar a través de email, etc., habría que cumplir también con todos los requisitos en cuanto a políticas de privacidad, de cookies, etc. Son muchos los requerimientos, pero a su vez, muy importantes para alcanzar el estado óptimo en cuanto a protección de datos.

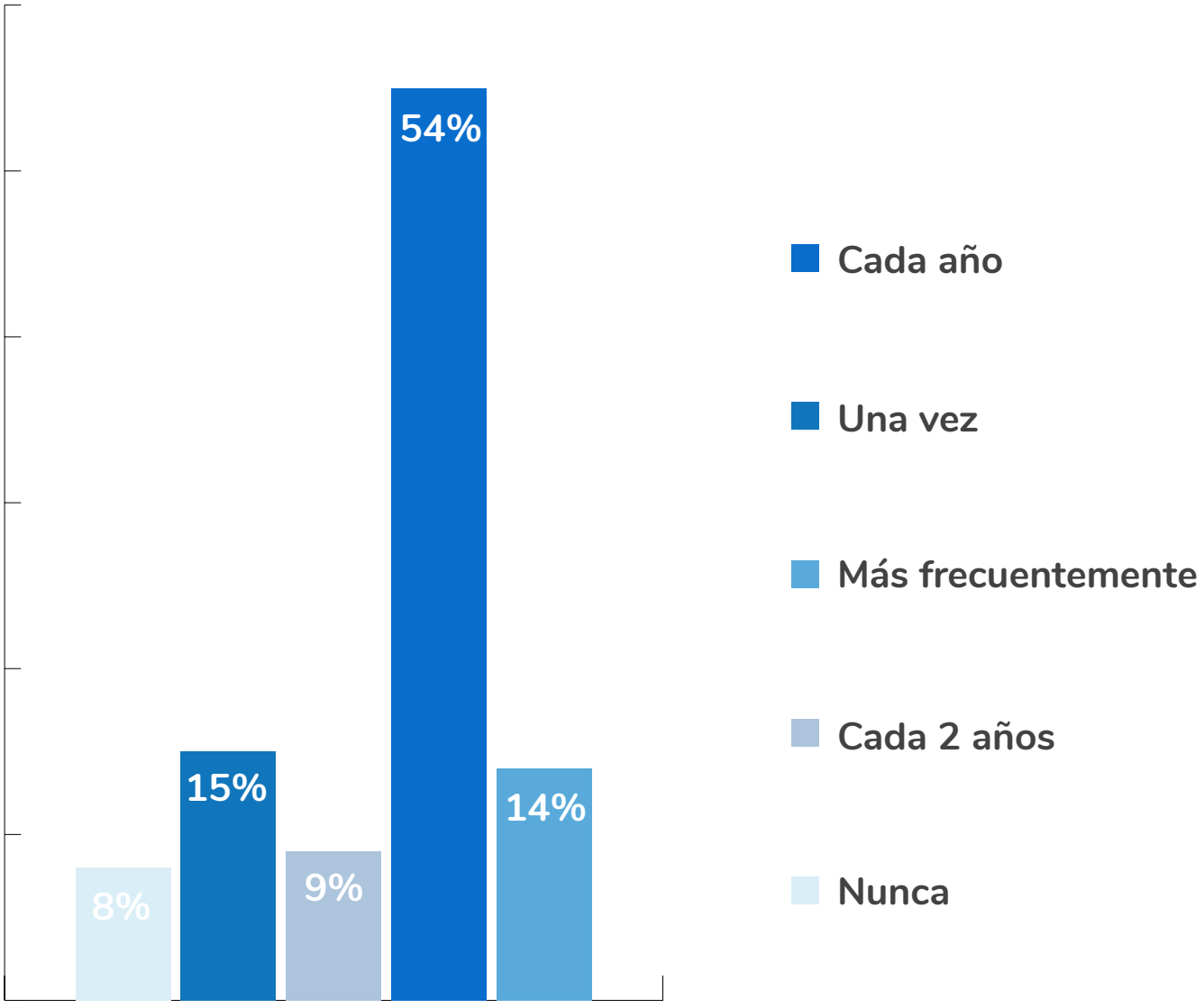
Además, el 12% de los encuestados en los niveles de gestión en el sector de la salud en España no saben con certeza si su organización cumple con los criterios para cumplir con el RGPD. El resultado a nivel europeo de organizaciones que no saben si cumplen o no con el RGPD, sube a un 42%.

Por ese motivo, hemos querido saber si las organizaciones del ámbito de la salud creen que reúnen o no todos los requisitos para cumplir con el RGPD.

Los resultados de nuestra encuesta muestran que un 85% de los encuestados en España sí afirman adaptarse al RGPD. Comparando estos datos con el resto de Europa, las respuestas no difieren mucho, por lo que estamos ante resultados bastante positivos en este aspecto. **Sin embargo,** resulta más alarmante ver que un 3% en España afirma ser consciente de no estar reuniendo todos los requisitos de cumplimiento.

Pregunta 3

¿Con cuánta frecuencia hace tu organización formaciones sobre protección de datos para los empleados?



A pesar de que los **directivos de las empresas** se están dando cuenta gradualmente de la importancia de la protección de datos en una empresa, en la práctica se ve cierto descuido respecto a este tema: generalmente son los empleados los que tienen que trabajar para cumplir con los requisitos de protección de datos en sus actividades diarias.

Aunque el **RGPD** no incluye ningún requisito de capacitación directa para los empleados, el cumplimiento de las obligaciones del RGPD es casi inalcanzable sin ellos. Cuando se procesan datos personales relativos a la salud, cada empleado debe asegurarse de cumplir con la regulación relativa a la protección de estos datos. Para poder cumplir con estas obligaciones, se requiere una capacitación y actualización constante.

El 8% de las organizaciones encuestadas en España no realiza ningún tipo de capacitación en protección de datos para sus empleados, y solamente un 54% lo hace al menos anualmente. Son muchas las empresas que solamente han hecho una capacitación, un 15% de las encuestadas. Un 9% afirman realizar una capacitación cada dos años, y solamente un 14% responden indicando que hacen capacitaciones con más frecuencia.

Hemos podido observar que a **nivel europeo, los datos son muy parecidos,** por lo que en este aspecto, la concienciación es similar. Únicamente es necesario destacar, que el número de empresas que en el resto de países hacen capacitaciones con más frecuencia, es superior, siendo el total de un 15%. Ante unas opiniones tan generalizadas, ¿podríamos decir que se está haciendo lo correcto?

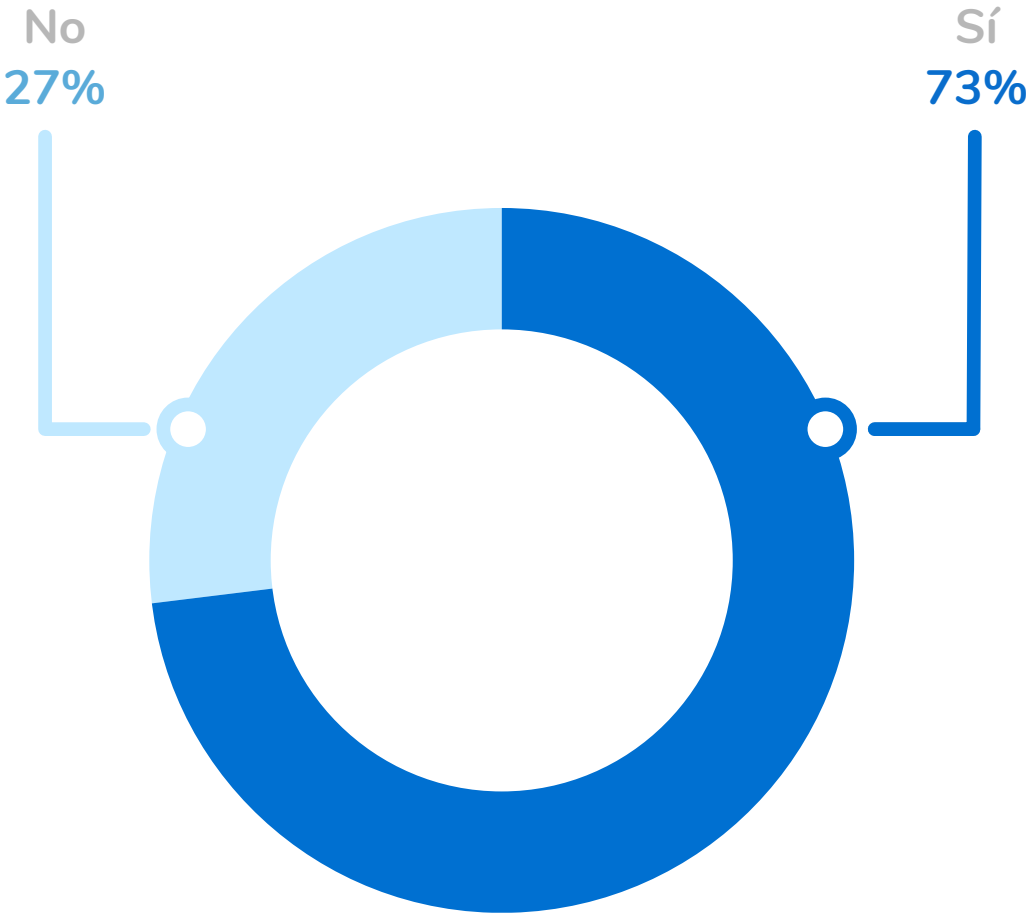
La protección de datos es un tema que evoluciona constantemente. Con el fin de garantizar que se tengan en cuenta los cambios organizativos internos y los cambios legales externos, los expertos en protección de datos recomiendan la capacitación regular de los empleados. La frecuencia depende de factores como la necesidad de procesamiento de datos de la compañía, pero lo que está claro, es que posiblemente una sola capacitación o cursos cada dos años no sea algo suficiente.

> *"Viendo que* **sólamente el 14% de las organizaciones garantiza de forma recurrente la formación para sus empleados en materia de protección de datos,** *es indudable que se necesita más inversión en esta medida organizativa, ya que es considerada la más eficaz para la mitigación de riesgos"*

Eva Estevez | DPO en Pridatect, abogada especialista en protección de datos

Pregunta 4

¿Tus clientes/pacientes preguntan sobre la protección de datos?



Un 73% de los pacientes o clientes del sector sanitario preguntan activamente a las empresas o centros sobre la protección de sus datos, y solamente **un 27% no lo hacen.**

Que más de dos tercios de los encuestados afirmen haberse encontrado esta situación, muestra claramente la importancia de que la persona que está tratando los datos lo haga de la forma correcta y sabiendo que descuidar cualquier detalle de la protección de datos puede **dañar la reputación de la empresa** y al negocio en sí.

Mostrar una información clara y dar las explicaciones necesarias para que las personas sepan qué se va a hacer con sus datos, así como poder demostrar que se están tomando las medidas necesarias para que esos datos no se pierdan, se alteren o se difundan, da una imagen de transparencia que después de la entrada en vigor del RGPD y del aumento de la consciencia de que cada individuo tiene derecho a que sus datos personales estén protegidos, ayuda a que la empresa ofrezca más confianza y daría un paso más para adaptarse a la normativa.

> *"Un 73% de los encuestados afirma que sus pacientes/clientes preguntan por la protección de datos, ello demuestra que* **la población cada vez tiene una mayor cultura de la privacidad;** *lo cual hace que el cumplimiento en materia de protección de datos sea, además de una obligación, una garantía de calidad y confianza para los clientes"*

Andrea González | Legal advisor en Pridatect y especialista en protección de datos

España, es el país en el que más clientes preguntan sobre la protección de datos, pero si nos fijamos de forma general en los datos europeos, un 66% de las respuestas son afirmativas y en menor medida, un 34% de los encuestados, indican que sus clientes no preguntan sobre la protección de sus datos.

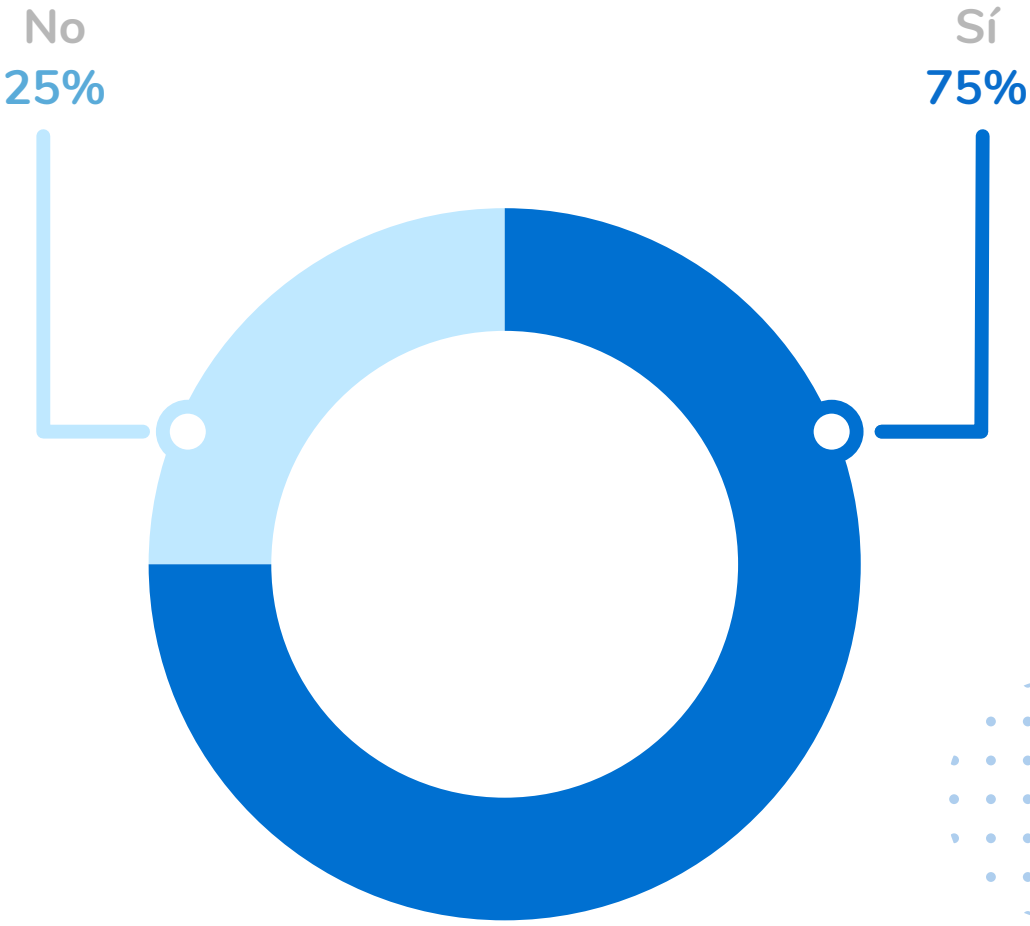
Datos Europeos

No
34%

Sí
66%

Pregunta 5

¿Tus clientes/pacientes se interesan sobre la finalidad de recoger su información personal?



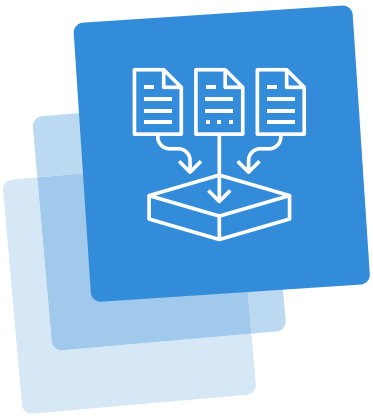
Una de las bases del RGPD es el derecho de un individuo a ser informado sobre el uso y recogida de sus datos personales. Con esta pregunta hemos podido observar que la gran mayoría de los pacientes quiere saber por qué se recogen sus datos, llegando a ser un 75% las organizaciones que afirman que sus clientes sí se interesan sobre el motivo por el que se están pidiendo sus datos, mientras que en un 25% no es algo que hayan preguntado notablemente. Estos datos han sido muy similares en toda Europa.

Al dar sus datos personales, los pacientes quieren saber **por qué se necesitan y qué se hará con toda esta información.** Algo lógico, teniendo en cuenta que se trata de datos bastante sensibles.

Se tiene que contar con una **política de privacidad** y con un **documento de consentimiento**, para que los clientes puedan leer de forma clara y aceptar que sus datos se van a recoger por unos motivos y para una finalidad específica, y así poder dar su consentimiento activamente de una forma libre, específica, informada e inequívoca.

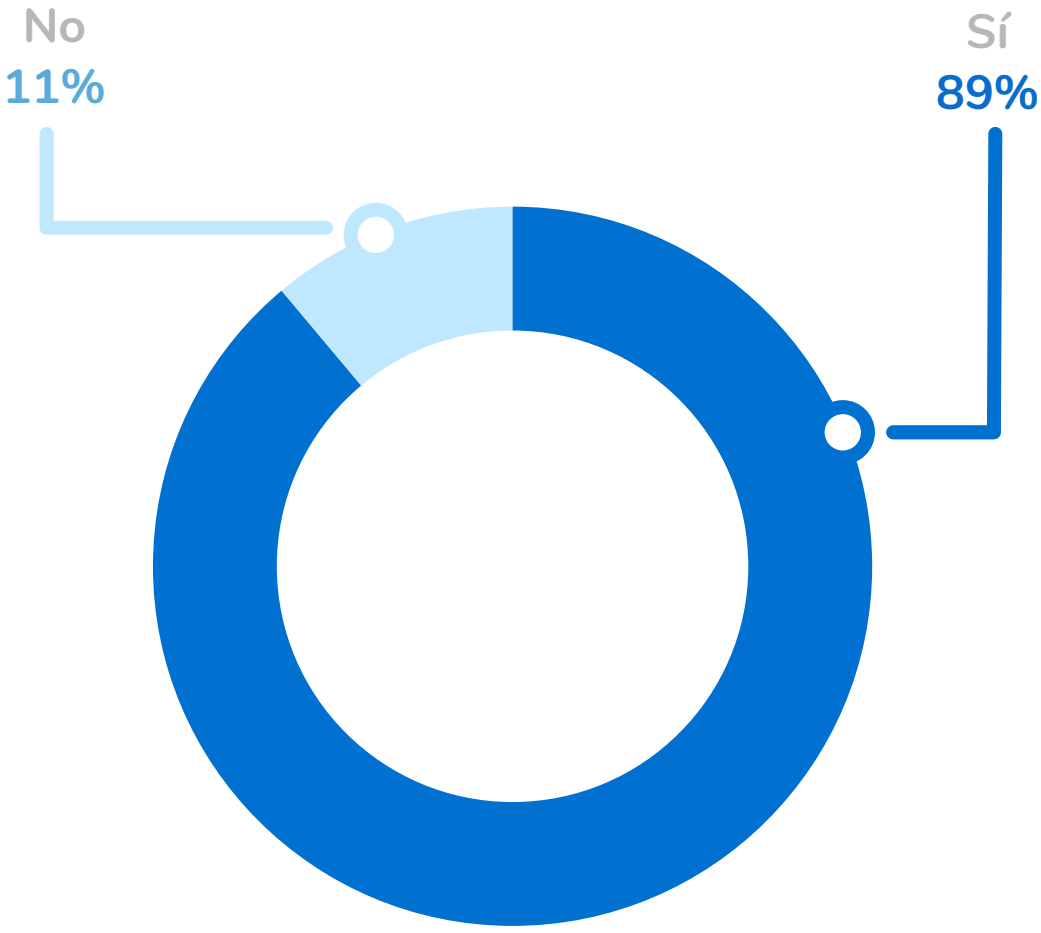
Existen muy pocas circunstancias en las que no sea necesario dar esta información a los clientes o pacientes, por lo que lo más recomendable es, en cualquier situación, dar todas las explicaciones necesarias en el momento de la recogida de datos inicial para que el usuario pueda tomar una decisión a la hora de dar su consentimiento.

Por otra parte, también es comprensible la necesidad por parte de las organizaciones del ámbito sanitario de recopilar datos: les ayuda a proporcionar la mejor atención posible al paciente. Pero a pesar de esta necesidad, no hay que olvidar que es algo que debe comunicarse y explicarse en el momento en que se recopila cualquier dato.



Pregunta 6

¿Tu organización informa a los pacientes/clientes sobre cómo están siendo tratados sus datos personales?



Tal y como hemos podido comprobar con la anterior pregunta, **la mayoría de los pacientes o clientes quiere saber cómo y por qué se tratan sus datos**. Esto, unido a que el RGPD entró en vigor hace más de 2 años, hace que sorprenda ver que, a pesar de que un 89% de los encuestados sí informe a sus clientes, haya un 11% de los encuestados que no informe a los clientes sobre cómo se van a tratar sus datos personales.

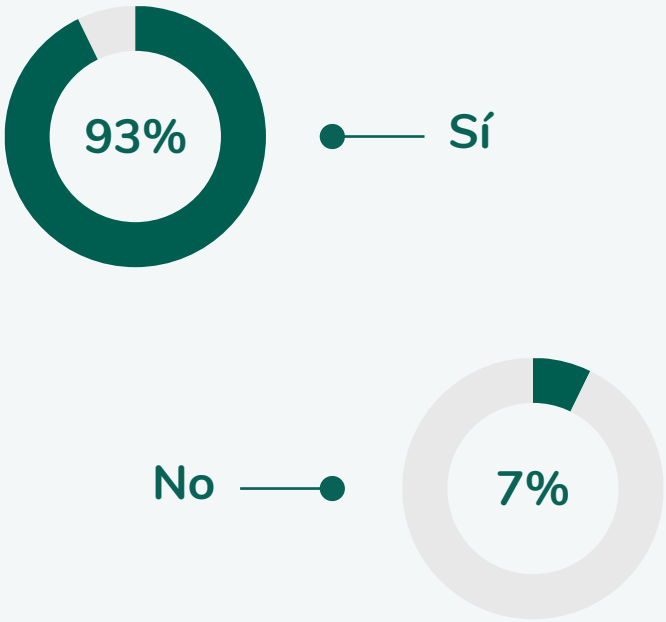
Este requisito básico que no cumplen una parte de los encuestados es preocupante. Informar a los clientes sobre el tratamiento de datos es algo bastante sencillo, mientras que no hacerlo puede conllevar a tener importantes sanciones.
El problema de no informar sería mayor y tendría aún más consecuencias si esos datos se van a compartir con otras empresas o se van a utilizar con otros fines. Esto, indudablemente, es algo de lo que se tiene que informar.

Además de las **multas,** también entra en juego la **confianza** que transmitimos al cliente. La transparencia que se de en cuanto al uso o recogida seguros de los datos es algo claramente positivo para la empresa.

"Las organizaciones están cada vez más concienciadas en el tratamiento de los datos personales de los grupos de interés con los que se relacionan *(clientes, proveedores, trabajadores, etc). Asimismo, el 89% de las organizaciones garantizan el deber de información en el tratamiento de los datos."*

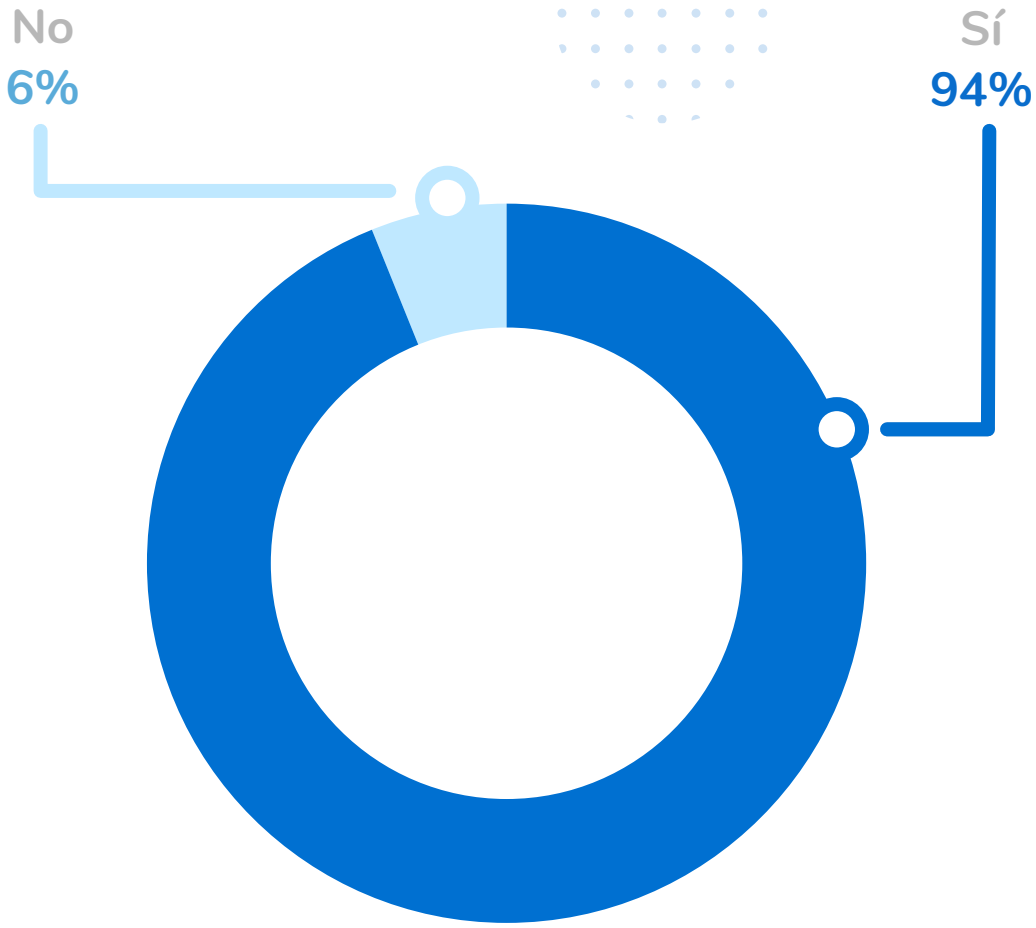
Eva Estevez | DPO en Pridatect, abogada especialista en protección de datos

Los datos en cuanto a respuestas a nivel europeo, indican que un 93% de las organizaciones sí informa a sus clientes y un 7% no lo hace.



Pregunta 7

¿Tu organización recoge el consentimiento (de los clientes/trabajadores/proveedores) para el tratamiento de datos?



¿Qué tipo de datos personales puede recoger una empresa?

Nombre y apellidos, edad, información sobre el domicilio o indicadores de sus necesidades, en función de los servicios que adquieren, entre muchos otros. Si nos vamos a organizaciones vinculadas al ámbito de la salud podemos encontrarnos con datos más sensibles, como resultados de pruebas, historial médico, listado de enfermedades que padecen o medicamentos que toman.

Parece que es casi inevitable tomar o conservar datos personales, algo para lo que se necesita una base de legitimación, que en muchas ocasiones será el consentimiento.

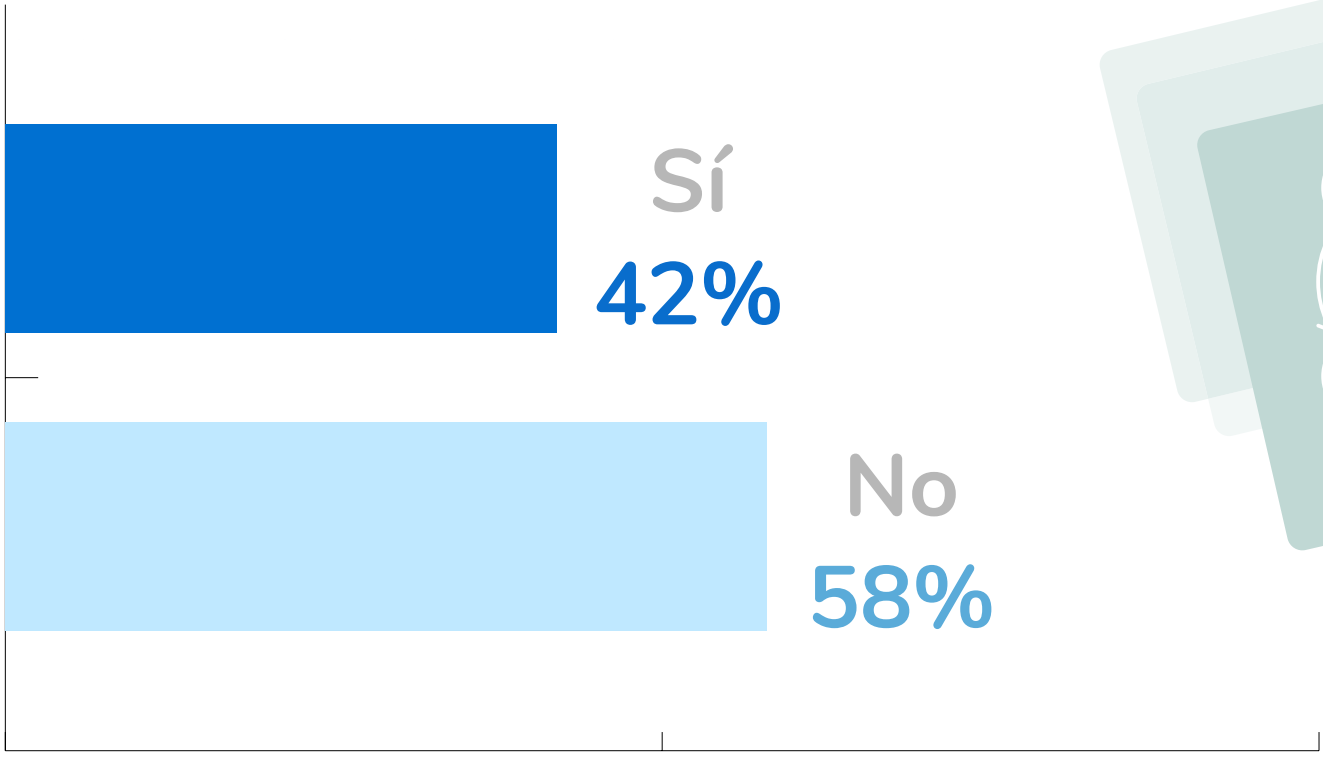
Recoger datos sin permiso puede suponer una de las mayores infracciones del RGPD. La mayor parte de los encuestados en organizaciones sanitarias dentro de España afirman rotundamente que sí piden el consentimiento para tratar datos personales, llegando hasta un 94% y siendo solamente un 6% los que contestan indicando no recoger en ningún momento el consentimiento para tratar datos personales.

Los datos a nivel europeo son similares, un 91% sí recoge el consentimiento, un 9% no lo recoge, incumpliendo de esta manera uno de los pilares básicos del RGPD.

El consentimiento siempre tiene que ser libre, específico, informado e inequívoco. Solamente de esta forma se garantiza que los clientes/pacientes van a saber todo lo que necesitan sobre la finalidad de sus datos y la empresa podrá tratarlos sabiendo que a los interesados previamente han aceptado.

Pregunta 8

¿Tu organización comparte datos personales con terceras partes (Softwares, colaboradores, gestorías, etc.)?



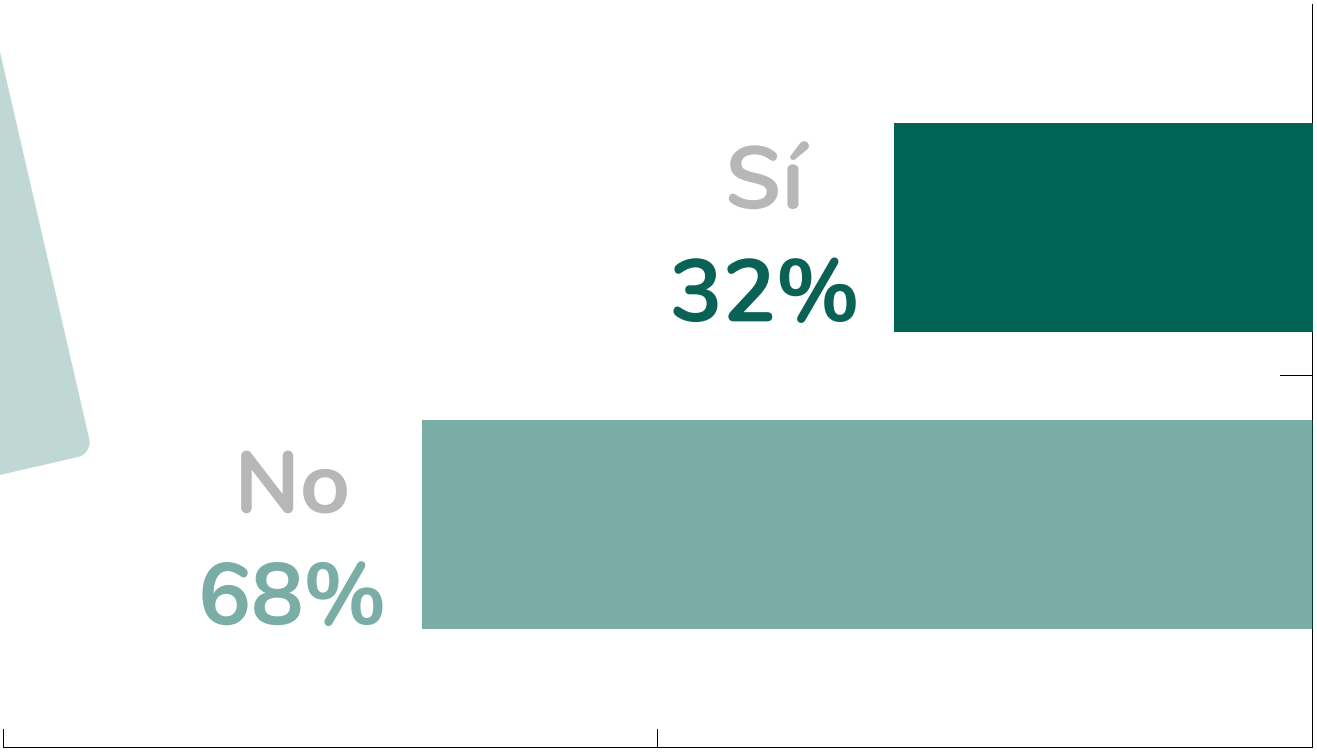
Un 42% de los encuestados dentro de España en este estudio indican que sí, mientras que un 58% asegura no compartir datos con terceros. Esta cifra es mayor que en el resto de organizaciones encuestadas en **Europa, donde solamente en un 32% de los casos, se compartían datos con terceros,** y eso hace ver que en España, sí es muy necesario ser más conscientes de lo que puede suponer a nivel legal y de protección de datos, realizar este tipo de prácticas.

A pesar de que es superior el número de empresas que tratan sus datos únicamente a nivel interno, **el tráfico de datos entre organizaciones es algo más común de lo que pensamos.**

En ocasiones, puede llegarse incluso a acuerdos de cesión de datos, en los que una organización le da a otra las medidas técnicas para el tratamiento de datos. Esto requeriría de forma ineludible contar con un consentimiento específico e inequívoco establecido mediante un contrato legal.

Aunque la cesión de datos no sea una práctica tan habitual, **si puede ser más común, de forma más o menos puntual, recurrir a la ayuda de un tercero para una necesidad concreta.** Por ejemplo, un centro de salud que tiene que enviar las pruebas de un paciente a un laboratorio para analizarlas, o una clínica dental que tiene que enviar datos y medidas de un paciente para la elaboración de materiales odontológicos. Aquí también estamos ante un caso en el que es necesario especificar mediante un contrato las obligaciones de la organización que va a tratar estos datos, y esta necesitaría seleccionar a un encargado de dichos datos. Son supuestos que, aunque no formen parte del día a día en tu organización, es necesario tenerlos en cuenta y tener previsto cómo se establecería legalmente esta relación para evitar un uso inadecuado de los datos o que estos corran algún riesgo.

Datos Europeos

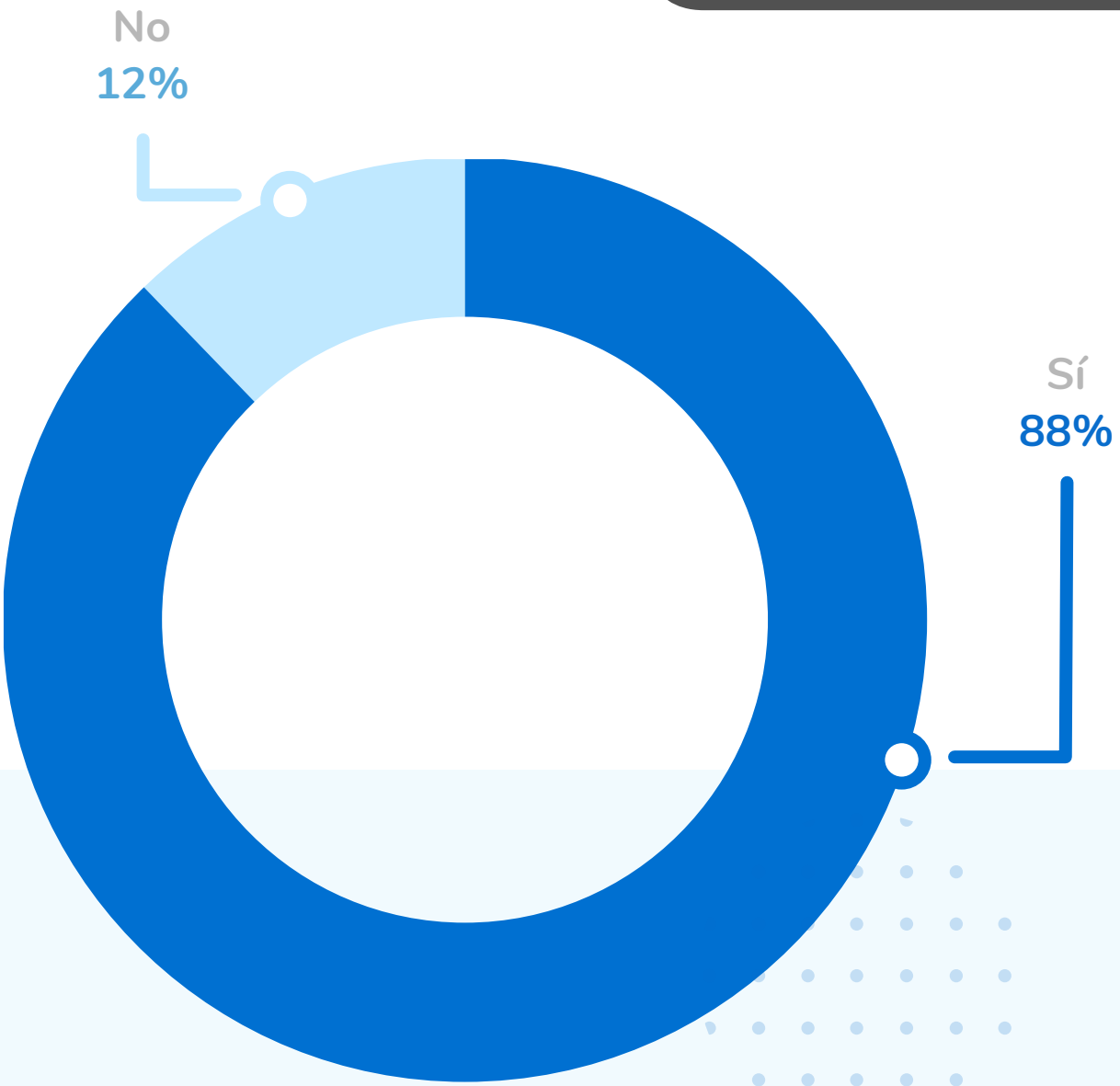


Pregunta 9

¿Tienes un acuerdo de confidencialidad firmado con terceras partes?

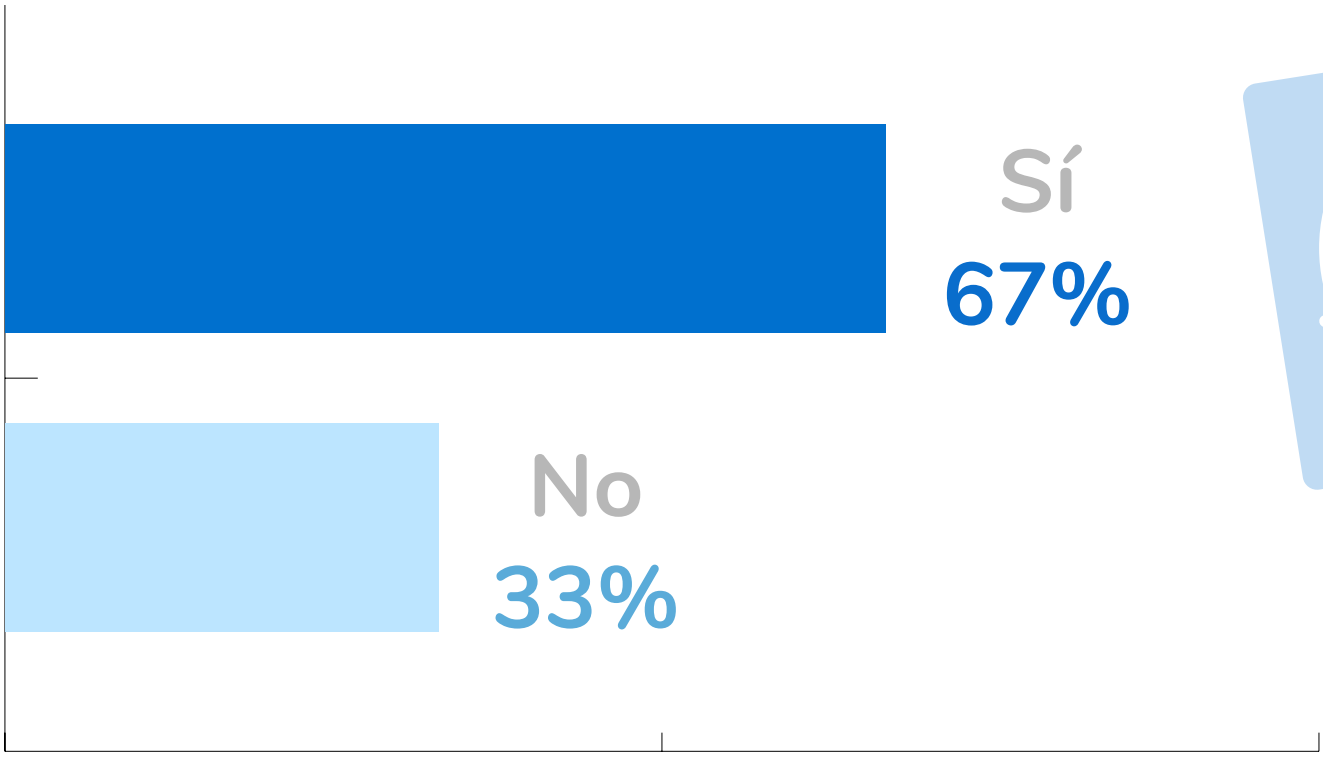
El 88% de las personas que trabajan en organizaciones de salud en España, y que a su vez, trabajan con terceras partes, sí cuentan con un acuerdo de confidencialidad, mientras que un 12% no lo tienen.

Ese tanto por ciento que no lo tiene, se tendría que **concienciar de la importancia de establecer por escrito y teniendo en cuenta los requerimientos legales,** la obligación para la empresa a la que se están prestando datos de respetar la confidencialidad y de no utilizar esa información para fines distintos a los estipulados en el contrato.



Pregunta 10

¿Has incorporado en tu organización alguna solución de software que trata datos de salud en los últimos 12 meses?

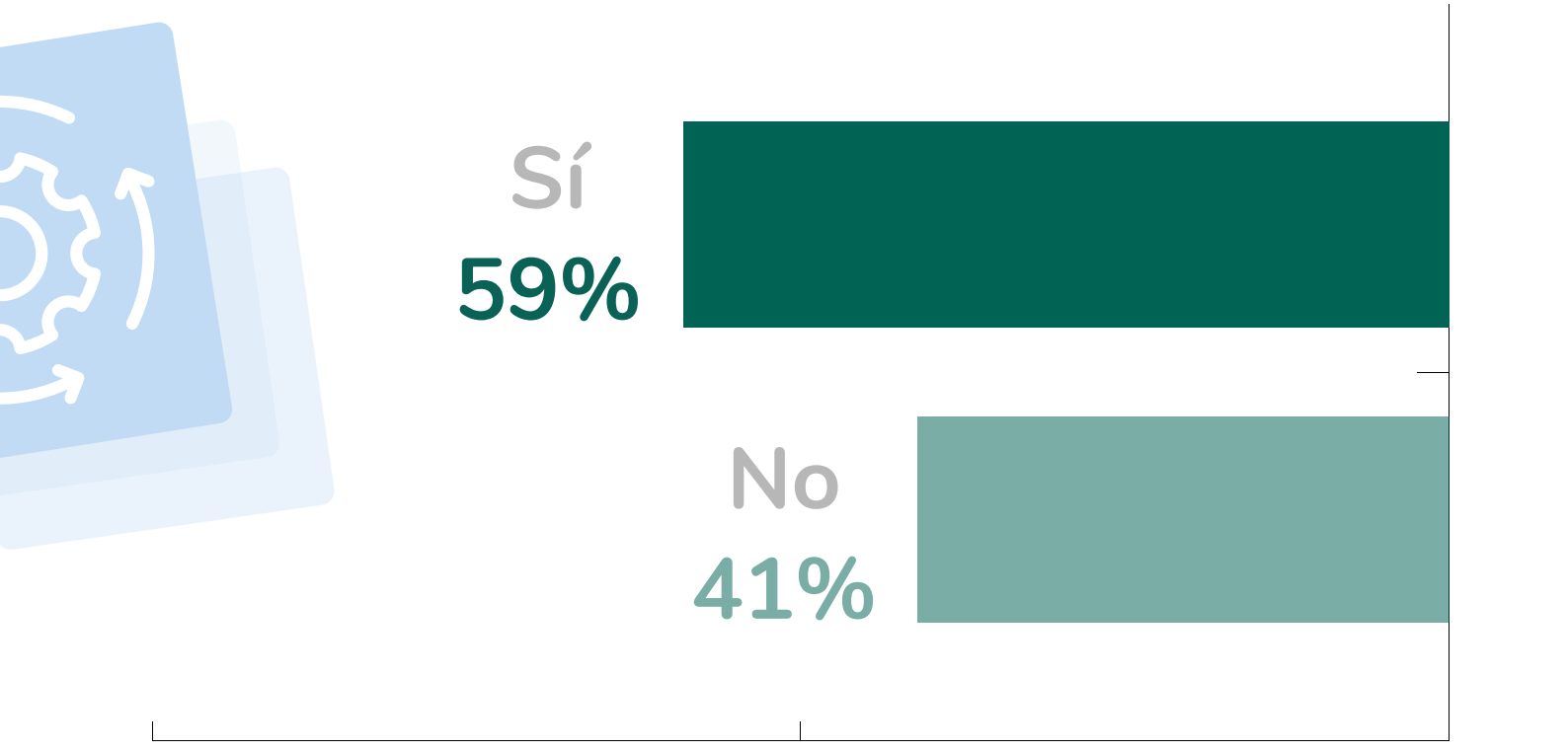


El 67% de las empresas sanitarias encuestadas dentro de España han implementado nuevas soluciones de software que procesan datos de salud en los últimos 12 meses, mientras que un 33% no lo ha hecho.

Dado que el procesamiento de datos de salud está dentro de la categoría de datos particularmente sensibles según el RGPD, siempre **es aconsejable en este caso llevar a cabo una evaluación de impacto de protección de datos antes de utilizar cualquier tipo de solución tecnológica.** Los riesgos asociados con el procesamiento deben determinarse y evaluarse, así como las medidas técnicas y organizativas adecuadas.

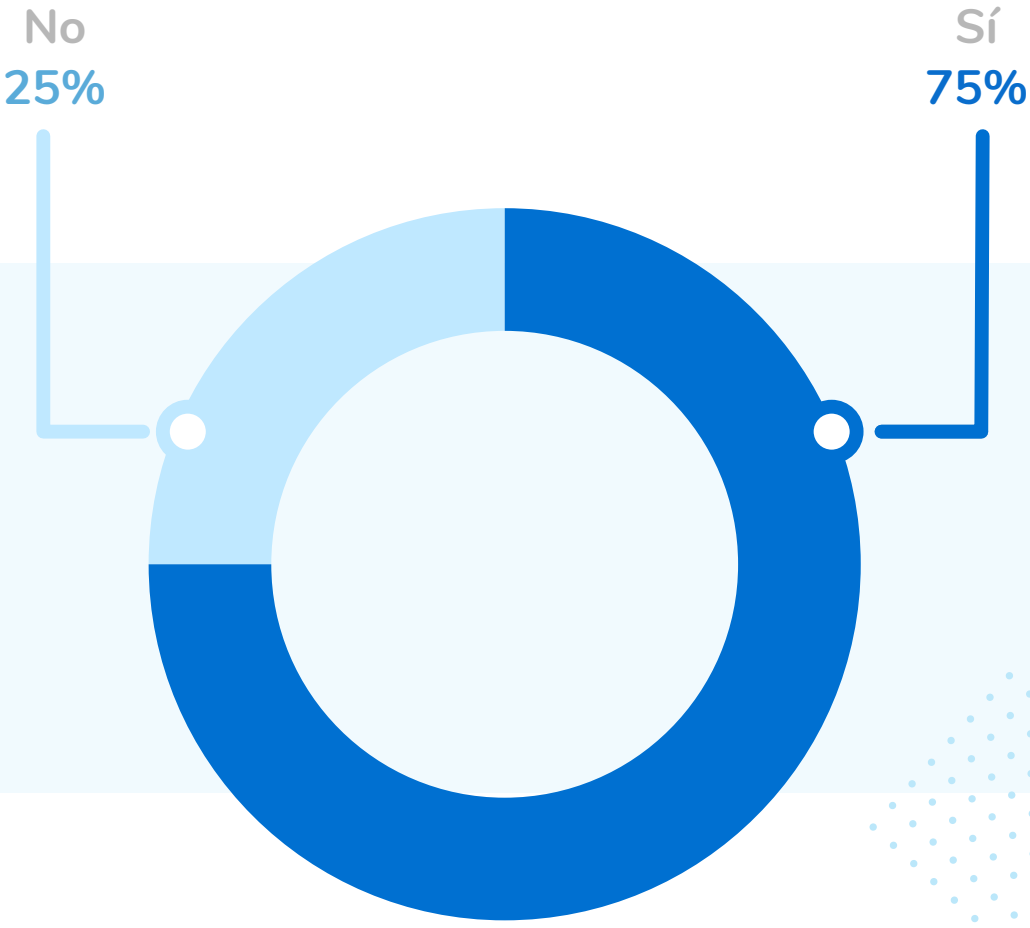
Por su parte, a nivel Europeo, los resultados nos indican que un 59% de las empresas encuestadas sí han introducido software para el tratamiento de datos y un 41% no lo ha hecho.

Datos Europeos



Pregunta 11

¿Tu organización tiene designado un DPO (Delegado de Protección de Datos)?



Un 75% de los encuestados en empresas o centros del ámbito de la salud en España ha contestado que sí cuenta con un DPO, y un 25% no. Hemos obtenido datos muy similares a nivel europeo, siendo un 76% del total los que sí tienen DPO y un 24% no lo tienen.

El los artículos 37 y 39 del RGPD se regula la obligación de contar con un DPO en determinados supuestos o tipos de empresas. Por ejemplos, están obligadas a contar con un DPO aquellas que estén categorizados como centros de salud. También las que traten datos a gran escala o sean instituciones públicas. Esto hace que para muchas empresas del sector salud el DPO sea una figura obligatoria.

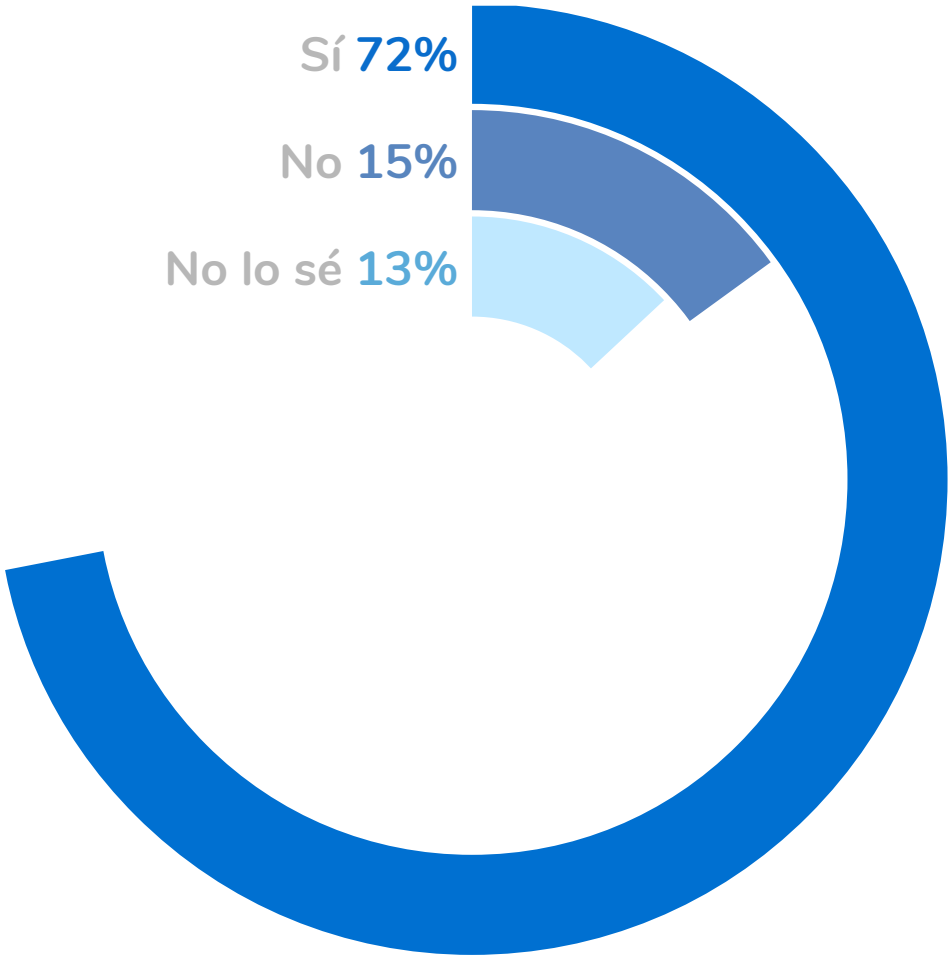
Contar con un DPO es de vital importancia para garantizar el cumplimiento del RGPD, puesto que la persona que asume este rol actúa como responsable e intermediario con la autoridad competente, puede ser muy importante para demostrar que se están tomando las medidas adecuadas.
Cuando hay un problema de seguridad en cuanto a protección de datos, muchas empresas intentan justificarse, por increíble que parezca, indicando que desconocían el riesgo al que se exponían, o salvaguardándose en el hecho de que al ser una empresa "demasiado pequeña" no pensaron que necesitasen este tipo de medidas. Y efectivamente, en estos casos, sería el DPO quien tendría que rendir cuentas.

El RGPD lleva vigente desde hace 2 años y a pesar de esto, un 25% de los encuestados, no cumplen con este criterio de cumplimiento. Por eso motivo, es importante hacer ver a las empresas los beneficios que puede traer contar con una persona que se responsabilice de garantizar que todos los procesos en los que se requieren datos personales se van mantener alineados con las últimas recomendaciones del RGPD, pero también va a ayudar a cualquier empresa a poder demostrar el esfuerzo que se está haciendo por proteger los datos personales y establecer medidas preventivas.

Con esta pregunta vemos que un **25% de las organizaciones encuestadas, puede que esté incumpliendo con la legislación,** a pesar de la clara directriz de que deben tener un DPO. Esto es un obstáculo para lograr el cumplimiento del RGPD, lo que deja a todas estas organizaciones expuestas al ataque de piratas informáticos y de multas por no haber tratado de evitarlo. El motivo es que al no haber designado un DPO, depende prácticamente de la suerte no sufrir un problema de seguridad, mientras que contar con esta figura ayuda a garantizar la protección de datos.

Pregunta 12

¿Tu organización ha realizado una Evaluación de Impacto para identificar y evaluar los riesgos a los que están expuestos los datos con los que trabajas?



Uno de los pasos clave para asegurar la protección de los datos en una empresa es la **Evaluación de Impacto.** Un profesional de la salud, un centro o empresa que trabaje con datos sensibles relativos a la salud de sus pacientes o clientes, tiene que saber cuál es la envergadura de los riesgos que tendría que asumir y del daño que podría ocasionarse si se sufriese un problema de seguridad o si estos datos no fuesen tratados correctamente.

En este estudio hemos querido saber **cuántas empresas del sector de la salud habían realizado una Evaluación de Impacto,** y un 72% han respondido de forma positiva, lo que apunta a que sí se tiene constancia de lo que una Evaluación de Impacto puede suponer a la hora de establecer las medidas necesarias. Sin embargo hay un 15% de encuestados que afirman no haberlo realizado, y un llamativo 13% que responden "no lo sé".

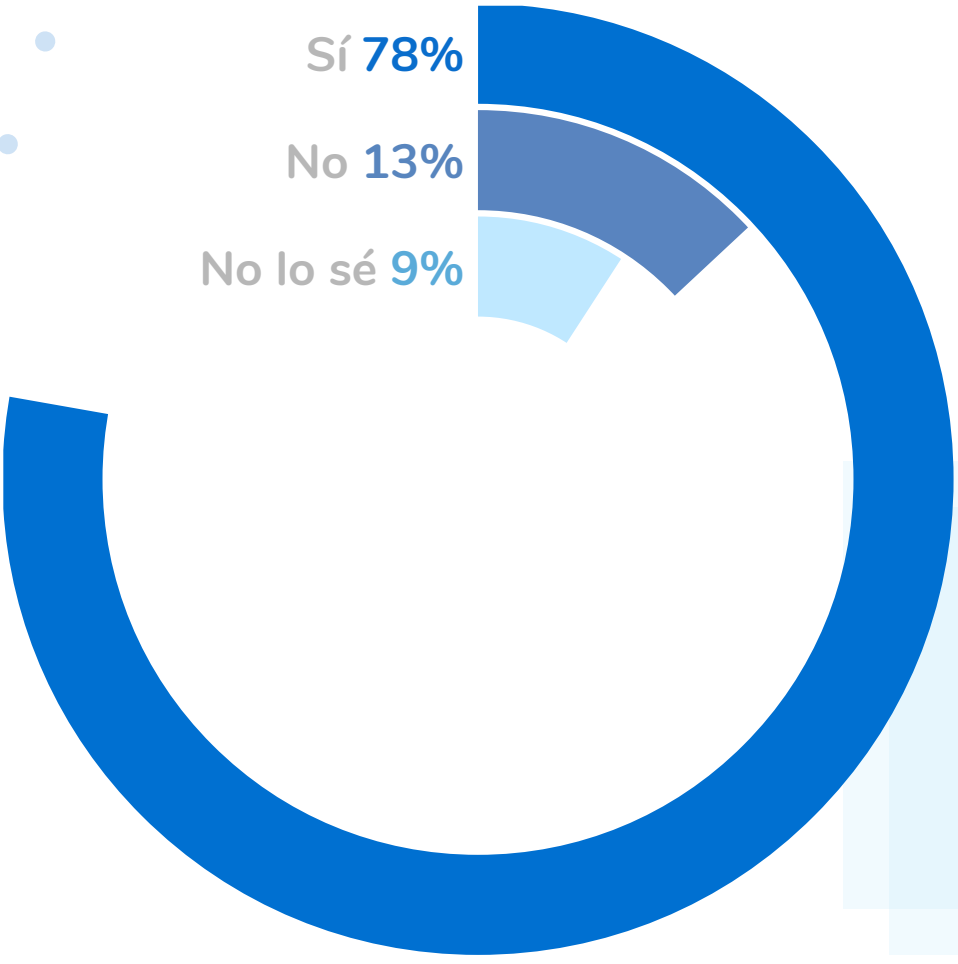
¿Quiere esto decir que desconocen las facilidades que podría traer para la gestión de sus datos? Muchas veces el desconocimiento es lo que da pie a los riesgos.

Conocer las características e impacto de los datos ayuda a **tomar mejores decisiones** para su tratamiento.

Las empresas del sector salud de España son las que más Evaluaciones de Impacto afirman haber realizado. Ese 72% supera al 62% del total de organizaciones europeas a las que se ha consultado.

Pregunta 13

¿Mantienes un registro actualizado de las actividades de tratamiento de datos?



El RGPD establece en el **artículo 30** la importancia de contar con un **registro de actividades de tratamiento**. Esta actividad, debe hacerse de forma continuada, debe actualizarse a medida que se implementen los cambios en el procesamiento.

El registro debe mantenerse actualizado con las siguientes actividades:

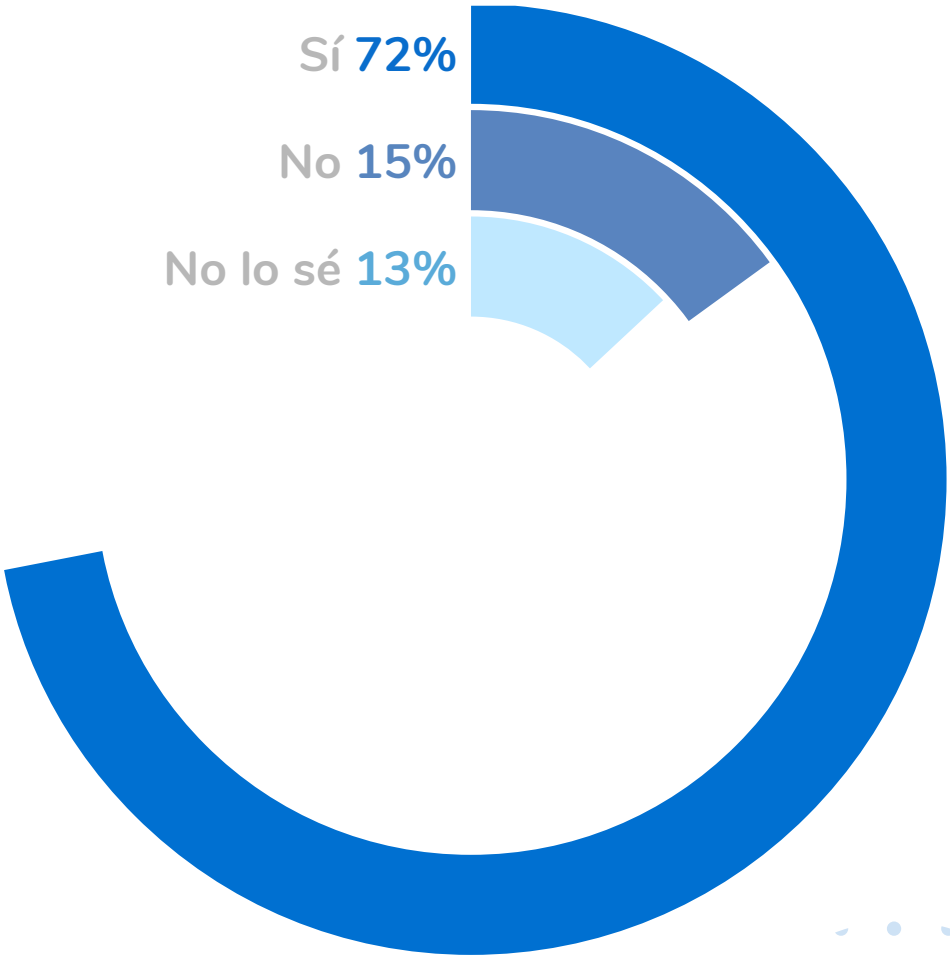
- El **nombre y datos** de contacto de todas las partes involucradas en el procesamiento de datos.
- Descripción de los **fines del tratamiento.**
- Descripción de las **categorías de los interesados y de las categorías de datos personales**, así como de las **categorías de destinatarios** a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países.
- Los **plazos previstos** para la supresión de las diferentes categorías de datos.
- Si es posible, la **descripción general de las medidas técnicas y organizativas de seguridad.**

El incumplimiento de este aspecto del RGPD puede conllevar a multas que pueden llegar hasta los 10 millones de euros o el 4% de los ingresos totales de la compañía.

Aunque un 78% de las organizaciones encuestadas han afirmado realizar un registro de actividades, un 13% ha respondido que no lo hace, y un 9% no lo sabe. Teniendo en cuenta que se trata de algo que debe actualizarse continuamente, **podemos pensar que si no son conscientes de si se hace o no, es porque no lo hacen o no lo llevan al día.**

Pregunta 14

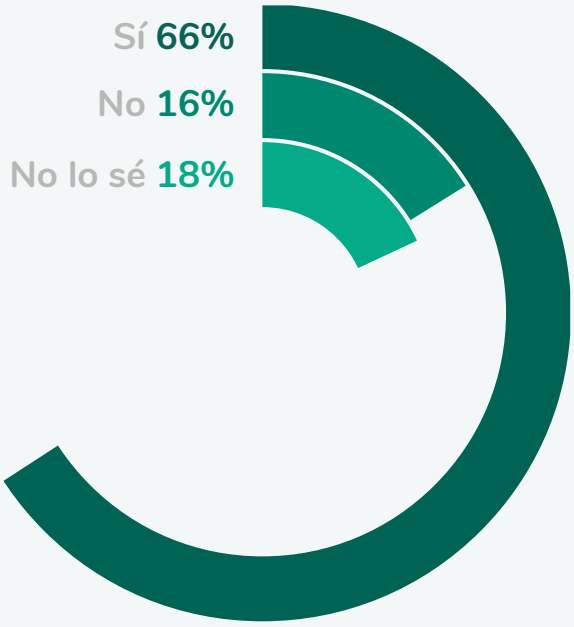
¿Has definido las Medidas Técnicas y Organizativas en tu organización para mitigar los riesgos de cada tratamiento de datos?



Tomar medidas técnicas y organizativas ayuda a garantizar la seguridad de los datos con los que se va a trabajar: se identifican los posibles riesgos y se toman medidas para evitarlos. Un 72% de los encuestados afirman sí tomarlas, pero hemos podido comprobar que un 15% no lo hace y un 13% contesta "no lo sé", dando a entender que desconocen esta práctica o que no son conscientes de si se ha realizado en su centro de trabajo.

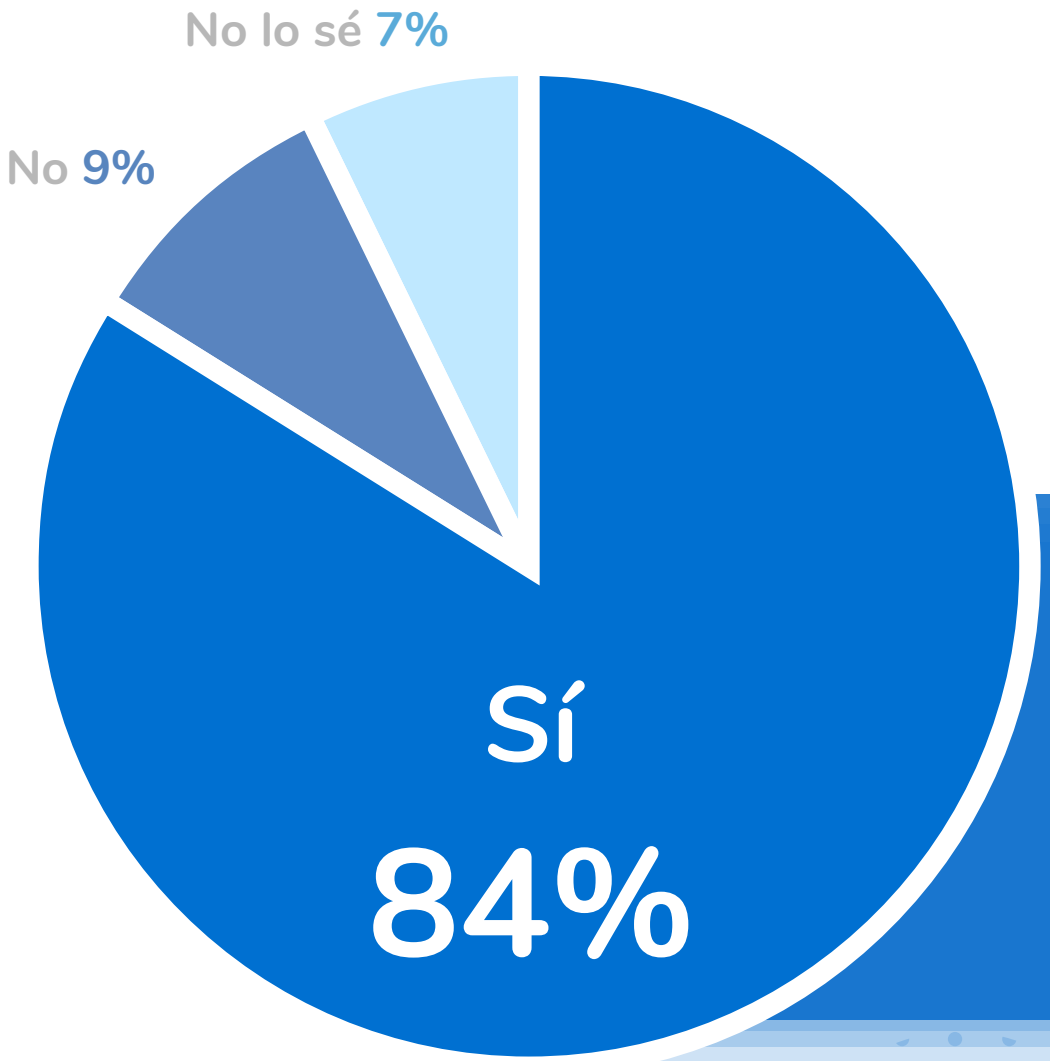
Tomar medidas técnicas y organizativas es algo impuesto en el artículo 32 del RGPD. **Es necesario demostrar que se han tomado las medidas necesarias para no incumplir con el RGPD**, o lo que es lo mismo, asegurar que se ha hecho todo lo posible por no poner en riesgo los datos personales. Eludir esta responsabilidad está sancionado, y por lo que hemos podido ver en este estudio, en muchos centros o empresas aún se está corriendo este riesgo.

El resultado a nivel más general, sumando el total de respuestas a nivel europeo, nos muestran que el 66% sí toma Medidas Técnicas y Organizativas, el 16% no lo hace y el 18% no lo sabe.



Pregunta 15

¿Tu organización tiene un protocolo de actuación en caso de que se de una brecha de seguridad (robo, pérdida, alteración de datos, etc)?



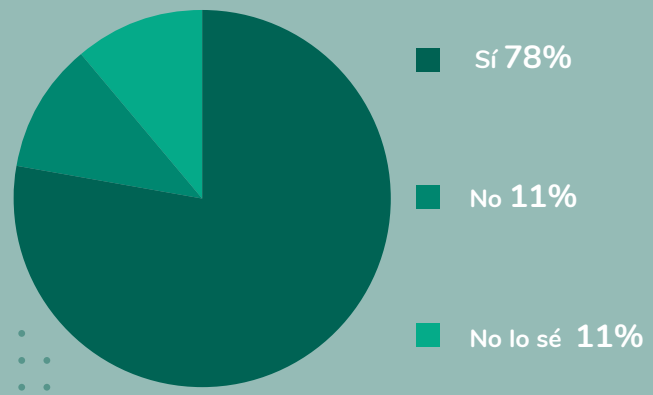
Cualquier empresa del sector de la salud puede sufrir una brecha de seguridad. Desde una pérdida o alteración de los datos de sus pacientes en una base de datos, hasta un acceso no autorizado a los mismos. Esto es algo para lo que cualquier organización debe estar preparada, y por ello es importante contar con un protocolo o plan de actuación, para tener perfectamente definido cómo se va a actuar si esto ocurriese, y para que la solución sea lo más rápida posible, se minimicen los daños y se eviten multas.

El artículo 33 del RGPD establece que cualquier brecha de seguridad debe de comunicarse en un plazo de 72 horas a la autoridad competente, en el caso de España, a la Agencia Española de Protección de Datos (AEPD). En este caso, el reloj comienza a contar desde el momento en el que se sufre el daño, y es importante comenzar a actuar para mitigar los daños lo antes posible.

No tener un plan de actuación hace que se pueda perder un tiempo muy valioso en la fase de descubrimiento inicial. En lugar de poder actuar rápido para reducir o solucionar los daños causados, se dedicaría ese tiempo a averiguar y a decidir qué se debe de hacer.

Precisamente, **un buen plan de respuesta,** incluiría los procedimientos de detección y de información para los implicados ante cualquier problema, y esto juega un papel importante a la hora de reducir los daños.

El 78% de las respuestas a nivel europeo son afirmativas, pero un 11% no lo tiene o no sabe si lo tiene.



A pesar de la efectividad de los planes de actuación ante una brecha de seguridad, en este estudio hemos podido comprobar que frente a un **84% que sí cuenta con este aspecto, el 7% de las organizaciones encuestadas, desconocen si lo tienen o no, y eso nos lleva a pensar que es bastante improbable que lo tengan y, por lo tanto, que posiblemente estén imcumpliento este requerimiento**. Esto sumado a que el 9% de los encuestado ha indicado que no tiene un plan de actuación hace que un 16% de las empresas encuestadas no tengan planes de respuesta ante una violación o pérdida de datos tan sensibles como son los datos relativos a la salud de sus clientes.

04. Psious. Así asegura el cumplimiento de la normativa en cuanto a protección de datos a nivel mundial

Psious es una solución de realidad virtual para profesionales de la salud mental. Ofrece un amplio catálogo de entornos terapéuticos para tratar múltiples trastornos, lo que ofrece a los profesionales de la salud parámetros para ayudar a tratar y a entender a sus pacientes. Estos recursos, **recogen un gran cantidad de datos sobre los clientes y la salud de sus pacientes,** por lo que para ellos, poder asegurar la protección de estos datos es uno de los requisitos fundamentales para poder ofrecer tranquilidad a sus clientes y dar un servicio seguro.

Son conscientes de que al estar en el ámbito de la salud trabajan con datos personales muy sensibles. Cualquier empresa debe cumplir con el RGPD pero la importancia de ello crece cuando se trabaja con datos tan sensibles relativos a la salud. **La pérdida o alteración de estos datos puede entorpecer el trabajo de los profesionales, poner en riesgo la intimidad de los pacientes, hacer que se pierda por completo la reputación de la empresa** y aumenta la posibilidad de exponerse a una importante multa.

Muchos de los clientes de Psious son psicólogos que incluso dejan guardadas las sesiones con sus clientes. Esto hace que para ellos, sea básico poder ofrecer la máxima garantía en cuanto a protección de datos sea una prioridad, tanto para evitar sanciones, como para poder dar la mayor seguridad a las personas con las que trabajan, sin olvidar la responsabilidad que supone no poner en riesgo tantos datos personales de pacientes.

Otro de los desafíos de Psious ha sido cumplir con diferentes regulaciones a nivel internacional en cuanto a protección de datos. La dificultad de adaptarse a la normativa crece cuando se trabaja en varios países, puesto que en cada territorio puede haber diferentes especificaciones y normas. Psious tiene un gran número de clientes en países como Estados Unidos, donde se rigen por una normativa diferente a la Europea, la **HIPAA.** Muchos de sus clientes exigen que se cumpla esta normativa concreta.

Gracias al trabajo realizado con Pridatect *para estar continuamente actualizados y poder adaptarse a nuevas necesidades, hace que puedan pasar todas estas regulaciones y trabajar con terapeutas a nivel global.*

Xavier Palomer | CEO y fundador de Psious

En este punto, **Psious buscó en Pridatect la ayuda para poder ser una empresa HIPAA Compliance para Estados Unidos.** Además de la posibilidad de cumplir con el RGPD, se les ha facilitado la adaptación a cada uno de los requisitos de la HIPAA, pudiendo dar la seguridad necesaria tanto a clientes como a pacientes de Estados Unidos. Todo esto ha permitido que hayan podido trabajar en este país y abrirse un importante nuevo mercado.

Actualmente, **Pridatect también está ayudando a que Psious pueda cumplir con la ISO 27001,** norma que garantiza la confidencialidad e integridad de los datos y de la información con la que se trabaja, así como de los sistemas que procesan estos datos.

05. Conclusiones

Dada la situación sanitaria que se ha vivido a nivel mundial, era de esperar ver un aumento de empresas y soluciones tecnológicas que tratarán directamente con datos de salud, indica David Casellas, CEO de Pridatect. **Lo preocupante es cómo pueden llegar a gestionar esos datos sensibles.** Cada una de esas organizaciones debe comprometerse al 100% con la seguridad de los datos.

El sistema de salud, como se acaba de demostrar, es la pieza clave de nuestra sociedad. **La digitalización también está suponiendo un salto decisivo en la industria de la salud,** pero también la hace más vulnerable.

"Considero que hay consciencia en el sector salud sobre el cumplimiento del RGPD pero en parte hay un desconocimiento de los requisitos que tienen que cumplir. *A la vista está según los resultados de este estudio que, pese a que sólo el 3% de las organizaciones reconoce no cumplir con el RGPD, un 25% no cuenta con un DPO, figura obligatoria en toda organización que trate con este tipo de datos a gran escala según el art 30 del RGPD"*

David Casellas | CEO de Pridatect

"Este sector debe tomar amplias medidas de seguridad para evitar problemas en cuanto a la protección de datos. *Por ejemplo, pese a que el 3% de las organizaciones declara que no cumple con las regulaciones de protección de datos del RGPD, vemos que el 11% no proporciona a los clientes/pacientes suficiente información sobre cómo se tratan sus datos personales, algo que es un requisito obligatorio para según el art. 13 del RGPD"*

Lisa Hofmann | Chief of Legal Operations, Pridatect

Además, el 59% de las organizaciones han declarado que han implementado una nueva solución de software para procesar datos de salud en los últimos 12 meses, pero no todas han llevado a cabo una evaluación de impacto de protección de datos, lo que sin duda sería necesario en la implementación. Solo el 78% indicó que mantienen un inventario actualizado de las actividades de tratamiento. Sin embargo, esta obligación afecta a casi todos los que tratan datos personales. Una autoridad supervisora siempre le pedirá el registro de actividades de tratamiento cuando audite a la organización. Por lo tanto, debería ser un pilar básico dentro marco de protección de datos de cualquier organización.

En base a estos resultados podemos concluir que sí existe conciencia sobre la importancia del RGPD, aunque queda alguna asignatura pendiente:

- Es necesario formar a todos los profesionales con más frecuencia.
- Hay organizaciones en las que los responsables no saben con certeza si se adaptan en todos los aspectos al RGPD o no. Por ese motivo, contar con ayuda profesional para analizar correctamente cada uno de los puntos en los que la protección de datos esté presente, puede ayudar a tener una visión más clara.

Está muy presente la necesidad de informar sobre la recopilación de datos.

- En el 76% de las organizaciones consultadas en España, los pacientes se interesan sobre la finalidad de recoger sus datos, y en muchas ocasiones, existe la necesidad de compartir datos con terceros.
- Para que un paciente pueda dar su consentimiento de forma libre, específica, informada e inequívoca la organización debería informar de su finalidad en el momento de recoger el consentimiento. Un 11% de las empresas, clínicas o centros consultados en España, afirman no informar, estando infringiendo de esta forma el RGPD. Es imprescindible recoger el consentimiento para cualquier transacción de datos y contar con un contrato si estos datos se compartirán con terceros.

Muchas de las organizaciones del ámbito de la salud están avanzando en el camino de adaptarse al RGPD realizando las acciones correctas para poder establecer todo tipo de medidas, pero no es algo que ocurra siempre.

- Un 75% de organizaciones sanitarias en España ya cuentan con un DPO. Hay que tener que cuenta que trabajan constantemente con datos muy sensibles y no están exentas de cambios que pueden hacer que lo que en un momento esté protegido, pueda no estarlo debido a un cambio.
- Es imprescindible realizar una Evaluación de Impacto (el 75% de las organizaciones del ámbito de sanitario, la hacen), y establecer Medidas Técnicas y Organizativas, así como contar con protocolos de actuación para posibles brechas de seguridad (algo con lo que cuentan el 84% de las empresas o centros sanitarios).

Todas las empresas y centros de salud que no están siguiendo estos protocolos y tomando las medidas mencionadas, o que no están seguras de estar haciendo lo correcto, (según este estudio, hasta un 15% de organizaciones del sector salud) están poniendo en riesgo datos sobre la salud de sus clientes y expuestas a sanciones por incumplimiento del RGPD.

Pridatect, plataforma para simplificar el proceso de identificar riesgos y proteger datos

DETECTAR E IDENTIFICAR RIESGOS

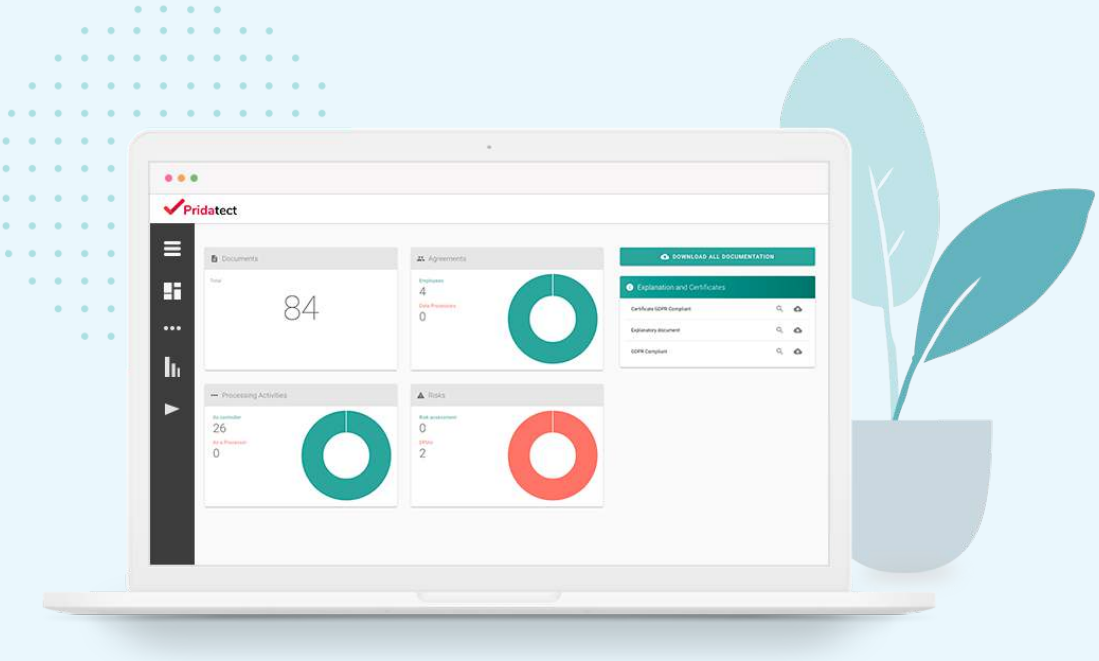
Detecta e identifica los riesgos en tu tratamiento de datos personales (clientes, empleados, proveedores...). Con la plataforma de Pridatect podemos identificar y analizar, las amenazas y vulnerabilidades en tus procesos.

DEFINIR Y SUGERIR MEDIDAS

El conocimiento de los riesgos en tu empresa nos permite definir las medidas necesarias para reducirlos y mitigarlos. Pridatect te ayuda con la definición y sugerencias de medidas para tu empresa.

SUPERVISIÓN E IMPLEMENTACIÓN DEL PROGRAMA

La protección de datos es una tarea constante dentro una empresa. Pridatect no solo ayuda con la implementación inicial, también con la supervisión continua de riesgos, medidas y administración de tareas entre empleados de tu empresa.



Contacta con nosotros para una demo gratuita o utiliza nuestra prueba gratuita durante 7 días