Pridatect

Estudio europeo sobre protección de datos en el sector SaaS, 2022.

CONTENIDO

1. Escenario actual

Gracias a los conocidos como **"software como servicio"**, también llamados **SaaS**, por sus siglas en inglés, miles de usuario pueden conectarse y trabajar con aplicaciones y recursos alojados en la nube. Esto implica que **una gran cantidad de los datos** de los usuarios sean administrados por las empresas proveedoras de SaaS.

Al utilizar un SaaS, el usuario se libera de muchas preocupaciones que pasan a ser responsabilidad del propio SaaS. Si entramos en el terreno de las empresas que **confía-n parte o totalmente su infraestructura e información a un SaaS**, a esa responsabilidad se le añade la necesidad de reducir el miedo que tienen las empresas a perder sus datos al utilizar este tipo de soluciones.

Precisamente, una de las barreras que suelen tener las empresas antes de contratar un SaaS es esa inseguridad o pérdida de con-trol sobre sus datos. ¿Qué implicaciones tienen esto para los proveedor-es? Las empresas que diseñan y suministran un SaaS de- ben **garantizar la seguridad, confidencialidad y disponibilidad de todos los datos** que entran en juego a la hora de utilizar la aplicación. Además, tienen que **comprometerse a realizar una óptima gestión de la protección de datos**, lo que implica cumplir con el **RGPD** y con otras normativas referentes a la **privacidad** y **seguridad de los datos**.

Son muchos los posibles **riesgos y errores de cumplimiento** a los que puede exponerse un SaaS de cara a la **protección de los datos,** que además de afectar a la seguridad y credibilidad del servicio, pueden hacer que la empresa sufra **sanciones económicas**. ¿Algunos ejemplos?. Desde una mala gestión de los controles de acceso, a no tener en cuenta si un menor de edad se puede registrar, pasando por obviar si se van a recopilar datos sensibles que necesiten un tratamiento especial, no preocuparse por recoger correctamente el consentimiento para el tratamiento de datos o no poder asegurar la recuperación de los mismos.

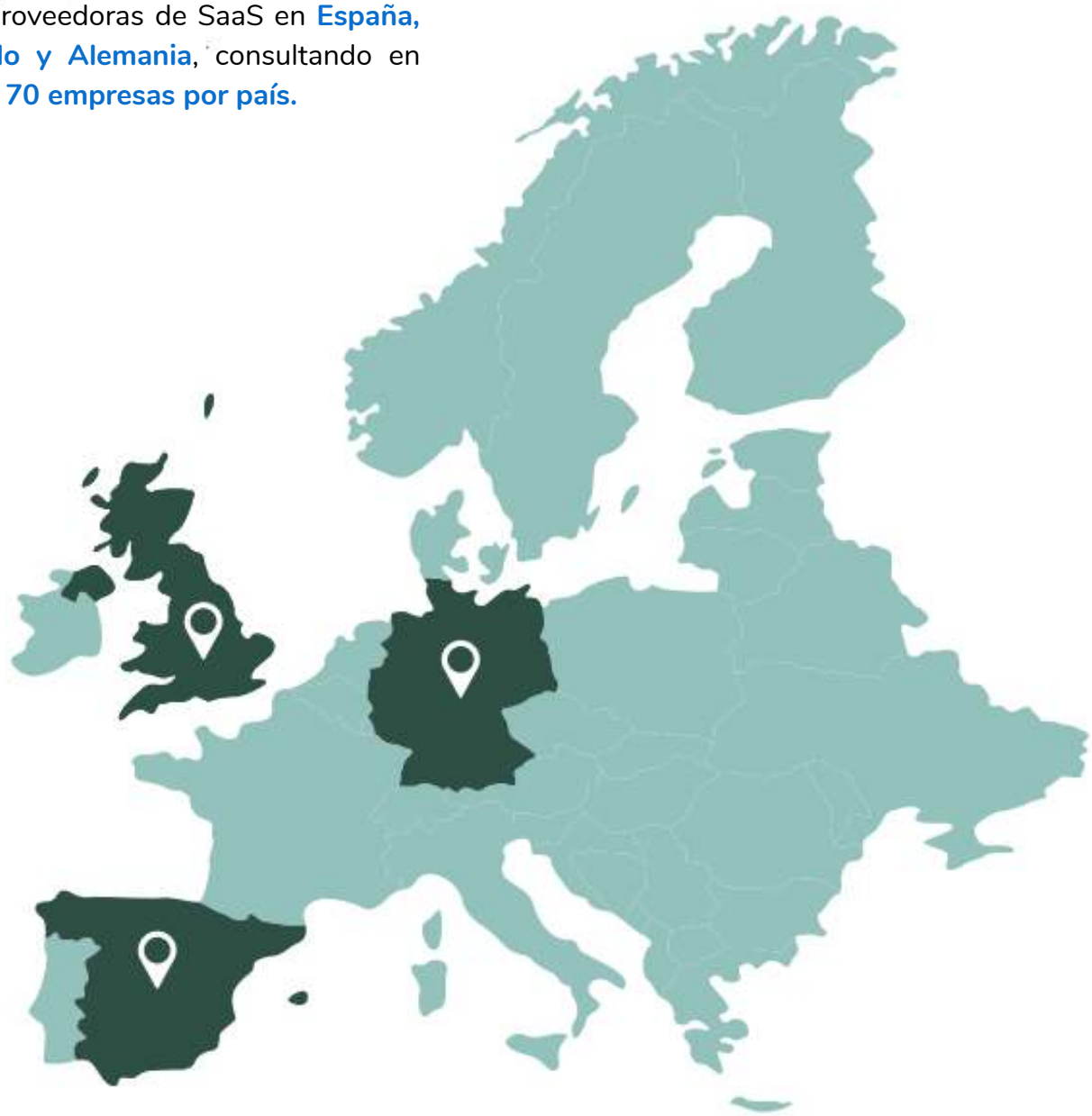
Estos fallos podrían incluso hacer **peligrar la continuidad de la empresa**: la protección de datos es algo que hay que tomarse muy en serio y que tiene que estar presente desde el momento en el que se desarrolla un SaaS, formando parte del ciclo de vida del servicio.

Vistos estos ejemplos, con este estudio hemos querido analizar si las **empresas proveedores de SaaS** tienen en cuenta todos estos aspectos relativos a la **protección de datos**, hasta qué punto están haciendo lo correcto, y de esta manera, poder analizar las consecuencias e implicaciones que la protección de datos puede tener para el éxito de los recursos que ofrecen.

2. Metodología

Con el objetivo de conocer cuál es el nivel de cumplimiento del RGPD en el sector SaaS y en función de las respuestas, poder dar recomendaciones sobre las mejores prácticas, **hemos preguntado a CEOs, Delegados de Protección de Datos, responsables legales y managers** de empresas proveedoras de SaaS en **España, Reino Unido y Alemania**, consultando en total a unas **70 empresas por país.**

En este estudio vamos a mostrar y a hacer un análisis más exhaustivo de los **resultados obtenidos en España**, no sin mencionar cuando sea necesario los datos obtenidos a nivel europeo.



3. Las empresas Saas y el cumplimiento de la protección de datos. ¿Qué están haciendo y qué se debe hacer?

A. Percepción de cumplimiento

Encuestamos a empresas de SaaS en el Reino Unido, España y Alemania para evaluar la importancia de la protección de datos en la industria de SaaS.

B. Recopilación y tratamiento de datos personales

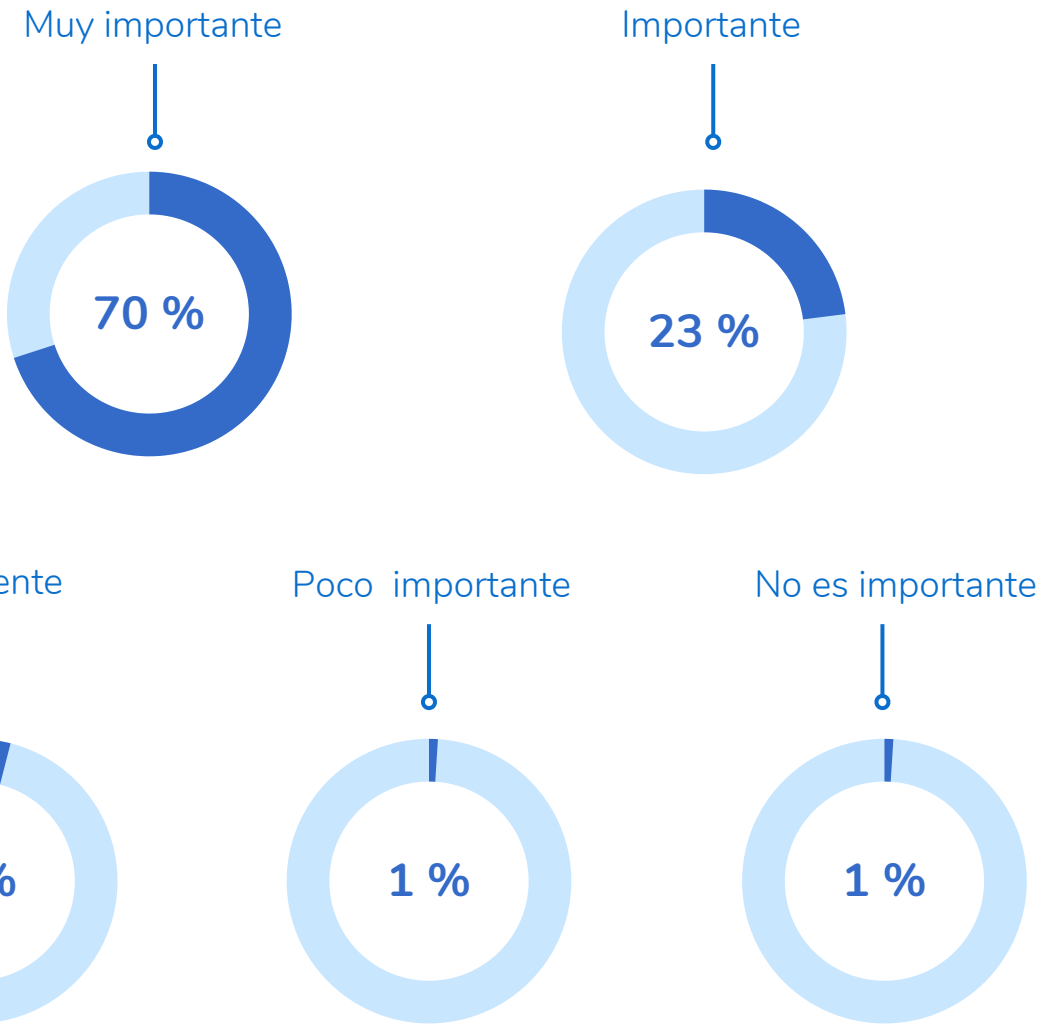
Examinamos el nivel de cumplimiento del RGPD que tienen las empresas de SaaS a la hora de informar a los usuarios / clientes sobre lo que se hace con sus datos, así como la frecuencia con la que imparten formación para que los empleados sepan cómo tratar datos personales.

C. Protocolos y medidas de seguridad implementadas en las organizaciones

Evaluamos si las organizaciones están utilizando o no las pautas recomendadas y protocolos para llevar a cabo procesos que aseguren la protección de los datos personales con los que trabajan.

Pregunta 1

En una escala del 1 al 5, ¿Cómo de importante es la protección de datos en tu organización?



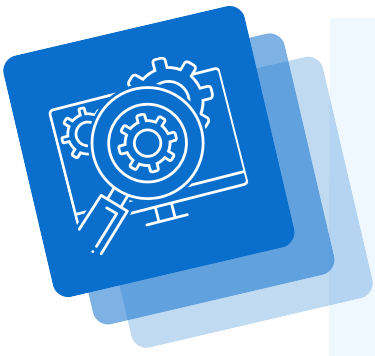
Para un 70% de los encuestados, la protección de datos es algo “muy importante”. Este resultado no sorprende, ya que la protección de datos es algo que valoran mucho los usuarios de los SaaS, e ignorarlo, podría llegar a poner en riesgo tanto al servicio ofrecido como a la empresa.

Entonces, ¿existen empresas SaaS que no den importancia a la protección de datos? Según nuestro estudio, sí.

Aunque en menor medida, **algunas de las empresas encuestadas tanto a nivel nacional como a nivel internacional**, han indicado que **para ellos la protección de datos no es para "nada importante" o que es "poco importante"**. Posiblemente den estas respuestas ajenas a todos los riesgos a los que se enfrentan, y no nos referimos solamente a la posibilidad de ser multadas si no cumplen el RGPD. Para un SaaS, ofrecer un adecuado nivel de seguridad, va unido a la **confianza** que se transmite al cliente.

¿Puede competir en el mercado un SaaS que no da garantías respecto a la protección de los datos que los clientes confían a su software?. Posiblemente lo tendría difícil, ya que la seguridad de sus datos es uno de los aspectos que más se tienen en cuenta.

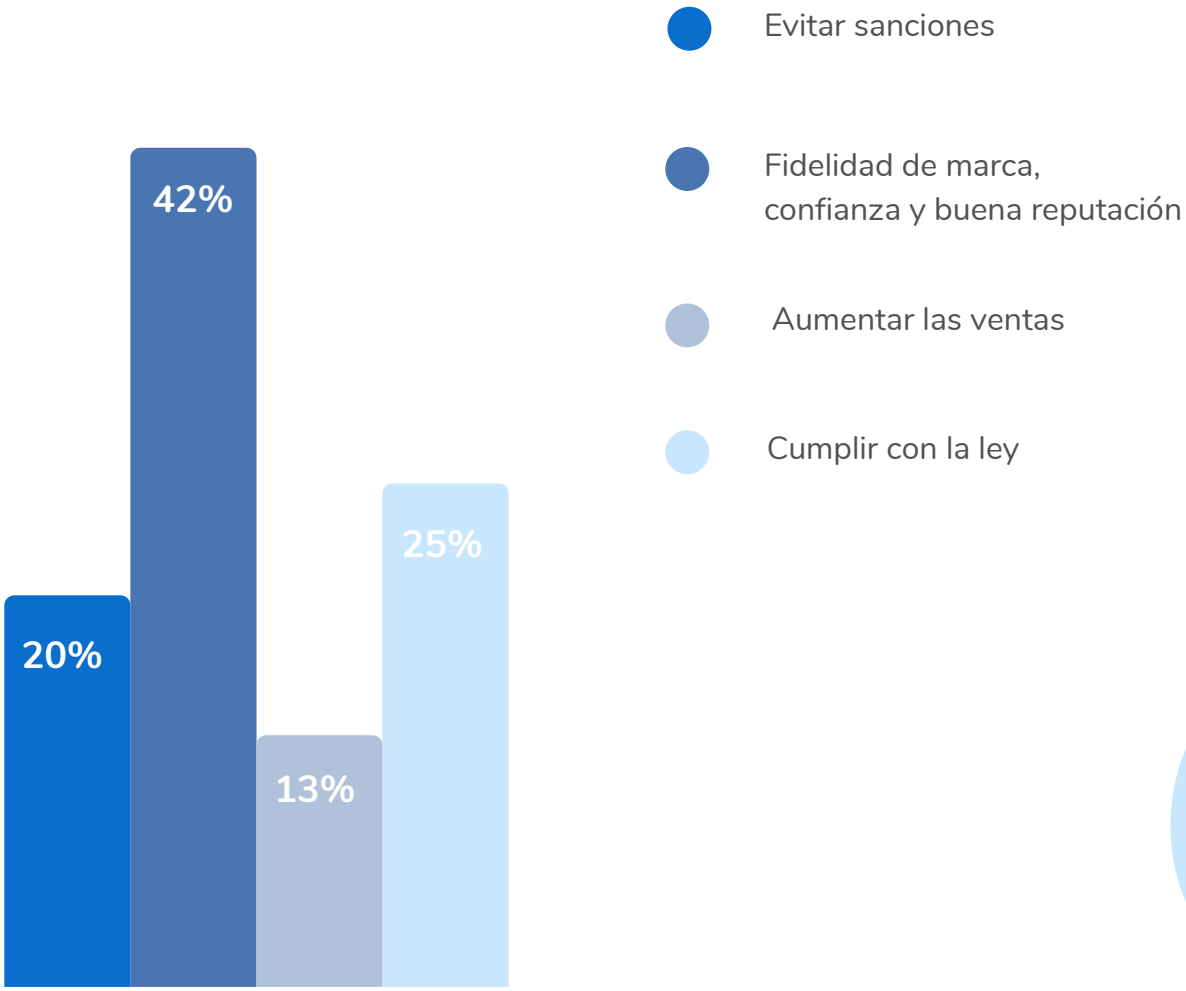
¿Cómo actuar ante una brecha de seguridad? ¿Qué medidas se establecen para minimizar riesgos? ¿Cómo se va a limitar el número de datos personales que se pida a cada usuario?. Estas preguntas, responden solamente a algunas de las necesidades que deberían **contemplarse en un programa de protección de datos**, y que a su vez, facilitarían cumplir con la normativa y poder operar de una manera más sencilla para ofrecer seguridad y limitar riesgos.



Poder transmitir que un SaaS se toma en serio la protección de datos y que tiene bajo control la privacidad y seguridad de la información de sus clientes, da la confianza que muchos necesitan para decantarse por un servicio u otro.

Pregunta 2

¿Cuál es el motivo por el que te esfuerzas por garantizar el cumplimiento del RGPD?



Los resultados de nuestra encuesta indican que **un 20% trata de evitar sanciones** y un **13% quiere aumentar las ventas**. Destaca un **42% que quiere mejorar la fidelidad de marca, confianza y buena reputación**, así como un **25% que quiere cumplir con la ley**.

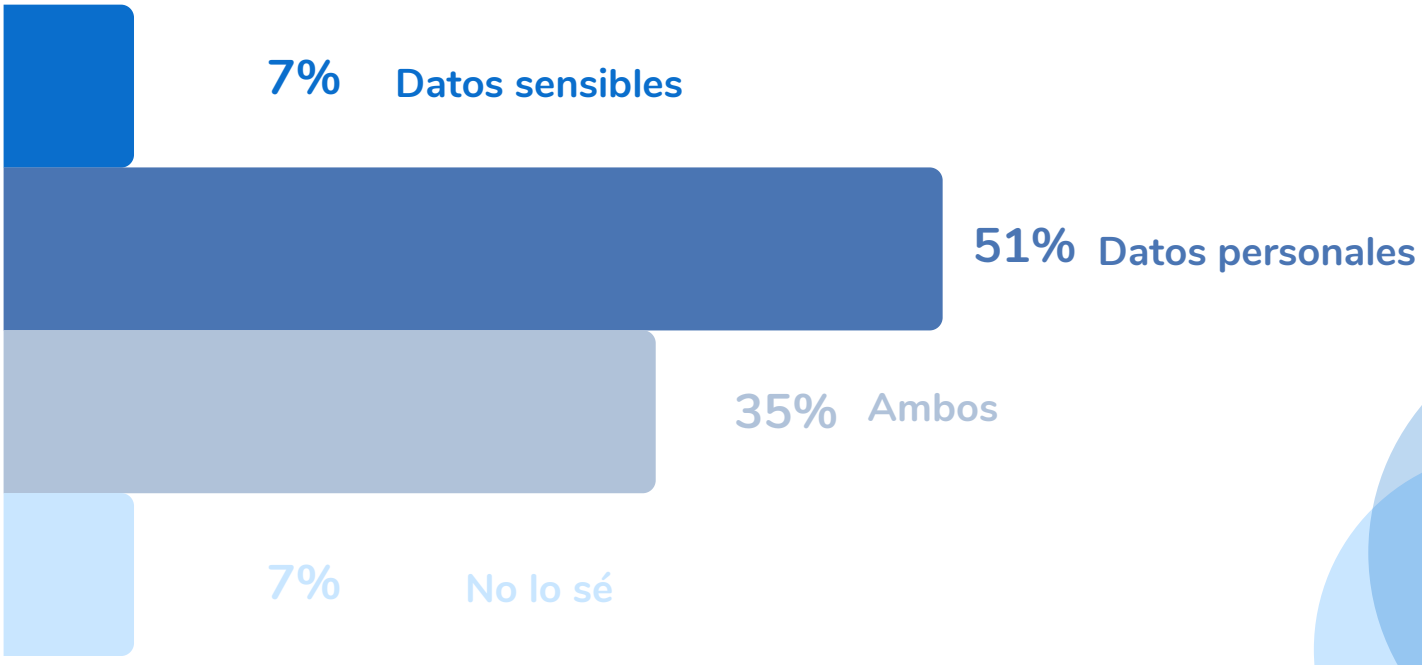
Fidelidad de marca, confianza y buena reputación ha sido la respuesta más votada, y no es algo que nos extrañe, ya que, como comentamos en la pregunta anterior, dar las garantías de ser un SaaS que hace todo lo posible por **asegurar la protección de los datos** de sus usuarios y ofrecer **transparencia** suma un punto más a la hora de **ofrecer tranquilidad**, y también puede influir notablemente en otra de las opciones planteadas, como es aumentar las ventas.

¿Qué aspecto nos ha resultado más llamativo? **Evitar sanciones ha sido la respuesta de solo el 20% de encuestados**, que aunque no es una cifra baja, es inferior a los resultados obtenidos en otras opciones. ¿Esto quiere decir que no existe una auténtica conciencia del riesgo de sufrir multas? Han sido noticia muchas grandes empresas por haber tenido multas millonarias al haber incumplido alguno de los supuestos del RGPD.

Son muchas las grandes empresas que han sido noticia por haber sufrido una multa millonaria al haber incumplido el RGPD. Posiblemente, empresas más pequeñas puedan pensar que las grandes sanciones o ser investigadas por las autoridades de protección de datos sea algo exclusivo para grandes corporaciones, pero no es así. **Cualquier usuario puede denunciar una irregularidad en la protección de datos**, que **será investigada y sancionada con una cantidad proporcional a la gravedad de la infracción y al tamaño de la empresa**, lo que en muchos casos, puede suponer una pérdida económica importante e incompatible con la continuidad del negocio.

Pregunta 3

¿Qué tipo de datos tratas?



Un **51%** de los encuestados afirma **tratar datos personales,** mientras que un **7%** indica que trata **datos sensibles.** Un **35%** de los encuestados **trata tanto datos personales como datos sensibles,** y un alarmante **7%, asegura no saber qué tipos de datos trata.**

No saber qué tipo de datos se tratan, es un problema muy grave.

Hemos realizado esta pregunta a personas que trabajan dentro del **departamento legal** de empresas de SaaS, **lo que demostraría que la protección de datos y los posibles riesgos asociados, son aspectos que no se han contemplado.** La pregunta también se ha lanzado a **CEOs y managers,** que aunque pueden **estar menos familiarizados con la protección de datos**, son en muchos casos la clave para que se disponga en una empresa de los medios que permitan trabajar en la privacidad desde el diseño o haya más recursos para formar a los empleados, por lo que si desconocen completamente uno de los aspectos más básicos de la protección de datos de las empresas que gestionan, podemos pensar que tienen mucho camino que recorrer hasta tener un nivel de cumplimiento óptimo.

Ahora vamos a centrarnos en explicar **qué consecuencias tiene ignorar el tipo de datos que se están tratando en un SaaS**:

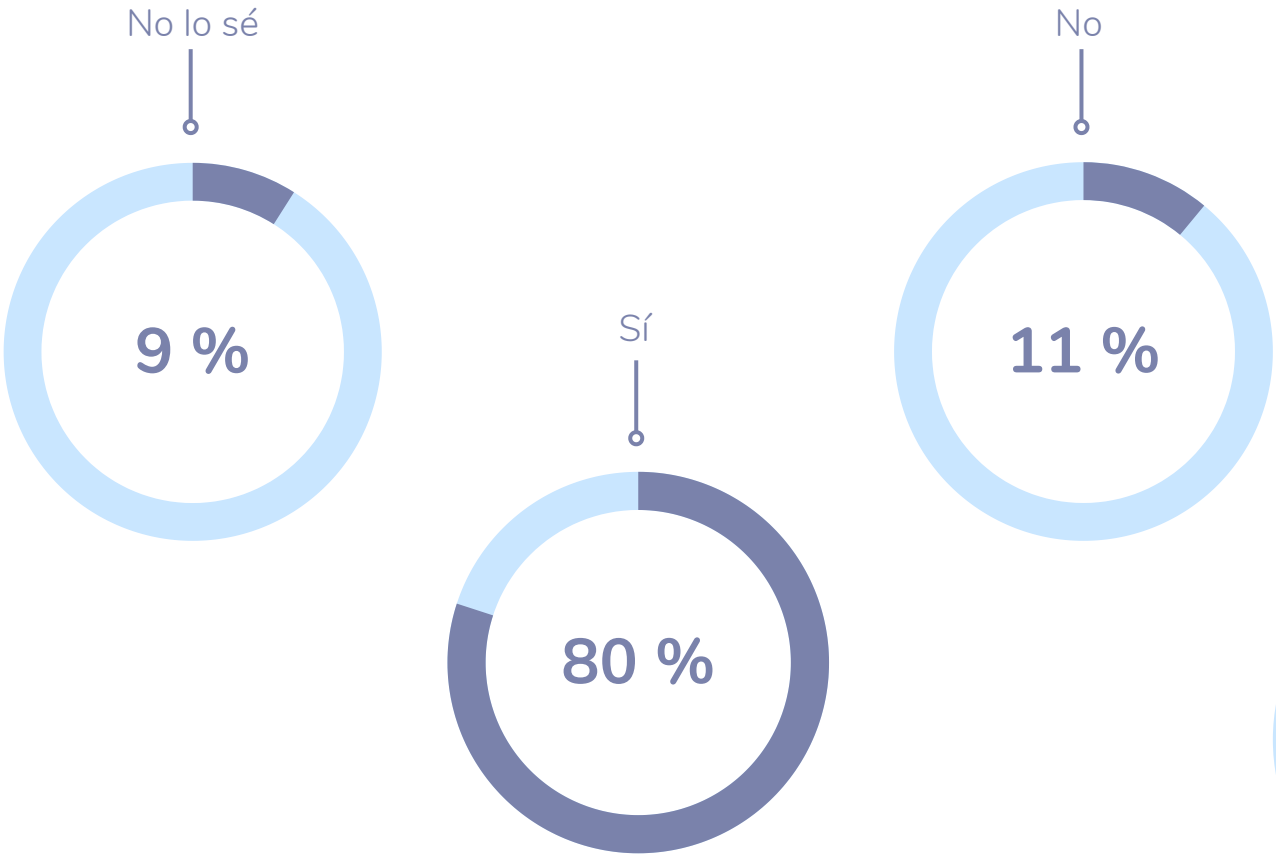
- No darles el tratamiento que requieren, poniendo en riesgo los derechos de las personas.
- Incumplir el RGPD al no contar con un DPO si se estuviesen tratando datos sensibles.
- No conocer el impacto que tendría una posible brecha de seguridad.
- Ausencia de medidas preventivas.
- Riesgo a sufrir una elevada sanción.

Independientemente de estos riesgos, cualquier cliente puede detectar fácilmente que no se cumple la normativa o que se le están dando pocas garantías sobre este aspecto.

Desde las primeras fases de diseño de un SaaS, se tendría que saber qué tipo de datos se van a pedir, tratar y alojar, para establecer una experiencia de usuario y unas medidas preventivas acordes a esta información.

Pregunta 4

¿Los empleados saben cómo funciona la retención y eliminación de datos del cliente y cómo proceder en cada caso?



Un **80% afirma que sí**, pero un **11% indica que no** y un **9% no lo sabe si sus empleados son conscientes de los protocolos para la retención y eliminación de datos**. En la pregunta anterior observamos que había un 7% de empresas que no saben qué tipo de datos tratan, y precisamente, podemos ver las primeras **consecuencias** de ignorar este aspecto reflejadas en esta pregunta. Es muy probable que si se desconoce el tipo de datos que se tratan en una empresa, tampoco exista un protocolo adecuado para su retención y eliminación, o que si alguna vez se ha realizado, no haya llegado al conocimiento de todos los empleados y responsables y por lo tanto, no se esté cumpliendo.

- Un SaaS, debería tener un **protocolo en el que se establezca qué información se necesita conservar en función de sus características y de la normativa**. Es importante establecer dicho protocolo teniendo en cuenta las **necesidades de la empresa** y hacer que cada **departamento** conozca qué datos necesita conservar en según los requerimientos de su trabajo y de la normativa
- Tiene que contemplarse la necesidad de **conservar los datos únicamente el tiempo estrictamente necesario** para las funciones que se realicen. El RGPD sustenta esta recomendación, pero también incluye **algunas excepciones que permiten plazos de conservación más largos** si los datos van a tener algún tipo de interés científico, informativo o histórico.
- Otro aspecto importante es contar con un **protocolo de eliminación** en el que se incluyan **recomendaciones**, como por ejemplo, las herramientas que van a utilizarse para dicha función con el fin de evitar errores humanos.

El protocolo de retención y eliminación de datos ayuda a tener un control de la información con la que trabaja y a poder anticiparse y minimizar riesgos, a la vez que les da un tratamiento adecuado y compatible con la normativa de protección de datos.

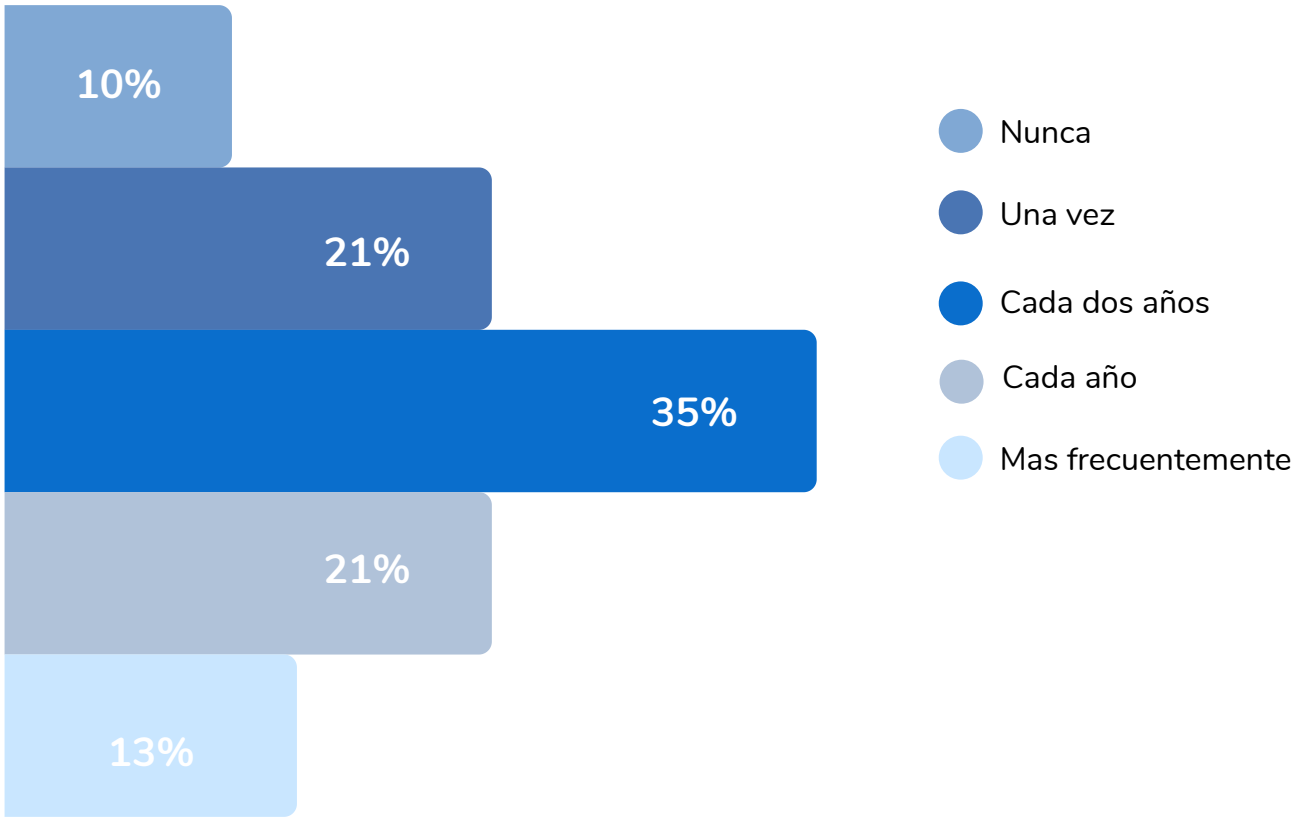
No sirve de mucho contar con este protocolo si los empleados lo desconocen, y por lo tanto, no lo aplican. En este punto la **formación** juega un importante papel, aspecto que analizamos en la siguiente pregunta.

Pregunta 5

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

La **formación para empleados** sobre **protección de datos** ayuda a que el plan de protección de datos pueda cumplirse. De nada sirven los esfuerzos por tener unas buenas bases establecidas, si los empleados las desconocen y no las cumplen.

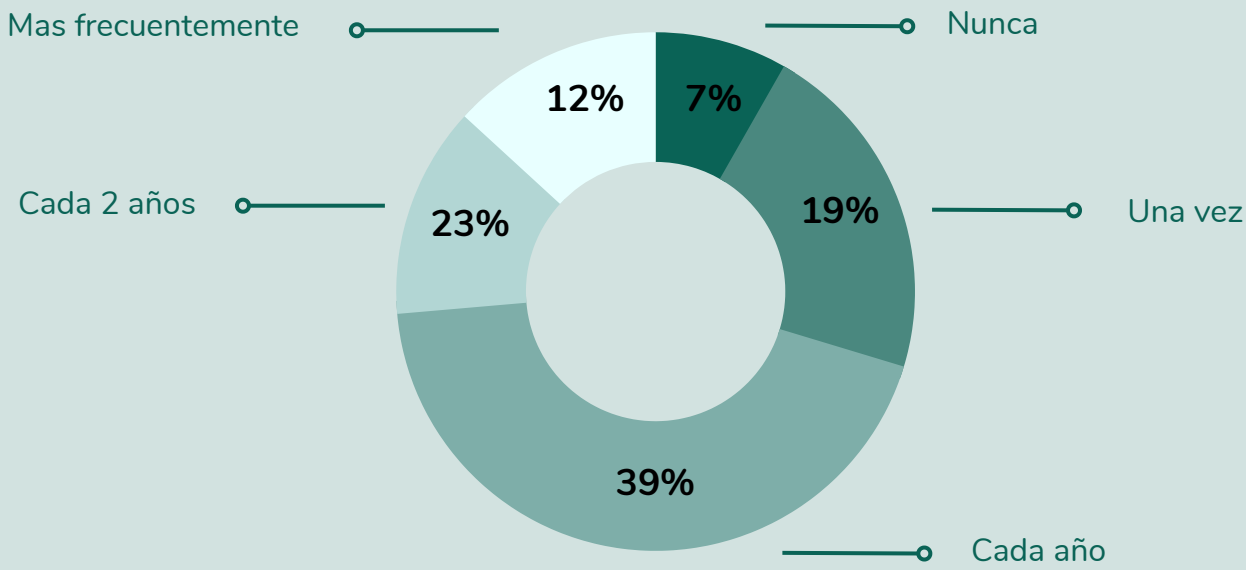
En la pregunta anterior detectamos que muchas empresas no son conscientes de si sus empleados conocen o no el protocolo de retención y eliminación de datos y analizamos las posibles consecuencias que esto podría tener. C**on una formación adecuada, no existiría este problema.** Esta es solamente una de las consecuencias negativas que podrían evitarse y que harían que el trabajo fuese más sencillo en lo que a protección de datos se refiere.



El **21%** de las empresas encuestadas en España afirman haber realizado **formación sólo una vez desde su creación**, un **21% la hace cada 2 años**, frente a un **35%**, que hace formación **una vez al año**. Un 13% de los encuestados indica que hace formaciones con más frecuencia, es decir, más de dos veces al año.

A **nivel europeo** observamos que hay un 39% que sí hace formaciones cada año y a un 12% que las hace con más frecuencia, frente a un 23% que las hace cada dos años, mientras que un 7% de las empresas, nunca ha hecho formación para sus empleados.

Si exceptuamos a ese 7%, podemos apreciar que sí existe concienciación sobre la necesidad de ofrecer formación, aunque la frecuencia en la que se realiza puede llegar a diferir mucho entre unas empresas y otras.



Ya hemos visto que con una formación adecuada se pueden evitar otros problemas de protección de datos. Viendo los resultados obtenidos, cabría preguntarse, qué es lo adecuado y cómo debería de ser esa formación.

La **frecuencia de la formación** sobre protección de datos debe depender de las características de la empresa, y tiene que tener en cuenta los cambios organizativos o de otros aspectos que se realicen a lo largo del tiempo.

¿Qué aspectos se deben contemplar para decidir cuándo se hace una nueva formación sobre protección de datos?

Nuevas funcionalidades que vayan a suponer un nuevo tratamiento de datos, empleados nuevos o que vayan a realizar nuevas tareas o cambios legislativos.

No hay que olvidar que la formación debe de estar centrada en **responder a las necesidades de cada empleado y departamento**. Entonces, ¿a qué puede deberse ese **7% que no realiza formación**? Si volvemos a repasar algunas de las respuestas obtenidas en este estudio puede resultar fácil entenderlo: el desconocimiento de la importancia de la protección de datos, ignorar el riesgo a multas o el efecto que puede tener en cuanto a la seguridad que se da al cliente.

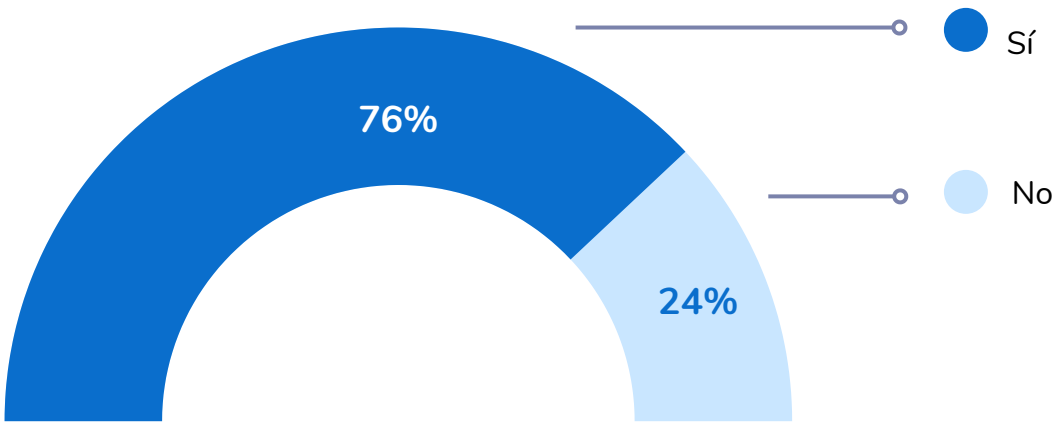
En **Pridatect ofrecemos formación** que se adapta a todas estas necesidades, basándonos en estas claves:

- Es online y accesible en cualquier momento: los empleados pueden realizarla o consultar los temas en cualquier momento.
- Está adaptada al número de empleados y a las necesidades de cada departamento, en función de las tareas que realiza y que implican el tratamiento de datos.
- Es específica para cada tipo de empresas: conocemos las necesidades formativas concretas y valoramos las incidencias que puedan tener en función de los datos que se tratan.

Pregunta 6

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

En cualquier momento puede nacer el interés de un usuario/cliente por conocer un aspecto relativo a sus datos.



Aunque un 24% de los encuestados indica que no reciben preguntas sobre protección de datos, un 76%, indica que sí, lo que nos sitúa ante una evidencia: **es común que los usuarios pregunten sobre la protección de sus datos,** y esto hace necesario que la empresa esté preparada para poder responder.

Parece algo evidente, pero, si volvemos a ver los resultados de preguntas anteriores, en las que pudimos observar que había empresas que no saben con exactitud el tipo de datos que tratan, o no forman adecuadamente a sus empleados en aspectos relativos a la protección de datos, **podríamos preguntarnos si estas empresas podrían ser capaces de responder con exactitud.**

Pongamos un ejemplo: un usuario quiere rectificar algunos datos relativos a su propia cuenta en un SaaS y suprimir otros que considera delicados.

¿La persona que atiende a esta petición, sería capaz de identificar que el usuario está ejerciendo algunos de sus derechos? ¿Conoce el tiempo establecido por el RGPD para poder contestar a estas peticiones? ¿Sabe a quién tiene que trasladar la petición?.

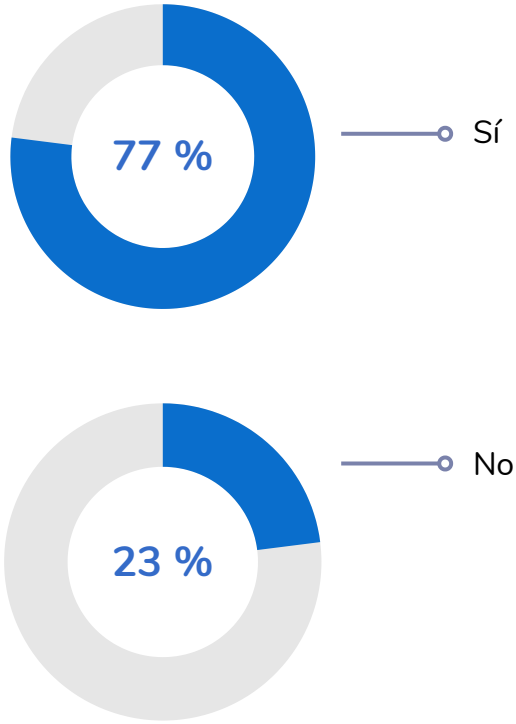
Posiblemente, si **no se ha realizado una formación adecuada a empleados, y si no se ha seguido un correcto protocolo de protección de datos,** pueda haber **errores** a la hora de gestionar este tipo de preguntas.

Tener un protocolo de protección de datos bien establecido, permite poder contestar a cualquier pregunta, ofreciendo tranquilidad y transparencia al usuario. No recibir respuesta ante una pregunta relativa a la protección de datos, no sólo puede suponer una pérdida de confianza, también puede llevar a incumplir el RGPD al no permitir a un usuario ejercer sus derechos.

Aunque nos encontremos ante una empresa en la que no ha sido habitual recibir muchas preguntas sobre protección de datos, es conveniente estar preparado. Además, hay que cumplir con el **deber de informar**, algo que destaca el RGPD y que veremos más desarrollado en la siguiente pregunta.

Pregunta 7

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



Que un 77% de los encuestados haya contestado que sí, ya denota que es algo bastante habitual, por lo que dar información sobre la finalidad de recoger los datos de una forma clara, inequívoca y fácil de entender, ya puede ahorrar problemas y dar transparencia, pero además, es algo que entra dentro de las obligaciones establecidas por el RGPD, permitiéndonos cumplir el deber de informar.

Independientemente de la información que se da sobre la forma en la que se van a proteger los datos y los derechos que los interesados tienen sobre ellos, es necesario explicar **por qué se necesita solicitar datos personales cuando,** por ejemplo, un usuario se da de alta en el servicio.

Para hacer entender la importancia de este asunto, podemos imaginarnos lo que ocurre, cuando un usuario está completando el formulario de registro de un SaaS, se le pide un dato que no considera necesario para el uso de la plataforma, y en ese momento, se pregunta el motivo por el que la empresa necesita tener esa información, generando de esa manera una desconfianza por el servicio ofrecido.

¿Esto es algo que le ocurre a las empresas a las que hemos encuestado?

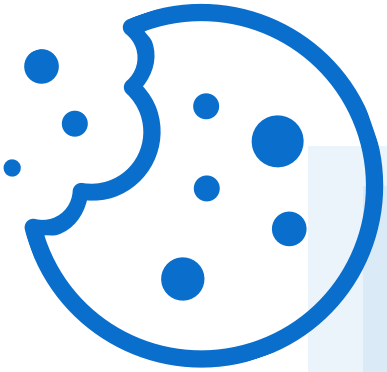
Un 77% de empresas confirman que sus usuarios o clientes sí hacen preguntas sobre el motivo por el que se están recogiendo sus datos, y un 23% indica que no.

La **normativa** establece la obligación de dejar claros aspectos como los **datos de contacto del DPO** si lo hubiera, la **base jurídica legitimación** para el tratamiento, los **plazos** o lo **criterios de conservación de la información** la existencia de **decisiones automatizadas o elaboración de perfiles,** la previsión de **transferencias a Terceros Países,** el derecho a presentar una **reclamación ante las Autoridades de Control** y en los casos en los que los datos no se obtengan del propio interesado, el **origen de los datos y las categorías de los datos.**

Además, hay que dar información detallada sobre la **finalidad del tratamiento,** sobre la **obligatoriedad o no de dar datos personales** y de sus **consecuencias**.

El responsable debe poder acreditar que ha cumplido con esta obligación de informar.

También hay que fijarse en la forma en la que se muestra la información en los **banners de cookies** que deben mostrarse en cada página web:, se exige establecer un sistema de **información por capas**, donde en una **primera capa** se de la información relativa a la finalidad, teniendo que hacer en la **segunda capa** una descripción más específica.



Seguir detalladamente las recomendaciones del RGPD ayudan a explicar mejor al usuario la finalidad de recoger sus datos pero en ocasiones puede ser algo complejo reflejar todo lo necesario y crear políticas que se apliquen a todos los ámbitos de la empresa. **En Pridatect podemos asesorarte, resolverte dudas** y ofrecerte el acceso a múltiples funcionalidades de nuestra plataforma que te facilitarán todas las tareas que tú y tu equipo debéis de hacer para cumplir la normativa. Puedes pedirnos información para saber en qué te podemos ayudar.

Pregunta 8

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

Pese a que **el 90% de las empresas encuestadas indicaron que obtienen el consentimiento del usuario para el tratamiento de datos**, sorprende que **el 10% restante no pide el consentimiento.**

Obtener el consentimiento de los usuarios antes de recoger sus datos **es uno de los puntos fundamentales que establece el RGPD**. Ese tanto por cierto que ha contestado que no lo pide, **está cumpliendo gravemente la normativa**. Estas cifras encajan con el porcentaje de empresas que no dan importancia a la protección de datos, que desconocen el tipo de datos que tratan o que no hacen una formación adecuada.

¿Cómo tendría que recogerse el consentimiento para no incumplir la normativa?

- La **solicitud** con la que se recoge el consentimiento debe especificar qué uso se hará con los datos personales, y debe incluir los datos de contacto de la empresa que trata los datos. El interesado, habrá sido **informado previamente de manera clara y concisa** de todos los aspectos para los que está dando su consentimiento.

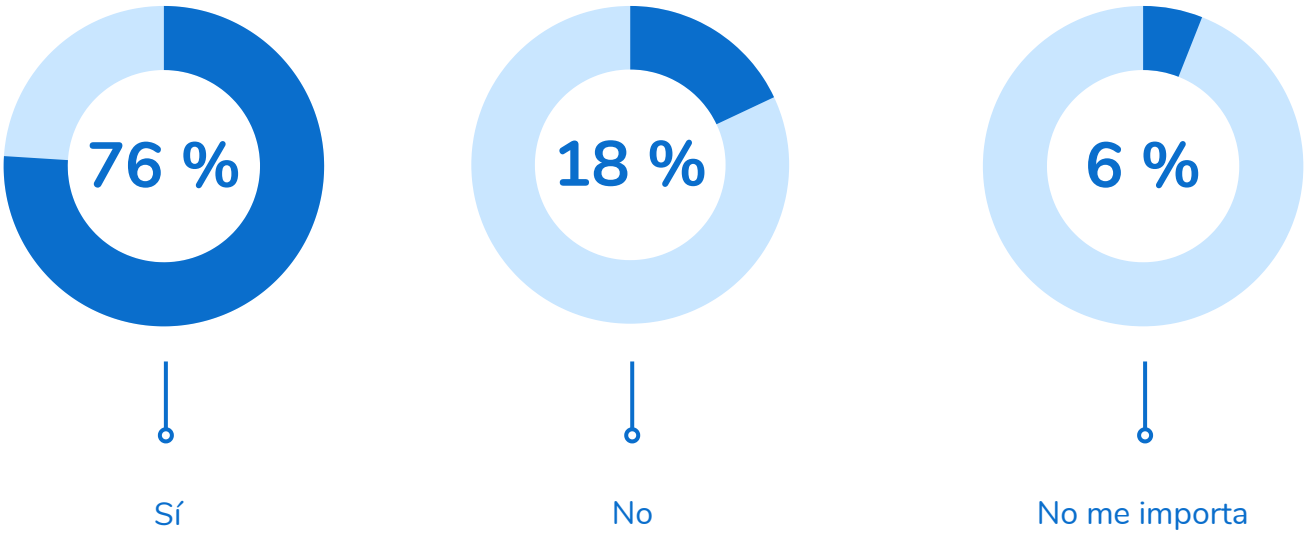
.

- Hay que tener en cuenta que cuando el cliente no dice nada al respecto, decide no marcar ninguna casilla a la hora de dar o rechazar dar su consentimiento o cuando cuenta con una casilla previamente marcada, no estaríamos ante una manera válida para recabar su consentimiento para el tratamiento de sus datos personales. **Para el RGPD, el consentimiento tácito no tiene validez.**

- Asimismo, no hay que olvidar que toda empresa tiene que ofrecer el **derecho al usuario o cliente de retirar el consentimiento en cualquier momento.**

Pregunta 9

¿Te preocupas por ver si tus proveedores externos cumplen con el RGPD?



Contar con proveedores y que estos requieran información para poder operar, puede ser algo a lo que tarde o temprano se exponga cualquier empresa.

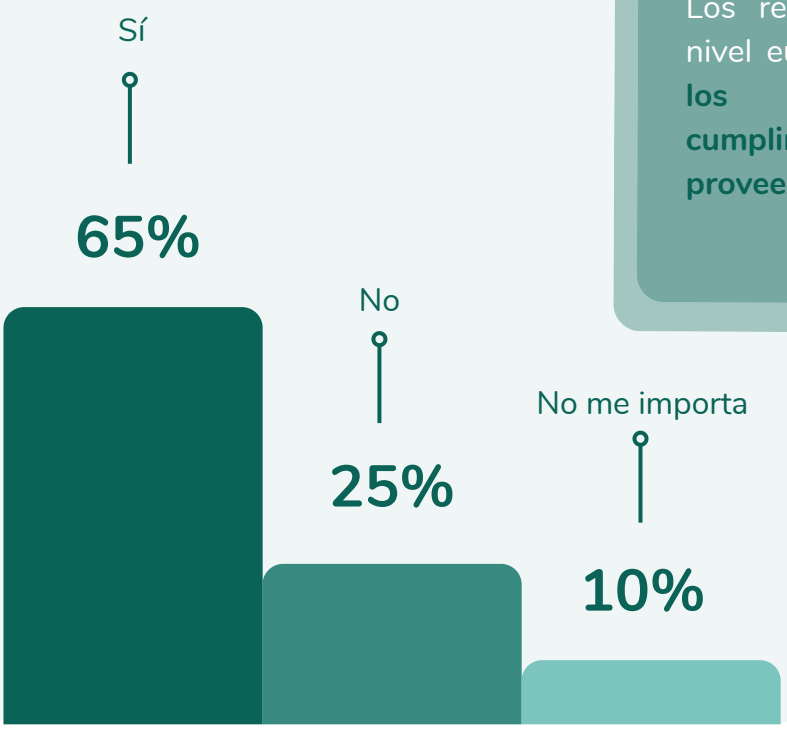
Las organizaciones que comparten información con proveedores externos, son responsables de lo que estos hagan con sus datos.

A pesar de esto, **solo el 76% de las organizaciones encuestadas en España verifican si sus proveedores cumplen o no con el RGPD,** habiendo un 18% que no lo hace. Los resultados son más preocupantes **a nivel europeo,** con **menos de un tercio de los encuestados verificando el cumplimiento por parte de sus proveedores externos.**

¿Por qué debería una empresa preocuparse por el cumplimiento de los proveedores externos? Esencialmente, para evitar riesgos operativos y daños reputacionales.

A la hora de elegir un proveedor, se debe valorar si cumple con las obligaciones que impone el RGPD. Si se detecta que un proveedor no está cumpliendo con el RGPD, la autoridad competente puede responsabilizar a la empresa contratante, por lo que para evitar multas y posibles daños, se recomienda hacer **una evaluación de riesgos a los proveedores** para determinar si son aptos para ser potenciales socios comerciales. Con esta evaluación se identifican riesgos y oportunidades asociados con los procesos, servicios y productos de un proveedor y se mostrará si cumple con los requisitos establecidos por la organización.

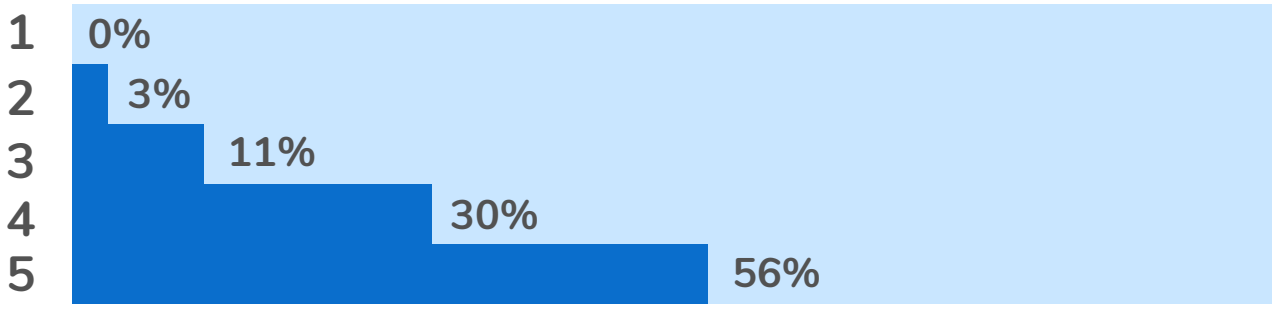
Es muy importante contar con una **lista actualizada de proveedores**, analizando tanto a los actuales proveedores como a los futuros proveedores que puedan irse contratando.



Los resultados son más preocupantes a nivel europeo, con **menos de un tercio de los encuestados verificando el cumplimiento por parte de sus proveedores externos.**

Pregunta 10

En una escala de 1 a 5 (0 = nada importante, 5 = muy importante), ¿qué importancia tiene el cumplimiento de la protección de datos para el desarrollo de su propio producto?



Para el **56%** de las empresas encuestadas **el cumplimiento es esencial para el desarrollo de productos.** Un **30%** lo considera **importante** aunque sin llegar a darle la mayor puntuación, y el **14%** restante **no cree que sea algo importante**

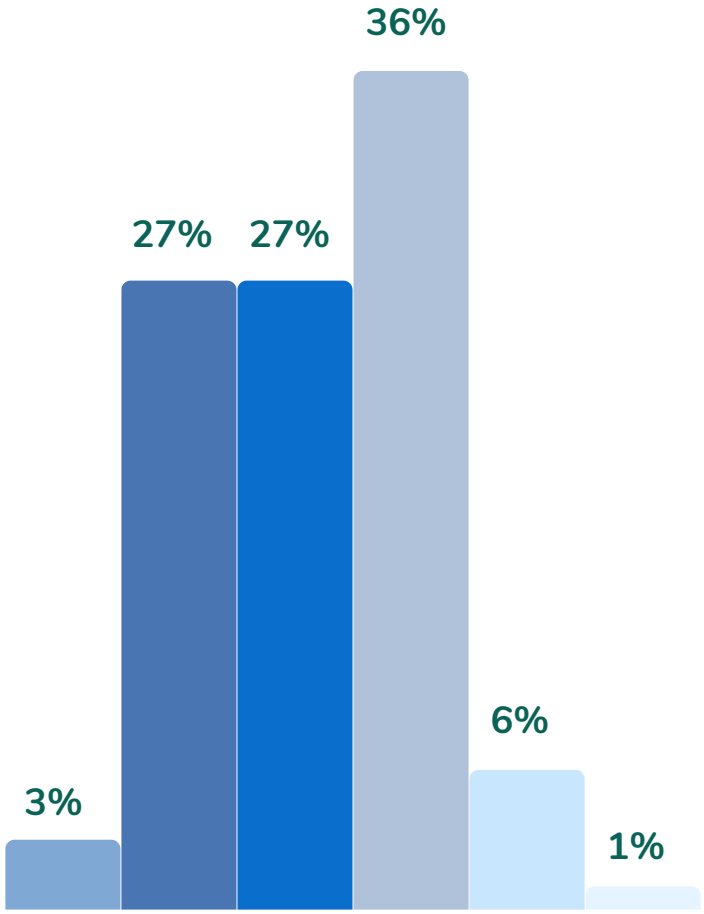
Si nos fijamos en las empresas que lo consideran clave para el desarrollo de sus productos, tenemos que destacar la importancia de la "privacidad desde el diseño", que tanto ha ayudado a dar forma a la industria del SaaS. **La privacidad desde el diseño, pretende hacer que una empresa sea proactiva, evitando de esta manera que sea reactiva, lo que implica tener en cuenta la protección de datos en todas las fases del diseño tecnológico.**

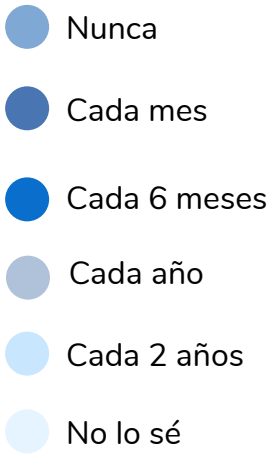
Al adoptar la **privacidad desde las fases de diseño** de un producto, se tienen en cuenta el cumplimiento de la normativa de protección de datos y el respeto de la privacidad de datos en todas las funcionalidades del mismo, lo que evitaría hacer cambios posteriormente para adaptarse. De esta forma, aspectos como "**la privacidad de forma predeterminada**", (selección predeterminada de las medidas o configuraciones de privacidad con un mayor nivel de protección) también serían tomadas en cuenta, pudiendo diseñar herramientas y productos con un **nivel óptimo de cumplimiento.**

La privacidad desde el diseño tiene un papel relevante a la hora de prevenir futuras brechas de seguridad, de garantizar que se respete la privacidad de los usuarios y de evitar el coste de realizar cambios radicales una vez desarrollado el producto o servicio.

Pregunta 11

¿Cada cuánto tiempo haces evaluaciones de cumplimiento para identificar y evaluar los riesgos a los que están expuestos los datos con los que trabajas?





En esta pregunta hemos querido saber si las empresas de SaaS **hacen evaluaciones de cumplimiento con la frecuencia adecuada**, y solo el **27%** de las empresas afirmó hacerlas **mensualmente.**

Las **evaluaciones de cumplimiento** pueden variar tanto en su propósito, como en los beneficios que aportan. Desde **evaluaciones de impacto** para conocer los daños y cómo afectaría una brecha de datos hasta **evaluaciones de riesgos,** que permitirían identificar los posibles incidentes que podrían afectar a los datos que una empresa aloja y trata, incluyendo **auditorías** más amplias. Todas ellas pueden darnos muchas pistas para mejorar la protección de datos.

¿En qué pueden ser útiles las evaluaciones de cumplimiento?

- Permiten tener una imagen clara de la situación actual de la empresa en cuanto a protección de datos se refiere.
- Ayuda a identificar riesgos potenciales.
- Permite evaluar los controles y medidas de seguridad existentes,
- Facilita la propuesta y determinación de mejoras.
- Reduce el riesgo de sufrir multas por incumplimiento.
- Incrementa el atractivo para los inversores, ya que estos pueden ver el estado real del nivel de protección de datos existente.

A pesar de los beneficios y la claridad que aportan sobre el estado real de la empresa, **el 3% de las empresas en España indica que no realiza evaluaciones periódicas de cumplimiento, teniendo que mencionar que un 1% no lo sabe**, lo que las deja susceptibles de ser multadas o de enfrentarse a riesgos que podrían haber evitado.

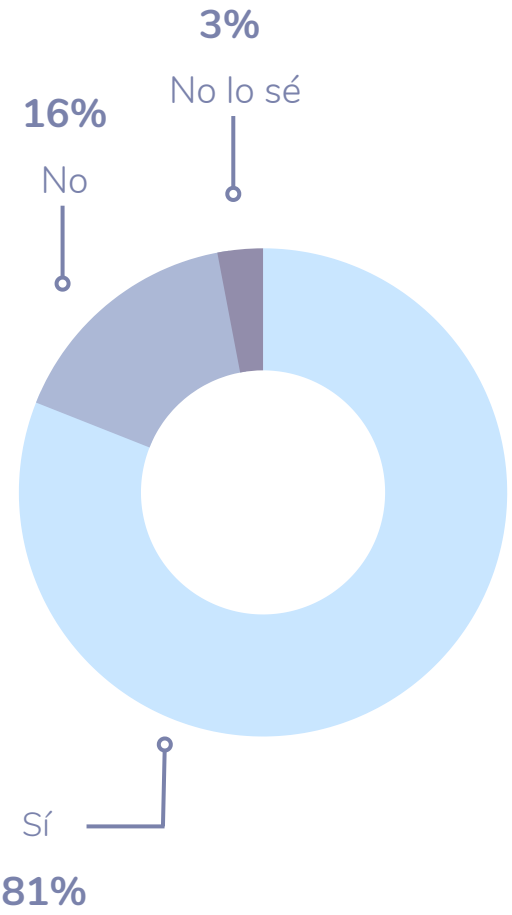
Haciendo mención al resto de empresas que sí realiza **evaluaciones de cumplimiento,** podemos hablar más detenidamente de la **frecuencia** con la que las hacen, aspecto que hemos querido analizar por suponer un importante factor a tener en cuenta para determinar si pueden dar un buen resultado o no, ya que la periodicidad va a influir, por ejemplo, a la hora de adaptarse a cambios en la empresa o a posibles cambios legislativos. Con esto podemos señalar, que al igual que ocurría en la pregunta número 5 de este estudio, referida a la frecuencia de la formación a empleados, **la protección de datos no es algo de lo que haya que preocuparse solo una vez**, sino que **tiene que irse actualizando** y tienen que irse teniendo en cuenta y evaluando los **cambios a lo largo del tiempo.**

Pregunta 12

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

La actualización del registro de actividades de tratamiento debe de ser una actividad continua. Si nos fijamos en la recomendación que hace la AEPD al respecto, hacen referencia a "tratar el registro como un documento vivo", por lo que al igual que vimos en la pregunta anterior, deben contemplarse los cambios en el tiempo.

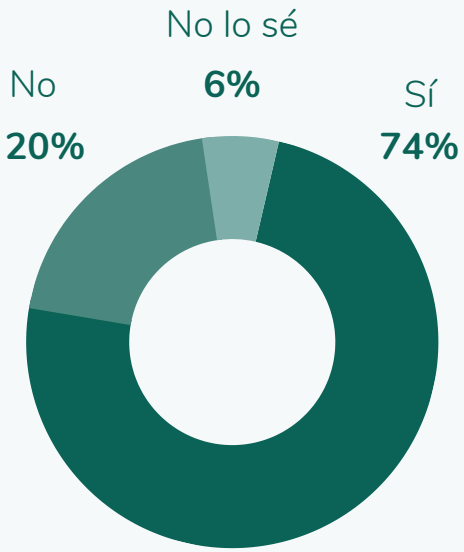
Como podemos ver en los resultados, el **81% de las empresas encuestadas en España, están prestando atención a los consejos de la AEPD**, lo que significa que **menos de las tres cuartas partes de los participantes están descuidando una tarea** que el organismo regulador ha recomendado que se realice de manera regular.



El registro de las actividades de tratamiento de datos debe mantenerse actualizado y debe reflejar:

- Quienes son las partes involucradas en el tratamiento de datos (responsable, encargados, representante, etc.)
- Categorías de datos tratados
- Finalidad del tratamiento
- Cuánto tiempo se conservarán los datos
- Las medidas de seguridad técnicas y organizativas (TOMS) implementadas (cuando sea posible).

No existe una estipulación sobre la frecuencia con la que se tiene que hacer el registro, pero sí que se establece la necesidad de mantenerlo actualizado a medida que se vayan implementando cambios en el tratamiento.



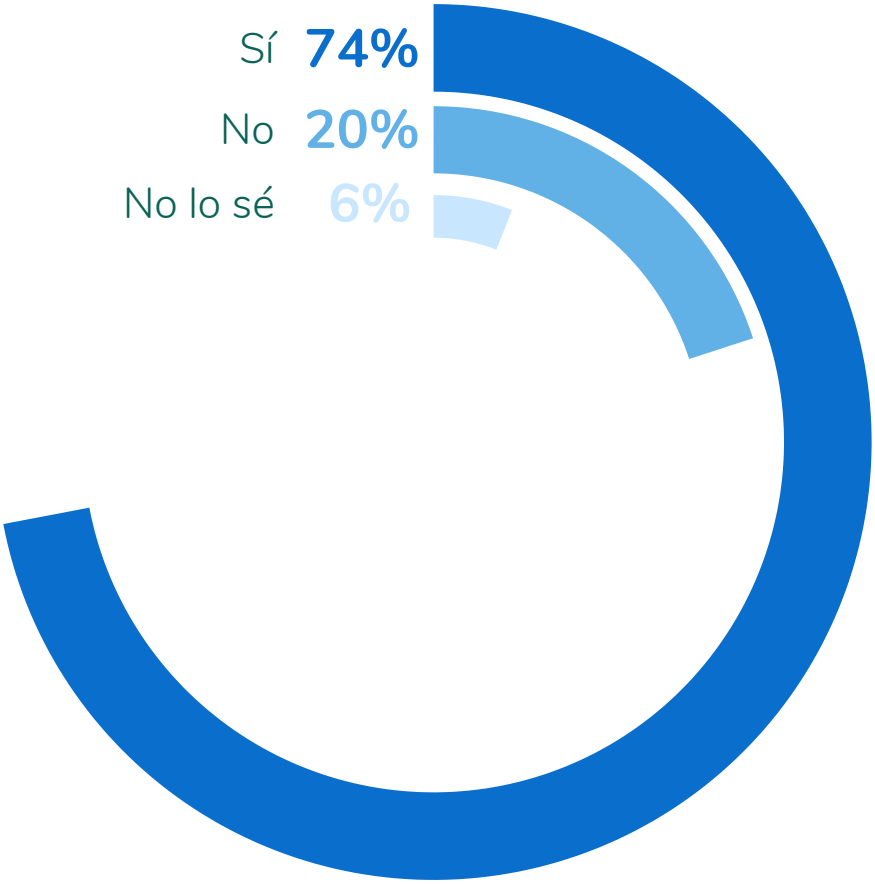
Si nos fijamos en los datos obtenidos **a nivel europeo**, podemos apreciar que la cifra baja, habiendo un 74% de empresas que cumplen con esta recomendación pero dejando a **un 20% que lo pasa por alto.**

Volviendo a los resultados obtenidos en esta pregunta, hay un **3%** de empresas que ha respondido que **"no sabe" si mantiene o no un registro actualizado de las actividades de tratamiento**, lo que hace más probable que no tengan registradas correctamente todas las actividades de tratamiento. Este documento, en el caso de existir, debería estar al día e incluir **todas las actividades actuales**, por lo que si lo estuviera haciendo con regularidad, se sabría la respuesta, lo que irremediablemente nos vuelve a llevar a incidir en la importancia de concienciarse sobre la protección de datos y sobre la formación al respecto, para que no se llegue a desconocer si se realiza o no algo tan importante y además obligatorio.

No realizar un registro de las actividades de tratamiento lleva a incumplir el RGPD, lo que conlleva a posibles multas de hasta 10 millones de euros o el 4% de los ingresos totales que tuviese la empresa durante el año anterior.

Pregunta 13

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



El **74% de los encuestados** indica que **sí tienen definidas esas medidas,** encontrándonos con un **26% que no lo hace o no sabe si lo hace**, lo que implica que **desconocen esta práctica** o que no saben que tiene que llevarse a cabo en su organización. Esto supone que el **26% de las empresas encuestadas no están cumpliendo con el RGPD.** Por mucha importancia que se le esté dando al cumplimiento de la protección de datos, realmente no están tomando las medidas necesarias para ello, ya que todas ellas están expuestas a ser sancionadas simplemente por no tener TOMs definidas.

Tomar medidas técnicas y organizativas **(TOMS) ayuda a garantizar la seguridad de los datos** con los que se va a trabajar; se identifican los riesgos potenciales y se pueden tomar medidas para evitarlos.

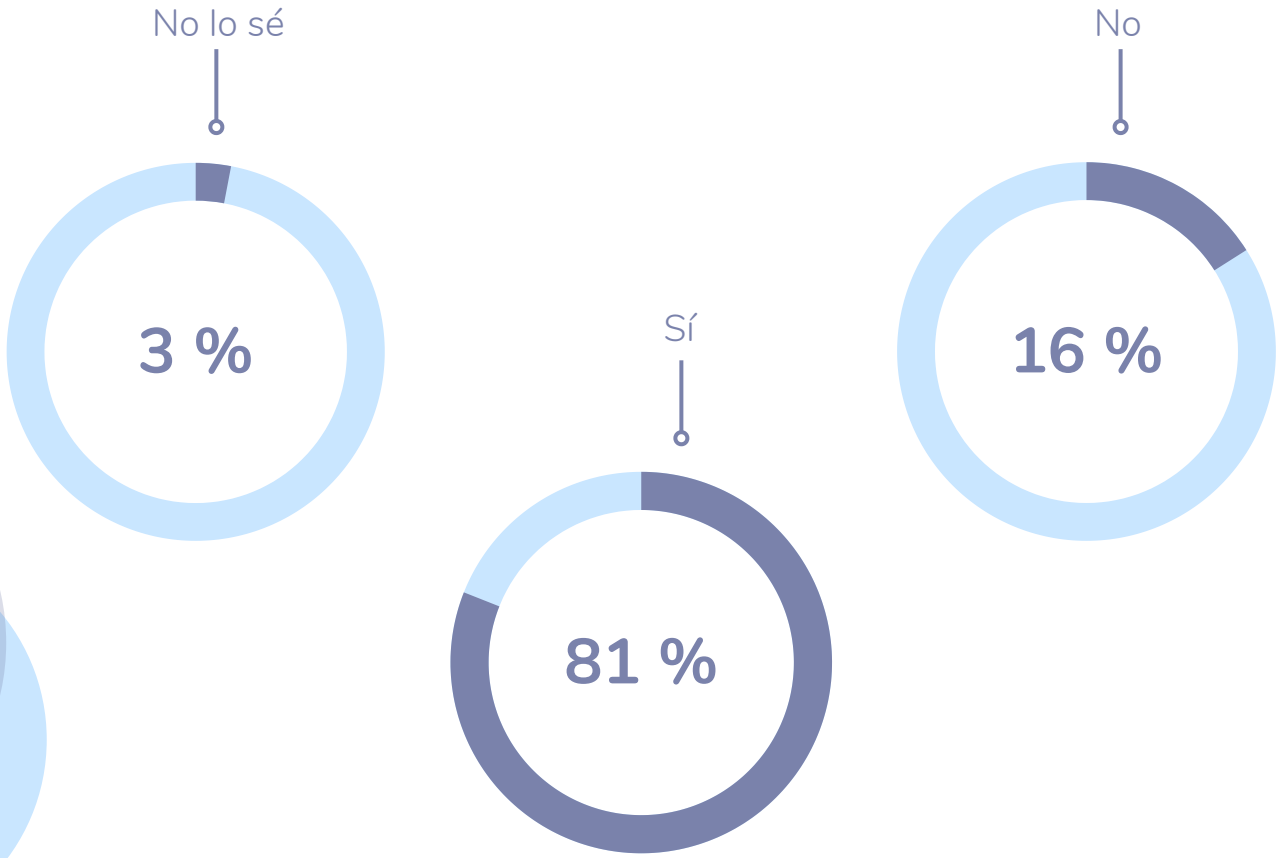
Demostrar que se han tomado medidas técnicas y organizativas es obligatorio. Así lo indica el art.32 del RGPD, que establece la imposición de establecer medidas técnicas y organizativas para acreditar y garantizar la seguridad de los datos personales que se tratan en una empresa. Estas medidas de seguridad tienen como fin último asegurar la integridad y confidencialidad de los datos.

¿Cómo se pueden establecer estas medidas de una forma sencilla? Se recomienda detectar los riesgos en función de los activos de la empresa y así poder identificar desde el inicio las medidas técnicas y organizativas que se deben implementar para cumplir con el RGPD.

La solución de **Pridatect te ayuda a identificar las TOM's mediante un proceso automatizado y con alertas periódicas** que te avisan de cambios en la normativa que te permiten actuar cuando sea necesario. Además, podrás asignar tareas a cada responsable de departamento para implementar acciones de protección de datos en la empresa.

Pregunta 14

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



El 16% de las organizaciones de España involucradas en la encuesta no tienen un protocolo de brechas de seguridad establecido, y por tanto **no cumplen con el RGPD**,

Para evitar multas y asegurar que se hacen las cosas correctamente, **tener un protocolo de respuesta ante un caso de brecha de seguridad es una necesidad absoluta**, un requisito previo para un programa de cumplimiento de protección de datos sólido. La AEPD tiene muy claro que cualquier incumplimiento debe ser reportado a la autoridad supervisora correspondiente dentro de las 72 horas.

Cabe destacar que a nivel **europeo no cuentan con un protocolo de actuación ante brechas de seguridad el 20%** de las empresas.

Una de las preguntas que más pueden plantearse las empresas, es **cuánto tiempo puede pasar desde que se sufre una brecha, hasta que se identifica y se notifica.** Lo cierto es que el tiempo comienza a contar desde que la brecha se ha producido, por lo que contar con un protocolo de actuación facilita siempre las cosas.

Un buen plan de respuesta debe incluir **procedimientos sólidos de detección y notificación de infracciones**, algo que juega un papel importante en la mitigación de daños.
Contar con una **solución que permita llevar a cabo un registro interno** de los incidentes que tengan lugar en la empresa y poder contar con un **modelo para informar** de la brecha de seguridad a los afectados si fuese necesario, también ayudaría a ahorrar tiempo. Comunicar la brecha de una forma adecuada permite **demostrar profesionalidad y transparencia** a clientes, proveedores y a las autoridades correspondientes.

4. FACTORIAL. Así asegura este SaaS la protección de datos

Factorial es un SaaS que permite **realizar toda la gestión y tareas administrativas de RRHH** a un gran número de empresas de diferentes países.

Con Factorial, cualquier empresa puede tener la oportunidad de gestionar online las bajas de los empleados, toda la documentación relativa a contratos o nóminas, controlar el horario y fichaje, así como contar con recursos que permiten evaluar el desempeño de la plantilla. Estas son sólo algunas de las múltiples opciones que permite, y que, inevitablemente, **requieren alojar una gran cantidad de datos personales.**

Todo esto hace que para Factorial, sea fundamental contar con un **óptimo programa de protección de datos.** Además, tienen una serie de factores que requieren tener un especial cuidado con la privacidad de los datos.

Sus clientes prestan mucha atención a la privacidad. Es lógico que quieran tener la certeza de saber qué se va a hacer con documentos tan importantes como sus nóminas. Factorial se esfuerza cada día por poder responder cualquier duda y dar la confianza que necesitan.

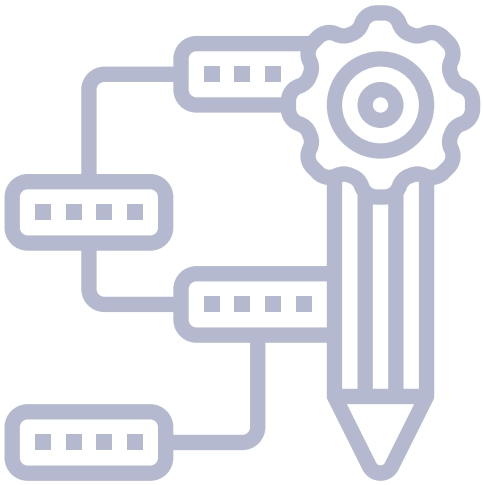
¿Cómo resuelven esta necesidad? Cuentan con el **servicio de DPO** para poder gestionar todas las consultas de clientes y tener al día la protección de datos. Con **Pridatect**, también tienen **automatizados todos los contratos con encargados de tratamiento** para todos los clientes.

En Factorial añadimos constantemente nuevas funcionalidades y alojamos información confidencial, lo que hace que la **privacidad y el cumplimiento** de la normativa sea algo **fundamental**. Hemos encontrado en **Pridatect el partner perfecto como DPO externo**. Además, nos ayuda a implementar un **completo y exitoso programa de protección de datos**

Pau Fernández | CFO en Factorial HR

Por otra parte, dan **mucha importancia a la formación de empleados** en protección de datos. Saben que no pueden poner en riesgo información tan sensible o arriesgarse a tener una **brecha de seguridad por errores o desconocimiento a nivel interno**, por lo que garantizar que se va a cumplir el programa de protección de datos en **cada uno de los departamentos** y que se sabe **qué hacer** para no inclumplir el RGPD es otra de las prioridades de Factorial.

Otro de los aspectos que más dudas puede conllevar, ha sido la reciente implantación de un sistema de fichaje mediante reconocimiento facial, para el que se **utilizan datos biométricos.** Al ser datos considerados como especialmente **sensibles**, necesitan un cuidadoso tratamiento. Para no correr ningún riesgo, con la ayuda de **Pridatect**, Factorial tiene muy en cuenta la obtención del **consentimiento para el tratamiento de los datos desde la fase del diseño,** para así no tener que hacer cambios o evitar costes de rediseño. Además, realizan **evaluaciones de impacto periódicas** y **actualizan** continuamente su **programa de protección de datos**, utilizando el sistema de **tareas automatizadas de Pridatect** para que cada departamento pueda ponerse al día en todo lo relativo a protección de datos.



5. Conclusiones

En este estudio hemos podido comprobar que **la mayoría de las empresas sí son conscientes de que existe una normativa que tienen que cumplir** y que deben velar por la seguridad de los datos, pero que **las acciones que implementan no son siempre las adecuadas** para asegurar la correcta protección de los datos.

Vemos que existe la voluntad y el deseo de cumplir con la legislación de protección de datos, pero las acciones no siempre coinciden por falta de conocimientos y cambios en la normativa (y no tener acceso a un experto), falta de recursos, tanto de tiempo como financieros; un DPO puede parecer costoso, pero la planificación de un plan sólido y llevarlo a cabo requiere mucha mano de obra.

Lisa Hofmann | CLO en Pridatect

Para el 90% de las empresas el cumplimiento es un tema muy importante: el objetivo ha sido a menudo evitar multas, pero la opinión del consumidor es un factor también muy importante. Aun así, el 12% de las empresas no recoge el consentimiento antes de tratar los datos, algo que lleva a incumplir el RGPD y a dar una mala imagen al consumidor.

David Casellas | CEO de Pridatect

La importancia del cumplimiento de la protección de datos desde las **primeras fases de diseño de un SaaS** es algo en lo que más de la mitad de los encuestados coinciden. Es fundamental tener un **amplio conocimiento del RGPD y de todas las recomendaciones** para evitar futuros costes añadidos y errores.

Nos encontramos muchos casos en los que se incumple el RGPD por no aplicar algunas de sus recomendaciones, aunque el objetivo sí sea cumplirlo.

- El 70% de las organizaciones señala que el cumplimiento es muy importante para ellos, pero un 10% no recoge el consentimiento para el tratamiento de datos, un 18% no se preocupa en comprobar si los proveedores externos que contrata cumplen con el RGPD o un 16% no lleva un registro actualizado de actividades de tratamiento.

- Detectamos que no se conocen por completo todos los pasos recomendados, sus beneficios o sus consecuencias.

Asegurar la protección de datos debe de ser una necesidad permanente, algo que a veces se desatiende. Deben prestarse atención a los cambios dentro de la organización que supongan un nuevo tratamiento de datos o a los cambios legislativos.

- Solamente un 27% de los encuestados hace evaluaciones mensualmente o cada 6 meses, dejando a un alto porcentaje de las empresas consultadas ignorando riesgos que pueden detectarse demasiado tarde.

- Casi la mitad de los encuestados no hace una formación en protección de datos con una frecuencia alta, a pesar de ser la clave para lograr el cumplimiento y debe realizarse con la frecuencia necesaria para atender a todos los cambios organizativos.

No contar con un correcto protocolo de protección de datos en el que se contemplen todos los riesgos y medidas necesarias puede tener fatales consecuencias.

- Un 16% tiene un protocolo de actuación ante una posible brecha de datos, mientras que un 3% no sabe si lo tiene. Hay que tener en cuenta que nunca se está exento de riesgos y que todas las medidas preventivas influyen a la hora de actuar para evitar o mitigar los posibles daños.

- Hemos detectado que existe un desconocimiento sobre lo que se está haciendo en otros departamentos de la empresa respecto a la protección de datos, incluso hemos podido observar que un 7% no sabe qué tipos de datos se tratan. Esto es algo que responsables legales y directivos tienen que evitar, siendo los primeros que deben estar implicados en la protección de datos y ofrecer medidas y recursos para la formación y prevención.

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

DETECTAR E IDENTIFICAR RIESGOS

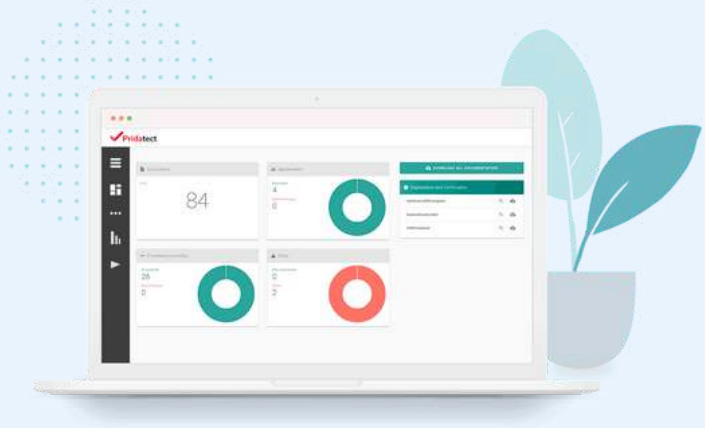
Detecta e identifica los riesgos en tu tratamiento de datos personales (clientes, empleados, proveedores..). Con la plataforma de Pridatect podemos identificar y analizar, las amenazas y vulnerabilidades en tus procesos.

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 de 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