

CÓMO CREAR UN PROGRAMA DE PROTECCIÓN DE DATOS CON ÉXITO



✓ Pridatect

Contenido

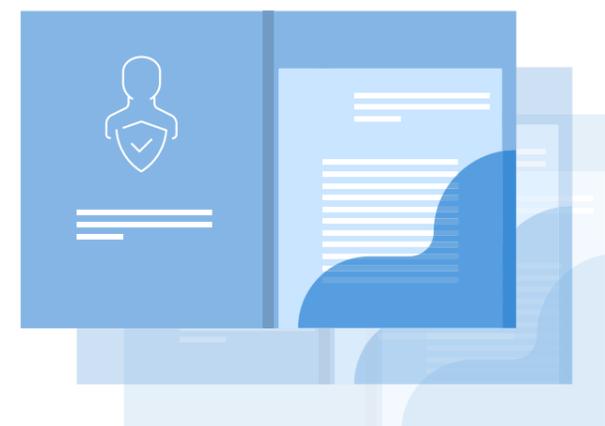
01	Introducción	
02	Pasos para crear un programa exitoso	
	a) Conocer las actividades que realiza la empresa.....	4
	b) Analizar los riesgos existentes.....	5
	c) Valora la necesidad de designar a un DPO	6
	d) Identificar las empresas que prestan servicios y tienen acceso a datos.....	7
	e) Informa a los interesados.....	8
	f) Dar una buena formación a la empresa y los empleados.....	9
03	Conclusión	

01. Introducción

La clave para realizar un buen programa de protección de datos es ser metodoso y seguir los pasos que se describen a continuación.

Sin embargo, debemos recordar que las organizaciones son entes cambiantes por lo que el verdadero éxito al realizar un programa de protección de datos radicará en realizar un seguimiento de la misma, a fin de mantenerse siempre actualizado.

A modo de ejemplo, si se listan los empleados de una empresa para saber qué personas tienen acceso a los datos personales, se deberá actualizar cada vez que haya un cambio en el personal de la empresa. De esta forma, se podrán depurar responsabilidades si se produce una brecha de seguridad. No es suficiente con actualizar el programa de protección de datos una vez al año, se deberá ir modificando periódicamente.



02. Pasos para crear un programa exitoso

Por tanto, los pasos que describimos a continuación deberán realizarse de forma cíclica:

a) Conocer las actividades que realiza la empresa

Como consultor en materia de protección de datos es fundamental que conozcas en profundidad la empresa a la que le vas a realizar el programa de cumplimiento.

Deberás conocer las actividades que realiza a fin de conocer cómo trata los datos personales.



Por ejemplo, no tratan los mismos datos un hospital que una comunidad de propietarios: en el primer caso se tratará una gran cantidad de datos entre los que se encontrarán datos especialmente protegidos como los datos de salud o de menores de edad, mientras que una comunidad de propietarios trata menos datos personales y no tan sensibles.

Una vez identificadas las actividades de tratamiento, se deberá realizar el registro previsto en el artículo 30 del RGPD, teniendo en cuenta qué actividades realiza la empresa como responsable, corresponsable, encargado o subencargado del tratamiento.

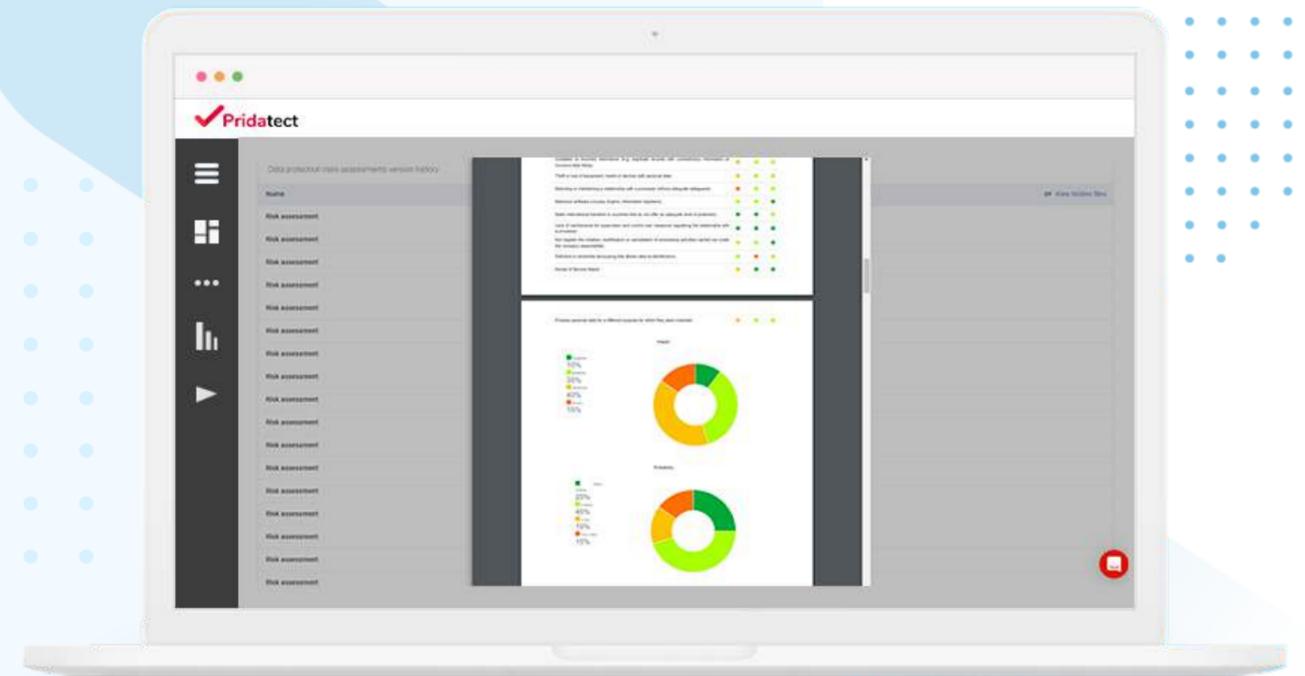
Realizar el registro de actividades de tratamiento o RAT será un paso fundamental a la hora de identificar las bases de legitimación de cada tratamiento, la duración de los mismos, sus finalidades, la existencia de transferencias internacionales, etc.

b) Analizar los riesgos existentes

Se deberá realizar un análisis de los riesgos que puedan afectar a las actividades de tratamiento a fin de poder dar medidas de seguridad adecuadas a cada escenario de riesgo.

Es fundamental identificar correctamente qué medidas deben aplicar, siendo coherentes con el tamaño de la empresa, el estado de la técnica y los riesgos que se han identificado. Las medidas implementadas deben ser preventivas, de contención y correctivas, pudiendo diferenciar entre medidas técnicas y organizativas.

En algunos casos, las empresas deberán realizar una evaluación de impacto. Un análisis previo de los riesgos te ayudará a determinar si es el caso de tu empresa.

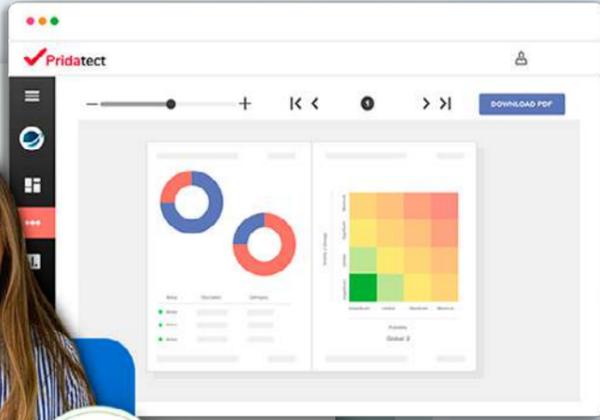


c) Valora la necesidad de designar a un DPO

El RGPD obliga a designar a un DPO en los casos establecidos en el art. 37:

- Si el tratamiento lo lleva a cabo una autoridad u organismo público.
- Cuando la actividad principal de la organización implica una observación habitual y sistemática de interesados a gran escala.
- Cuando las actividades principales de la organización consistan en el tratamiento a gran escala de categorías especiales de datos personales.

Aún así, en los casos en que no sea obligatorio será más que recomendable designar un DPO, la empresa puede beneficiarse de contar con esta figura para supervisar el cumplimiento.



¡Hola! Soy Eva y voy a ayudarte a saber si estás obligado a contar con un DPO. Antes de nada, ¿cuál es tu nombre?

Escribe aquí tu respuesta...

EMPEZAR TEST

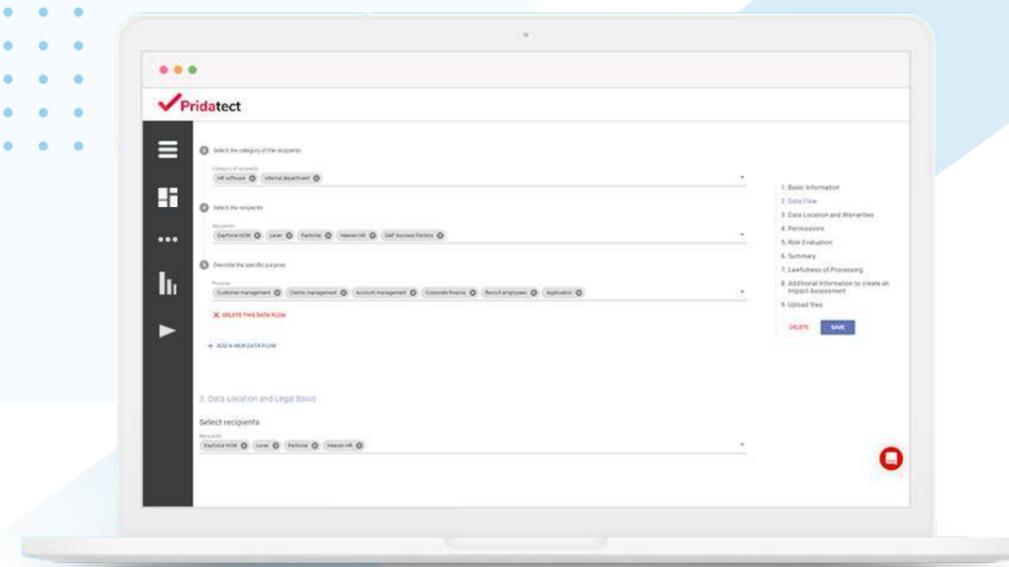
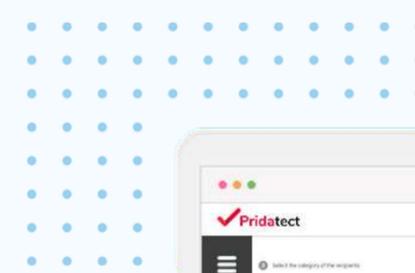
d) Identificar las empresas que prestan servicios y tienen acceso a datos

Otro punto muy importante para garantizar la seguridad del tratamiento de datos es identificar qué empresas u organizaciones prestan servicios y acceden a datos, a fin de categorizarlas como encargados del tratamiento, destinatarios o cesionarios.

Identificar estas empresas también ayudará a definir si existen o no transferencias internacionales de datos y si se aplican las garantías que permiten transferir datos fuera de la UE.

Será necesario establecer los acuerdos o contratos para el tratamiento de datos por parte de terceros y deconfidencialidad en la prestación de servicios. No se podrá contar con encargados de tratamiento que no accedan a firmar dichos acuerdos o que no cumplan con las medidas establecidas en los mismos

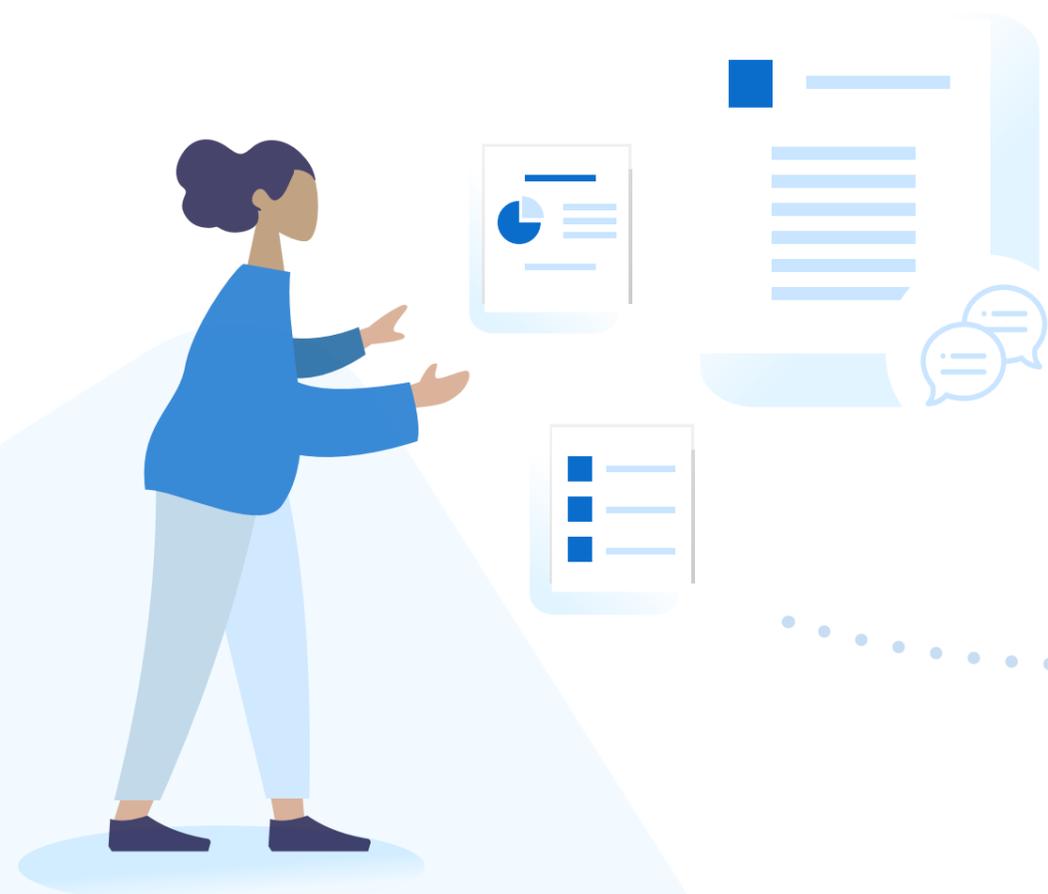
ni tampoco podrán realizarse transferencias internacionales de datos sin sus correspondientes garantías, por lo que la organización deberá ser especialmente cuidadoso en la selección de proveedores e incluso tendría que dejar de trabajar con algunos de ellos si no le garantiza el cumplimiento.



e) Informa a los interesados

La **obligación más importante que impone el Reglamento** es la de **informar** a los interesados sobre el tratamiento de sus datos. Esta obligación deberá llevarse a cabo en el momento de la recogida del dato.

Es especialmente relevante la necesidad de informar en las comunicaciones comerciales o en los datos recabados de forma online. Una buena praxis para realizar un programa de protección de datos exitoso es informar mediante una doble capa: dar una primera capa de información básica e incluir un enlace con la información adicional. De esta forma, incluso cuando el usuario no acceda a la segunda capa tendrá una vista general de la información básica.



f) Dar una buena formación a la empresa y los empleados

Por último, uno de los puntos cruciales para que la empresa u organización cumpla con la protección de datos es **dar formación** a todas las personas que forman parte de la misma a fin de que conozcan cómo deben tratar los datos, cómo actuar ante una brecha de seguridad o cómo gestionar una petición de derechos

Este punto es el que hará que la organización tenga una política y una cultura de **compliance** adecuada.



03. Conclusión



Un buen programa de protección de datos deberá ser completo y cubrir con todas las obligaciones que impone la normativa así como garantizar todos los derechos de las personas físicas. Todo ello se materializa en los pasos que hemos visto, los cuales deberán repetirse de forma periódica.



Si bien el RGPD no establece ningún plazo de tiempo para realizar auditorías, será muy beneficioso realizarlas para así poder comprobar que la empresa mantiene el cumplimiento y ha implementado todas las medidas recomendadas.



Como ocurre siempre, lo más importante para que un programa de protección de datos sea exitoso son las personas. Por lo que sería importante formar a cada nuevo empleado e ir haciendo pequeñas formaciones cada cierto tiempo. Hay que tener en cuenta que los errores humanos son una de las causas más comunes de la brecha de seguridad e incluso estos pueden evitarse o reducirse gracias a una buena formación.



Asimismo, una buena forma de realizar un programa de protección de datos es utilizar un software como Pridatect que facilitará todos aquellos procesos repetitivos y que requieren de mayor detalle.

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.



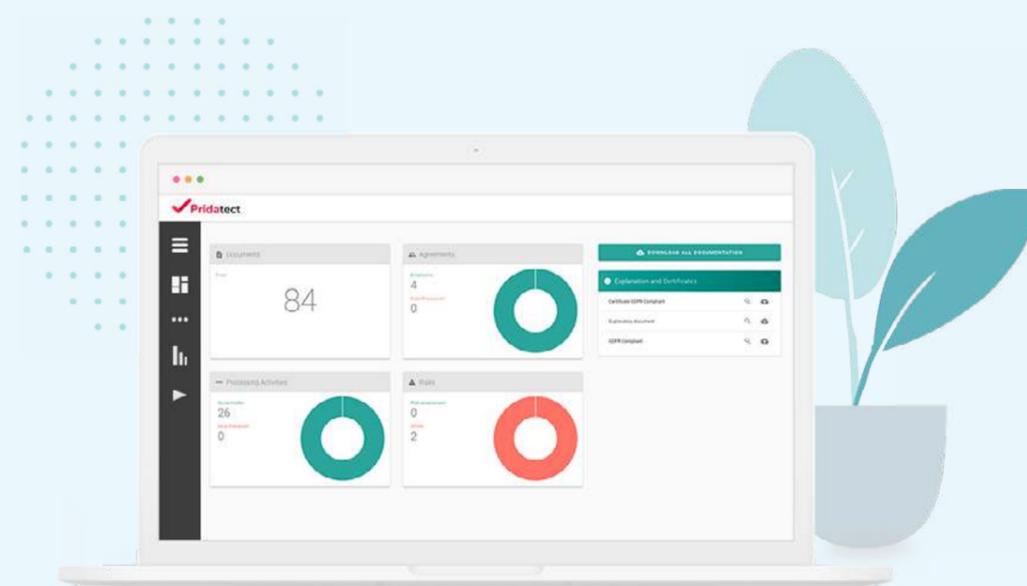
DEFINIR Y SUGERIR MEDIDAS

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