

# Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos (RGPD) es un reglamento de la Unión Europea (UE) que establece un nuevo marco legal para gestionar y proteger los datos personales de los residentes de la UE.

Presenta nuevas obligaciones y responsabilidades para todas las empresas que gestionen este tipo de datos, además de nuevos derechos de las personas físicas sobre cómo deben recogerse, procesarse y almacenarse sus datos.

## Impacto del RGPD

Si tu empresa tiene que cumplir la RGPD, hay una serie de factores que deberías tener en cuenta. Te recomendamos encarecidamente que cuentes con un asesor legal para determinar qué se puede llegar a necesitar en tu situación particular.

### 1. Entender los datos

Proteger los datos significa entender cómo se tratan en tu empresa; es decir, cómo se gestionan, comparten, utilizan, archivan y eliminan los datos personales. A la hora de desarrollar la estrategia del RGPD en tu empresa, es vital entender qué son estos datos y cómo deben utilizarse y guardarse.

### 2. Definir la propiedad y la responsabilidad

Es importante nombrar a un propietario responsable del cumplimiento de la protección de datos. En el caso de algunas empresas, es obligatorio designar un responsable de la protección de datos. El RGPD también presenta un nuevo principio de "responsabilidad" que exige que las empresas adopten un programa de cumplimiento de protección de datos. Esto significa que tienen que desarrollar políticas internas de protección de datos que garanticen dicha seguridad, además de formar a sus empleados.

### 3. Garantizar una base legal para el procesamiento de datos

Otro componente del RGPD que deben documentar las empresas es el aspecto legal relativo al procesamiento de los diferentes tipos de datos personales que se gestionan. Por ejemplo, si utilizas el consentimiento como base de dicho procesamiento, tendrás que plantearte cómo lo obtienes y poder demostrar claramente cómo y cuándo se da.

### 4. Entender los derechos de los interesados

Para asegurarte de que tus procedimientos se ajustan a los usuarios, tendrás que entender muy bien los derechos que tienen las personas sobre sus datos personales. Por ejemplo, los interesados tienen el derecho de acceder a sus datos personales, así como a corregirlos, eliminarlos o exportarlos de forma electrónica. En determinadas circunstancias, también tienen el derecho a oponerse a la toma de decisiones automatizada y a la realización de perfiles.

### 5. Asegurar la privacidad desde el diseño

Es la primera vez que la privacidad es un requisito legal explícito, por lo que es importante empezar a considerar cómo implementarla en tus procesos de negocio. En algunos casos, resulta necesario llevar a cabo evaluaciones de impacto de la privacidad.

### 6. Prepararse para gestionar las brechas de datos

A la hora de tener un programa de protección de datos sólido, es fundamental asegurarse de que las políticas y procesos de gestión de las brechas de datos están actualizadas y probadas. Detectar e informar de las brechas a las autoridades designadas en el momento adecuado es un requisito del RGPD. Las multas pueden deberse tanto a las brechas en sí mismas como a la falta de diligencia a la hora de informar de las mismas.

### 7. Comunicar la información básica

Esto se refiere a la importancia que tiene que las políticas de privacidad en línea de la empresa, así como otro tipo de advertencias, estén al día y reflejen las prácticas en materia de protección de datos. Entre los nuevos requisitos se incluye el desglose de la base legal de tu proceso y la necesidad de conseguir que los usuarios sean conscientes de la autoridad que tienen en caso de que se produzca algún problema.

### 8. Trabajar con tus proveedores

Cumplir con las obligaciones del RGPD va mucho más allá de cumplir las políticas propias de tu empresa. Aquellas terceras partes que procesen datos personales en tu nombre también tendrán que cumplir los estándares necesarios a la hora de protegerlos. Plantéate hacer estas preguntas a tus proveedores:

- ¿Son sólidas tus prácticas relativas a la red y la seguridad de la información, la privacidad y la protección de datos?
- ¿Trabajas de acuerdo a los estándares aceptados a nivel internacional y verificas su cumplimiento?
- ¿Cómo puedes demostrar que en efecto tienes una cultura fuerte de confianza y seguridad? ¿Y qué controles ofreces para ayudarme a gestionar mis datos y cumplir con mis obligaciones como encargado del tratamiento de los datos?



## En Dropbox protegemos tus datos

### La confianza es la base de nuestra relación con millones de personas y empresas de todo el mundo.

Valoramos la confianza que has depositado en nosotros y nos tomamos muy en serio la responsabilidad de proteger tu información. Para ser merecedores de tu confianza, el diseño y las mejoras de Dropbox se centran en gran medida en la seguridad, la conformidad y la privacidad.

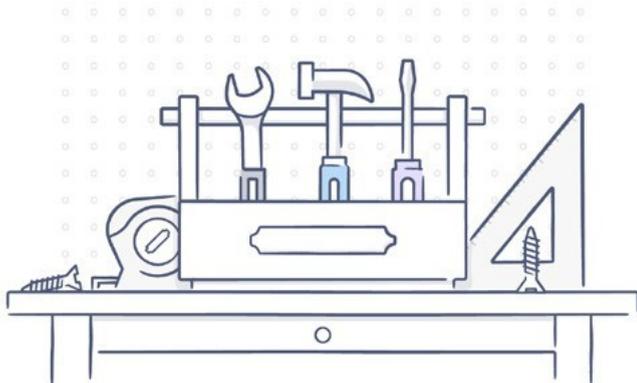
### Seguridad: Protección y control

#### Protección: Arquitectura y seguridad de la información

Dropbox se ha diseñado con una infraestructura segura, distribuida y con numerosas capas de protección, como la transferencia segura de datos, el cifrado, la configuración de red y los controles a niveles de aplicación distribuidos sobre una infraestructura escalable y segura. Nuestro marco de gestión de seguridad de la información es muy sólido y se ha creado para evaluar los riesgos y desarrollar una cultura en torno a la seguridad. Revisamos y actualizamos con frecuencia nuestras políticas de seguridad; ofrecemos a nuestros empleados formación en materia de seguridad; llevamos a cabo pruebas relacionadas con la seguridad de la red y la aplicación (como la prueba de penetración); realizamos evaluaciones de los riesgos; y monitorizamos el cumplimiento de este tipo de políticas. Puedes encontrar más información en nuestro [Informe técnico sobre la seguridad de Dropbox Business](#).

#### Control: Capacitar a los administradores TI

Dropbox ofrece las funciones de [control y visibilidad](#) que los administradores TI necesitan, lo cual te ayuda a gestionar el cumplimiento con las obligaciones fácilmente. Nuestro panel para administradores te permite monitorizar la actividad del equipo, ver los dispositivos conectados y revisar cómo se comparte el contenido. Puedes crear grupos para gestionar fácilmente el acceso de los miembros del equipo a carpetas específicas. Por otra parte, el gestor de carpetas de equipo te aporta la visibilidad y el control que buscas sobre las carpetas de equipo, incluida la gestión de la sincronización. La función que regula los permisos de los enlaces te ofrece la posibilidad de proteger con contraseña los enlaces compartidos, establecer fechas de vencimiento para otorgar acceso temporal y limitar el acceso para que solo puedan entrar personas de tu empresa. Nuestra herramienta de transferencia de cuentas te permite transferir archivos fácilmente desde un usuario a otro cuando cambien las responsabilidades. El borrado remoto facilita la eliminación de archivos desde dispositivos robados o perdidos.



### Conformidad: Confianza y verificación

La conformidad permite validar la fiabilidad de los servicios. Te animamos, y esperamos que así lo hagas, a que [verifiques](#) que nuestras prácticas de seguridad cumplen con los [estándares](#) más aceptados [y con normativas](#) como ISO 27001, y SOC 1, 2 y 3. Nuestros auditores externos independientes realizan comprobaciones de nuestros controles y ponen a nuestra disposición sus informes y opiniones, que compartimos contigo siempre que sea posible. Puedes consultar más información sobre los estándares que cumplimos y la forma en la que verificamos nuestras prácticas de seguridad en nuestra página web de [cumplimiento](#).

### Privacidad: Nuestro compromiso

Eres dueño de tus propios datos, ya sean profesionales o personales, y nos tomamos la confianza de nuestros usuarios muy en serio, trabajando muy duro para asegurarnos de que todos los datos que hay en nuestro sistema están protegidos. Nuestra [Política de privacidad](#) describe de forma clara cómo gestionamos y protegemos la información. Publicamos un [informe de transparencia](#) y nuestras principios respecto a las solicitudes de datos por parte [del sector público](#) para compartir con qué frecuencia recibimos, revisamos y respondemos a dichas solicitudes; y, además, también tratamos de reformar las leyes para que protejan mejor tu seguridad.

### Trabajamos juntos para garantizar la seguridad de tus datos

En Dropbox trabajamos con nuestros clientes profesionales para mantener sus datos a salvo. Tomamos amplias medidas para proteger nuestra infraestructura, red y aplicaciones; formamos a nuestros empleados en materia de prácticas de seguridad y privacidad; desarrollamos una cultura donde la prioridad es ser dignos de confianza; y contamos con terceros que prueban y auditan nuestros sistemas y prácticas. Los clientes también juegan un papel fundamental a la hora de asegurar que sus equipos y datos están protegidos y seguros. En ese sentido, Dropbox te permite configurar, utilizar y monitorizar tu cuenta de forma que cumpla con las necesidades de cumplimiento, seguridad, privacidad de tu empresa. Nuestra [guía de responsabilidad compartida](#) puede ayudarte a entender mejor qué hacemos para mantener a salvo tu cuenta y qué acciones puedes llevar a cabo para mantener la visibilidad y el control sobre los datos de tu equipo.

Los contenidos de esta guía pretenden facilitar el acceso a la información, pero no son consejos legales. Es posible que los lectores tengan que contratar a sus propios asesores legales.

