Dropbox

Privacidad y protección de datos

Introducción

Los datos personales juegan un papel muy importante en nuestra sociedad y economía. Cada vez más, buscamos un mayor control y claridad sobre cómo se gestionan y protegen los datos personales en las empresas con las que interactuamos. Al mismo tiempo, se espera que las empresas ofrezcan directrices claras sobre cómo proteger estos datos personales.

En Dropbox, la confianza es la base de nuestra relación con millones de personas y negocios de todo el mundo. Valoramos la confianza que has depositado en nosotros y nos tomamos muy en serio la responsabilidad de proteger tus datos personales.

Nuestro compromiso contigo

Nos comprometemos a proteger tus datos personales. En las Condiciones del servicio de Dropbox encontrarás tus responsabilidades a la hora de utilizar nuestros servicios. Además, en la Política de privacidad se describen nuestros compromisos en materia de privacidad con los usuarios y se explica cómo recogemos, usamos y tratamos tus datos personales cuando utilizas nuestros servicios. Si eres residente de la Unión Europea (UE), la oficina responsable de tus datos personales es la Dropbox International Unlimited Company, con sede en Irlanda.

Si eres usuario de Dropbox Business o Dropbox Education, tu empresa actúa como responsable de los datos para todo tipo de datos entregados a Dropbox que estén relacionados con el uso de Dropbox Business o Dropbox Education. Es el responsable de los datos el encargado de determinar el objetivo y los medios para procesar los datos personales. Dropbox se encarga del procesamiento, puesto que procesa los datos en nombre de tu empresa cuando haces uso de Dropbox Business o Dropbox Education. Y, por último, en nuestro Acuerdo empresarial se recogen nuestros compromisos relacionados con el procesamiento de datos y la transferencia internacional de datos.

Nuestro registro: cumplimiento

La conformidad normativa es una manera muy efectiva que tienen las empresas de demostrar que sus servicios son dignos de confianza. Estamos siempre dispuestos a compartir las verificaciones independientes que demuestran que nuestras prácticas de seguridad y privacidad cumplen con estándares y regulaciones ampliamente aceptados, como la ISO 27001, ISO 27017, ISO 27018, BSI C5 en Alemania y SOC 1, 2 y 3. Por ejemplo, fuimos uno de los primeros proveedores de servicios en la nube en conseguir la certificación ISO 27018, un estándar internacionalmente reconocido relacionado con las prácticas de privacidad en la nube y protección de datos. Nuestros auditores independientes llevan a cabo evaluaciones sobre nuestros controles y redactan informes con su opinión. Trataremos de compartirlos contigo cuando sea posible.

Ten en cuenta que, aunque la mayoría de las certificaciones e informes de auditoría se refieren a Dropbox Business y Dropbox Education, la mayoría de los controles se aplican a usuarios de Dropbox Basic, Plus y Professional. En la sección de nuestra página web sobre cumplimiento, encontrarás más información sobre los estándares que cumplimos y cómo verificamos nuestras prácticas.

Para obtener información detallada sobre las políticas y las funciones de seguridad de Dropbox, consulta el Informe de seguridad de Dropbox Business o ponte en contacto con sales@dropbox.com.

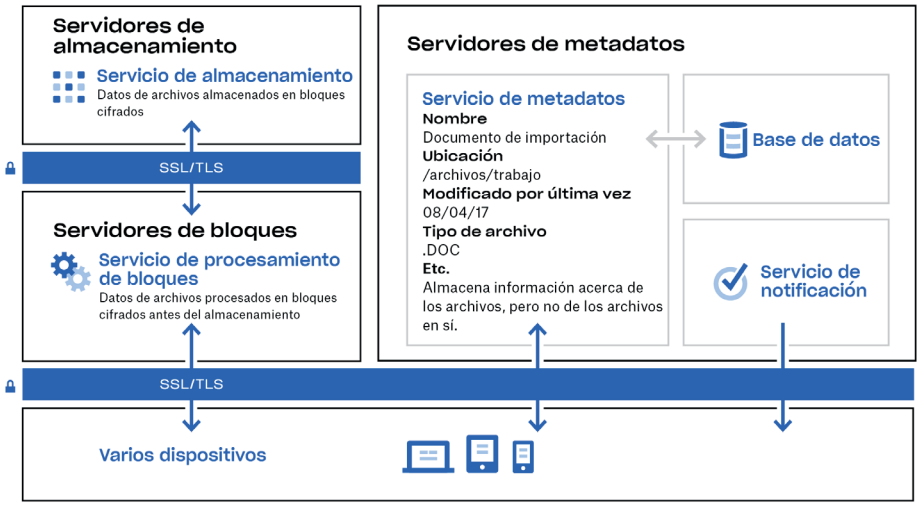
Dropbox

Arquitectura de Dropbox: protegemos tus datos personales

En Dropbox, creemos que el primer paso para proteger tus datos personales es mantenerlos a salvo. Para conseguirlo, Dropbox se ha diseñado con varias capas de protección que incluyen transferencia de datos segura, cifrado y controles a nivel de aplicación. Todas estas capas están distribuidas en una infraestructura segura y ampliable.

Nuestra infraestructura: archivos

En el caso de los archivos, la infraestructura de Dropbox se compone de los elementos que se exponen en el diagrama que se presenta a continuación.



Servidores de bloque

Gracias a su diseño, Dropbox proporciona un mecanismo de seguridad único que no se limita al cifrado tradicional para proteger los datos de los usuarios. Los servicios de cifrado procesan archivos de las aplicaciones de Dropbox dividiéndolos en bloques, cifrando cada bloque con códigos seguros y sincronizando únicamente aquellos que se hayan modificado entre una revisión y otra. Cuando una aplicación de Dropbox detecta un archivo nuevo o cambios en un archivo existente, notifica el cambio a los servidores de bloque y los bloques de archivo nuevos o modificados se procesan y se transfieren a los servidores de almacenamiento.

Servicio de notificación

Este servicio independiente está dedicado a supervisar si se han realizado cambios o no en las cuentas de Dropbox. Aquí no se almacenan ni se transfieren archivos ni metadatos. Cada cliente establece una conexión prolongada de consulta con el servicio de notificación y espera. Cuando se produce un cambio en cualquier archivo de Dropbox, el servicio de notificación señala un cambio a los clientes pertinentes cerrando la sesión de consulta. El cierre de conexión sirve como señal de que el cliente debe conectarse de forma segura a los servidores de metadatos para sincronizar los cambios.

Servidores de metadatos

Los metadatos, es decir la información básica, se conserva en un servicio de almacenamiento propio y discreto que actúa como un índice para los datos de las cuentas de los usuarios. Los metadatos de Dropbox se almacenan en un servicio de base de datos respaldado por MySQL y se fragmentan y replican según sea necesario para cumplir los requisitos de rendimiento y alta disponibilidad. Entre los metadatos se incluye información básica del usuario y la cuenta, como la dirección de correo electrónico, el nombre y los nombres de los dispositivos. También se incluye información básica sobre los archivos como sus nombres y tipos, lo que hace que se puedan usar funciones como el historial, la recuperación y la sincronización de versiones.

Servidores de almacenamiento

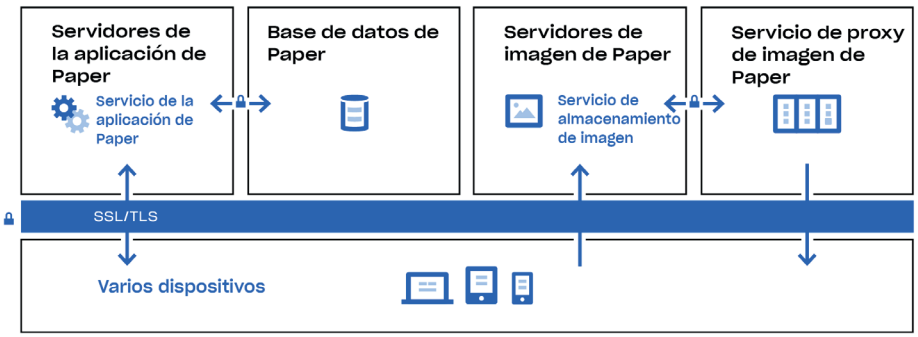
Cuando los servidores de cifrado ya han dividido y cifrado los archivos, los contenidos de estos bloques de archivo se almacenan en los servidores de almacenamiento. Los servidores de almacenamiento actúan como un sistema de almacenamiento de contenido direccionable (en inglés, Content-Addressable Storage o CAS) y cada bloque de archivo cifrado se recupera según su valor de hash.

Para obtener información detallada sobre las políticas y las funciones de seguridad de Dropbox, consulta el Informe de seguridad de Dropbox Business o ponte en contacto con sales@dropbox.com.

Dropbox

Nuestra infraestructura: Paper

Dropbox Paper (también conocido como Paper) es una función del producto Dropbox. Sin embargo, Paper hace uso de un conjunto de sistemas diferentes dentro del entorno de infraestructura de Dropbox. En el caso de los archivos, la infraestructura de Paper se compone de los elementos que se exponen a continuación en el diagrama.



Servidores de la aplicación de Paper

Los servidores de la aplicación de Paper procesan solicitudes de usuario, devuelven el resultado de documentos de Paper editados al usuario y llevan a cabo los servicios de notificación. Los servidores de la aplicación de Paper escriben las ediciones entrantes del usuario en las bases de datos de Paper y, una vez allí, se colocan en un almacenamiento persistente. Las sesiones de comunicación entre los servidores de la aplicación de Paper y las bases de datos de Paper se cifran utilizando un cifrado sólido.

Servicio de proxy de Paper Image

El servicio de proxy de Paper Image ofrece vistas previas de imagen tanto para imágenes subidas a documentos de Paper como hiperenlaces incrustados dentro de documentos de Paper. Cuando se suben imágenes a documentos Paper, el servicio proxy de Paper Image busca los datos de imagen almacenados en los servidores de imagen de Paper a través de un canal cifrado. En el caso de los hiperenlaces incrustados en documentos de Paper, el servicio proxy de imágenes de Paper busca los datos de imagen en el enlace de la fuente e interpreta una vista previa de la imagen mediante HTTP o HTTPS, según especifique el enlace de la fuente.

Bases de datos de Paper

Los contenidos reales de los documentos de Paper de los usuarios, así como ciertos metadatos de estos documentos de Paper, se cifran en un almacenamiento persistente en las bases de datos de Paper. Esto incluye información sobre un documento de Paper (como el título, pertenencia y permisos compartidos, asociaciones de carpetas y proyectos, y otro tipo de información), así como contenido dentro del propio documento de Paper, como comentarios y tareas. Las bases de datos de Paper se fragmentan y replican tanto como se necesite para cumplir los requisitos de rendimiento y alta disponibilidad.

Los servidores de las imágenes de Paper

Las imágenes subidas a los documentos de Paper se almacenan y cifran en reposo en los servidores de Paper Images. La transmisión de datos de imagen entre la aplicación de Paper y los servidores de imagen de Paper tiene lugar en una sesión cifrada.

Para obtener información detallada sobre las políticas y las funciones de seguridad de Dropbox, consulta el Informe de seguridad de Dropbox Business o ponte en contacto con sales@dropbox.com.

Dropbox

Controles de Dropbox: nuestras prácticas internas

Adoptamos medidas integrales para proteger nuestra infraestructura, nuestra red y nuestras aplicaciones; formamos a nuestros empleados en las prácticas de seguridad y privacidad; y creamos una cultura en la que ser digno de confianza es la máxima prioridad. A continuación, describimos algunos de los controles que llevamos a cabo.

Formación

Parte de nuestro trabajo a la hora de proteger los datos personales de nuestros usuarios implica desarrollar y contribuir al crecimiento de una cultura en la que la seguridad y la privacidad sean muy importantes. Nuestros empleados deben estar de acuerdo con las políticas de seguridad para trabajar con nosotros, lo cual incluye una política de privacidad de datos del usuario, antes incluso de darle acceso al sistema. Nuestros empleados también deben formarse de forma obligatoria en materia de seguridad y privacidad, cuando se incorporen y, posteriormente, de forma periódica. Reciben, además, otro tipo de formación a través de correos informativos, charlas, presentaciones y recursos disponibles en nuestra intranet.

Cifrado en tránsito

Para proteger los datos en tránsito entre el cliente de Dropbox (actualmente de escritorio, móvil, API o web) y los servidores front-end de Dropbox, se negocia una conexión cifrada para asegurar una entrega segura. De forma similar, se negocia una conexión cifrada para proteger los datos de documentos de Paper en tránsito entre el cliente de Paper (actualmente de escritorio, móvil, API o web) y el servicio hospedado. Estas conexiones se cifran con Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para crear un túnel seguro protegido por un cifrado con Advanced Encryption Standard (AES) de 128 bits o superior.

Cifrado en reposo

Los archivos que suben los usuarios se almacenan en los servidores de almacenamiento de Dropbox como bloques de archivo discretos. Cada bloque se cifra usando el estándar Advanced Encryption Standard (AES) de 256 bits. Solo se sincronizan los bloques que se hayan modificado desde la versión anterior. De forma similar, los datos de los documentos de Paper de las bases de datos de Paper también se cifran en reposo usando un estándar Advanced Encryption Standard (AES) de 256 bits.

Borrado permanente de archivos y documentos Paper

Cuando un usuario de Dropbox, un administrador de Dropbox Business o un equipo de Dropbox Education marcan un archivo para que se elimine de forma permanente, desencadenan un proceso que provoca este resultado. De la misma forma, cuando un usuario, administrador de Dropbox Business o equipo de Dropbox Education marcan un documento de Paper para eliminarlo, tiene lugar un proceso parecido que lleva a la eliminación de los datos del documento e imágenes de Paper.

Solicitudes de acceso a datos personales

Para obtener más información sobre cómo se almacenan los archivos y documentos de Paper con Dropbox, los usuarios pueden iniciar sesión en la web y visitar la página de su cuenta. Allí encontrarán más detalles como el nombre y el correo electrónico asociado a su cuenta. Además, pueden ver las direcciones IP de las sesiones conectadas, ordenadores y dispositivos móviles, así como aplicaciones conectadas a sus cuentas, concretamente en las páginas de seguridad y aplicaciones conectadas.

Los usuarios de Dropbox tienen la capacidad de solicitar acceso o eliminar otros datos personales que hayamos recogido. En el Centro de ayuda podrán encontrar más información al respecto.

Para obtener información detallada sobre las políticas y las funciones de seguridad de Dropbox, consulta el Informe de seguridad de Dropbox Business o ponte en contacto con sales@dropbox.com.

Dropbox

Principios de solicitud de datos por parte de los gobiernos

Creemos que, si los usuarios nos confían sus datos, esperan de nosotros confidencialidad absoluta. Como muchos servicios en línea, Dropbox recibe a menudo solicitudes por parte de los gobiernos en referencia a los datos de nuestros usuarios.

Estos principios detallados a continuación describen cómo gestionamos las solicitudes gubernamentales que recibimos.

Ser transparentes

Creemos que nuestros servicios en línea deberían obtener permiso para publicar el número y tipos de solicitudes gubernamentales recibidas y notificar a los interesados cuando se ha solicitado información sobre ellos mismos. Este tipo de transparencia le otorga poder a los usuarios ayudándoles a entender mejor algunos ejemplos y patrones en los que los gobiernos se extralimitan. Continuaremos publicando información detallada sobre estas solicitudes y defenderemos el derecho a ofrecer este tipo de información tan importante.

Defensa contra las peticiones de carácter amplio

Las peticiones de datos por parte de los gobiernos deberían limitarse a la información que buscan y a una serie de personas específicas e investigaciones legítimas. Nos oponemos a las peticiones arbitrarias y de carácter amplio.

Ofrecer servicios de confianza

Los gobiernos no deberían instalar "puertas traseras" en servicios de Internet ni poner en peligro las infraestructuras para obtener datos de los usuarios. Seguiremos esforzándonos para proteger nuestros sistemas y cambiar las leyes vigentes con el fin de dejar claro que estas actividades son ilegales.

Proteger a todos los usuarios

Las leyes que otorgan protección a las personas según dónde residan o dónde tengan su ciudadanía están anticuadas y no reflejan la naturaleza global de los servicios en línea. Seguiremos defendiendo la reforma de estas leyes.

Estos principios, así como nuestro informe anual de transparencia, están publicados en la web de Dropbox: https://www.dropbox.com/transparency.

Para obtener más detalles sobre los controles y nuestro enfoque a la hora de proteger tus datos personales, consulta el Informe Técnico sobre seguridad de Dropbox.

El caso de las personas que trabajan para Dropbox

Dropbox gestiona la mayoría de actividades relacionadas con el aprovisionamiento de nuestro servicios; sin embargo, contamos con terceras partes de confianza a la hora de ofrecer nuestros servicios (por ejemplo, proveedores que nos ofrecen atención al cliente y servicio de TI). Estas terceras partes solo tendrán acceso a tu información para llevar a cabo tareas en nuestro nombre y en cumplimiento con nuestra Política de privacidad. En este caso, nosotros seguiremos siendo responsables del tratamiento de tu información de acuerdo con nuestras propias instrucciones. Todos los proveedores externos pasan un riguroso proceso de investigación, que incluye revisiones de seguridad y revisiones contractuales periódicas para evaluar su capacidad de cumplir con nuestros requisitos de protección de datos.

Transferencias internacionales de datos

Dropbox confía en una serie de mecanismos legales a la hora de transferir datos personales a nivel internacional, de la UE a Estados Unidos. Disponemos de la certificación en los programas Privacy Shield entre la UE y Estados Unidos y Suiza y Estados Unidos en relación a la recogida, uso y retención de los datos personales y su transferencia entre la UE y Suiza a los Estados Unidos. Además del Privacy Shield, Dropbox también ofrece garantías con respecto a la privacidad de sus servicios y confía en las cláusulas del modelo contractual de la UE para cubrir las transferencias de datos a nivel internacional.

Para obtener información detallada sobre las políticas y las funciones de seguridad de Dropbox, consulta el Informe de seguridad de Dropbox Business o ponte en contacto con sales@dropbox.com.

Dropbox

RGPD: el Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos o RGPD es un reglamento de la Unión Europea que establece un nuevo marco legal para proteger los datos personales de los residentes de la Unión Europea. El RGPD es la regulación europea en materia de datos más importante desde la Directiva de Protección de Datos de la UE de 1995. Muchas empresas, incluida Dropbox, que operan en Europa, han invertido para poder cumplir con el RGPD.

El RGPD trata de armonizar y ofrecer un marco legal sobre protección de datos en Europa para sincronizarse con el cambio tecnológico que se ha producido en las últimas dos décadas. Se ha desarrollado en base a marcos legales previos de la UE, incluida la Directiva de Protección de Datos, e incluye nuevas obligaciones y derechos para empresas que tratan datos personales, así como nuevos derechos para los individuos en relación a sus datos personales. Las empresas que se han establecido en la UE, así como las que tratan datos personales de los residentes de la UE, deben cumplir con el RGPD.

Cómo cumple Dropbox con el RGPD

En Dropbox estamos comprometidos con el cumplimiento del RGPD. El respeto por la privacidad y la seguridad siempre ha estado presente en nuestra organización y, a medida que hemos crecido, hemos priorizado la gestión y protección de los datos que los usuarios nos han confiado. Dropbox siempre se ha mantenido un paso por delante en lo relativo al cumplimiento. Tal y como mencionábamos anteriormente, fuimos uno de los primeros proveedores en conseguir la certificación ISO 27018 para nuestros usuarios de empresa. A partir de estas sólidas bases, Dropbox considera el cumplimiento con el RGPD como una evolución de las prácticas y controles que ya llevábamos a cabo.

El camino hacia el cumplimiento de Dropbox empezó cuando se aprobó la normativa en 2016. Nuestro primer paso fue contar con un equipo multidisciplinar de especialistas en protección de datos compuesto por profesionales expertos en asesoría, seguridad y cumplimiento, así como ingenieros de producto e infraestructura. Después, llevaron a cabo una evaluación completa para ver hasta qué punto nuestras prácticas de seguridad y protección de datos cumplían con los requisitos del RGPD. Nuestro próximo paso fue llevar a cabo una evaluación de nuestras actividades relativas al procesamiento de los datos personales para trazar el ciclo de vida de los datos personales en nuestros sistemas. En ocasiones, estos ejercicios consisten en llevar a cabo mapeos de datos y completar evaluaciones del impacto de la protección de datos.

Desde entonces, hemos continuado desarrollando nuestros procesos y procedimientos internos para asegurar que cumplimos con los principios de responsabilidad que exige el RGPD. Esto resulta clave ya que el nuevo reglamento se centra especialmente en documentar las decisiones y prácticas que implican datos personales.

Para obtener información detallada sobre las políticas y las funciones de seguridad de Dropbox, consulta el Informe de seguridad de Dropbox Business o ponte en contacto con sales@dropbox.com.

Dropbox

Ayudar a nuestros usuarios en su cumplimiento con el RGPD

Dropbox ofrece funciones de control y visibilidad que pueden ayudarte a gestionar fácilmente tus obligaciones de protección de datos, incluidas las relativas al RGPD. Por supuesto, el cumplimiento con el RGPD en tu empresa no empieza o termina en la relación con tus proveedores de servicio, como es el caso de Dropbox. Nuestras funciones pueden ayudarte a gestionar tus obligaciones pero no aseguran el cumplimiento por sí mismas. El cumplimiento del RGPD exige una concepción más amplia sobre cómo se transportan y se protegen los datos en tu empresa. Cada organización debería llevar a cabo sus propios pasos para alcanzar el cumplimiento, teniendo en cuenta a los proveedores como una pieza clave para cumplir este objetivo.

Minimización de los datos

Un elemento a tener en cuenta dentro de los requisitos del RGPD relativos a la Privacidad por diseño es que las organizaciones deberían diseñar servicios de forma que se minimice el tratamiento de datos. Esto implica tener una buena visibilidad y control sobre los datos en tu empresa para poder gestionarlos. El panel de administrador de Dropbox resulta muy útil a este respecto pues te permite monitorizar la actividad del equipo, ver los dispositivos conectados y auditar la actividad relativa al contenido compartido.

Protección y restauración de los datos

La protección para los dispositivos perdidos, historial de versiones y recuperación de archivos pueden ayudarte a protegerte ante pérdidas, daños o destrucción de datos personales de carácter accidental, y pueden contribuir a la hora de restaurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma puntual en caso de incidente. La autenticación de dos factores es otra medida importante que recomendamos a la hora de proteger los datos.

Mantenimiento de registros

El RGPD también aumenta las obligaciones a la hora de mantener un registro de las actividades de procesamiento de datos por parte de las empresas. Nuestro registro de auditoría y registro de actividades pueden ayudarte a entender mejor tus actividades de procesamiento y facilitarte el mantenimiento de un registro.

Acceso al administrador

Dentro del panel de administrador de Dropbox puedes gestionar fácilmente el acceso de los miembros del equipo a archivos, carpetas y documentos de Paper. En el caso de los enlaces compartidos de archivo, nuestra función de permisos de enlace te permite proteger con contraseña los enlaces compartidos, establecer fechas límites para conceder acceso temporal y limitar el acceso a los usuarios que decidas dentro de la empresa. En caso de que cambien las responsabilidades entre los usuarios, nuestra herramienta de transferencia de cuenta te permite realizar transferencias fácilmente, así como traspasar la propiedad de documentos Paper de un usuario a otro. Los administradores también tienen la capacidad de deshabilitar el acceso de usuario a su cuenta, al tiempo que conservan sus datos y la relación a la hora de compartir con la intención de mantener los datos a salvo. Por último, la función de borrado remoto permite borrar los archivos y documentos de Paper en los dispositivos que se pierdan o hayan sido robados.

Infraestructura de la UE

Aunque el RGPD no exige guardar los datos personales dentro de la UE, en muchas circunstancias, Dropbox ofrece a los clientes que cumplan los requisitos de Dropbox Business y Dropbox Education la capacidad de almacenar archivos (bloques) en la UE. La infraestructura Amazon Web Services (AWS) ofrece el servicio de almacenamiento de archivos en la UE. Para obtener más información sobre la infraestructura de la UE, ponte en contacto con nuestro equipo de ventas.

Para obtener información detallada sobre las políticas y las funciones de seguridad de Dropbox, consulta el Informe de seguridad de Dropbox Business o ponte en contacto con sales@dropbox.com.

Dropbox

Trabajar juntos para proteger tus datos personales

Dropbox trabaja codo con codo con sus usuarios para proteger sus datos personales. Adoptamos medidas integrales para proteger nuestra infraestructura, nuestra red y nuestras aplicaciones; formamos a nuestros empleados en las prácticas de seguridad y privacidad; creamos una cultura en la que ser digno de confianza es la máxima prioridad; y sometemos nuestros sistemas y prácticas a rigurosas pruebas y auditorías externas.

Sin embargo, los usuarios también juegan un papel fundamental a la hora de proteger sus datos personales. Dropbox te permite configurar, utilizar y monitorizar tu cuenta de varias formas con el objetivo de que puedas cumplir con las necesidades de seguridad, privacidad y cumplimiento normativo de tu empresa. En nuestra guía de responsabilidad compartida encontrarás más información que puede ayudarte a entender mejor lo que hacemos para mantener más segura tu cuenta. Además también te explicamos qué puedes hacer para mantener la visibilidad y el control sobre tus datos personales.

Resumen

Cada día, millones de usuarios confían en Dropbox. Para merecernos esa confianza, hemos desarrollado una plataforma que crece priorizando la seguridad y la privacidad. Nuestro compromiso con la protección de nuestros datos personales se refleja en cada decisión que tomamos. Para obtener más información, envíanos un email a privacy@dropbox.com. Para obtener más información sobre el RGPD, puedes visitar nuestro centro de ayuda del RGPD.

Para obtener información detallada sobre las políticas y las funciones de seguridad de Dropbox, consulta el Informe de seguridad de Dropbox Business o ponte en contacto con sales@dropbox.com.