Dropbox

Privacidad y protección de datos

Introducción

Los datos personales juegan un papel fundamental en la sociedad y en la economía. Cada vez es más habitual que las personas busquen un mayor control y claridad sobre la forma en que las organizaciones con las que interactúan utilizan y protegen sus datos personales.

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

Nuestros compromisos contigo

Nos comprometemos a proteger tus datos personales. En las Condicionesde servicio de Dropbox se destacan cuáles son tus responsabilidades al utilizar nuestros servicios. En nuestra Política de privacidad se describen nuestros compromisos de seguridad con los usuarios y se explica cómo recopilamos, usamos y tratamos tus datos personales cuando utilizas Dropbox. Si resides en América del Norte (Estados Unidos, Canadá y México), Dropbox, Inc, actúa como tu proveedor de servicios.

Para los demás usuarios, Dropbox International Unlimited Company actúa como responsable de sus datos personales.

Si eres usuario de Dropbox Business o de Dropbox Education, tu organización actúa como responsable del tratamiento de todos los datos personales proporcionados a Dropbox en relación con tu uso de Dropbox Business o Dropbox Education. El responsable del tratamiento determina los propósitos y los medios del tratamiento de datos personales. Dropbox actúa como encargado del procesamiento de datos al procesar información en nombre de tu empresa cuando utilizas Dropbox Business o Dropbox Education. En nuestro Acuerdo para empresas se incluyen los compromisos relacionados con el tratamiento de datos y la transferencia internacional de los mismos.

Nuestra trayectoria: la conformidad normativa

La conformidad permite validar la fiabilidad de los servicios. Te animamos a que nos solicites la verificación independiente que demuestra que nuestras prácticas de seguridad y privacidad cumplen con las normas y regulaciones más aceptadas, tales como ISO 27001, ISO 27017, ISO 27018, HIPPA/HITECH, BSI C5 en Alemania y SOC 1, 2 y 3. Estaremos encantados de proporcionarte dicha verificación.

Además, fuimos uno de los primeros proveedores de servicios en la nube que obtuvo la certificación ISO 27018, el estándar reconocido internacionalmente sobre prácticas líderes en privacidad en la nube y protección de datos. Nuestros auditores externos independientes prueban nuestros controles, redactan sus informes y aportan sus opiniones. Siempre que sea posible, los compartiremos contigo.

Ten en cuenta que, si bien el alcance de nuestras certificaciones e informes de auditoría generalmente se refieren a Dropbox Business y Dropbox Education, la mayoría de nuestros controles también se aplican a los usuarios de Dropbox Basic, Plus y Professional. Puedes encontrar más información sobre los estándares que cumplimos y cómo verificamos nuestras prácticas en nuestra página sobra cumplimiento.

Para obtener más información sobre las características y las políticas de seguridad de Dropbox, puedes consultar el Informe técnico sobre seguridad de Dropbox Business o ponerte en contacto con sales@dropbox.com.

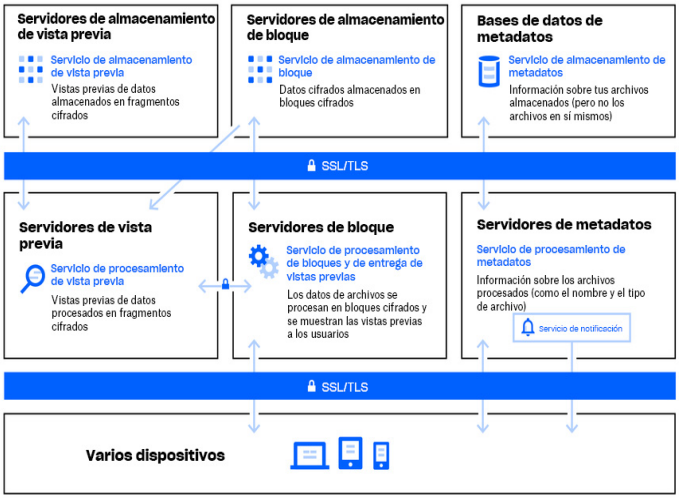
Dropbox

La arquitectura de Dropbox: Protección de tus datos personales

En Dropbox, creemos que la protección de tus datos personales empieza por mantener tus datos seguros. Por este motivo, Dropbox se ha diseñado con varias capas de protección: transferencia de datos segura, cifrado, configuración de red y controles a nivel de aplicación, todo ello distribuido en una infraestructura segura y ampliable.

Nuestra infraestructura: Archivos

La infraestructura de Dropbox para los archivos está formada por los componentes que se muestran en el siguiente diagrama:



Servidores de metadatos

Cierta información básica sobre los datos del usuario —lo que se conocen como "metadatos"—, se guarda en su propio servicio de almacenamiento discreto y actúa como índice para los datos en las cuentas de los usuarios. Los metadatos incluyen información básica de la cuenta y del usuario como, por ejemplo, la dirección de correo electrónico, el nombre y los nombres de los dispositivos. Los metadatos también incluyen información básica sobre los archivos como nombres y tipos de archivos. Esta información ayuda a admitir funciones como el historial de versiones, la recuperación y la sincronización.

Bases de datos de metadatos

Los metadatos de los archivos se almacenan en un servicio de base de datos basado en MySQL y se fragmentan y replican según sea necesario para cumplir con los requisitos de rendimiento y alta disponibilidad.

Servidores de bloques

El diseño de Dropbox proporciona un mecanismo de seguridad único para proteger los datos del usuario que va más allá del cifrado tradicional. Los servidores de bloques procesan los archivos de las aplicaciones de Dropbox dividiendo cada archivo en bloques, cifrando cada bloque mediante un sistema de cifrado reforzado y sincronizando solo los bloques que se han modificado entre revisiones. Cuando una aplicación de Dropbox detecta un nuevo archivo o cambios en un archivo existente, la aplicación notifica a los servidores de bloques el cambio, y los bloques de archivos nuevos o modificados se procesan y transfieren al servidor de almacenamiento.

Servidores de bloques de almacenamiento

El contenido real de los archivos de los usuarios se almacena en bloques cifrados con los servidores de bloques de almacenamiento. Antes de la transmisión, el cliente de Dropbox divide los archivos en bloques de archivos para preparar el almacenamiento. Los servidores de bloques de almacenamiento actúan como un sistema de almacenamiento direccionable por contenido (o CAS, por sus siglas en inglés) con cada bloque de archivo cifrado individual recuperado en función de su valor hash.

Servidores de vistas previas

Los servidores de vistas previas son responsables de generar las vistas previas de los archivos. Las vistas previas son una representación del archivo de un usuario en un formato diferente y más adecuado para una visualización rápida en el dispositivo de un usuario final. Los servidores de vistas previas recuperan bloques de archivos de los servidores de bloques de almacenamiento para generar vistas previas. Cuando se solicita una vista previa del archivo, los servidores de vistas previas recuperan la vista previa en caché de los servidores de almacenamiento de vistas previas y la transfieren a los servidores de bloque. Finalmente, las vistas previas llegan a los usuarios a través de los servidores de bloque.

Servidores de almacenamiento de vistas previas

Las vistas previas en caché se almacenan en un formato cifrado en los servidores de almacenamiento de vistas previas.

Servicio de notificaciones

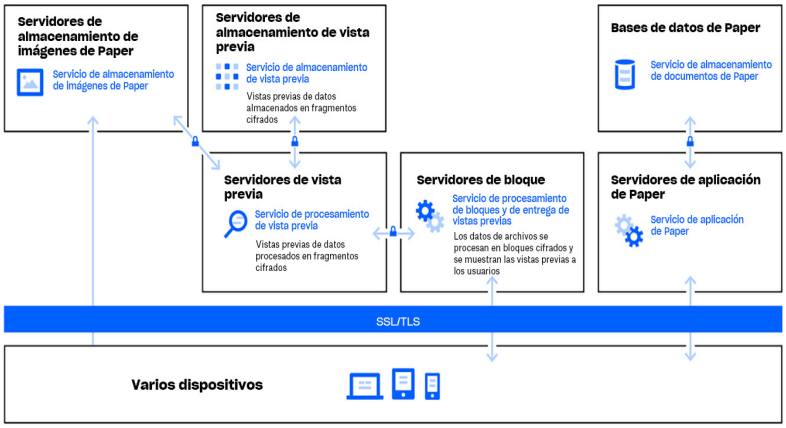
Este servicio independiente está dedicado a supervisar si se han realizado cambios o no en las cuentas de Dropbox. Aquí no se almacenan ni transfieren archivos ni metadatos. Cada cliente establece una conexión prolongada de consulta con el servicio de notificación y espera. Cuando se produce un cambio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

Para obtener más información sobre las características y las políticas de seguridad de Dropbox, puedes consultar el Informe técnico sobre seguridad de Dropbox Business o ponerte en contacto con sales@dropbox.com.

Dropbox

Nuestra infraestructura: Paper

Dropbox Paper (Paper) es una función del producto Dropbox. Sin embargo, Paper utiliza un conjunto de sistemas distintos dentro del entorno de infraestructura de Dropbox. La infraestructura de Dropbox está formada por los componentes que se muestran en el siguiente diagrama:



Servidores de aplicaciones de Paper

Los servidores de aplicaciones de Paper procesan solicitudes de usuarios, representan el resultado de los documentos de Paper editados para el usuario y realizan servicios de notificación. Los servidores de aplicaciones de Paper escriben las modificaciones de los usuarios en las bases de datos de Paper, donde se conservan en un almacenamiento persistente. Las sesiones de comunicación entre los servidores de aplicaciones de Paper y las bases de datos de Paper se cifran con un sistema de cifrado reforzado.

Bases de datos de Paper

El contenido real de los documentos de Paper de los usuarios, así como determinados metadatos acerca de estos documentos de Paper, se cifran en un almacenamiento persistente en las bases de datos de Paper. Esto incluye información acerca de un documento de Paper (como el título, la pertenencia compartida y los permisos, las asociaciones de proyectos y carpetas, y otra información), así como contenido incluido dentro del documento de Paper en sí, incluyendo los comentarios y las tareas. Las bases de datos de Paper se dividen y replican según sea necesario para cumplir con los requisitos de disponibilidad total y rendimiento.

Servidores de almacenamiento de imágenes de Paper

Las imágenes que se suben a los documentos de Paper se almacenan y cifran almacenadas en los servidores de imágenes de Paper. La transmisión de datos de imagen entre la aplicación de Paper y los servidores de imágenes de Paper se produce a lo largo de una sesión cifrada.

Servidores de vistas previas

Los servidores de vistas previas crean vistas previas tanto para imágenes cargadas en documentos de Paper como para hipervínculos incrustados en documentos de Paper. Para las imágenes subidas en documentos de Paper, los servidores de vistas previas obtienen datos de imágenes almacenados en los servidores de almacenamiento de imágenes de Paper a través de un canal cifrado. En el caso de los hipervínculos incrustados en los documentos de Paper, los servidores de vistas previas obtienen los datos de la imagen y presentan una vista previa de la imagen mediante el cifrado según lo que se especifica en el enlace de origen. Finalmente, las vistas previas llegan a los usuarios a través de los servidores de bloque.

Servidores de almacenamiento de vistas previas

Paper utiliza los mismos servidores de almacenamiento de vistas previas descritos en el diagrama de infraestructura de Dropbox para almacenar las vistas previas de imágenes en caché. Las vistas previas en caché se almacenan en un formato cifrado en los servidores de almacenamiento de vistas previas.

Dropbox

Los controles de Dropbox: Nuestras prácticas internas

Tomamos medidas integrales para proteger nuestra infraestructura, red y aplicaciones. Algunas de las medidas de seguridad que tenemos implementadas incluyen el cifrado en reposo, el cifrado en tránsito y el borrado permanente de archivos.
También ofrecemos una capacitación en privacidad y seguridad sólida para todos nuestros empleados con el propósito de construir una cultura en la que ser dignos de confianza sea una prioridad. A continuación, encontrarás la descripción detallada de algunos de nuestros controles:

Formación

Proteger los datos personales de nuestros usuarios implica en gran parte construir y desarrollar una cultura de seguridad y concienciación de la privacidad. Antes de poder acceder a los sistemas, los empleados de Dropbox tienen que aceptar las políticas de seguridad y también una política de privacidad de los datos del usuario. Solo los empleados con necesidades específicas tienen acceso a dichos sistemas.
El personal también recibe anualmente una formación obligatoria sobre seguridad y privacidad.

Cifrado en curso

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

Cifrado en pausa

Los archivos que suben los usuarios se almacenan en los servidores de almacenamiento de Dropbox como bloques de archivos discretos. Cada bloque se cifra con el Advanced Encryption Standard (AES) de 256 bits. Solo se sincronizan los bloques que se han modificado entre revisiones. De forma similar, los datos de documentos de Paper almacenados en las bases de datos de Paper también se cifran en reposo utilizando el Advanced Encryption Standard (AES) de 256 bits.

Eliminación permanente de archivos y documentos en Paper

Cuando un usuario de Dropbox o un administrador de un equipo de Dropbox Business o Dropbox Education marca un archivo para su eliminación definitiva, se activa un proceso para eliminarlo de forma permanente. Del mismo modo, cuando un usuario o un administrador de un equipo de Dropbox Business o Dropbox Education marca un documento de Paper para su eliminación definitiva, hay un proceso similar para eliminar permanentemente los datos del documento de Paper y de imagen.

Solicitudes de acceso a datos personales

Para acceder a datos personales más allá de los archivos y los documentos de Paper que se almacenan en Dropbox, los usuarios pueden iniciar sesión en el sitio web e ir a la página de su cuenta. Esta página muestra información como el nombre y la dirección de correo electrónico asociada a la cuenta. Los usuarios también pueden ver las direcciones de IP de las sesiones, ordenadores o dispositivos móviles conectados, así como las aplicaciones conectadas a sus cuentas desde la página de seguridad y la página de aplicaciones conectadas.

Los usuarios de Dropbox también tienen la opción de solicitar el acceso a otros datos personales que Dropbox haya recopilado sobre ellos. También pueden solicitar que dichos datos se eliminen. Podrás encontrar más información sobre este proceso en el Centro de ayuda de Dropbox.

Gobernanza de privacidad en Dropbox

La gestión del Programa de privacidad de Dropbox recae sobre un equipo completamente dedicado a esta tarea. Este se encarga de implementar nuestras iniciativas de privacidad clave y propugna la privacidad mediante el diseño en nuestro ciclo de vida de los datos. El Programa de privacidad de Dropbox cuenta con el respaldo de varios subequipos jurídicos multifuncionales. Estos subequipos proporcionan la experiencia adicional requerida para gestionar y supervisar las tareas diarias del Programa de Privacidad.

El equipo de protección de datos opera de forma independiente al resto de funciones de privacidad y actúa como herramienta que garantiza el cumplimiento de las garantías de privacidad y, también, como mecanismo de supervisión. Este equipo respalda de forma directa al responsable de la protección de datos en la realización de sus funciones. El responsable de la protección de datos es el representante local de la UE y se puede contactar con él a través de la siguiente dirección de correo electrónico privacy@dropbox.com.

Para obtener más información sobre las características y las políticas de seguridad de Dropbox, puedes consultar el Informe técnico sobre seguridad de Dropbox Business o ponerte en contacto con sales@dropbox.com.

Dropbox

Principios relativos a las solicitudes de datos de los gobiernos

Entendemos que cuando los usuarios nos confían sus datos personales, esperan que los mantengamos como confidenciales. Al igual que muchos servicios en línea, Dropbox suele recibir requerimientos gubernamentales solicitando información sobre nuestros usuarios.

Los principios que se muestran a continuación describen cómo manejamos las solicitudes de datos gubernamentales que recibimos.

Ser transparentes

Los servicios en línea deberían tener permiso para publicar el número y los tipos de solicitudes gubernamentales que reciben, así como para notificar a los particulares cuando se solicite información acerca de ellos. Este tipo de transferencia beneficia a los usuarios, pues les ayuda a entender mejor los casos y los patrones de las extralimitaciones de los gobiernos. Seguiremos publicando información detallada sobre estas solicitudes y defendiendo el derecho a ofrecer tipos similares de información importante.

Hacer frente a solicitudes demasiado amplias

Las solicitudes gubernamentales de datos deberían limitar la información que requieren y centrarse en personas específicas e investigaciones legítimas. Nos opondremos a solicitudes excesivamente amplias y generales.

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 una protección diferente a las personas en función de su residencia o nacionalidad son obsoletas y no reflejan la naturaleza global de los servicios en línea. Seguiremos reivindicando la reforma de estas leyes.

Estos principios, junto con nuestro informe anual de transparencia, se ponen a disposición del público en el sitio web de Dropbox en: https://www.dropbox.com/transparency.

Para obtener más información acerca de nuestros controles y nuestro enfoque para proteger tus datos personales, consulta nuestro Informe técnico de seguridad de Dropbox Business.

Terceros que trabajan para y con Dropbox

Dropbox gestiona la mayoría de las actividades relacionadas con la prestación de nuestros servicios; sin embargo, utilizamos algunos terceros de confianza en relación con nuestros servicios (por ejemplo, proveedores de atención al cliente y servicios de TI).

Estos terceros solo accederán a tu información para realizar tareas en nuestro nombre de conformidad con nuestra Política privacidad, y seguiremos siendo responsables del tratamiento de tu información de acuerdo con nuestras instrucciones.

Cada tercero pasa por un riguroso proceso de investigación, que incluye revisiones de seguridad y revisiones contractuales regulares, con el fin de evaluar su capacidad para cumplir con nuestros compromisos de protección de datos.

Transferencias internacionales de datos

Dropbox confía en varios mecanismos legales para la transferencia internacional de datos personales de la UE a los Estados Unidos. Además, cuenta con la certificación del marco del Escudo de la Privacidad entre la UE/EE. UU. y entre EE. UU./Suiza relacionada con la recopilación, uso y retención de datos personales y su transferencia de la UE y Suiza a los Estados Unidos. Además del Escudo de Privacidad, Dropbox también ofrece sólidas garantías contractuales en torno a la privacidad de sus servicios y ha implementado cláusulas contractuales modelo de la UE para cubrir las transferencias internacionales de datos.

Para obtener más información sobre las características y las políticas de seguridad de Dropbox, puedes consultar el Informe técnico sobre seguridad de Dropbox Business o ponerte en contacto con sales@dropbox.com.

Dropbox

RGPD: Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos, o RGPD, es un reglamento de la UE que establece un marco legal para proteger los datos personales de los interesados de la UE.

El RGPD es la regulación más importante de la legislación europea de protección de datos desde la Directiva de Protección de Datos de la UE de 1995, y muchas empresas, incluida Dropbox, que hacen negocios en Europa han hecho grandes inversiones para cumplir el RGPD.

El RGPD unifica las leyes de protección de datos en toda Europa y las pone al día para adaptarse a la rapidez de los cambios tecnológicos que se han producido en las últimas dos décadas.

Se basa en marcos legales anteriores en la UE, incluida la Directiva de Protección de Datos de la UE, e introduce nuevas obligaciones y responsabilidades para las organizaciones que tratan datos personales, así como nuevos derechos para las personas con respecto a sus datos personales. datos personales. Las organizaciones establecidas en la UE, así como las organizaciones que procesan datos personales de los interesados de la UE, deben cumplir con el RGPD.

El proceso de cumplimiento del RGPD de Dropbox

Dropbox está comprometido con el cumplimiento del RGPD. En nuestro negocio incorporamos el respeto por la privacidad y la seguridad desde el principio y, a medida que hemos ido creciendo, nuestro enfoque en la gestión y la protección de los datos que nuestros usuarios nos confían ha seguido siendo una prioridad. Dropbox se ha mantenido por delante de la curva de cumplimiento; tal y como se ha descrito anteriormente, fuimos uno de los primeros proveedores de servicios en la nube que obtuvo la certificación ISO 27018 para nuestros usuarios empresariales. Si tenemos en cuenta sus sólidas bases, Dropbox considera que el cumplimiento del RGPD es una evolución de nuestras prácticas y controles existentes, y representa un conjunto continuo y en evolución de iniciativas para garantizar que los datos personales de nuestros usuarios siempre estén protegidos.

El viaje de Dropbox hacia el cumplimiento de RGPD comenzó tan pronto como se adoptó la regulación en 2016. Lo primero que hicimos fue formar un equipo multifuncional de especialistas en protección de datos compuesto por asesores legales, profesionales de seguridad y cumplimiento e ingenieros de producto e infraestructura. Luego, nuestro equipo realizó una evaluación completa de nuestras prácticas actuales de seguridad y protección de datos con respecto a los requisitos del RGPD.

A continuación, realizamos una evaluación de nuestras actividades de procesamiento de datos personales y rastreamos el ciclo de vida de los datos personales a través de nuestros sistemas. Estos ejercicios a veces se refieren a la consecución de mapeos de datos y a la ejecución de evaluaciones sobre el impacto de la protección de datos.

Asignaciones de datos y completar evaluaciones de impacto de protección de datos.

Desde entonces, hemos seguido construyendo sobre nuestros procesos internos y procedimientos para asegurarnos de que cumplimos con los principios de responsabilidad según los requisitos del RGPD. Esto es muy importante ya que la nueva normativa prioriza cada vez más las decisiones en torno a la documentación y las prácticas que afectan a los datos personales.

Para obtener más información sobre las características y las políticas de seguridad de Dropbox, puedes consultar el Informe técnico sobre seguridad de Dropbox Business o ponerte en contacto con sales@dropbox.com.

Dropbox

Capacitar a nuestros usuarios para cumplir con los requisitos del RGPD

Dropbox proporciona funciones de control y visibilidad que pueden ayudarte a gestionar más fácilmente tus obligaciones de protección de datos, incluidos los requisitos del RGPD. Es evidente que el cumplimiento de RGPD de tu organización ni empieza ni termina con la relación con tus proveedores como Dropbox. Si bien es cierto que nuestras funciones pueden ayudarte a gestionar tus obligaciones, tienes que tener en cuenta que no pueden garantizar el cumplimiento en sí mismas. Para cumplir con la obligaciones del RGPD hay que pensar de manera más amplia cómo gestionas y proteges los datos. Cada organización debe llevar a cabo sus propios pasos para cumplir con estas obligaciones y debe hacerlo junto a sus proveedores y socios, que también son importantes en este viaje.

Minimización de datos

Un elemento importante del requisito de privacidad por diseño del RGPD es que las organizaciones deben diseñar sus servicios de manera que minimicen los datos. Esto significa tener buena visibilidad y control de los datos dentro de Tu organización para que sea más fácil gestionarlos. El panel de administración de Dropbox Business te puede ayudar con esto, ya que te permite controlar la actividad del equipo, ver los dispositivos conectados y auditar la actividad de uso compartido. Trabajamos para incorporar los principios de privacidad por diseño a nuevos productos y características.

Protección y restauración de datos

La protección de los dispositivos perdidos, el historial de versiones y la recuperación de archivos pueden ayudar a proteger las perdidas accidentales de dispositivos, los dalos o la destrucción de datos personales. Además, estas funciones te permiten restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de que se produzca algún incidente. La doble autenticación es otra medida importante que te animamos a utilizar para proteger tus datos.

Mantenimiento de registros

El RGPD también aumenta las obligaciones de las organizaciones de mantener registros detallados de sus actividades de procesamiento. Nuestros registros de auditoría y nuestros registros de actividad pueden ayudarte a comprender mejor tus actividades de procesamiento para facilitarte la tarea de mantenimiento de registros.

Acceso de administrador

Desde el panel de administración de Dropbox Business, podrás gestionar de forma fácil el acceso a determinados archivos, carpetas y documentos de Paper de los miembros del equipo. Para los enlaces a archivos compartidos, 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. En caso de que se produzcan cambios de responsabilidades entre los usuarios, nuestra herramienta de transferencia de cuenta te permite transferir archivos y documentos de Paper de un usuario a otro de forma sencilla.

Los administradores también tienen la capacidad de deshabilitar el acceso de un usuario a su cuenta. En este caso los datos de dicha cuenta no se pierden y los archivos que se habían compartido siguen disponibles para mantener protegida la información. Por último, la función de borrado remoto te permite borrar archivos y documentos de Paper de dispositivos perdidos o robados.

La infraestructura de la UE

Aunque el RGPD no requiere que los datos personales se alojen en la UE, Dropbox ofrece a los clientes calificados de Dropbox Business y Dropbox Education la capacidad de almacenar archivos (bloques) en la UE. El almacenamiento de archivos en la UE se proporciona en la infraestructura de Amazon Web Services (AWS). Para obtener más información sobre nuestra infraestructura en la UE, puedes ponerte en contacto con nuestro equipo de ventas.

Para obtener más información sobre las características y las políticas de seguridad de Dropbox, puedes consultar el Informe técnico sobre seguridad de Dropbox Business o ponerte en contacto con sales@dropbox.com.

Dropbox

Trabajando juntos para proteger tus datos personales

Dropbox trabaja con sus usuarios para proteger sus datos personales. Tomamos medidas integrales para proteger nuestra infraestructura, red y aplicaciones, formar a los empleados en prácticas de seguridad y privacidad, construir una cultura en la que la mayor prioridad sea ser dignos de confianza y, por último, para someter nuestros sistemas y prácticas a pruebas rigurosas y auditorías de terceros.

Sin embargo, los usuarios también juegan un papel muy importante en la protección de sus datos personales. Dropbox te permite configurar, usar y controlar tu cuenta para satisfacer las necesidades de privacidad, seguridad y cumplimiento de tu organización. Nuestra guía sobre responsabilidad compartida puede ayudarte a comprender mejor todo lo que hacemos para proteger tu cuenta y lo que puedes hacer tú para mantener la visibilidad y el control sobre tus datos personales.

Resumen

Cada día, millones de usuarios confían en Dropbox. Para ser dignos de esa confianza, creamos y seguiremos haciendo crecer Dropbox con énfasis en la seguridad y la privacidad. Nuestro compromiso de proteger los datos personales de nuestros usuarios es el núcleo de todas nuestras decisiones. Para obtener más información sobre este tema, puedes enviar un correo electrónico a privacy@dropbox.com. Para obtener más información sobre el RGPD, también puedes visitar nuestro Centro de orientación sobre el RGPD.

Para obtener más información sobre las características y las políticas de seguridad de Dropbox, puedes consultar el Informe técnico sobre seguridad de Dropbox Business o ponerte en contacto con sales@dropbox.com.