Seguridad de Dropbox Business

Informe técnico de Dropbox

©2023 Dropbox. Todos los derechos reservados. V2023.01



Contenidos

Descripción general	
Entre bastidores	3
Infraestructura de archivos	3
Almacenamiento de datos de archivos	5
Infraestructura de Paper	5
Almacenamiento de documentos Paper	7
Programa de confianza de Dropbox	7
Seguridad de categoría empresarial	8
Nuestras políticas	8
Política y acceso de empleados.	9
Gestión de vulnerabilidades	10
Seguridad física	12
Oficinas corporativas.	12
Respuesta a incidentes	12
Infraestructura de seguridad	13
Seguridad de la red	13
Fiabilidad	14
Centros de datos y proveedores de servicios gestionados	
Continuidad del negocio	18
Recuperación ante desastres	19
Seguridad de la aplicación	20
Interfaces de usuario de Dropbox	20
Interfaces de usuario de Paper	20
Cifrado	21
Asignación de certificados	22
Protección de los datos de autenticación	22
Análisis de software dañino	22
Seguridad del producto	22
Controles de contenido	23
Visibilidad del contenido	25
Controles de equipo	27
Dispositivos administrados e inicio de sesión	30
Dropbox Passwords	39
Seguridad, privacidad y transparencia de los datos	42
Certificaciones de privacidad, confirmaciones y cumplimiento normativo	43
Conformidad	45
Aplicaciones para Dropbox	50
Integraciones con la API de Dropbox Business	51
Asociaciones de API	53
Integraciones de Dropbox	54
Resumen	54



Descripción general

Las transformaciones digitales continúan arraigándose en una gran cantidad de sectores, y es vital que los datos, los equipos y los dispositivos estén protegidos dondequiera que estén. Las organizaciones que confían en soluciones en la nube como Dropbox Business a fin de que los flujos de trabajo en remoto y distribuidos sean posibles necesitan optimizar la colaboración, gestionar de forma proactiva los riesgos de la nube e implementar controles efectivos que garanticen la confidencialidad de su propiedad intelectual y la integridad de los datos almacenados y los datos compartidos, así como la disponibilidad de los datos a través de un servicio en la nube administrado y resistente.

Más de 600 000 empresas y organizaciones confían en Dropbox Business como solución para que los equipos distribuidos y que trabajan en remoto puedan colaborar de forma segura. El núcleo central de la solución Dropbox Business incluye el espacio de trabajo inteligente para colaborar, la sincronización de archivos y las funciones de uso compartido. Nuestras soluciones están respaldadas por las infraestructuras líderes del sector, así como por funciones de seguridad avanzadas, protección del equipo y del contenido, firma electrónica, transferencias seguras y gobierno de datos. Excepto cuando se indique lo contrario, la información que encontrarás en este informe técnico se aplica a todos los productos de Dropbox Business (Standard, Advanced y Enterprise) y Dropbox Education. Paper es una función de Dropbox Business y Dropbox Education.

La pieza central de Dropbox Business es nuestro programa de seguridad integral, el Programa de confianza de Dropbox, que adopta un enfoque de seguridad multicapa, que es esencial a medida que evoluciona el enfoque global hacia el teletrabajo.

En este informe técnico, se detallan las funcionalidades de seguridad de los productos de Dropbox Business, las medidas de seguridad operativa de Dropbox, nuestro compromiso de privacidad y transparencia, así como las políticas de backend, las certificaciones independientes y las medidas de cumplimiento de la normativa que hacen que Dropbox sea una solución segura para tu organización.

Excepto cuando se indique lo contrario, la información que encontrarás en este informe técnico se aplica a todos los productos de Dropbox Business (Standard, Advanced y Enterprise) y Dropbox Education. Paper es una función de Dropbox Business y Dropbox Education.

Entre bastidores

Nuestras interfaces son muy fáciles de usar y están respaldadas por una infraestructura que trabaja entre bambalinas para asegurar que la sincronización, colaboración y forma de compartir son rápidas y fiables. Para que esto sea posible, siempre estamos mejorando nuestro producto y su arquitectura con el objetivo de acelerar la transferencia de datos, mejorar su fiabilidad y adaptarnos a los cambios del entorno. En esta sección explicamos cómo se transfieren, almacenan y procesan los datos de forma segura.

Infraestructura de archivos

Los usuarios de Dropbox pueden acceder a sus archivos y carpetas en cualquier momento desde las aplicaciones web, móvil y de escritorio, o bien mediante aplicaciones de terceros vinculadas a Dropbox. Todas estas aplicaciones se conectan a servidores seguros para proporcionar acceso a los archivos, permitir que se compartan archivos con otros usuarios y actualizar los dispositivos vinculados cuando se añaden, modifican o eliminan archivos.



La infraestructura de archivos de Dropbox se compone de los siguientes elementos:



Servidores de metadatos

Los metadatos, es decir, la información básica sobre los usuarios, se conserva en un servicio de almacenamiento propio y discreto que actúa como un índice para los datos de las cuentas de los usuarios. 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.

· Bases de datos de metadatos

Los metadatos de los archivos se guardan en un almacén de valor clave transaccional con control de simultaneidad de varias versiones y se fragmentan y replican según sea necesario para cumplir con los requisitos de rendimiento y alta disponibilidad.

· Servidores de bloques

Dropbox ofrece un mecanismo de seguridad único que va más allá del cifrado tradicional para proteger los datos de los usuarios. Los servidores de bloque procesan los archivos de las aplicaciones de Dropbox dividiendo cada archivo en bloques, cifrando cada bloque con una codificación sólida y sincronizando solo los bloques que se han modificado de una revisión a otra. Cuando una aplicación de Dropbox detecta un archivo nuevo o cambios en un archivo existente, notifica el cambio a los servicios de bloque y los bloques de archivos nuevos o modificados se procesan y se transfieren a los servidores de almacenamiento de bloque. Además, los servidores de bloque se utilizan para ofrecer archivos y vistas previas a los usuarios. Para obtener más información acerca del cifrado que usan estos servicios para los datos almacenados y en tránsito, consulta la sección Cifrado.

Servidores de bloques de almacenamiento

Los verdaderos contenidos de los archivos de los usuarios se almacenan en bloques cifrados mediante los servidores de almacenamiento de bloques.

Antes de la transmisión, el cliente de Dropbox divide los archivos en bloques a modo de preparación para el almacenamiento. Los servidores de almacenamiento de bloques 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.

Servidores de vistas previas

Los servidores de vista previa son los responsables de ofrecer las vistas previas de los archivos. Estas previsualizaciones consisten en una renderización del archivo de un usuario en un formato de archivo diferente y más adecuado para mostrarse rápidamente en el dispositivo del usuario final. Los servidores de vista previa recuperan los bloques de archivo de los servidores de almacenamiento de bloques para generar vistas previas. Cuando se solicita la vista previa, los servidores de vistas previas recuperan la vista previa almacenada en caché de los servidores de almacenamiento de vistas previas y la transfieren a los servidores de bloques. Los servidores de bloque son los que muestran finalmente las vistas previas a los usuarios.

· Servidores de almacenamiento de vistas previas

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

Servicio de notificación

Este servicio independiente supervisa 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 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.

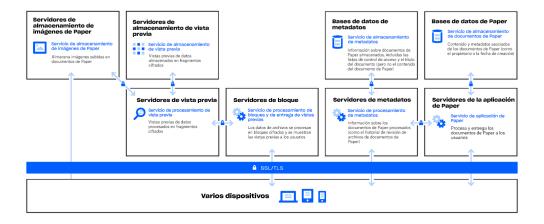
Almacenamiento de datos de archivos

Principalmente, Dropbox almacena dos tipos de datos de archivo: metadatos acerca de los archivos (como la fecha y la hora en que el archivo se modificó por última vez) y el contenido real de los archivos (bloques de archivos). Los metadatos de los archivos se almacenan en servidores de Dropbox. Los bloques de archivo se almacenan en uno de estos dos sistemas: Amazon Web Services (AWS) o Magic Pocket, el sistema de almacenamiento interno de Dropbox. Magic Pocket consta de hardware y software registrados, y se ha diseñado desde cero de modo que sea seguro y fiable. Tanto en Magic Pocket como en AWS, los bloques de archivos se cifran cuando están estáticos; además, ambos sistemas cumplen altos estándares de fiabilidad. Para obtener más información, consulta la sección Fiabilidad.

Infraestructura de Paper

Los usuarios de Dropbox pueden acceder a documentos de Paper en cualquier momento desde el sitio web y móvil, o bien mediante aplicaciones de terceros conectadas a la aplicación Dropbox Paper. Todos estos clientes se conectan a servidores seguros para proporcionar acceso a los documentos de Paper, permiten compartir documentos con otros usuarios y actualizan los dispositivos vinculados cuando se añaden, modifican o eliminan archivos.

La infraestructura de archivos de Dropbox Paper se compone de los siguientes elementos:





· Servidores de aplicaciones 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 aplicaciones en Paper y las bases de datos en Paper están protegidas con el protocolo Secure Hypertext Transfer Protocol (HTTPS).

· 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, el propietario, la fecha de creación y otras informaciones), 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.

Servidores de metadatos

Paper utiliza los mismos servidores de metadatos descritos en el diagrama de la infraestructura de Dropbox para procesar la información sobre los documentos de Paper, como el historial de revisión de los documentos de Paper y la pertenencia a carpetas compartidas. Dropbox gestiona directamente los servidores de metadatos, ubicados en centros de datos de terceros.

· Bases de datos de metadatos

Paper utiliza las mismas bases de datos de metadatos que se describen en el diagrama de la infraestructura de Dropbox para almacenar información relacionada con los documentos de Paper, como el uso compartido, los permisos y las asociaciones de carpetas. Los metadatos de los documentos de Paper 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.

Servidores de almacenamiento de imágenes de Paper

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

· Servidores de vistas previas

Los servidores de vistas previas ofrecen vistas previas de imágenes subidas a documentos de Paper, así como de los hiperenlaces incrustados dentro de documentos de Paper. Para las imágenes cargadas en documentos de Paper, los servidores de vistas previas capturan los datos de imagen almacenados en los servidores de almacenamiento de imágenes de Paper a través de un canal cifrado. En el caso de los hiperenlaces incrustados en documentos de Paper, los servidores de vistas previas buscan los datos de imagen en el enlace de la fuente e interpreta una vista previa de la imagen mediante cifrado, tal y como especifique el enlace de la fuente. Los servidores de bloque son los que muestran finalmente las vistas previas a los usuarios.

Servidores de almacenamiento de vistas previas

Paper utiliza los mismos servidores de almacenamiento de vistas previas que se describen en el diagrama de infraestructura de Dropbox para almacenar las vistas previas de imágenes en caché. Los fragmentos de vistas previas almacenadas en caché se almacenan en un formato cifrado en los servidores de almacenamiento de vistas previas.



Almacenamiento de documentos de Paper

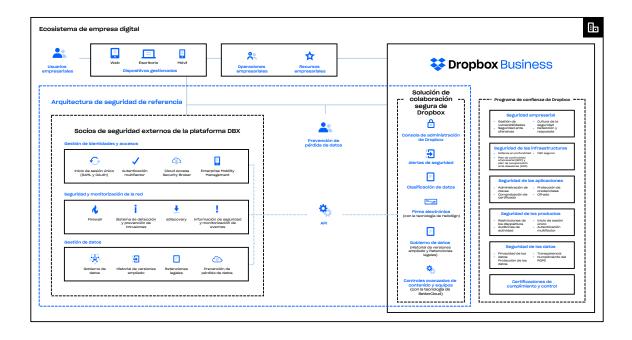
Dropbox almacena principalmente los siguientes tipos de datos en documentos de Paper: metadatos sobre documentos de Paper (como los permisos compartidos de documento) y los propios contenidos de los documentos de Paper que sube el usuario. De forma colectiva se conoce todo esto como "los datos de imagen de Paper". Cada uno de estos tipos de datos se almacena en Amazon Web Services (AWS). Los documentos de Paper se cifran en reposo en AWS, que cumple altos estándares de fiabilidad. Para obtener más detalles, consulta la sección de Fiabilidad que encontrarás más adelante.

Programa de confianza de Dropbox

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, en Dropbox ponemos el acento en la seguridad, la privacidad, la transparencia y la conformidad; y lo seguiremos haciendo.

El programa de confianza de Dropbox establece un proceso de evaluación de riesgos pensado para cumplir las leyes y normativas medioambientales, físicas, de usuarios y de terceros aplicables, los requisitos contractuales y otros riesgos que puedan afectar a la disponibilidad, integridad, confidencialidad y seguridad del sistema, así como a la privacidad. Realizamos evaluaciones de rendimiento como mínimo una vez al año. Consulta más información acerca del programa de confianza de Dropbox en dropbox.com/business/trust.

Seguimos un enfoque multicapa para proteger la empresa, la infraestructura, las aplicaciones y los productos que afectan a tu organización.



Seguridad de categoría empresarial

Dropbox ha establecido un marco para gestionar la seguridad de la información donde se describen el propósito, el sentido, los principios y las reglas básicas que rigen nuestra forma de mantener la confianza. Lo conseguimos mediante la evaluación de los riesgos y la mejora continua de la seguridad, confidencialidad, integridad, disponibilidad y privacidad de los sistemas de Dropbox Business. Revisamos y actualizamos periódicamente las políticas de seguridad, ofrecemos formación sobre seguridad, realizamos pruebas de seguridad de las aplicaciones y las redes (incluidas pruebas de penetración), supervisamos la conformidad con las normativas de seguridad y realizamos evaluaciones de riesgos internas y externas.

Nuestras políticas

Hemos establecido un conjunto de políticas de seguridad para que el equipo de seguridad y protección ante abusos de Dropbox las aplique. Revisamos y volvemos a aprobar estas políticas al menos una vez al año. Nuestros empleados, personal en prácticas y contratistas cursan una formación obligatoria sobre seguridad cuando se unen a la empresa y, después, reciben constantemente información orientada a aumentar sus conocimientos sobre seguridad.

· Seguridad de la información

Protegemos la información del usuario y de Dropbox.

Autenticación

Describe cómo se autentican los empleados de Dropbox para acceder a los sistemas de información y a los datos.

· Seguridad de dispositivos

Los requisitos mínimos de seguridad para los dispositivos móviles utilizados para acceder a la información de la empresa.

· Control de acceso lógico

Mantener el acceso a los sistemas de Dropbox, a los usuarios y a la información de forma segura. Incluye el control de acceso tanto a los entornos corporativos como a los de producción.

· Seguridad de los datos

Describe cómo Dropbox protege los datos mediante requisitos específicos de almacenamiento, acceso y uso.

· Seguridad en caso de viaje

Describe lo que los empleados de Dropbox deben hacer antes de viajar al extranjero.

Directrices de seguridad para la experiencia de cliente y ventas (CX)

Mantener la información de los usuarios segura, protegiendo a nuestros empleados y proporcionando asistencia a nuestros usuarios.

Seguridad física

Mantener un entorno seguro para las personas y la propiedad en Dropbox.

Directrices para la seguridad física de la producción

Gestionar el acceso físico a las instalaciones de producción.

· Respuesta a incidentes

Describe la forma en que Dropbox gestiona la seguridad, la privacidad y los eventos del sitio reportados y documenta los planes de respuesta a cada uno de ellos.

Materiales con derechos de autor no autorizados

Prohíbe a los empleados utilizar Dropbox o los sistemas de Dropbox para almacenar o compartir contenido no autorizado.

Gestión de cambios

Gestión de cambios en los sistemas de producción. Destinado a todos los empleados, contratistas y trabajadores en prácticas de Dropbox con acceso a los sistemas.

· Privacidad de los datos del usuario

Proteger y manejar la información y los datos de los usuarios en Dropbox de acuerdo con nuestra Política de privacidad.

· Política de continuidad del negocio y gestión de emergencias

Describe la preservación, la protección y la seguridad de las personas (empleados de Dropbox), la propiedad y los procesos (empresariales).

Programa de privacidad de Dropbox

Los objetivos, los principios y la responsabilidad del Programa de privacidad de Dropbox.

Programa de confianza de Dropbox

Describe cómo funciona Dropbox y por qué se puede confiar en su solución.

· Seguridad en entornos de pago

Proteger y mantener los entornos de pagos que se utilizan en Dropbox para aceptar pagos con tarjeta de crédito.

Política y acceso de empleados

Los nuevos empleados de Dropbox deben someterse a una comprobación exhaustiva de sus antecedentes, firmar su conformidad con las políticas de seguridad y un acuerdo de confidencialidad, y realizar una formación en materia de seguridad. Solo las personas que han completado estos procedimientos obtienen acceso físico y lógico a los entornos corporativos y de producción, según sus responsabilidades profesionales. Además, todos los empleados deben participar en cursos de formación anuales en materia de seguridad y reciben información periódica relativa a la seguridad en mensajes de correo informativos, presentaciones y charlas, así como en los recursos disponibles en nuestra intranet.

El acceso de los empleados al entorno de Dropbox se mantiene mediante un directorio central y se autentica con una combinación de contraseñas seguras, claves SSH protegidas y la autenticación en dos fases. El acceso remoto requiere el uso de una VPN protegida con autenticación en dos fases y los accesos especiales están sujetos a la revisión y la aprobación del equipo de seguridad. El acceso a la red corporativa y la red de producción está estrictamente limitado de acuerdo con unas políticas definidas. Por ejemplo, el acceso a la red de producción se basa en una clave SSH y está restringido a los equipos de ingenieros que necesitan acceder para cumplir con sus obligaciones. La configuración del cortafuegos está muy controlada y se limita a un reducido número de administradores.



Además, nuestras políticas internas requieren que los empleados que accedan al entorno corporativo y al de producción respeten las prácticas recomendadas de creación y almacenamiento de claves SSH privadas. El acceso a otros recursos, como centros de datos, servicios de configuración de servidores, servidores de protección y servicios de desarrollo en código abierto se garantiza mediante la aprobación explícita por parte de los gestores adecuados. Los supervisores mantienen un registro de la solicitud de acceso, su justificación y aprobación, y el acceso lo autoriza el personal pertinente.

Dropbox emplea controles de acceso técnicos y políticas internas para impedir que los empleados accedan de forma arbitraria a los archivos de los usuarios y para restringir el acceso a los metadatos y a otros datos acerca de las cuentas de los usuarios. Para proteger la privacidad y la seguridad del usuario final, solo el grupo reducido de ingenieros responsables de desarrollar los servicios esenciales de Dropbox tiene acceso al entorno donde se almacenan los archivos de los usuarios. El acceso de cualquier empleado se elimina de inmediato en cuanto deja de trabajar con nosotros.

Puesto que Dropbox se convierte en una extensión de la infraestructura de nuestros clientes, estos pueden estar seguros de que custodiamos sus datos de forma responsable. Consulta la sección Privacidad más adelante para obtener más información.

Gestión de vulnerabilidades

Nuestro equipo de seguridad lleva a cabo pruebas de seguridad automatizadas y manuales regulares y administración de parches, y trabaja con especialistas externos para identificar y reparar posibles vulnerabilidades de seguridad y errores.

Como componente necesario de nuestro sistema de gestión de seguridad de la información, las conclusiones y recomendaciones resultado de todas estas actividades de evaluación se comunican al departamento de dirección de Dropbox, se evalúan y se toman las medidas oportunas en función de las necesidades. Los ingenieros de seguridad asignados documentan, realizan un registro y resuelven los aspectos de alta gravedad.

Gestión de cambios

Todos los procesos de desarrollo, resolución de problemas y parches siguen nuestra Política de gestión de cambios formal, definida por el equipo de Ingeniería de Dropbox para garantizar que los cambios del sistema se hayan probado y autorizado antes de su implementación en los entornos de producción. Los cambios en el código fuente los inician desarrolladores que quieren realizar mejoras en la aplicación o el servicio de Dropbox. Todos los cambios se guardan en un sistema de control de versiones y deben someterse a procedimientos de pruebas de control de calidad para verificar que cumplen los requisitos de seguridad. Si un cambio supera correctamente los procedimientos de control de calidad, termina por aplicarse. Todos los cambios que superan el proceso de control de calidad se implementan automáticamente en el entorno de producción. Para nuestro ciclo de vida de desarrollo de software (SDLC) es necesario adherirse a directrices de codificación así como a la visualización de cambios de código para posibles problemas de seguridad a través de nuestros procesos de revisión manual y garantía de calidad. Los cambios publicados en producción se registran y archivan, y las alertas se envían automáticamente a la administración del equipo de ingeniería de Dropbox.

Los cambios en la infraestructura de Dropbox están restringidos exclusivamente al personal autorizado. El equipo de seguridad de Dropbox es responsable de mantener la seguridad de la infraestructura y garantizar que el servidor, el cortafuegos y otros parámetros de configuración relacionados con la seguridad se actualicen según los estándares del sector. Los conjuntos de reglas del cortafuegos y el acceso a los servidores de producción se revisan de forma periódica.



Pruebas de penetración de seguridad y análisis (internas y externas)

Nuestro equipo de seguridad realiza pruebas de seguridad manuales y automatizadas de las aplicaciones de forma periódica con el fin de identificar y corregir posibles vulnerabilidades y errores de seguridad en nuestras aplicaciones para escritorio, web (Dropbox y Paper) y para móviles (Dropbox y Paper).

Además, Dropbox contrata a proveedores externos para realizar pruebas periódicas de vulnerabilidad y penetración en los entornos de producción. Colaboramos con especialistas externos, otros equipos de seguridad del sector y la comunidad de investigación sobre seguridad para garantizar la seguridad de nuestras aplicaciones. También aprovechamos los sistemas de análisis automáticos para identificar las vulnerabilidades. Este proceso incluye sistemas que desarrollamos de manera interna, sistemas de código abierto que modificamos según nuestras necesidades o proveedores externos que contratamos para un análisis automatizado continuo.

Mantener el contenido dañino alejado de Dropbox

Tenemos funcionalidades de escaneo dedicadas a prevenir el almacenamiento y la distribución de contenido dañino en Dropbox. Nuestros escáneres aprovechan la tecnología propia y las funcionalidades de vanguardia de socios como Microsoft y Google para hacer de Dropbox un lugar seguro para nuestros clientes.

Recompensas por fallos

Aunque trabajamos con empresas profesionales de la identificación de penetración y hacemos nuestras propias pruebas internas, las recompensas por fallos (o programas de recompensas ante vulnerabilidades) sacan partido al conocimiento experto de las comunidades de seguridad. Nuestro programa de recompensas por fallos supone un incentivo para que los investigadores informen de los fallos de software de forma responsable. Esta implicación de la comunidad externa ofrece a nuestro equipo de seguridad un escrutinio independiente de nuestras aplicaciones para mantener a salvo a los usuarios. Nos esforzamos para estar entre los referentes de la industria mediante la generosidad, además de nuestros tiempos de respuesta y reparación.

Hemos definido un ámbito para envíos aptos y aplicaciones de Dropbox, así como una política de divulgación responsable que fomenta la identificación y notificación de vulnerabilidades de seguridad para aumentar la seguridad de los usuarios. Esta política establece las siguientes directrices:

- Comparte todos los detalles del problema de seguridad con nosotros.
- Por favor, respeta nuestras aplicaciones existentes. Las formas de spamming a través de escáneres automatizados de vulnerabilidad no darán lugar a ninguna recompensa o premio, ya que se encuentran explícitamente fuera de alcance.
- Danos un plazo razonable para responder al problema antes de publicar información sobre la incidencia de seguridad.
- · No accedas a los datos de los usuarios ni los modifiques sin el permiso del propietario de la cuenta.
- No veas, modifiques, guardes, almacenes, transfieras ni accedas de ningún otro modo a los datos, ni depures inmediatamente toda la información local al informar de la vulnerabilidad a Dropbox.
- Actúa de buena fe para evitar vulneraciones de la privacidad, destrucción de datos e interrupción o degradación de nuestros servicios (incluida la denegación del servicio).

Se puede avisar de los problemas enviando un informe a Bugcrowd a la siguiente dirección: bugcrowd.com/dropbox.



Seguridad física

Infraestructura

El acceso físico a las instalaciones del entorno de producción de las organizaciones que nos prestan sus servicios está restringido al personal autorizado por Dropbox, según sea necesario para realizar su trabajo. Cualquier persona que requiera un acceso adicional a las instalaciones del entorno de producción tendrá que recibir dicho acceso mediante la aprobación expresa de los supervisores correspondientes.

La administración mantendrá un registro de la solicitud, de la justificación y de la aprobación del acceso que será concedido por el personal pertinente. Una vez recibida la aprobación, un miembro responsable del equipo de infraestructura se pondrá en contacto con la organización que nos presta sus servicios a fin de solicitar el acceso para la persona autorizada. La organización introducirá la información del usuario en sus propios sistemas y ofrecerá al personal autorizado por Dropbox una identificación y, de ser posible, un acceso mediante sensores biométricos. Una vez que se conceda el acceso a las personas autorizadas, el centro de datos será responsable de garantizar que el acceso esté restringido exclusivamente a dichas personas autorizadas.

Oficinas corporativas

Seguridad física

El equipo de seguridad física de Dropbox es responsable de aplicar la política de seguridad física y supervisar la seguridad de nuestras oficinas.

· Política de acceso y visitantes

El acceso físico a las instalaciones corporativas, salvo las entradas públicas y los vestíbulos, está restringido al personal de Dropbox autorizado y a los visitantes registrados que vayan acompañados de empleados de Dropbox. Un sistema de acceso mediante identificación garantiza que solo las personas autorizadas tienen acceso a las zonas restringidas de las instalaciones corporativas.

Acceso a los servidores

El acceso a las zonas donde se encuentran los servidores corporativos y el equipamiento de red está restringido al personal autorizado a través de funciones de acceso elevado que se otorgan mediante un sistema de identificaciones. La lista de personas autorizadas para acceder físicamente al entorno corporativo y al de producción se revisa al menos una vez por trimestre.

Respuesta a incidentes

Contamos con procedimientos y políticas de respuesta a incidentes para abordar los problemas de disponibilidad, integridad, seguridad, privacidad y confidencialidad del servicio. Como parte de nuestros procedimientos de respuesta ante incidentes, tenemos equipo formados para:

- · Responder rápidamente a alertas de posibles incidentes.
- Determinar la gravedad del incidente.



- Si fuera necesario, tomar las medidas necesarias para mitigar y contener el problema.
- Contactar con las partes interesadas internas y externas, así como notificar a los clientes afectados conforme a las obligaciones contractuales relativas a la notificación de incidentes o incumplimiento y a la normativa relevante
- · Recopilar y preservar información relevante para ponerla a disposición de los agentes investigadores.
- Elaborar un análisis de los resultados y desarrollar un plan permanente de evaluación de prioridades.

Los procesos y políticas de respuesta a incidentes se revisan durante las auditorías de SOC 2 e ISO/IEC 27001, entre otras.

Infraestructura de seguridad

Seguridad de la red

Dropbox mantiene de forma diligente la seguridad de la red back-end. Nuestras técnicas de supervisión y seguridad de la red están diseñadas para ofrecer múltiples capas de protección y defensa. Empleamos las técnicas de protección estándar del sector, como cortafuegos, análisis de vulnerabilidades de red, supervisión de la seguridad de la red y sistemas de detección de intrusiones, a fin de garantizar que solo el tráfico permitido y el tráfico no malicioso puedan llegar a nuestra infraestructura.

Nuestra red interna privada está segmentada según el uso y el nivel de riesgo. Las redes principales son las siguientes:

- · Zona DMZ con conexión a Internet
- Zona DMZ de infraestructura prioritaria
- Red de producción
- Red corporativa

El acceso al entorno de producción está restringido a las direcciones IP autorizadas y requiere autenticación en todos los terminales. Las direcciones IP que tienen acceso están asociadas a la red corporativa o a personal autorizado de Dropbox. Las direcciones IP autorizadas se revisan cada trimestre para garantizar la seguridad del entorno de producción. La posibilidad de modificar la lista de direcciones IP está restringida a ciertas personas autorizadas.

El tráfico de Internet destinado a nuestra red de producción está protegido mediante diversas capas de cortafuegos y proxies.

Mantenemos estrictas limitaciones entre la red interna de Dropbox y la red pública con acceso a Internet. El tráfico de la red de producción con origen o destino en Internet se controla cuidadosamente mediante un servicio de proxy específico que, a su vez, está protegido por las restricciones de las reglas del cortafuegos.

Dropbox usa sofisticados conjuntos de herramientas para supervisar los portátiles y ordenadores de sobremesa con sistemas operativos y de producción de Mac y Windows a fin de evitar actividades malintencionadas. Los



registros de seguridad se guardan en una ubicación central para análisis forenses y respuestas a incidentes de conformidad con las políticas de retención estándares del sector.

Dropbox identifica y mitiga los riesgos mediante pruebas de redes y de auditorías periódicas través de equipos de seguridad internos dedicados y especialistas externos.

Puntos de presencia (PoP)

Para optimizar el rendimiento del sitio web de cara a los usuarios, Dropbox utiliza redes de distribución de contenido (CDN) de terceros y puntos de presencia (PoP) alojados en 31 ubicaciones de todo el mundo. Los datos de los usuarios no se almacenan en caché en esas ubicaciones y todos los datos transferidos se cifran con SSL/TLS. El acceso físico y lógico a los PoP alojados por Dropbox está restringido exclusivamente al personal de Dropbox autorizado. Dropbox realiza optimizaciones tanto en la capa de transporte (TCP) como en la capa de aplicación (HTTP).

Emparejamiento

Dropbox cuenta con una política de emparejamiento abierta a todos los clientes que deseen emparejarse con nosotros. Para obtener más información, consulta dropbox.com/peering.

Fiabilidad

Un sistema de almacenamiento solo es bueno si es fiable. Hemos desarrollado Dropbox con varias capas de redundancia con este fin, para proteger el servicio contra pérdidas de datos y garantizar la disponibilidad.

Metadatos de los archivos

Se distribuyen copias redundantes de los metadatos de los archivos entre dispositivos independientes dentro de un centro de datos con, al menos, un modelo de disponibilidad N+2. Se realizan copias de seguridad incrementales al menos cada hora y copias de seguridad totales cada 36 horas. Los metadatos se almacenan en servidores alojados y gestionados por Dropbox en Estados Unidos.

Bloques de archivo

Las copias redundantes de los bloques de archivos se almacenan de forma independiente en, al menos, dos regiones geográficas distintas y se replican de manera fiable en cada región. **Nota:** En el caso de los clientes que opten por que sus archivos se almacenen en nuestra infraestructura alemana, australiana, japonesa o británica, los bloques de archivos se replican únicamente dentro de su respectiva región. Para obtener más información, consulta Centros de datos y proveedores de servicios gestionados a continuación. Tanto Magic Pocket como AWS están diseñados para ofrecer una durabilidad anual de los datos de, al menos, un 99,99999999 %.

La arquitectura, las aplicaciones y los mecanismos de sincronización de Dropbox funcionan conjuntamente para proteger los datos de los usuarios y garantizar su alta disponibilidad. En el caso poco probable de que el servicio se interrumpiera, los usuarios de Dropbox seguirían teniendo acceso a la última copia de sus archivos sincronizada en la carpeta de Dropbox local de los ordenadores vinculados. Se puede acceder a las copias de los archivos sincronizados en la carpeta de Dropbox local o en el cliente de Dropbox para escritorio desde el disco duro de un usuario durante la interrupción del servicio o cuando no haya conexión. Los cambios realizados en los archivos y las carpetas se sincronizan en Dropbox cuando se restaura el servicio o la conectividad.



Documentos de Paper

Distribuimos copias redundantes de datos de documentos de Paper entre dispositivos independientes dentro de un centro de datos con un modelo de disponibilidad N+1. También se realizan copias de seguridad completas de datos de documentos de Paper a diario. Para almacenar documentos de Paper, Dropbox utiliza la infraestructura de AWS en Estados Unidos, diseñada para ofrecer una durabilidad anual de los datos de, al menos, un 99,99999999 %. En el caso poco probable de la interrupción del servicio, los usuarios seguirán teniendo acceso a las últimas copias sincronizadas de sus documentos de Paper en el modo sin conexión dentro de la aplicación móvil.

Sincronización de archivos

Dropbox ofrece un servicio de sincronización de archivos líder en el sector. Nuestros mecanismos de sincronización garantizan una transferencia rápida y eficaz, y permiten acceder a los datos desde cualquier dispositivo. La sincronización de Dropbox es, además, resistente. Si se produce un error de conexión al servicio de Dropbox, el cliente lo restablecerá correctamente cuando se recupere la conexión. Los archivos solo se actualizan en el cliente local si se han sincronizado por completo y se han validado con el servicio de Dropbox. La distribución de carga entre varios servidores garantiza la redundancia y una experiencia de sincronización constante para el usuario final.

Sincronización delta

Este modo de sincronización solo descarga y sube segmentos de archivos. Dropbox almacena cada archivo subido en bloques cifrados individuales, y solo actualiza los bloques modificados.

Sincronización de difusión

En lugar de esperar a que termine la subida de archivos, la sincronización de difusión inicia la descarga de bloques cifrados a un segundo dispositivo antes de que todos los bloques terminen de subirse desde el primer dispositivo. Esta sincronización se utiliza automáticamente cuando se vinculan ordenadores independientes a la misma cuenta de Dropbox o cuando varias cuentas de Dropbox comparten una carpeta.

Ahorrar espacio en el disco duro

Los usuarios pueden liberar espacio de almacenamiento en sus ordenadores definiendo que solo los archivos que quieran de su disco duro estén disponibles sin conexión. Esto libera espacio en el ordenador, ya que se mantiene todo lo demás solo online en dropbox.com.

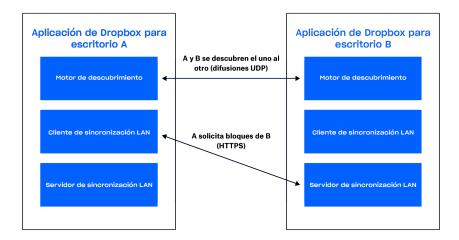
Sincronización LAN

Cuando está activada, esta función descarga los archivos nuevos y actualizados de otros ordenadores que estén conectados a la misma red de área local (LAN). De esta manera, se ahorra tiempo y ancho de banda en comparación con la descarga de archivos de los servidores de Dropbox.

Arquitectura

El sistema de sincronización LAN cuenta con tres componentes principales que se ejecutan en la aplicación para escritorio: el motor de detección, el servidor y el cliente. El motor de detección busca equipos en la red con los que pueda sincronizarse. Solo tendrá en cuenta los equipos que tengan acceso autorizado a las mismas carpetas personales o compartidas de Dropbox. El servidor gestiona las solicitudes de otros equipos de la red y sirve los bloques de archivos solicitados. El cliente solicita a la red bloques de archivos.





Motor de detección

Periódicamente, los diferentes equipos de la red LAN envían paquetes de difusión UDP a través del puerto 17500 (que IANA reserva para la sincronización LAN) y están atentos a estos. Estos paquetes contienen la versión del protocolo que utiliza el ordenador, las carpetas personales y compartidas de Dropbox compatibles, el puerto TCP que se usa para ejecutar el servidor (que puede ser otro si el 17500 no está disponible) y un identificador aleatorio del equipo. Cuando se detecta un paquete, la dirección IP del equipo se añade a una lista para cada carpeta personal o compartida, indicando así que se trata de un posible destino.

Protocolo

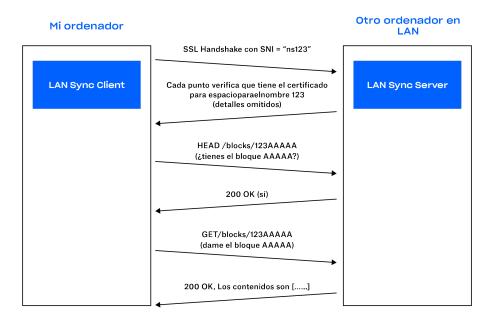
La transferencia de bloques de archivos se realiza mediante el protocolo HTTPS. Cada ordenador ejecuta un servidor HTTPS con terminales. Un cliente sondea varios pares para comprobar si tienen los bloques, pero solo descarga los bloques de un servidor.

Para proteger todos tus datos, nos aseguramos de que solo los clientes autenticados en una carpeta puedan solicitar bloques de archivos. También nos aseguramos de que los ordenadores no se hagan pasar por servidores en las carpetas que no controlan. Para conseguirlo, generamos pares clave/certificado SSL para todas las carpetas compartidas o cuentas de Dropbox personales. Los servidores de Dropbox envían estos pares a los ordenadores del usuario que están autenticados en la carpeta. Los pares clave/certificado rotan cada vez que se produce un cambio en los miembros (por ejemplo, cuando se elimina un usuario de una carpeta compartida). Los dos extremos de la conexión HTTPS deben autenticarse con el mismo certificado (el de la carpeta compartida o de Dropbox). Así, se demuestra que ambos extremos de la conexión están autenticados.

Al establecer una conexión, le indicamos al servidor a qué Dropbox o carpeta personal estamos tratando de conectarnos mediante el indicador de nombre de servidor (SNI), para que el servidor use el certificado correcto.



Dropbox distribuye certif./pares de claves para espacioparaelnombre 123



Servidor/cliente

Con el protocolo descrito anteriormente, el servidor solo necesita saber qué bloques hay y dónde se encuentran.

Según los resultados del motor de detección, el cliente mantiene una lista de pares para cada carpeta compartida y carpeta de Dropbox personal. Cuando el sistema de sincronización LAN recibe una solicitud para descargar un bloque de archivos, envía una solicitud a una muestra aleatoria de los pares que ha detectado para la carpeta compartida o cuenta de Dropbox personal; después, solicita el bloque al primer par que responda positivamente.

Para evitar latencias, empleamos grupos de conexiones que nos permiten reutilizar las conexiones ya iniciadas. No iniciamos una conexión hasta que es necesario y, cuando lo hacemos, la mantenemos activa por si la volvemos a necesitar. También limitamos el número de conexiones a un mismo par.

Si no se encuentra un bloque de archivos o este no se descarga correctamente, o si la conexión es demasiado lenta, el sistema recurre a los servidores de Dropbox para obtener el bloque.

Centros de datos y proveedores de servicios gestionados

Los sistemas corporativos y de producción de Dropbox están alojados en centros de datos de organizaciones de subservicios y proveedores de servicios gestionados situados en diferentes regiones de los Estados Unidos. Los informes de SOC y/o cuestionarios de seguridad y obligaciones contractuales de los proveedores de seguridad del centro de datos de la organización de subservicios se analizan como mínimo una vez al año para garantizar el control de la seguridad. Estos proveedores externos son responsables de los controles de seguridad física, del entorno y funcionales en los límites de la infraestructura de Dropbox. Dropbox es responsable de la seguridad lógica, de red y de aplicaciones de la infraestructura alojada en los centros de datos de terceros.

Nuestro proveedor de servicios gestionados para el procesamiento y el almacenamiento, Amazon Web Services (AWS), es responsable de la seguridad lógica y de red de los servicios de Dropbox proporcionados a través de su infraestructura. Las conexiones están protegidas mediante su cortafuegos, que se configura en un modo de denegación total predeterminado. Dropbox restringe el acceso al entorno a un número limitado de direcciones IP y empleados.

Infraestructura en Alemania, Australia, Japón y el Reino Unido

Dropbox ofrece almacenamiento de bloques de archivo en regiones fuera de Estados Unidos a una serie de clientes que cumplen ciertos requisitos. Nuestra infraestructura está alojada por Amazon Web Services (AWS) en Alemania, Australia, Japón y el Reino Unido, y se replica dentro de la región respectiva para garantizar la redundancia y la protección contra la pérdida de datos. Los archivos de metadatos se almacenan en Estados Unidos en los servidores exclusivos de Dropbox. Los documentos de Paper y las vistas previas se almacenan en este momento en Estados Unidos en todos los casos.

Continuidad del negocio

Dropbox ha establecido un sistema de gestión de la continuidad del negocio (BCMS) en el que se indica cómo reanudar el servicio o seguir proporcionándoselo a los usuarios, así como la manera de actuar en el caso de que se produzca una interrupción de las actividades y procesos esenciales de la empresa. Aplicamos un proceso cíclico que consta de las fases siguientes:

· Evaluación de riesgos y del impacto en el negocio

Analizamos el impacto en el negocio al menos una vez al año para identificar los procesos fundamentales para Dropbox, valorar el impacto potencial de las interrupciones, definir plazos priorizados para la recuperación e identificar tanto nuestras dependencias como a nuestros proveedores más importantes. También evaluamos el riesgo en toda la empresa una vez al año como mínimo. Esta evaluación nos ayuda a identificar, analizar y valorar de manera sistemática el riesgo de que se produzcan interrupciones en Dropbox. La evaluación conjunta del impacto y los riesgos permite conocer las prioridades de continuidad, así como identificar estrategias de mitigación y recuperación para los planes de continuidad del negocio.

· Planes de continuidad del negocio

Los equipos que se han identificado como fundamentales para la continuidad de Dropbox en la evaluación del impacto en el negocio utilizan esta información para desarrollar planes de continuidad del negocio para sus procesos más importantes. Gracias a estos planes, los equipos saben quién es el responsable de reanudar los procesos en caso de emergencia, qué personas de otra oficina o ubicación de Dropbox pueden retomar los procesos durante una interrupción y qué métodos de comunicación deben utilizarse durante un evento de continuidad. Asimismo, nos ayudan a prepararnos para una interrupción al centralizar nuestros planes de recuperación y otra información importante: cuándo y cómo se debe utilizar el plan, datos de contacto y de reunión, aplicaciones importantes y estrategias de recuperación, entre otros datos. Los planes de continuidad de Dropbox se integran en el plan de gestión de crisis de la empresa, donde se establecen los equipos de gestión de crisis y respuesta a incidentes de Dropbox.



· Prueba de los planes

Dropbox prueba determinados elementos de sus planes de continuidad del negocio al menos una vez al año. Estas pruebas se realizan de acuerdo con el ámbito y los objetivos del BCMS, se basan en escenarios apropiados y están bien diseñadas, con objetivos claramente definidos. El ámbito de las pruebas puede ser muy diverso: desde ejercicios de mesa hasta simulaciones de incidentes reales a gran escala. Según los resultados de las pruebas y la experiencia adquirida con incidentes reales, los equipos actualizan y perfeccionan sus planes para solucionar problemas y reforzar sus capacidades de respuesta.

Revisión y aprobación del BCMS

Al menos una vez al año, el equipo directivo revisa los BCMS en el marco de la revisión del Programa de confianza de Dropbox.

Recuperación ante desastres

Disponemos de un plan de recuperación ante desastres para responder a los requisitos de seguridad de la información durante crisis o desastres graves que afecten al funcionamiento de Dropbox Business. El equipo de ingeniería de Dropbox revisa este plan con carácter anual y realiza pruebas de elementos concretos al menos una vez al año. Los hallazgos pertinentes se documentan y registran hasta su resolución.

Nuestro plan de recuperación ante desastres cubre tanto los desastres de durabilidad como de disponibilidad, según se definen a continuación:

- Un desastre de durabilidad consta de uno o varios de los siguientes elementos:
 - Una pérdida completa o permanente de un centro de datos primario que almacena metadatos o varios centros de datos que almacenan bloques de archivo.
 - Pérdida de la capacidad para comunicar o suministrar datos desde un centro de datos donde se almacenan metadatos o desde varios centros de datos donde se almacena el contenido de los archivos.
- Un desastre de disponibilidad consta de uno o varios de los siguientes elementos:
 - · Una interrupción del servicio superior a 10 días.
 - Pérdida de la capacidad para comunicar o suministrar datos desde un servicio de almacenamiento o centro de datos donde se almacenan metadatos, o desde varios servicios de almacenamiento o centros de datos donde se almacenan bloques de archivo.

Definimos un tiempo de recuperación objetivo (RTO, Recovery Time Objective), que es la duración y el nivel de servicio en el que el proceso o servicio de la empresa debe restaurarse tras un desastre, y un punto de recuperación objetivo (RPO, Recovery Point Objective), que es el periodo tolerable máximo en el que podrían perderse los datos como consecuencia de una interrupción del servicio. También medimos el tiempo de recuperación real (RTA, Recovery Time Actual) durante la prueba de recuperación ante desastres, que se lleva a cabo al menos una vez al año.

Los planes de recuperación ante desastres, continuidad del negocio y respuesta a incidentes de Dropbox se deben probar periódicamente y siempre que se produzca un cambio considerable del entorno o la organización.



Seguridad de la aplicación

Interfaces de usuario de Dropbox

Puedes acceder al servicio de Dropbox y utilizarlo a través de diferentes interfaces. Todas tienen funciones y configuraciones de seguridad que procesan y protegen los datos de los usuarios a la vez que garantizan un acceso sencillo.

Web

Esta interfaz está disponible a través de cualquier navegador web moderno. Permite a los usuarios cargar, descargar, ver y compartir sus archivos. La interfaz web también permite a los usuarios abrir versiones locales existentes de archivos a través de la aplicación predeterminada del ordenador.

Escritorio

La aplicación de Dropbox para escritorio es un potente cliente de sincronización que almacena los archivos de manera local para ofrecer acceso sin conexión. Proporciona a los usuarios acceso completo a sus cuentas de Dropbox y se ejecuta en sistemas operativos de Windows y Mac. Los archivos se ven y se pueden compartir directamente dentro de los exploradores de archivos del sistema operativo.

Dispositivos móviles

La aplicación Dropbox está disponible para dispositivos iOS y Android, y permite a los usuarios acceder a todos sus archivos sobre la marcha. Las aplicaciones móviles también permiten acceder a los archivos sin conexión.

API

Las API de Dropbox proporcionan una forma flexible de leer y escribir en cuentas de usuario, y de acceder a funciones avanzadas como la búsqueda, las revisiones y la restauración de archivos. Las API se pueden utilizar para gestionar el ciclo de vida del usuario de una cuenta de Dropbox Business, realizar acciones que afecten a todos los miembros de un equipo y habilitar el acceso a las funciones de administración.

Interfaces de usuario de Paper

Existe la posibilidad de utilizar y acceder al servicio de Paper a través de diferentes interfaces. Cada una de ellas tiene funciones y configuraciones de seguridad que procesan y protegen los datos de los usuarios a la vez que garantizan la facilidad de acceso.

Web

Esta interfaz está disponible a través de cualquier navegador web moderno. Permite a los usuarios crear, ver, editar, descargar y compartir sus documentos de Paper.

Dispositivos móviles

La aplicación móvil de Paper está disponible para dispositivos y tabletas iOS y Android, de modo que los usuarios pueden acceder a todos sus documentos de Paper estén donde estén. La aplicación móvil se ha desarrollado como aplicación híbrida y consiste en código nativo (iOS o Android) alrededor de un navegador web interno.

API

La API de Dropbox que acabamos de describir contiene los puntos de destino y tipos de datos necesarios para gestionar documentos y carpetas en Dropbox Paper, incluyendo asistencia para funcionalidades como gestión de permisos, archivado y borrado permanente.

Cifrado

Datos en tránsito

Para proteger los datos en tránsito entre las aplicaciones de Dropbox y nuestros servidores, Dropbox emplea las tecnologías Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para la transferencia de datos, creando un túnel seguro protegido por un cifrado con Advanced Encryption Standard (AES) de 128 bits o superior. Los datos de archivos en tránsito entre un cliente de Dropbox (actualmente para escritorio, dispositivos móviles, API o web) y el servicio alojado se cifran mediante SSL/TLS. Los datos de documentos Paper en tránsito entre un cliente de Paper (actualmente para dispositivos móviles, API o Web) y el servicio alojado siempre están cifrados mediante SSL/TLS. En los puntos de destino que controlamos (escritorio y dispositivos móviles) y los navegadores actuales, usamos un cifrado robusto compatible con mecanismos de confidencialidad directa total ("perfect forward secrecy") y comprobación de certificado ("certificate pinning"). Además, en el sitio web identificamos todas las cookies de autenticación como seguras y habilitamos la tecnología HTTP Strict Transport Security (HSTS) con includeSubDomains habilitado.

Nota: Dropbox utiliza exclusivamente TSL y ha dejado de usar SSLv3 debido a sus ya conocidas vulnerabilidades. Sin embargo, con mucha frecuencia se hace referencia a TSL como "SSL/TSL", por lo que en el presente documento utilizamos dicha denominación.

Para evitar los ataques "de intermediario", la autenticación de los servidores frontend de Dropbox se lleva a cabo a través de certificados públicos propiedad del cliente. Se negocia una conexión cifrada antes de que se transfiera ningún archivo o documento de Paper para garantizar la entrega segura de los archivos a los servidores frontend de Dropbox.

Datos en reposo

Los archivos de Dropbox subidos por los usuarios se cifran mediante Advanced Encryption Standard (AES) de 256 bits. Los archivos se guardan principalmente en varios centros de datos en bloques de archivos individuales. Cada bloque se fragmenta y se cifra mediante un potente cifrado. Solo se sincronizan los bloques que se hayan modificado desde la versión anterior. Los documentos de Paper en reposo también se cifran mediante Advanced Encryption Standard (AES) de 256 bits. Los documentos de Paper se almacenan en diferentes zonas de disponibilidad mediante sistemas de terceros.

Gestión de claves

La infraestructura de gestión de claves de Dropbox está diseñada con controles de seguridad operativos, técnicos y de procedimientos, con acceso muy limitado a las claves. La generación, el intercambio y el almacenamiento de las claves de cifrado se distribuyen para que el procesamiento esté descentralizado.

· Claves de cifrado de archivos

Por defecto, Dropbox administra las claves de cifrado de archivos en representación de los usuarios para eliminar complejidades, así como para habilitar funciones avanzadas del producto y un control de cifrado potente. Las claves del cifrado de archivos se crean, almacenan y protegen mediante controles de seguridad de infraestructura de sistemas de producción y políticas de seguridad.



· Claves SSH internas

El acceso a los sistemas de producción se restringe con un par de claves SSH únicas. Los procedimientos y las políticas de seguridad requieren la protección de las claves SSH. Un sistema interno gestiona el proceso de intercambio de claves públicas seguras y las claves privadas se almacenan de forma segura. Las claves SSH internas no pueden utilizarse para acceder a sistemas de producción sin un factor secundario para autenticarse.

Distribución de claves

Dropbox automatiza la gestión y distribución de claves confidenciales en los sistemas necesarios para el funcionamiento.

Asignación de certificados

Dropbox proporciona asignación de certificados en navegadores web modernos que admiten la especificación HTTP Public Key Pinning, así como en nuestros clientes de escritorio o móviles. La asignación de certificados es una verificación adicional para garantizar la identidad real del servicio al que te estás conectando y evitar impostores. La utilizamos como medida de protección frente a los métodos que puedan utilizar los hackers para espiar tu actividad.

Protección de los datos de autenticación

Dropbox no se limita a aplicar un algoritmo de hash estándar para proteger las credenciales de inicio de sesión de los usuarios. Siguiendo las prácticas recomendadas del sector, se añade a cada contraseña un resumen criptográfico generado aleatoriamente y, después, se utiliza un algoritmo de hash iterativo para ralentizar el cálculo. Estas prácticas contribuyen a la protección frente ataques de fuerza bruta, diccionario y arcoíris. Como medida de precaución adicional, ciframos los hashes con una clave que se almacena por separado de la base de datos, de modo que las contraseñas están más protegidas cuando solo la base de datos se ve afectada.

Análisis de software dañino

Hemos desarrollado un sistema automatizado que analiza en busca de malware cualquier contenido se comparta fuera de la cuenta del usuario de origen. El sistema emplea tecnología patentada y motores de detección estándares del sector y está diseñado para detener la propagación del malware.

Seguridad del producto

Dropbox ofrece funciones de visibilidad y control administrativo que permiten tanto al departamento técnico como a los usuarios finales gestionar de forma eficiente su empresa y sus datos. Con Dropbox, tienes todo lo que necesitas para trabajar en un solo lugar: tus herramientas, contenido y colaboradores. Es más que almacenamiento seguro, ya que te ofrece una forma inteligente de optimizar tu flujo de trabajo actual.

A continuación se destacan algunas funciones disponibles para los administradores y los usuarios, así como integraciones con terceros para gestionar procesos técnicos básicos.



Nota: Las funciones disponibles varían dependiendo del plan de suscripción. Consulta dropbox.com/business/plans para obtener más información.

Controles de contenido

Proteger los activos comerciales sensibles, como la propiedad intelectual (PI) y la información de identificación personal (PII), es crucial para los equipos de seguridad informática y de datos. Desde permisos de contenido granulares hasta políticas de retención de datos y retenciones legales, Dropbox ofrece soluciones líderes en el sector para administrar, supervisar y proteger tu contenido. A continuación, se presentan los principales productos y funciones de Dropbox que permiten el control de los archivos.

Permisos de contenido detallados y permisos de carpetas y archivos compartidos

Permisos para archivos compartidos

Un miembro del equipo que sea el propietario de un archivo compartido puede eliminar el acceso a éste para usuarios específicos e inhabilitar la publicación de comentarios en el documento.

· Permisos para archivos compartidos

Un miembro del equipo que sea el propietario de una carpeta compartida puede eliminar el acceso a la carpeta para determinados usuarios, cambiar los permisos de visualización o edición de ciertos usuarios y transferir la propiedad de la carpeta. En función de cuáles sean los permisos globales para compartir del equipo, es posible que el propietario de cada carpeta compartida tenga también la opción de controlar si esta se puede compartir con usuarios ajenos al equipo, si otras personas con permisos de edición pueden gestionar la pertenencia y si los enlaces se pueden compartir con usuarios ajenos a la carpeta.

Contraseñas para enlaces compartidos

Todos los enlaces compartidos se pueden proteger con una contraseña definida por el propietario. Antes de que se transmitan los datos del archivo o la carpeta, una capa de control de acceso verifica que se ha enviado la contraseña correcta y que se han cumplido los demás requisitos (por ejemplo, la ACL del equipo, del grupo o de la carpeta). En caso afirmativo, se almacena una cookie en el navegador para que este recuerde que la contraseña se ha verificado. Con los controles para compartir, los administradores también pueden establecer contraseñas predeterminadas en lugar de marcarlas como opcionales para proteger mejor el contenido de tu equipo.

· Caducidad para enlaces compartidos

Los usuarios pueden configurar la fecha de caducidad de los enlaces compartidos para ofrecer acceso temporal a archivos o carpetas. Con los controles para compartir, los administradores también pueden establecer una caducidad predeterminada en lugar de marcarlas como opcionales para proteger mejor el contenido de tu equipo.

Permisos de los documentos y carpetas compartidas de Paper

· Permisos para documentos y carpetas compartidas de Paper

Un miembro del equipo que sea propietario de un documento o carpeta compartida de Paper puede eliminar el acceso a este para usuarios específicos e inhabilitar la edición del documento de Paper.

· Permisos de los documentos de Paper

Un miembro del equipo que sea el propietario de un documento de Paper puede eliminar el acceso a este para usuarios específicos que aparezcan de forma explícita en el panel de compartir. Tanto el propietario como los editores de un documento de Paper pueden cambiar los permisos de vista/edición para usuarios

específicos, así como cambiar la política de enlaces del documento. La política de enlaces regula qué usuarios pueden abrir el documento y qué clase de permiso tienen. El administrador del equipo puede configurar políticas en todo el equipo para los enlaces y el uso compartido de documentos.

Permisos para carpetas de Paper

Un miembro del equipo que forme parte de una carpeta puede cambiar la política de carpeta compartida y eliminar el acceso a usuarios específicos que se hayan añadido de forma explícita a la carpeta.

Acciones de archivo y carpeta

Carpetas de equipo para los archivos

Los administradores pueden crear carpetas del equipo que, de forma automática, conceden a los grupos y otros colaboradores el nivel de acceso pertinente (visualización o edición) al contenido que necesitan.

Controles granulares de acceso y de uso compartido

Los controles de uso compartido permiten a los administradores gestionar la pertenencia y los permisos en el nivel superior o de subcarpeta, para que los usuarios y los grupos dentro y fuera de la empresa solo tengan acceso a carpetas específicas.

· Herramienta de gestión de carpetas de equipo

Los administradores pueden ver sus carpetas del equipo y personalizar las políticas de uso compartido desde una ubicación centralizada para contribuir a evitar el uso indebido de materiales confidenciales.

Carpetas compartidas para documentos de Paper

Los administradores pueden crear carpetas de Paper compartidas que, de forma automática, conceden a los grupos y otros colaboradores el nivel de acceso pertinente (para comentar o editar) al contenido que necesitan.

Borrado remoto

Si un empleado deja el equipo o se pierde algún dispositivo, los administradores pueden borrar de forma remota los datos de Dropbox y las copias locales de los archivos. Los archivos se eliminarán de ordenadores y dispositivos móviles cuando estos se conecten a la red y la aplicación de Dropbox se esté ejecutando.

Transferencia de cuenta

Después de eliminar los permisos de un usuario (ya sea manualmente o mediante servicios de directorio), los administradores pueden transferir tanto los archivos de su cuenta como la propiedad de los documentos de Paper creados por el anterior miembro del equipo desde su cuenta a la de otro a usuario del equipo. La función de transferencia de cuentas puede utilizarse al eliminar un usuario o en cualquier momento, después de eliminar la cuenta del usuario.

Las siguientes capacidades están disponibles como funciones de complemento (ponte en contacto con el departamento de ventas para obtener más información).

· Escanear contenido

Con el complemento Controles avanzados de equipo y contenido, los clientes de Dropbox Business Advanced y Enterprise pueden explorar el contenido nuevo y existente de Dropbox para localizar y evitar las vulnerabilidades de los datos.



· Configuración y activación de flujos de trabajo personalizados

Con el complemento Controles avanzados de contenido y equipos, los administradores pueden tomar medidas personalizadas contra los archivos que infrinjan las políticas de la empresa.

· Configuración de alertas

Los administradores pueden vigilar las amenazas de seguridad en tiempo real y evitar las vulnerabilidades de los datos. Recibe alertas sobre los archivos que se comparten externamente y los datos sensibles que se escanean.

Visibilidad del contenido

Alertas y notificaciones de seguridad

Los administradores de Dropbox Enterprise pueden recibir notificaciones en tiempo real cuando se detecten actividades abusivas o de riesgo, o bien posibles filtraciones de datos en sus cuentas. Se pueden supervisar los siguientes eventos:

- · Supresiones masivas
- Movimientos masivos de datos
- · Contenido sensible compartido de forma externa
- Malware compartido desde fuera de tu equipo
- · Malware compartido desde dentro de tu equipo
- Demasiados intentos fallidos de inicio de sesión
- · Inicio de sesión desde un país de alto riesgo
- · Detección de ransomware

Dropbox también permite configurar los límites de las alertas, determinar quién las recibe y activarlas para que aparezcan cuando los datos confidenciales se compartan a nivel externo. Los administradores también pueden marcar las alertas como en revisión, resueltas o descartadas. Además, un widget muestra la información general de las alertas del equipo y las tendencias de la última semana.

Informe y página de uso compartido externo

Dropbox proporciona visibilidad adicional con el informe y la página de uso compartido externo. Los administradores pueden crear un informe desde la página de información o desde la página de uso compartido externo. El informe enumera todos los archivos y las carpetas del equipo que se comparten fuera del equipo y todos los vínculos compartidos. La página de uso compartido externo es una página adicional de la Consola de administración que permite a los administradores ver y filtrar (tipo de archivo, quién lo compartió, configuración de enlaces y muchos más) a través de los archivos y las carpetas compartidos directamente fuera del equipo y los enlaces compartidos.



Controles para compartir

La configuración de uso compartido les da a los administradores del equipo más control sobre el uso compartido y el acceso al contenido de su equipo. Los administradores pueden establecer caducidades por defecto a nivel de equipo, restricciones de contraseña o ambas. Estas restricciones reducen el riesgo de pérdida de datos, ya que los usuarios no tienen que establecer restricciones.

Clasificación de datos

Los equipos en Dropbox Enterprise pueden tener los datos personales y confidenciales etiquetados automáticamente para protegerlos mejor de ser expuestos. Los administradores recibirán alertas de prevención de pérdida de datos (DLP) por correo electrónico y en la Consola de administración cuando los archivos o carpetas guardados dentro de las carpetas del equipo que contienen información confidencial se compartan fuera de su equipo. Los administradores tienen la capacidad de identificar y clasificar automáticamente los datos confidenciales almacenados en las carpetas compartidas y en las carpetas personales de los miembros del equipo. Los administradores de Dropbox Enterprise pueden activar la clasificación automática de datos en la Consola de administración.

Complemento de gobierno de datos

El gobierno de datos es el conjunto de procesos, tecnologías y equipos que se unen para gestionar y proteger los recursos de información de una empresa. Esto incluye la capacidad de almacenar, identificar, descubrir y recuperar datos corporativos según sea necesario.

El complemento de gobierno de datos de Dropbox incluye un conjunto de funciones con las que las organizaciones pueden controlar y proteger mejor sus datos, además de reducir los riesgos y costes asociados a la satisfacción de las necesidades normativas y de cumplimiento. Actualmente, este complemento incluye cuatro funciones clave para los administradores de equipo y los administradores de cumplimiento.

· Historial de versiones ampliado

Tu historial de versiones de archivos predeterminado depende del tipo de cuenta de Dropbox que tengas. Sin embargo, con Dropbox Business puedes adquirir el complemento Historial de versiones ampliado (EVH) por separado o como parte del paquete de complementos de gobernanza de datos que permite recuperar cualquier archivo eliminado o modificado en los últimos 10 años.

Retenciones legales

Si se aplica una retención legal a un miembro del equipo, los administradores de equipo y de cumplimiento podrán ver y exportar el contenido que ese miembro haya creado o modificado. A los miembros a los que se les aplica una retención legal no se les notifica dicha retención y siguen teniendo los mismos permisos para crear, editar y eliminar archivos.

Retención de datos

La retención de datos permite a los equipos y a los administradores de cumplimiento evitar la eliminación accidental de contenido requerido por las regulaciones que se retendrá durante cierto tiempo. Esta función permitirá a los clientes conservar los datos más allá de 10 años desde la última fecha de "revisión".

· Eliminación de datos

La eliminación de datos permite a los administradores de equipos y de cumplimiento eliminar permanentemente los datos en una fecha específica para cumplir con los requisitos de retención y eliminación de los datos. Los administradores pueden supervisar la actividad recibiendo informes que les avisan de las próximas eliminaciones de archivos.



Recuperación y control de versiones

Los clientes de Dropbox Business tienen la posibilidad de restaurar archivos y documentos de Paper eliminados y recuperar versiones anteriores de sus archivos y documentos de Paper, lo que garantiza que sea posible supervisar y recuperar los cambios realizados en los datos más importantes.

Seguridad de datos en dispositivos móviles

Borrado de datos

Para reforzar la seguridad, el usuario puede habilitar la opción para borrar todos los datos de Dropbox en el dispositivo si se introducen códigos incorrectos 10 veces seguidas.

Almacenamiento interno y archivos sin conexión

De forma predeterminada, los archivos no se guardan en la memoria de almacenamiento interna de los dispositivos móviles. Los clientes de Dropbox para dispositivos móviles ofrecen la posibilidad de guardar archivos y carpetas individuales en el dispositivo para verlos sin conexión. Si un dispositivo se desvincula de una cuenta de Dropbox, ya sea desde la interfaz para dispositivos móviles o desde el sitio web, esos archivos y carpetas se eliminan automáticamente del almacenamiento interno del dispositivo.

Documentos de Paper sin conexión

Cuando se desvincula un dispositivo de Paper a través de la página de seguridad de la cuenta de Dropbox, se cierra la sesión del usuario y se eliminan los documentos de Paper sin conexión del almacenamiento interno del dispositivo.

Controles de equipo

No hay dos organizaciones exactamente iguales, por lo que hemos desarrollado varias herramientas que permiten a los administradores personalizar Dropbox Business según las necesidades específicas de sus equipos. Dropbox Business incluye herramientas para que los usuarios finales puedan proteger mejor sus cuentas y sus datos. La autenticación, la recuperación, el registro y otras funciones de seguridad que se describen a continuación están disponibles a través de las diferentes interfaces de usuario de Dropbox.

A continuación, se muestran varias funciones de control y visibilidad disponibles en la Consola de administración de Dropbox Business.

Permisos de contenido detallados

· Roles de administrador por niveles

Dropbox ofrece roles de administrador por niveles que permiten gestionar el equipo de forma más eficiente. A los administradores de cuenta se les puede asignar uno de los tres niveles de acceso. No hay límite de administradores en los equipos y cualquier miembro puede ser designado como tal.

Administrador de equipo

Pueden establecer permisos globales de seguridad y de uso compartido, crear administradores y gestionar a los miembros. El administrador de equipo tiene todos los permisos de administración disponibles. Además, es el único que puede asignar o cambiar los roles de administrador. Debe haber siempre al menos un administrador de equipo en cada cuenta de Dropbox Business.



· Administrador de gestión de usuarios

Pueden encargarse de la mayoría de las tareas de administración del equipo, como añadir y eliminar miembros, administrar grupos y ver los registros de actividad del equipo.

· Administrador de apoyo

Pueden responder a solicitudes de servicio comunes de los miembros del equipo; por ejemplo, restaurar archivos eliminados o ayudar a los miembros del equipo que tengan problemas con la verificación en dos pasos. Los administradores de asistencia también pueden restablecer contraseñas de usuarios que no sean administradores y exportar un registro de la actividad de un miembro del equipo concreto.

Administrador de facturación

Puede acceder a las páginas de facturación en la consola de administración.

Administrador de contenidos

Puede crear y administrar carpetas de equipo dentro del Administrador de contenido.

· Administrador de informes

Puede crear informes dentro de la Consola de administración y tiene acceso a la página Actividad.

Administrador de seguridad

Puede administrar alertas de seguridad, uso compartido externo y riesgos para la seguridad.

· Administrador de cumplimiento (solo disponible para equipos con el complemento Gobierno de datos)

Puede gestionar las páginas de Gobierno de Datos (retenciones legales, retención de datos y eliminación de datos) y también acceder al Administrador de contenido.

Grupos

Los equipos pueden crear y gestionar listas de miembros dentro de Dropbox y concederles acceso a carpetas específicas con facilidad. Dropbox también puede sincronizar grupos de Active Directory con el conector de Active Directory.

Grupos administrados por la empresa

Solo los administradores pueden establecer, revocar y gestionar la pertenencia a este tipo de grupo. Los usuarios no pueden solicitar unirse a un grupo gestionado por la empresa ni abandonarlo.

· Grupos administrados por usuarios

Los administradores pueden elegir si los usuarios pueden crear y gestionar sus propios grupos. Los administradores también pueden hacer que un grupo gestionado por usuarios pase a ser un grupo gestionado por la empresa en cualquier momento para obtener el control sobre dicho grupo.

· Restricción de varias cuentas en ordenadores

Los administradores pueden impedir que los miembros del equipo vinculen una segunda cuenta de Dropbox a ordenadores que estén vinculados a su cuenta de Dropbox del trabajo.



· Estado de usuario suspendido

Los administradores pueden inhabilitar el acceso de un usuario a su cuenta y, al mismo tiempo, conservar sus datos y relaciones de uso compartido a fin de proteger la información de la empresa. Posteriormente, los administradores pueden reactivar o eliminar la cuenta.

Inicio de sesión como usuario

Los administradores de equipo pueden iniciar sesión como miembros de sus equipos. De este modo, tienen acceso directo a los archivos, carpetas y documentos de Paper de las cuentas de los miembros para hacer cambios, compartir contenido en nombre de estos o llevar a cabo auditorías de las acciones realizadas en los archivos. Las actividades de inicio de sesión se capturan en el registro de actividad del equipo, y los administradores pueden determinar si los miembros reciben notificaciones de dichas actividades.

· Permisos para compartir

Los administradores del equipo tienen un control absoluto sobre la capacidad del equipo para compartir contenido a través de Dropbox. Pueden controlar lo siguiente:

- Si los miembros del equipo pueden compartir archivos y carpetas con usuarios ajenos al equipo.
- · Si los miembros del equipo pueden editar carpetas pertenecientes a usuarios ajenos al equipo.
- Si los usuarios ajenos al equipo pueden utilizar los enlaces compartidos que creen los miembros del equipo.
- Si los miembros del equipo pueden crear solicitudes de archivos y recopilar archivos de miembros del equipo o usuarios ajenos a este.
- · Si otras personas pueden ver y comentar archivos pertenecientes al equipo.
- Si los miembros del equipo pueden compartir documentos y carpetas de Paper con usuarios ajenos al equipo.
- · Se otorgan permisos de eliminación permanente.

El administrador de equipo de una cuenta de Dropbox Business puede limitar la capacidad de eliminar archivos y documentos de Paper únicamente a los administradores de equipo.

Incorporación y aprovisionamiento de usuarios

Métodos de aprovisionamiento de usuarios y gestión de identidad

Invitación por correo electrónico

En la Consola de administración de Dropbox Business está disponible una herramienta que permite a los administradores generar manualmente invitaciones por correo electrónico.

Active Directory

Los administradores de Dropbox Business pueden automatizar la creación y eliminación de cuentas desde un sistema de Active Directory existente a través de nuestro conector de Active Directory o un proveedor de identidades externo. Una vez integrado, Active Directory se puede utilizar para gestionar los miembros del equipo.

· Inicio de sesión único

Dropbox Business se puede configurar de modo que los miembros del equipo puedan acceder iniciando sesión en un proveedor de identidades centralizado. Nuestra implementación de inicio de sesión único, que utiliza el estándar Security Assertion Markup Language 2.0 (SAML 2.0), consigue que el aprovisionamiento sea más fácil y seguro al encargar a un proveedor de identidades de confianza la autenticación y el acceso de miembros



del equipo a Dropbox sin necesidad de gestionar contraseñas adicionales. Dropbox también cuenta con los principales proveedores de gestión de identidades para el aprovisionamiento y desaprovisionamiento automático de usuarios. Consulta la sección Integraciones con la API de Dropbox Business a continuación.

API

Los clientes pueden utilizar la API de Dropbox Business para crear soluciones personalizadas de gestión de identidades y aprovisionamiento de usuarios. Consulta la sección Integraciones con la API de Dropbox Business a continuación.

Verificación en dos pasos

Esta función de seguridad tan recomendable añade una capa adicional de protección a la cuenta de Dropbox de un usuario. Una vez habilitada la verificación en dos pasos, además de la contraseña, Dropbox solicitará un código de seguridad de seis dígitos al iniciar sesión o vincular un nuevo dispositivo (equipo de escritorio, teléfono o tablet).

- Los administradores pueden exigir la verificación en dos pasos a todos los miembros del equipo o solo a algunos.
- Los administradores pueden supervisar qué miembros del equipo tienen habilitada la verificación en dos pasos.
- Los códigos de autenticación en dos pasos de Dropbox se pueden recibir en un mensaje de texto o por contraseñas temporales de un solo uso (TOPT).
- En caso de que un usuario no pueda recibir códigos de seguridad por estos métodos, puede emplear un código de recuperación de 16 dígitos. Si lo prefiere, también puede usar un número de teléfono secundario para recibir un mensaje de texto con el código de recuperación.
- Dropbox también es compatible con el estándar Universal 2nd Factor (U2F) de FIDO, que permite a los usuarios autenticarse con una llave de seguridad USB que hayan configurado, en lugar de con un código de seis dígitos.

Instalador de empresa

Los administradores que requieran un aprovisionamiento a escala y deseen instalar Dropbox para escritorio pueden usar nuestro instalador de empresa para Windows, que permite hacerlo de forma silenciosa y remota mediante soluciones de gestión de software y mecanismos de implementación.

Dispositivos administrados e inicio de sesión

Administración de movilidad empresarial (EMM)

Dropbox se integra con proveedores de EMM externos para que los administradores de Dropbox Business con un plan Enterprise puedan controlar mejor cómo utilizan Dropbox en dispositivos móviles los miembros del equipo. Los administradores pueden restringir el uso de aplicaciones móviles en las cuentas de Dropbox Enterprise únicamente a los dispositivos gestionados (ya sean personales o facilitados por la empresa), obtener visibilidad del uso de las aplicaciones (incluidos el almacenamiento disponible y las ubicaciones de acceso) y efectuar un borrado remoto de un dispositivo en caso de pérdida o robo. Ten en cuenta que no es posible gestionar la aplicación móvil de Paper por EMM.

· Aprobaciones de dispositivos

Dropbox permite a los administradores de Dropbox Education y Dropbox Business con planes Advanced y Enterprise establecer límites en lo que respecta al número de dispositivos que un usuario puede sincronizar con la aplicación, así como elegir si las aprobaciones las gestionan los usuarios o los administradores.



Además, los administradores pueden crear una lista de excepciones de usuarios que no están restringidos a un número determinado de dispositivos. Ten en cuenta que la aplicación móvil de Paper no se incluye en la aprobación de dispositivos.

· Requisito de verificación en dos pasos

Los administradores pueden requerir la verificación en dos pasos a todos los miembros del equipo o solo a miembros específicos. Se puede forzar el uso de otros métodos de autenticación multifactorial a través de la implementación del inicio de sesión único (SSO).

· Control de contraseñas

Los administradores de equipos de Education, Advanced y Enterprise pueden exigir a los miembros que establezcan y mantengan contraseñas fuertes y complejas para sus cuentas. Cuando esta función está activada, la sesión web se cerrará para los miembros del equipo y se les pedirá que generen una nueva contraseña cuando inicien sesión. Una herramienta integrada analiza la seguridad de las contraseñas al compararlas con una base de datos de palabras, nombres, patrones y números que suelen utilizarse mucho. Si un usuario introduce una contraseña habitual, se le pedirá que genere una más original y difícil de adivinar. Los administradores también pueden restablecer contraseñas para todo el equipo o de cada usuario por separado.

· Administración de dominios

Dropbox proporciona un conjunto de herramientas para que las empresas simplifiquen y agilicen el proceso de incorporación de usuarios y el control del uso de Dropbox.

Verificación de dominios.

Las empresas pueden reclamar la propiedad de sus dominios y desbloquear otras herramientas de qestión de dominios.

Imposición de invitaciones.

Los administradores pueden exigir a los usuarios individuales que hayan sido invitados al equipo de Dropbox de la empresa que migren al equipo o cambien la dirección de correo electrónico de su cuenta personal.

· Información de dominio.

Los administradores pueden ver información clave, como el número de cuentas de Dropbox individuales que utilizan direcciones de correo electrónico de la empresa.

Captura de cuentas.

Los administradores pueden obligar a todos los usuarios de Dropbox que utilicen una dirección de correo electrónico de la empresa a que se unan al equipo de la empresa o cambien la dirección de correo electrónico de su cuenta personal.

Control de la sesión web

Los administradores pueden controlar cuánto tiempo pueden mantener una sesión iniciada en dropbox.com los miembros del equipo. También pueden limitar la duración de todas las sesiones web y/o las inactivas. Las sesiones que lleguen a los límites establecidos se cerrarán automáticamente. Los administradores también pueden hacer un seguimiento y finalizar las sesiones web de los usuarios individuales.

· Acceso a aplicaciones

Los administradores disponen de capacidad para ver y revocar el acceso de aplicaciones externas a las cuentas de los usuarios.

Dispositivos desvinculados

El administrador puede desvincular los ordenadores y dispositivos móviles conectados a cuentas de usuarios a través de la Consola de administración o de la configuración de seguridad de la cuenta del usuario. En



ordenadores, la desvinculación elimina los datos de autenticación y ofrece la posibilidad de eliminar las copias locales de los archivos la próxima vez que el ordenador se conecte (consulta **Borrado remoto** a continuación). En dispositivos móviles, la desvinculación elimina los archivos marcados como favoritos, los datos almacenados en la memoria caché y la información de inicio de sesión. La desvinculación también elimina los documentos de Paper sin conexión de la aplicación móvil. Si está habilitada la verificación en dos pasos, los usuarios tendrán que autenticar otra vez los dispositivos para volver a vincularlos. Además, la configuración de las cuentas de usuario incluye una opción para enviar automáticamente una notificación cuando se vincule un dispositivo.

Control de la red

Los administradores de Dropbox Business con un plan Enterprise pueden restringir el uso de Dropbox dentro de la red de la empresa para que solo puedan acceder con la cuenta del equipo Enterprise. Esta función se integra con el proveedor de seguridad de la red de la empresa para bloquear el tráfico que provenga del exterior de la cuenta autorizada en ordenadores. Ten en cuenta que Paper no permite la gestión a través del control de red.

Seguridad móvil

Escáner de huella dactilar

Los usuarios pueden habilitar Touch ID o Face ID en los dispositivos iOS y el desbloqueo con huella dactilar (si se admite) en los dispositivos Android como método de desbloqueo de la aplicación de Dropbox para móviles.

Visibilidad de acceso

Verificación de identidad ante el servicio de asistencia técnica

Antes de resolver un problema o de que el servicio de asistencia técnica de Dropbox proporcione información sobre la cuenta, el administrador de la cuenta deberá proporcionar un código de seguridad aleatorio de un solo uso para validar su identidad. Este PIN solo está disponible en la Consola de administración.

Actividad de la cuenta de usuario

Cada usuario puede ver las siguientes páginas de la configuración de su cuenta para obtener información actualizada acerca de sus propias actividades.

Página compartida

En esta página se muestran las carpetas compartidas que hay en la cuenta de Dropbox del usuario, así como las carpetas compartidas que este puede añadir. Un usuario puede dejar de compartir carpetas y archivos y establecer permisos para compartir.

Página de archivos

Esta página muestra los archivos que han sido compartidos con el usuario y la fecha en la que esta actividad tuvo lugar. El usuario tiene la opción de eliminar su acceso a estos archivos. Para ver documentos de Paper que otras personas hayan compartido con el usuario, solo hay que dirigirse a la página "Compartido conmigo", en la interfaz de navegación de Paper.

Página de enlaces

En esta página se muestran todos los enlaces compartidos activos que ha creado el usuario y la fecha de creación de cada uno. También se muestran todos los enlaces que otras personas han compartido con el usuario. Los usuarios pueden inhabilitar enlaces o cambiar los permisos.



· Notificaciones por correo electrónico

El usuario puede optar por recibir una notificación por correo electrónico de inmediato cuando un nuevo dispositivo o una aplicación se vinculen a su cuenta de Dropbox.

Permisos de cuenta de usuario

· Dispositivos vinculados

La sección Dispositivos de la configuración de seguridad de la cuenta de un usuario muestra todos los equipos de escritorio y los dispositivos móviles vinculados a la cuenta del usuario. Se muestran la dirección IP, el país y la hora aproximada de la actividad más reciente para cada equipo de escritorio. El usuario puede desvincular cualquier dispositivo, con la posibilidad de hacer que los archivos se eliminen la próxima vez que el dispositivo vuelva a conectarse.

Sesiones web activas

La sección **Sesiones** muestra todos los navegadores web con sesión iniciada actualmente en la cuenta del usuario. Para cada uno de ellos, se muestran la dirección IP, el país y la hora de inicio de la última sesión, así como la hora aproximada de la actividad más reciente. El usuario puede cancelar cualquier sesión de forma remota desde la configuración de seguridad de la cuenta.

Aplicaciones enlazadas

La sección Aplicaciones vinculadas ofrece una lista de todas las aplicaciones externas que tienen acceso a la cuenta del usuario, así como el tipo de acceso del que dispone cada aplicación. El usuario puede revocar el permiso de cualquier aplicación para acceder a su Dropbox.

Feed de actividad

Dropbox Business registra las acciones de los archivos en el feed de actividad del equipo, al que se puede acceder desde la Consola de administración. El feed de actividad ofrece opciones de filtro flexibles que permiten a los administradores llevar a cabo investigaciones centradas en actividades relativas a archivos, cuentas o documentos de Paper. Por ejemplo, pueden ver el historial completo de un archivo o documento de Paper y cómo han interactuado con él los usuarios, o bien ver toda la actividad del equipo durante un periodo determinado. El feed de actividad se puede exportar como un informe en formato CSV y también se integra directamente en un producto de SIEM (gestión de eventos e información de seguridad) u otra herramienta de análisis a través de soluciones de colaboradores externos. En el feed de actividad se registran los siguientes eventos:

· Compartir archivos, carpetas y enlaces

Cuando procede, los informes especifican si las acciones implican a usuarios ajenos al equipo.

Archivos compartidos

- · Adición o eliminación de un miembro del equipo o un usuario ajeno a este.
- · Cambio en los permisos de un miembro del equipo o un usuario ajeno a este.
- Adición o eliminación de un grupo.
- · Adición de un archivo compartido a la cuenta de Dropbox del usuario.
- Visualización del contenido de un archivo compartido a través de una invitación a un archivo o una carpeta.
- · Copia del contenido compartido en la cuenta de Dropbox del usuario.
- · Descarga del contenido compartido.
- · Comentario en un archivo.



- · Comentario resuelto o no resuelto.
- · Eliminación de un comentario.
- · Suscripción o anulación de la suscripción a las notificaciones de comentarios.
- · Reclamación de una invitación a un archivo perteneciente al equipo.
- Solicitud de acceso a un archivo perteneciente al equipo.
- · Revocación del uso compartido de un archivo.

Carpetas compartidas

- · Creación de una carpeta compartida.
- Adición o eliminación de un miembro del equipo, un usuario ajeno a este o un grupo.
- Adición de una carpeta compartida a la cuenta de Dropbox del usuario, o revocación del usuario de su propio acceso a una carpeta compartida.
- Adición de una carpeta compartida desde un enlace.
- Cambio en los permisos de un miembro del equipo o un usuario ajeno a este.
- · Transferencia de la propiedad de una carpeta a otro usuario.
- · Revocación del uso compartido de una carpeta.
- · Reclamación de la pertenencia a una carpeta compartida.
- Solicitud de acceso a una carpeta compartida.
- · Adición del usuario solicitante a una carpeta compartida.
- Bloqueo o desbloqueo de usuarios ajenos al equipo para añadirlos a una carpeta.
- · Permiso para que cualquier miembro del equipo o solo el propietario añada personas a una carpeta.
- · Cambio del acceso de grupo a una carpeta compartida.

Enlaces compartidos

- · Creación o eliminación de un enlace.
- Permiso para que cualquier persona que tenga el enlace o solo los miembros del equipo puedan ver el contenido de un enlace.
- · Protección con contraseña del contenido de un enlace.
- · Definición o eliminación de la fecha de caducidad de un enlace.
- Visualización de un enlace.
- Descarga del contenido de un enlace.
- Copia del contenido de un enlace en la cuenta de Dropbox del usuario.
- · Creación de un enlace a un archivo por medio de una aplicación de API.
- · Enlace compartido con un miembro del equipo, un usuario ajeno a este o un grupo.
- Autorización o desautorización de usuarios ajenos al equipo para ver enlaces a los archivos de una carpeta compartida.
- · Uso compartido de un álbum.



Solicitud de archivos

- · Creación, cambio, cierre o eliminación de una solicitud de archivos.
- Adición de usuarios a una solicitud de archivos.
- · Adición o eliminación de la fecha límite de una solicitud de archivos.
- Cambio de una carpeta de solicitudes de archivos.
- · Archivos recibidos a través de una solicitud de archivos.
- · Archivos recibidos a través de Email to Dropbox.

Actividades relacionadas con carpetas y archivos individuales

- · Adición de un archivo a Dropbox.
- · Carpeta creada
- · Visualización de un archivo.
- · Edición de un archivo.
- · Descarga de un archivo.
- · Copia de un archivo o una carpeta.
- · Traslado de un archivo o una carpeta.
- · Archivo o carpeta renombrados
- · Recuperación de la versión anterior de un archivo.
- · Recuperación de cambios en archivos.
- · Restauración de un archivo eliminado.
- Eliminación de un archivo o una carpeta.
- · Eliminación permanente de un archivo o una carpeta.

Inicios de sesión correctos y fallidos.

- · Intento de inicio de sesión correcto o fallido.
- · Intento de inicio de sesión fallido o error mediante el inicio de sesión único (SSO).
- Intento de inicio de sesión fallido o error a través de EMM.
- Cierre de sesión.
- · Cambio de dirección IP de la sesión web.

Contraseñas

Cambios en la configuración de contraseñas o de la verificación en dos pasos. Los administradores no pueden ver las contraseñas de los usuarios.

- · Cambio o restablecimiento de contraseña.
- · Habilitación, restablecimiento o inhabilitación de la verificación en dos pasos.



- · Configuración o modificación de la verificación en dos pasos para utilizar SMS o una aplicación móvil.
- · Adición, modificación o eliminación de un número de teléfono para la verificación en dos pasos.
- · Adición o eliminación de una clave de seguridad para la verificación en dos pasos.

Pertenencia

Usuarios incorporados al equipo o que lo han abandonado.

- Invitación de un miembro del equipo.
- · Incorporación al equipo.
- · Eliminación de un miembro del equipo.
- · Suspensión o anulación de un miembro del equipo.
- · Recuperación de un miembro del equipo eliminado.
- · Solicitud de incorporación al equipo basada en el dominio de la cuenta.
- · Aprobación o rechazo de una solicitud de incorporación al equipo basada en el dominio de la cuenta.
- Envío de invitaciones a cuentas del dominio.
- · Incorporación de un usuario al equipo en respuesta a la captura de cuentas.
- · Abandono de un usuario del dominio en respuesta a la captura de cuentas.
- Autorización o desautorización de miembros del equipo para sugerir nuevos miembros.
- · Sugerencia de nuevo miembro del equipo.

Aplicaciones

Vinculación de aplicaciones de terceros a cuentas de Dropbox.

- · Autorización o eliminación de una aplicación.
- · Autorización o eliminación de una aplicación del equipo.

Dispositivos

Vinculación de ordenadores o dispositivos móviles a cuentas de Dropbox.

- Vinculación o desvinculación de un dispositivo.
- · Uso del borrado remoto y eliminación correcta de todos los archivos o eliminación fallida de algunos.
- · Cambio de dirección IP de un ordenador o dispositivo móvil.

Acciones administrativas

Cambios en la configuración de la Consola de administración, como los permisos de carpetas compartidas.

- Autenticación e inicio de sesión único
 - · Restablecimiento de la contraseña de un miembro del equipo.
 - · Restablecimiento de las contraseñas de todos los miembros del equipo.
 - · Autorización o desautorización de miembros del equipo para inhabilitar la verificación en dos pasos.



- Habilitación o inhabilitación del inicio de sesión único.
- · Imposición del uso del inicio de sesión único.
- Cambio o eliminación de la URL de inicio de sesión único.
- · Actualización del certificado de inicio de sesión único.
- Cambio del modo de identidad del inicio de sesión único.

Pertenencia

- Autorización o desautorización de usuarios para solicitar la incorporación al equipo basada en el dominio de la cuenta
- Configuración de las solicitudes de incorporación al equipo para que se aprueben automáticamente o requieran la aprobación manual de un administrador.

Gestión de cuentas de miembros

- · Cambio de nombre de un miembro del equipo.
- Cambio de dirección de correo electrónico de un miembro del equipo.
- · Concesión o eliminación de estado administrativo, o cambio de rol administrativo.
- Inicio o cierre de sesión como miembro del equipo.
- · Transferencia o eliminación del contenido de la cuenta de un miembro eliminado.
- Eliminación permanente del contenido de la cuenta de un miembro eliminado.

Configuración global de uso compartido

- Autorización o desautorización de miembros del equipo para añadir carpetas compartidas pertenecientes a usuarios ajenos al equipo.
- Autorización o desautorización de miembros del equipo para compartir carpetas con usuarios ajenos al equipo.
- Activación de las advertencias que se muestran a los usuarios antes de compartir carpetas con usuarios ajenos a su equipo.
- · Autorización o desautorización de usuarios ajenos al equipo para ver enlaces compartidos.
- · Configuración de los enlaces compartidos para que sean exclusivos del equipo de forma predeterminada.
- Autorización o desautorización de personas para hacer comentarios en archivos.
- Autorización o desautorización de miembros del equipo para crear solicitudes de archivos.
- · Adición, cambio o eliminación de un logotipo para las páginas de enlaces compartidos.
- Autorización o desautorización de miembros del equipo para compartir documentos y carpetas de Paper con usuarios ajenos al equipo.

Gestión de carpetas de equipo para archivos

- · Creación de una carpeta del equipo.
- Cambio de nombre de una carpeta del equipo.
- · Archivado o desarchivado de una carpeta del equipo.
- · Eliminación permanente de una carpeta del equipo.
- · Conversión de una carpeta del equipo en una carpeta compartida.



Administración de dominios

- Intento de verificar o verificación correcta de un dominio, o eliminación de un dominio.
- · Verificación o eliminación de un dominio.
- Habilitación o inhabilitación del envío de invitaciones de dominio.
- · Activación o desactivación de la invitación automática de nuevos usuarios.
- · Cambio del modo de captura de cuentas.
- · Concesión o revocación de la captura de cuentas por parte de la asistencia de Dropbox.

Gestión de movilidad empresarial (EMM)

- · Activación de EMM para el modo de prueba (opcional) o de implantación (obligatoria).
- · Actualización del token de EMM.
- Adición o eliminación de miembros del equipo en la lista de usuarios excluidos de EMM.
- · Inhabilitación de EMM.
- · Ha creado un informe de listas de excepciones de EMM.
- · Creación de un informe de uso de aplicaciones móviles de EMM.

Cambios en otra configuración del equipo

- Fusión de equipos.
- Actualización del equipo a Dropbox Business o a un equipo gratuito.
- Cambio de nombre del equipo.
- · Creación de un informe de actividad del equipo.
- Autorización o desautorización de miembros del equipo para tener más de una cuenta vinculada a un ordenador.
- · Permiso para que todos los miembros del equipo o solo los administradores puedan crear grupos.
- · Autorización o desautorización de miembros del equipo para eliminar archivos de forma permanente.
- Inicio o finalización de una sesión de asistencia de Dropbox para un distribuidor.

Grupos

Creación, eliminación e información de la pertenencia para grupos.

- · Creación, cambio de nombre, traslado o eliminación de un grupo.
- · Adición o eliminación de un miembro.
- · Cambio del tipo de acceso de un miembro del grupo.
- · Cambio del grupo a "gestionado por el equipo" o "gestionado por el administrador".
- · Cambio del ID externo de un grupo.

Registro de actividad de Paper

Los administradores pueden elegir un tipo de actividad de Paper en el feed de actividad o descargar un informe completo de actividad. Las actividades relativas a Paper se registran en los siguientes casos:



- Habilitación o inhabilitación de Paper.
- · Creación, edición, exportación, archivo, eliminación permanente o restauración de un documento de Paper.
- Comentarios o resolución de comentarios en documentos de Paper.
- Uso compartido y cancelación del uso compartido de documentos de Paper con miembros del equipo y usuarios ajenos.
- · Solicitudes de acceso por parte de miembros del equipo y usuarios ajenos a un documento de Paper.
- · Menciones a miembros del equipo y usuarios ajenos en un documento de Paper.
- · Visualización de un documento de Paper por parte de miembros del equipo y usuarios ajenos.
- · Seguimiento de un documento de Paper.
- Cambios en los permisos de los miembros de un documento de Paper (edición, comentarios o solo lectura).
- · Cambios en la política a la hora de compartir un documento de Paper.
- · Creación, archivo y eliminación permanente de un documento de Paper
- · Adición o eliminación de un documento de Paper en una carpeta.
- · Cambio de nombre de una carpeta de Paper.
- · Transferencia de un documento o carpeta de Paper.

Dropbox Passwords

Dropbox Passwords es una forma segura y sencilla de almacenar, sincronizar y completar automáticamente los nombres de usuario, las contraseñas y las tarjetas de crédito o débito en todos los dispositivos para que puedas proteger tus credenciales online. Dropbox Passwords protege tus nombres de usuario, contraseñas y tarjetas de crédito o débito confidenciales online con un cifrado de conocimiento cero en la nube y en tus dispositivos. Nuestros productos están diseñados para el uso diario y son seguros por naturaleza.

Cifrado de conocimiento cero

Dropbox Passwords almacena tus datos cifrados en la nube, pero las claves para descifrar esos datos solo se almacenan en tus dispositivos. **Dropbox no puede acceder a ellos en ningún momento.** Dichas claves son largas, aleatorias y se generan en tu dispositivo. Nunca abandonarán tu dispositivo, excepto cuando decidas emparejar o inscribir un nuevo dispositivo. Esta transferencia utiliza criptografía de clave pública para firmar y proteger criptográficamente las claves durante la transferencia, de modo que puedas asegurarte de que nadie más pueda descifrarlas y al mismo tiempo verificar que son auténticas. Esta propiedad se denomina con frecuencia "cifrado de conocimiento cero", porque los datos cifrados no tienen ninguna utilidad para una persona que no tenga las claves, incluido Dropbox. Esto significa que **solo tú puedes ver tu información** y, en el improbable caso de que Dropbox sufriera un ataque, tu información seguiría estando a salvo. Los datos cifrados se separan de las carpetas visibles de Dropbox y no se pueden cruzar con los clientes o las API de Dropbox.



Detalles sobre el cifrado

Dropbox cifra tus datos mediante XChaCha20-Poly1305 en modo combinado para una autenticación implícita. Todas nuestras extensiones de navegador web y aplicaciones móviles utilizan implementaciones de cifrado respaldadas por libsodium, que es una bifurcación de NaCl auditada y ampliamente distribuida.

Cada operación de cifrado genera una combinación aleatoria de 192 bits, que se almacena con la carga útil cifrada para su posterior descifrado. A diferencia de AES-GCM, XChaCha20-Poly1305 admite combinaciones aleatorias. Al descifrarse, la combinación de 192 bits se lee de la carga útil y se utiliza para descifrar la carga útil cifrada. Cualquier cifrado posterior genera una combinación aleatoria de 192 bits independiente de la anterior. Dropbox Passwords genera números aleatorios mediante libsodium, que de forma predeterminada es un generador de números aleatorios criptográficamente seguro en cada una de las plataformas que admitimos.

Claves y palabras de recuperación

Generamos una clave simétrica de 256 bits (la clave de cifrado) a partir de 128 bits de entropía (la clave de usuario) a través del hash Blake2. Esta clave de cifrado solo permanece en los dispositivos de su propietario y, siempre que sea posible, permanecerá en el almacenamiento más seguro al que tengamos acceso en esos dispositivos. Por ejemplo, en los iPhone, almacenamos la clave de cifrado en el llavero de iCloud.

Usamos 128 bits de entropía como nuestra fuente porque ofrece suficiente seguridad y solo requiere 12 palabras de recuperación mediante el estándar BIP-39 como respaldo. BIP-39 proporciona una manera humana de representar grandes claves aleatorias al transformarlas en una lista de 12 palabras. Cualquier clave de 128 bits tiene una lista de palabras correspondiente y cada lista de 12 palabras identifica de forma única 128 bits. La única advertencia es que las 12 palabras en realidad corresponden a 132 bits, por lo que los cuatro bits adicionales se usan como suma de verificación para identificar errores. Las palabras de recuperación te proporcionan una forma de recuperar tu clave de cifrado en caso de pérdida o robo de tu dispositivo. Te recomendamos imprimirlas y guardarlas en un lugar seguro. También puedes considerar la posibilidad de decírselas a un amigo o familiar de confianza o almacenarlas en una memoria USB.

Inscripción de dispositivos

Cuando un usuario inicie sesión en Dropbox Passwords desde un dispositivo nuevo, ese dispositivo deberá completar un procedimiento de registro seguro para acceder a los datos de Passwords del usuario. Este procedimiento ayuda a garantizar que la clave secreta de un usuario y los datos de las contraseñas sean accesibles solo entre los dispositivos inscritos del usuario. También ayuda a garantizar que un usuario solo pueda inscribir dispositivos adicionales si tiene acceso a un dispositivo inscrito existente o a sus palabras de recuperación. El procedimiento de inscripción del dispositivo se realiza de la siguiente manera.

Un nuevo dispositivo de inscripción genera aleatoriamente un par de claves de dispositivo público/privado de 256 bits y sube la clave pública al servidor de Dropbox. A continuación, tiene lugar el escenario **A**, **B** o **C**.

A: Si el usuario no ha inscrito previamente un dispositivo, el dispositivo de inscripción generará aleatoriamente una clave de usuario secreta de 128 bits. Tanto la clave de usuario como el par de claves del dispositivo se almacenarán en una ubicación segura específica del sistema operativo, como se describe en la siguiente sección Almacenamiento de claves. El dispositivo inicializará los datos de Passwords del usuario, los cifrará y subirá la carga útil cifrada al servidor de Dropbox.



B: Si el usuario tiene algún dispositivo inscrito anteriormente, se enviará una solicitud de aprobación de inscripción a cada uno de esos dispositivos. La clave pública del dispositivo de registro se adjuntará a la solicitud. Luego, el usuario deberá aprobar la solicitud en uno de sus dispositivos inscritos. Si se aprueba, el dispositivo registrado cifrará la clave de usuario mediante su clave privada y la clave pública del dispositivo registrado a través de X25519 ECDH con XSalsa20-Poly1305. El dispositivo inscrito subirá la clave de usuario cifrada al servidor de Dropbox para enviarla al dispositivo de inscripción. El dispositivo de registro descargará y descifrará la clave de usuario usando su clave privada y la clave pública del dispositivo registrado. A continuación, el dispositivo de registro descargará los datos de carga útil de las contraseñas cifradas y los descifrará con la clave de usuario.

C: Si el usuario ha inscrito previamente un dispositivo, pero ya no puede acceder a él, podrá especificar sus 12 palabras de recuperación para reconstruir localmente la clave de usuario. A continuación, el dispositivo de registro descargará los datos de carga útil de las contraseñas cifradas y los descifrará con la clave de usuario.

Almacenamiento de claves

Extensiones de navegador web

En los navegadores web, la clave de usuario se almacena en el área de almacenamiento local de la extensión del navegador. Solo se podrá acceder a los valores de almacenamiento local de la extensión del navegador desde la extensión. Cualquier código que se ejecute en los sitios web que el usuario visite no se podrá leer desde el área de almacenamiento local de la extensión del navegador. Además, las extensiones del navegador no permiten la ejecución de ningún código que no esté incluido en el paquete de extensión firmado, lo que elimina el riesgo de una vulnerabilidad XSS que accedería a los valores de almacenamiento local.

Un atacante con acceso sin restricciones al dispositivo del usuario puede acceder a la clave de usuario leyendo el archivo de almacenamiento local en el disco. Entre los ejemplos de tales amenazas, se incluyen los siguientes: atacantes con acceso físico al dispositivo o atacantes que ejecuten malware malintencionado en el dispositivo. Para protegerse de esas situaciones, el usuario puede configurar una frase de contraseña en el dispositivo local.

Cuando se configure una frase de contraseña, la clave de usuario se cifrará en reposo en el almacenamiento local de la extensión del navegador. La clave de cifrado se derivará de la frase de contraseña a través del hash de contraseña de Argon2, y el método de cifrado utilizado será XChaCha20-Poly1305. Cada vez que se reinicie la extensión del navegador, el usuario deberá proporcionar su frase de contraseña para descifrar la clave de usuario y desbloquear sus datos. En consecuencia, un atacante sin la frase de contraseña no podrá descifrar la clave de usuario almacenada en el archivo de almacenamiento local en el disco.

ios

En iOS, la clave de usuario se almacena en el llavero de iCloud, que es un archivo de base de datos cifrado en el disco. Este archivo está cifrado con una clave secreta que se almacena en el módulo de hardware de Secure Enclave mediante AES256-GCM como método de cifrado. Solo la aplicación de Dropbox Passwords para iOS firmada podrá acceder a los elementos que se hayan almacenado en el llavero. Esto evita que el resto del código que se ejecute en el dispositivo del usuario acceda a la clave de usuario.



Android

En Android, la clave de usuario se almacena en un objeto EncryptedSharedPreferences, que es un archivo de preferencias cifrado en el disco. Este archivo está cifrado con una clave maestra que se almacena en el hardware seguro de Android Keystore mediante AES256-GCM como método de cifrado. Solo la aplicación de Dropbox Passwords para Android firmada podrá acceder a la clave maestra que se utiliza para descifrar el archivo de preferencias.

Autenticación local

Dropbox Passwords proporciona medidas de autenticación local opcionales para restringir aún más el acceso a los datos de contraseñas de un usuario en su dispositivo físico. Para las aplicaciones móviles, se puede reutilizar el gesto de autenticación del sistema operativo local (es decir, un código de acceso con autenticación biométrica adicional). Para las extensiones del navegador web, se puede configurar una frase de contraseña opcional. Estos mecanismos proporcionan una capa adicional de seguridad de la aplicación por si se desbloquea el sistema operativo del dispositivo del usuario. De esta forma, el usuario protegerá sus datos de Passwords cuando otro usuario acceda a su dispositivo, como un familiar o un compañero de trabajo.

Sugerencia de seguridad de la contraseña

Dropbox creó la herramienta zxcvbn de código abierto que utilizan varios administradores de contraseñas para estimar la seguridad de las contraseñas. La herramienta compara las contraseñas con una base de datos de 30 000 contraseñas comunes, así como nombres y apellidos comunes según los datos del censo de EE. UU., palabras populares en inglés de Wikipedia y de la televisión y películas de EE. UU. También las compara con otros patrones comunes como fechas, repeticiones (aaa), secuencias (abcd), patrones de teclado (qwertyuiop) y 1337 en la escritura leet. Si la contraseña que un usuario especifique es común, la herramienta le pedirá que escriba algo más único y difícil de adivinar. El uso de la configuración **Muy segura** ayuda a garantizar el más alto nivel de seguridad de la cuenta para los usuarios.

Seguridad, privacidad y transparencia de los datos

Tanto los usuarios individuales como las organizaciones confían a Dropbox sus archivos de trabajo más importantes. Por ello, es nuestra responsabilidad proteger esa información y preservar su privacidad.

Política de privacidad

Nuestra Política de privacidad está disponible en dropbox.com/privacy. En la Política de privacidad, el Acuerdo de servicios, los Términos del servicio y la Política de uso aceptable se proporciona información sobre los puntos siguientes:

- Qué tipo de datos recopilamos y por qué.
- · Con quién podemos compartir la información.



- Cómo protegemos los datos y cuánto tiempo los conservamos.
- · Dónde guardamos y transmitimos tus datos.
- · Qué ocurre si cambia la política o si tienes alguna pregunta.

Transparencia

Dropbox se compromete a gestionar de forma transparente las solicitudes de información de los usuarios por parte de organismos legales, así como la cantidad y los tipos de solicitudes que recibamos. Analizamos todas las solicitudes de datos para comprobar su conformidad con la ley y, en la medida en que la ley nos lo permita, nos comprometemos a avisar a los usuarios cuando se identifiquen sus cuentas en una solicitud de aplicación de la ley.

Estos esfuerzos subrayan nuestro compromiso de salvaguardar la privacidad de nuestros usuarios y sus datos. Con este objetivo, mantenemos un informe de transparencia y hemos establecido un conjunto de Principios sobre solicitudes de los gobiernos. Los siguientes principios rigen nuestras acciones cuando recibimos, analizamos y respondemos a las solicitudes de los gobiernos de los datos de nuestros usuarios:

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 una serie de personas específicas e investigaciones legítimas. Nos oponemos a las peticiones arbitrarias y de carácter amplio.

· 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 online. Seguiremos defendiendo la reforma de estas leyes.

· 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.

Nuestros informes de transparencia se pueden consultar en dropbox.com/transparency.

Certificaciones de privacidad, confirmaciones y cumplimiento normativo

Tanto los usuarios individuales como las organizaciones confían sus archivos de trabajo más importantes a Dropbox. Por eso tenemos la responsabilidad de proteger esos archivos y preservar su privacidad. Tomamos todas nuestras decisiones pensando en el compromiso que tenemos con tu seguridad.

El código profesional ISO/IEC 27018 para proteger los datos personales en la nube y la extensión ISO/IEC 27701 para ISO/IEC 27001, y la ISO/IEC 27002 para la gestión privada de la información

Dropbox Business fue uno de los primeros y principales proveedores de servicios en la nube en lograr la certificación con ISO/IEC 27018 e ISO/IEC 27701.

ISO/IEC 27018 es un estándar global para la privacidad y la protección de datos en la nube y se publicó en agosto de 2014 para abordar específicamente la privacidad de los usuarios y la protección de datos.

ISO/IEC 27701 es el primer estándar global certificable para la gestión de la privacidad de la información y se publicó en 2019 para ofrecer un marco de trabajo con el que ampliar el sistema de gestión de seguridad de la información (ISMS, por sus siglas en inglés) desde la ISO/IEC 27001 a un sistema de gestión de la información privada (PIMS) al incluir consideraciones en torno a la privacidad de los datos.

Los estándares exponen muchos requisitos relativos al uso que puede hacer Dropbox de la información de tu organización:

· Tu organización tiene el control de tus datos.

Solo utilizamos la información personal que nos facilitas para poder ofrecerte los servicios en los que te has registrado. Puedes añadir, modificar o eliminar archivos y documentos de Paper cuando sea necesario.

· Seremos transparentes en cuanto a tus datos.

Comunicaremos con transparencia en qué lugar de nuestros servidores están almacenados tus datos. Además, te informaremos de quiénes son nuestros socios de confianza. También te explicaremos qué ocurre cuando cierras una cuenta o eliminas un archivo o documento de Paper. Y por último, te avisaremos si algunos de estos aspectos cambia.

Tus datos siempre están protegidos y a salvo.

ISO/IEC 27018 y ISO/IEC 27701 se diseñaron como mejoras y extensiones de ISO/IEC 27001, uno de los estándares de seguridad de la información más aceptados a nivel mundial. Recibimos la renovación del ISO/IEC 27001 en octubre de 2021.

Nuestras prácticas se revisan con regularidad

De conformidad con los estándares ISO/IEC 27018, ISO/IEC 27701 e ISO/IEC 27001, nos sometemos a auditorías anuales realizadas por auditores externos independientes para mantener estas certificaciones. Puedes consultar todos nuestros certificados aguí.

Transferencias de datos

Al transferir los datos desde la Unión Europea, el Espacio Económico Europeo, el Reino Unido y Suiza, Dropbox cuenta con diferentes mecanismos jurídicos, como contratos con nuestros clientes y entidades afiliadas, cláusulas contractuales tipo y las decisiones de adecuación de la Comisión Europea sobre ciertos países, si procede.

Dropbox cumple con los marcos del programa Escudo de la privacidad UE-EE. UU. y Escudo de la privacidad Suiza-EE. UU como establece el Departamento de Comercio de los Estados Unidos respecto a la recogida, el uso y la conservación de datos personales que se transfieran desde la Unión Europea, el Espacio Económico



Europeo, el Reino Unido y Suiza a Estados Unidos. No obstante, Dropbox no cuenta con los marcos Escudo de la privacidad UE-EE. UU. y Escudo de la privacidad Suiza-EE. UU. como base legal para transferir datos personales. Dropbox ha certificado al Departamento de Comercio que cumple los principios del Escudo de la privacidad con respecto a dichos datos. También puedes obtener más información acerca del Escudo de la privacidad en https://www.privacyshield.gov.

Las reclamaciones y disputas relacionadas con el cumplimiento de nuestro Escudo de Privacidad se investigan y resuelven a través de JAMS, un tercero de carácter independiente. Puedes consultar más información echando un vistazo a nuestra Política de privacidad (dropbox.com/privacy).

El Reglamento General de Protección de Datos de la UE

El Reglamento General de Protección de Datos (RGPD) es un reglamento de la Unión Europea que entró en vigor en 2018 y que establece un nuevo marco legal integral para gestionar y proteger los datos personales.

En Dropbox nos comprometemos en todo momento con la seguridad y la protección de los datos de nuestros usuarios de acuerdo con los requisitos legales y las mejores prácticas. Para demostrar nuestro compromiso con los usuarios, hemos trabajado mucho para asegurarnos de que Dropbox cumple con la RGPD, e incluye un responsable de la protección de datos. También hemos rediseñado la arquitectura de nuestro programa de privacidad para asegurarnos de que los usuarios pueden ejercer sus derechos relacionados con los datos; además de documentar nuestras actividades de procesamiento de datos y reforzar nuestros procesos internos en caso de brecha en la seguridad. Continuamos realizando ajustes para asegurarnos de que, a medida que las autoridades de la protección de datos siguen guiándonos, nuestros procesos y prácticas cumplen o superan los elementos específicos requeridos en las nuevas reglas.

Código de conducta en la nube de la UE

El Código de conducta en la nube de la UE es un instrumento que los proveedores de servicios en la nube, como Dropbox, pueden usar de forma voluntaria para demostrar su compromiso con el cumplimiento del RGPD. Se ha declarado que Dropbox Business, que se compone de los planes Standard, Advanced, Enterprise y Education para equipos, cumple con el Código de conducta en la nube de la UE. Estos servicios han recibido una marca de cumplimiento de nivel 2, lo que significa que han implementado medidas técnicas, organizativas y contractuales en consonancia con los requisitos del código. Para obtener más información sobre el Código de conducta en la nube de la UE y el cumplimiento del mismo por parte de Dropbox, visita el sitio web oficial del código.

Para obtener información sobre nuestras prácticas y políticas de privacidad, consulta el Informe técnico sobre la privacidad y protección de datos de Dropbox.

Cumplimiento

Existen diferentes normativas y estándares de conformidad sobre seguridad y privacidad que pueden ser aplicables a tu organización. Nuestro enfoque se fundamenta en la combinación de los estándares más aceptados con medidas de conformidad adaptadas a las necesidades de los sectores o empresas de nuestros clientes.



ISO

La Organización Internacional de Normalización (International Organization for Standardization, ISO) ha desarrollado una serie de estándares de seguridad social y de la información de primera clase para ayudar a las organizaciones a crear productos y servicios innovadores y fiables. En Dropbox, hemos certificado nuestros centros de datos, sistemas, aplicaciones, personal y procesos de acuerdo a una serie de auditorías realizadas por una empresa externa, EY CertifyPoint, con sede en los Países Bajos. EY CertifyPoint cuenta con acreditaciones ISO del Raad voor Accreditatie (consejo de acreditación neerlandés).

ISO/IEC 27001 (Seguridad de la información)

Se reconoce que la ISO 27001 es el principal estándar de sistemas de gestión de la seguridad de la información (ISMS) del mundo. El estándar emplea las prácticas recomendadas de seguridad detalladas en la ISO/IEC 27002. Para merecer tu confianza, en Dropbox, gestionamos de forma continua y exhaustiva nuestros controles físicos, técnicos y legales.

Consulta el certificado ISO/IEC 27001 de Dropbox Business y Education.

ISO/IEC 27017 (Seguridad en la nube)

La ISO/IEC 27017 es un nuevo estándar internacional de seguridad en la nube que ofrece directrices sobre los controles de seguridad aplicables al aprovisionamiento y el uso de servicios en la nube. Los requisitos de seguridad, privacidad y conformidad que Dropbox y sus clientes pueden cumplir juntos se explican en nuestra Guía de responsabilidad compartida.

Consulta el certificado ISO/IEC 27017 de Dropbox Business y Education.

ISO/IEC 27018 (Privacidad en la nube y protección de datos)

La ISO/IEC 27018 es un estándar internacional relativo a la protección de los datos y la privacidad que se aplica a proveedores de servicios en la nube como Dropbox que procesan información personal en nombre de sus clientes y proporciona una base a partir de la cual los clientes pueden abordar los requisitos normativos y contractuales o las preguntas habituales.

Consulta el certificado ISO/IEC 27018 de Dropbox Business y Education.



ISO/IEC 22301 (Continuidad empresarial)

La ISO/IEC 22301 es un estándar internacional de continuidad empresarial que ofrece consejos a las organizaciones sobre cómo reducir la probabilidad de que se produzcan interrupciones de servicio y cómo responder a estas de forma adecuada (si se produjera alguna) minimizando los posibles daños. El sistema de gestión de continuidad empresarial de Dropbox (BCMS) forma parte de nuestra estrategia global de gestión de los riesgos para proteger a las personas y a las operaciones en momentos de crisis.

Consulta el certificado ISO/IEC 22301 de Dropbox Business y Education.

ISO/IEC 27701 (Gestión de la privacidad de la información)

ISO 27701 es un estándar internacional para la gestión de información privada. Este estándar ofrece un marco de trabajo para mejorar y ampliar el sistema de gestión de seguridad de la información de la ISO 27001 a un sistema de gestión de la información privada (PIMS) Dropbox Business y Dropbox Education han recibido su certificación como Procesador de información de Identificación personal (PII).

Consulta el certificado ISO 27701 de Dropbox Business y Dropbox Education.

SOC

Los informes de controles de organizaciones de servicios (Service Organization Controls, SOC), también conocidos como el SOC 1, SOC 2 o SOC 3, son marcos que establece el Instituto Americano de Contables Públicos Certificados (American Institute of Certified Public Accountants, AICPA) para informar sobre los controles internos implementados en una organización. Dropbox ha validado sus sistemas, aplicaciones, personal y procesos a través de una serie de auditorías realizadas por un auditor externo independiente, Ernst & Young LLP.

SOC 3 sobre seguridad, confidencialidad, integridad, disponibilidad y privacidad

El informe de control SOC 3 abarca los cinco Criterios de Servicios de Confianza (TSP) en cuanto a seguridad, confidencialidad, integridad, disponibilidad y privacidad (TSP sección 100). El informe de uso general de Dropbox es un resumen ejecutivo del informe SOC 2 e incluye la opinión del auditor externo independiente sobre la eficacia del diseño y funcionamiento de nuestros controles.

Consulta el examen del SOC 3 de Dropbox Business y Education.



SOC 2 sobre seguridad, confidencialidad, integridad, disponibilidad y privacidad

El informe SOC 2 proporciona a los clientes un nivel detallado de garantía basada en controles, que abarca los cinco Criterios de Servicios de Confianza de seguridad, disponibilidad, integridad de los procesos, confidencialidad y privacidad (TSP, sección 100). En el informe SOC 2, se incluye una descripción detallada de los procesos de Dropbox y más de 100 controles que hemos implementado para proteger tus cosas. Además de la opinión de nuestro auditor externo independiente sobre la eficacia del diseño y funcionamiento de nuestros controles, en el informe se recogen los procedimientos y resultados de las pruebas del auditor para cada control. El examen SOC 2 (conocido como SOC 2+) también incluye un mapeo auditado de nuestros controles según los estándares ISO mencionados previamente, para ofrecer aún más transparencia a nuestros clientes. El examen SOC 2 de Dropbox Business y Education se encuentra disponible a petición.

SOC 1 / SSAE 18 / ISAE 3402 (antes, SSAE 16 o SAS 70)

El informe SOC 1 ofrece garantías específicas para clientes que determinen que Dropbox Business o Education representan un elemento fundamental de su programa de control interno sobre información financiera (ICFR). Estas garantías específicas se usan principalmente para la conformidad de nuestros clientes con Sarbanes-Oxley (SOX). La auditoría externa independiente se realiza de acuerdo con las normas Statement on Standards for Attestation Engagements No. 18 (SSAE 18) e International Standard on Assurance Engagements No. 3402 (ISAE 3402). Estos estándares han sustituido a las obsoletas Statement on Standards for Attestation Engagement No. 16 (SSAE16) y Statement on Auditing Standards No. 70 (SAS 70). El examen del SOC 1 de Dropbox Business y Education se encuentra disponible a petición.

CSA

Alianza por la seguridad en la nube: registro de seguridad, confianza y aseguramiento (CSA STAR)

El registro de seguridad, confianza y aseguramiento (STAR) de la CSA es un registro gratuito y de libre acceso que ofrece un programa de garantía de la seguridad para servicios en la nube, con lo que ayuda a los usuarios a evaluar el estado de la seguridad de los proveedores de servicios en la nube que usen actualmente o con los que se estén planteando firmar un contrato.

Tanto Dropbox Business como Dropbox Education han recibido la Certificación CSA STAR Nivel 2 y la Evaluación a Nivel 2. La CSA STAR Nivel 2 requiere una evaluación externa independiente de nuestros controles de seguridad a cargo de EY CertifyPoint (para la certificación) y Ernst & Young LLP (para la autenticación), basada en los requisitos de la ISO/IEC 27001, los criterios de servicios de confianza SOC 2 y el CSA Cloud Controls Matrix (CCM) v.4.0.2.

Consulta nuestra certificación y atestación CSA STAR Nivel 2 en el sitio web de CSA.



HIPAA/HITECH

Dropbox firmará acuerdos de asociación comercial (BAA) con aquellos clientes de Dropbox Business y Dropbox Education que los requieran a fin de cumplir con la HIPAA (Ley de portabilidad y responsabilidad de seguros médicos) y la HITECH (Ley de tecnología de la información de salud para la salud económica y clínica). Para obtener más información, consulta Dropbox y las normativas HIPAA/HITECH.

Dropbox pone a disposición de los clientes un informe de garantías de terceros que evalúa nuestros controles de seguridad HIPAA/HITECH, privacidad y reglas de notificación de infracciones, además de realizar un mapeo de nuestras prácticas y recomendaciones internas para clientes que desean cumplir los requisitos de la regla de seguridad y privacidad de HIPAA/HITECH con Dropbox Business o Education.

Los clientes interesados en solicitar estos documentos u obtener más información sobre cómo comprar Dropbox Business o Dropbox Education pueden ponerse en contacto con nuestro equipo de ventas. Si administras un equipo de Dropbox Business o Dropbox Education, puedes firmar un acuerdo electrónico de asociación comercial en la página Cuenta de la Consola de administración.

Ten en cuenta que la capacidad de firmar un acuerdo electrónico de asociación comercial a través de la Consola de administración solo está disponible para clientes con sede en Estados Unidos.

NIST 800-171

El National Institute of Standards and Technology (NIST) de Estados Unidos promueve y mantiene estándares y directrices para ayudar a proteger los sistemas de información. El NIST Special Publication (SP) 800171 Revision 2 (R2) ofrece directrices sobre cómo proteger Información controlada no clasificada (CUI, por sus siglas en inglés) en sistemas y organizaciones de información no federales. Cualquier entidad que procese o almacene información CUI del gobierno de Estados Unidos, como las instituciones de investigación y el sector educativo, debería cumplir con el NIST SP 800-171 R2. Un auditor independiente, Ernst & Young LPP, validó los sistemas, procesos y controles CUI de Dropbox.

El informe NIST SP 800-171 R2 para Dropbox Business y Dropbox Education está disponible bajo solicitud a través de nuestro equipo de ventas o la asistencia (para aquellos que sean clientes de Dropbox Business).

Ten en cuenta que Dropbox Paper no está incluido en el marco del informe del NIST SP 800-171 R2.

FERPA y COPPA (Estudiantes y niños)

Dropbox Business y Education permite a los clientes usar los servicios de conformidad con las obligaciones impuestas a los proveedores por la Ley de Derechos Educativos y Privacidad Familiar (FERPA). Las instituciones educativas con estudiantes menores de 13 años también pueden usar Dropbox Business y Education de acuerdo con la Ley de Protección de la Privacidad Infantil en Internet (COPPA), siempre que acepten unas disposiciones contractuales específicas que exigen que la institución obtenga el consentimiento de los padres para utilizar nuestros servicios.



FDA 21 CFR Parte 11

El Título 21 del Código de regulaciones federales (CFR, por sus siglas en inglés) legisla con respecto a la alimentación y los medicamentos dentro de Estados Unidos para la Food and Drug Administration (FDA), la Drug Enforcement Administration y la Office of National Drug Control Policy. La Parte 11 del Título 21 expone los criterios según los cuales la FDA considera que los registros electrónicos y las firmas son de confianza, fiables y generalmente equivalentes a los registros en papel y las firmas a mano en papel.

Consulta nuestro libro técnico sobre Dropbox y la FDA 21 CFR Parte 11 y elartículo del centro de ayuda para más información sobre cómo puede ayudarte Dropbox con tus acciones de cumplimiento con la parte 11 del CFR 21.

PCI DSS

Dropbox cumple la norma de seguridad de datos del sector de tarjetas de pago (Payment Card Industry Data Security Standard, PCI DSS). Sin embargo, Dropbox Business, Education y Paper no se han diseñado para procesar ni almacenar transacciones de tarjetas de crédito. El documento PCI Attestation of Compliance (AoC), que confirma nuestro estado de comerciante, está disponiblebajo petición.

Para obtener más información sobre el cumplimiento de Dropbox Business y Education, visita dropbox.com/business/trust/compliance.

Aplicaciones para Dropbox

La plataforma DBX cuenta con un sólido ecosistema de programadores que emplean nuestra flexible interfaz de programación de aplicaciones (API) para desarrollar sus proyectos de software. Más de 750 000 desarrolladores han desarrollado aplicaciones y servicios en la plataforma relacionados con la productividad, colaboración, seguridad, administración y mucho más.

Componentes predesarrollados

Chooser, Saver y Embedder son componentes web y móviles predesarrollados que permiten acceder de forma fácil a Dropbox en aplicaciones/sitios de terceros con solo unas pocas líneas de código.

- · Chooser permite seleccionar archivos de Dropbox.
- Saver permite a los usuarios guardar archivos directamente en Dropbox.
- Embedder permite a los usuarios ver archivos y carpetas desde Dropbox.

La autorización de estos componentes se realiza enteramente a través de Dropbox. Las aplicaciones tienen acceso a los archivos seleccionados a través de los enlaces compartidos de Dropbox o de los enlaces de descarga de corta duración. Estos componentes predesarrollados pueden utilizarse de forma independiente o en conjunto con la API, que se describe a continuación.



Integraciones con la API de Dropbox Business

La API de Dropbox pública permite a desarrolladores terceros la capacidad de acceder e interactuar con Dropbox dentro de sus aplicaciones. Esto incluye la interacción de archivos y metadatos, el intercambio y la funcionalidad del equipo.

Autorización

Dropbox emplea OAuth, un protocolo de autorización estándar del sector, que permite a los usuarios acceder a sus cuentas sin revelar sus credenciales. Ofrecemos compatibilidad con OAuth 2.0 para la autenticación de las solicitudes de API; las solicitudes se autentican mediante el sitio web de Dropbox o la aplicación móvil. Dropbox soporta las mejores prácticas de OAuth, incluidos los tokens de acceso de corta duración y PKCE para las aplicaciones distribuidas.

Permisos de usuario

Las aplicaciones que utilizan la API de Dropbox pueden compilarse con el siguiente nivel de acceso al contenido de la cuenta de Dropbox del usuario final:

Carpeta de aplicación.

Dentro de la carpeta Aplicaciones de la cuenta de Dropbox del usuario se crea una carpeta exclusiva con el nombre de la aplicación. La aplicación recibe acceso de lectura y escritura solamente en esta carpeta, y los usuarios pueden proporcionar contenido a la aplicación moviendo archivos a dicha carpeta. Además, la aplicación puede solicitar acceso a archivos o carpetas mediante las funciones Chooser y Saver.

Todo Dropbox.

La aplicación recibe un acceso completo a todos los archivos y carpetas de la cuenta de Dropbox de un usuario y también puede solicitar acceso a archivos y carpetas a través de las funciones Chooser y Saver.

Las aplicaciones también pueden solicitar alcances específicos, restringiendo sus comportamientos mediante el acceso a subconjuntos de puntos finales de la API. Por ejemplo, las aplicaciones pueden estar limitadas al acceso de solo lectura de los archivos, o a la capacidad de cargar contenido, pero no a la creación de acciones.

Permisos de equipo

Los administradores de Dropbox Business pueden autorizar aplicaciones para que dispongan de la funcionalidad de administración que se encuentra en la Consola de administración del equipo. Las acciones que las aplicaciones vinculadas al equipo pueden realizar se limitan a través de alcances en los que se especifica qué configuraciones del equipo puede leer o administrar la aplicación.

Las combinaciones más comunes de alcances incluyen:

Información del equipo

Información de solo lectura sobre el equipo y uso de alto nivel.

Auditoría del equipo

Acceso de solo lectura a la información del equipo y registro detallado del evento.

Acceso a los archivos de los miembros del equipo

Capacidad para realizar acciones en nombre de los usuarios del equipo, como la gestión de sus carpetas de archivos.

Gestión de miembros del equipo

Añadir y eliminar miembros del equipo.

Webhooks

Webhooks es una solución gracias a la cual las aplicaciones web pueden recibir notificaciones en tiempo real sobre los cambios que lleva a cabo un usuario de Dropbox. Una vez que una URI se registra para recibir webhooks, se envía una solicitud HTTP a esa URI cada vez que uno de los usuarios registrados en la aplicación realiza un cambio. Mediante la API de Dropbox Business (que describimos más adelante), los webhooks también pueden utilizarse para generar notificaciones sobre los cambios a los miembros del equipo. Muchas aplicaciones de seguridad utilizan los webhooks para ayudar a los administradores a hacer seguimiento y gestionar las actividades del equipo.

Extensions

Es posible que las aplicaciones registren URI de extensión para permitir que las acciones aparezcan en los menús "Compartir" y "Abrir" en la UI de Dropbox. Con las extensiones, los usuarios pueden iniciar flujos de trabajo personalizados de terceros directamente desde un archivo en una superficie de Dropbox. Al desencadenar una acción, Dropbox redirigirá a los usuarios a la URI especificada, pasando un identificador de archivo que puede utilizarse con la API para realizar cualquier operación de archivo. Es necesario autorizar una aplicación para que el usuario pueda ver una extensión registrada. Es posible que promovamos un conjunto determinado de integraciones de extensión en los menús "Compartir" y "Abrir", aunque estas aplicaciones no tendrán acceso al contenido hasta que el usuario lo autorice.

Directrices para desarrolladores de Dropbox

Proporcionamos una serie de directrices y recomendaciones para que los desarrolladores puedan crear aplicaciones de API que respeten y protejan la privacidad de los usuarios, además de mejorar su experiencia en Dropbox.

Claves de la aplicación

Cada aplicación diferente que cree un desarrollador debe emplear una clave de aplicación única de Dropbox. Además, si una aplicación ofrece servicios o software que ponga la plataforma DBX a disposición de otros desarrolladores, cada desarrollador tendrá que registrarse igualmente para obtener claves para sus aplicaciones de Dropbox.

Permisos de aplicaciones

Se indicará a los desarrolladores que una aplicación debe usar el permiso con la menor cantidad de privilegios posible. Cuando un desarrollador envía una aplicación para que se apruebe el estado de producción, comprobamos que la aplicación no solicite un permiso con privilegios innecesarios para la funcionalidad que ofrece.

· Proceso de revisión de aplicaciones

• Estado de desarrollo. Cuando se crea una aplicación con la API de Dropbox, se le asigna el estado de desarrollo. La aplicación funciona igual que cualquiera con estado de producción, con la única diferencia de que solo se puede vincular a 500 usuarios de Dropbox como máximo. Cuando una aplicación se vincula a 50 usuarios de Dropbox, el desarrollador dispone de dos semanas para solicitar y recibir la aprobación del estado de producción. De no cumplirse este plazo, se congelará la capacidad de vincular usuarios de Dropbox adicionales.

· Estado de producción y aprobación.

Para recibir la aprobación del estado de producción, todas las aplicaciones que usen la API deben adherirse a las normas de marcas para desarrolladores y a nuestros términos y condiciones, que incluyen una serie de usos prohibidos de la plataforma DBX. Estos usos son: promoción de infracciones de propiedad intelectual o copyright, creación de redes para compartir archivos y descargas ilegales de contenido. Antes de su envío a revisión, los desarrolladores deben indicar información adicional acerca de las funciones de su aplicación y cómo utilizarán la API de Dropbox. Cuando se apruebe el estado de producción de la aplicación, todos los usuarios de Dropbox que lo deseen podrán vincular la aplicación a su cuenta.



Administración de la aplicación de equipo

Dentro de la Consola de administración del equipo, los administradores de Dropbox Business pueden administrar las aplicaciones e integraciones vinculadas para su equipo.

Asociaciones de API

Dropbox ha trabajado estrechamente con sus socios tecnológicos para permitirles desarrollar integraciones de sus paquetes de software más conocidos. Estos socios construyen aplicaciones utilizando las API de Dropbox, trabajando codo con codo con los arquitectos de Dropbox para seguir las mejores prácticas de seguridad y experiencia del usuario. Entre ellas, se incluyen una gran variedad de aplicaciones de productividad para el usuario final, así como herramientas de gestión y seguridad como, por ejemplo:

Gestión de eventos e información de seguridad (SIEM) y analítica

Conecta tu cuenta de Dropbox Business a herramientas de análisis y SIEM para observar y evaluar la actividad compartida de los usuarios, los intentos de inicio de sesión, las acciones de los administradores y mucho más. Accede a los registros de actividad de los empleados y datos relevantes para la seguridad, y adminístralos a través de tu herramienta de gestión de registro central.

Prevención de pérdidas de datos (DLP)

Analiza automáticamente contenido y metadatos de archivos para generar alertas, informes y acciones cuando se realicen cambios importantes en tu cuenta de Dropbox Business. Aplica políticas de empresa a tu implementación de Dropbox Business y cumple los requisitos de conformidad obligatorios.

eDiscovery y retención legal

Responde a litigios, arbitrajes e investigaciones reglamentarias con datos de tu cuenta de Dropbox Business. Busca y recopila información relevante almacenada electrónicamente, y guarda tus datos a través del proceso de eDiscovery, con lo que le ahorrarás tiempo y dinero a tu empresa.

Gestión de derechos digitales (DRM)

Añade protección de terceros para datos confidenciales y protegidos mediante derechos de autor que se encuentran almacenados en cuentas de empleados. Obtén acceso a potentes funciones DRM, incluidos el cifrado por parte del cliente, la incorporación de marcas de agua, procesos de auditoría, la revocación de accesos y el bloqueo de usuarios o dispositivos.

Migración de datos y copia de seguridad in situ

Migra datos a Dropbox desde servidores existentes u otras soluciones basadas en la nube y ahorra tiempo, dinero y esfuerzo. Automatiza las copias de seguridad desde tu cuenta de Dropbox Business en servidores in situ

Gestión de identidad e inicio de sesión único (SSO)

Automatiza el proceso de aprovisionamiento y desaprovisionamiento y acelera la integración de nuevos empleados. Optimiza la gestión y seguridad mediante la integración de Dropbox Business con un sistema de identidad existente.

Flujos de trabajo personalizados

Crea aplicaciones in situ que integren Dropbox en procesos existentes de la empresa para mejorar sus flujos de trabajo internos.

Consulta las Integraciones de la aplicación Dropbox para obtener una lista de estos socios tecnológicos. Los usuarios finales pueden descubrir aplicaciones e integraciones de primera y tercera parte en el Centro de aplicaciones.



Integraciones de Dropbox

También hemos trabajado con algunos de nuestros mejores socios tecnológicos para construir las integraciones que se muestran en las superficies de Dropbox. Estas integraciones más profundas se desarrollan de forma conjunta entre Dropbox y el socio en cuestión. Entre estos recursos, se incluyen los siguientes:

Dropbox Extensions

Estas integraciones te permiten usar varios tipos de extensiones de aplicaciones para realizar determinadas acciones de forma sencilla, como publicar un vídeo, añadir archivos a los correos electrónicos y chats, enviar un archivo para que lo firmen electrónicamente, etc., directamente desde Dropbox. Las aplicaciones las crea el socio y Dropbox facilita el descubrimiento de socios de extensión seleccionados a través de los menús "Abrir con" y "Compartir con".

Slack, Zoom y Trello

Estas integraciones las ha construido Dropbox para permitir a los usuarios iniciar conversaciones en Slack, iniciar reuniones y crear tareas desde dentro de Dropbox. Los usuarios finales se autentican en estas herramientas mediante OAuth.

Microsoft Office para dispositivos móviles y para la web

Nuestras integraciones con Microsoft Office permiten a los usuarios abrir archivos de Word, Excel y PowerPoint almacenados en su Dropbox; realizar cambios en las aplicaciones de Office para la Web o dispositivos móviles; y guardar esos cambios directamente en Dropbox. Cuando los usuarios intentan abrir un archivo de Dropbox en una aplicación de Office para la Web o dispositivos móviles, se les pide que otorguen acceso. En los accesos posteriores se mantiene la vinculación.

Adobe Acrobat y Acrobat Reader

Nuestras integraciones de las versiones de escritorio y móvil (Android y iOS) de estas aplicaciones permiten a los usuarios visualizar, editar y compartir los archivos PDF almacenados en su cuenta de Dropbox. La primera vez que los usuarios intentan abrir un archivo de Dropbox en una aplicación, se les pide que permitan el acceso. Los cambios efectuados en los archivos PDF se guardan automáticamente en Dropbox.

Resumen

Dropbox Business ofrece herramientas fáciles de utilizar que permiten a los equipos colaborar de forma sencilla a la vez que proporciona las medidas de seguridad y las certificaciones de cumplimiento que requieren las organizaciones. Con un modelo de varias capas que combina una infraestructura de backend sólida con un conjunto de políticas personalizable, ofrecemos a las empresas una solución potente que se puede ajustar a sus necesidades específicas. Para saber más acerca de Dropbox Business, ponte en contacto con nosotros a través de sales@dropbox.com.

