Seguridad de Dropbox Business

Documento técnico de Dropbox

Dropbox

Contenido

Información general

Las transformaciones digitales continúan estableciéndose en diversas industrias, y es fundamental que los datos, los equipos y los dispositivos estén protegidos dondequiera que estén. Las organizaciones que dependen de soluciones en la nube como Dropbox Business para habilitar flujos de trabajo remotos y distribuidos necesitan optimizar la colaboración, gestionar los riesgos de la nube de manera proactiva e implementar controles efectivos que garanticen la confidencialidad de su propiedad intelectual (PI), la integridad de los datos almacenados y compartidos, y la disponibilidad de los datos a través de un servicio administrado y sólido en la nube.

Más de 600 000 empresas y organizaciones confían en Dropbox Business como la solución para que los equipos remotos y distribuidos puedan colaborar de manera segura. El núcleo de la solución de Dropbox Business incluye un espacio de trabajo inteligente para la colaboración y capacidades de uso compartido, así como la sincronización de archivos. Nuestras soluciones cuentan con el respaldo de una infraestructura de vanguardia en la industria y también poseen características de seguridad empresarial avanzada, seguridad de equipos y contenidos, firma electrónica, transferencia segura y gobierno de datos. A menos que se indique lo contrario, la información contenida en el presente informe técnico aplica a todos los productos de Dropbox Business (Standard, Advanced y Enterprise) y Dropbox Education. Paper es una característica de Dropbox Business y Dropbox Education.

En el núcleo de Dropbox Business se encuentra nuestro programa de seguridad integral, el Programa de confianza de Dropbox, que utiliza un enfoque de seguridad de múltiples capas, fundamental a medida que evolucionan los enfoques globales del trabajo remoto.

Este documento técnico describe las capacidades de seguridad de producto de Dropbox Business, las medidas de seguridad operativa de Dropbox, nuestro compromiso con la privacidad y la transparencia, así como también las políticas de back-end, certificaciones independientes y las medidas de cumplimiento normativo que hacen que Dropbox sea la solución segura para tu organización.

A menos que se indique lo contrario, la información contenida en el presente informe técnico aplica a todos los productos de Dropbox Business (Standard, Advanced y Enterprise) y Dropbox Education. Paper es una característica de Dropbox Business y Dropbox Enterprise.

Descripción de las características

Nuestras sencillas interfaces están respaldadas por una infraestructura que funciona tras bastidores para garantizar rapidez y fiabilidad en la sincronización, colaboración y el uso compartido de archivos. Para que ello sea posible, mejoramos constantemente nuestro producto y nuestra arquitectura, a fin de acelerar la transferencia de datos, mejorar la fiabilidad y ajustarnos a los cambios en el entorno. En esta sección, explicaremos cómo se transfiere, almacena y procesa la información de forma segura.

Infraestructura de archivos

Los usuarios de Dropbox pueden acceder a los archivos y a las carpetas en cualquier momento a través de los clientes para escritorio, Internet y dispositivos móviles, o bien a través de aplicaciones de terceros vinculadas a Dropbox. Todos estos clientes se conectan a servidores seguros para ofrecer acceso a los archivos, permitir el uso compartido de archivos y actualizar los dispositivos vinculados cuando se agregan, modifican o eliminan archivos.

La infraestructura de archivo de Dropbox está conformada por los siguientes componentes:

- ***Servidores de metadatos***

  Cierta información básica acerca de los datos de los usuarios se conserva en su propio servicio de almacenamiento exclusivo y funciona como un índice para los datos en las cuentas de los usuarios; esta información se denomina "metadatos". Los metadatos incluyen información básica sobre la cuenta y el usuario, como la dirección de correo electrónico, el nombre del usuario y el nombre de los dispositivos. Los metadatos también incluyen información básica acerca de los archivos, como los nombres y los tipos de archivos, lo que ayuda a admitir características, como el historial de versiones, la recuperación y la sincronización.

- ***Bases de datos de metadatos***

  Los metadatos de los archivos se almacenan en una tienda de valor clave transaccional con control de concurrencia de varias versiones y se comparten y replican según sea necesario, para cumplir con los requisitos de rendimiento y alta disponibilidad.

- ***Servidores de bloques***

  El diseño de Dropbox proporciona un mecanismo de seguridad único que va más allá del cifrado tradicional para proteger los datos del usuario. Los servidores de bloques procesan los archivos de las aplicaciones de Dropbox al dividir cada archivo en bloques, encriptar cada bloque de archivos con un potente cifrado y sincronizar solamente aquellos bloques que se modificaron entre revisiones. Cuando una aplicación de Dropbox detecta un archivo nuevo o cambios en un archivo existente, la aplicación notifica a los servidores de bloques del cambio, y los bloques de archivos nuevos o modificados se procesan y transfieren a los servidores de almacenamiento de bloques. Además, los servidores de bloques se utilizan para proporcionar archivos y vistas previas a los usuarios. Para obtener información detallada acerca del cifrado utilizado por estos servicios, tanto en tránsito como en almacenamiento, consulta la sección de Cifrado a continuación.

- ***Servidores de almacenamiento en bloque***

  El contenido efectivo de los archivos de los usuarios se almacena en bloques cifrados a través de los servidores de almacenamiento de bloques.

  Antes de la transmisión, el cliente de Dropbox divide los archivos en bloques de archivos a fin de prepararlos para el almacenamiento. Los servidores de almacenamiento de bloques funcionan como un sistema de memoria asociativa (CAS), en el que cada bloque de archivos cifrado se recupera en función de su valor hash.

- ***Servidores de vistas previas***

  Los servidores de vistas previas generan vistas previas de archivos. Las vistas previas son una representación del archivo de un usuario en un formato de archivo diferente que es más adecuado para una visualización rápida en el dispositivo de un usuario final. Los servidores de vistas previas recuperan bloques de archivos de los servidores de almacenamiento de bloques para generar vistas previas. Cuando se solicita una vista previa de un archivo, 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. Finalmente, los servidores de bloques proporcionan 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 notificaciones***

  Este servicio independiente supervisa si se implementaron cambios en las cuentas de Dropbox. Aquí no se almacenan ni transfieren archivos ni metadatos. Cada cliente establece una conexión de sondeo de larga duración con el servicio de notificación y espera. Cuando se produce un cambio en un archivo cualquiera en Dropbox, el servicio de notificación envía una señal de cambio al cliente relevante; para ello, cierra la conexión de sondeo de larga duración. El cierre de la conexión le indica al cliente que debe conectarse al servicio de metadatos de forma segura a fin de sincronizar los cambios.

Almacenamiento de datos de archivos

Dropbox almacena principalmente dos tipos de datos de archivos: metadatos sobre archivos (como la fecha y hora en que se modificó por última vez un archivo) y el contenido efectivo de los archivos (bloques de archivos). Todos los metadatos de archivos se almacenan en los servidores de Dropbox. Los bloques de archivos se almacenan en uno de dos sistemas: Amazon Web Services (AWS) o Magic Pocket, el sistema de almacenamiento interno de Dropbox. Magic Pocket comprende software y hardware exclusivos, y se ha diseñado desde cero para que sea confiable y seguro. Tanto en Magic Pocket como en AWS, los datos se cifran en reposo y ambos sistemas cumplen con altos estándares de confiabilidad. Para obtener más detalles, consulta la sección de Confiabilidad a continuación.

Infraestructura de Paper

Los usuarios de Dropbox pueden acceder a los documentos de Paper en cualquier momento desde la web y dispositivos móviles, o bien a través de aplicaciones de terceros vinculadas a la aplicación de Dropbox Paper. Todos estos clientes se conectan a servidores seguros para ofrecer acceso a los documentos de Paper, permitir el uso compartido de archivos y actualizar los dispositivos vinculados cuando se agregan, modifican o eliminan documentos.

La infraestructura de Dropbox Paper está conformada por los siguientes componentes:

- ***Servidores de aplicaciones de Paper***

  Los Servidores de aplicación de Paper procesan las solicitudes de usuario, devuelven al usuario los resultados de los documentos de Paper editados y llevan a cabo servicios de notificación. Los Servidores de aplicación de Paper llevan las ediciones entrantes de usuarios a las bases de datos de Paper, donde se almacenan de forma duradera. Las sesiones de comunicación entre los Servidores de aplicación de Paper y las bases de datos de Paper se cifran con el Protocolo de Transferencia Segura de Hipertexto (HTTPS).

- ***Bases de datos de Paper***

  El contenido efectivo de los documentos de Paper de los usuarios, así como determinados metadatos sobre dichos documentos, se cifran en un almacenamiento duradero dentro de las bases de datos de Paper. Esto incluye información sobre un documento de Paper (como el título, el propietario, la fecha y hora de creación y otra información), así como contenido que se encuentre dentro del documento de Paper como tal, incluidos comentarios y tareas. Las bases de datos de Paper se comparten y replican según sea necesario para cumplir con los requisitos de rendimiento y alta disponibilidad.

- ***Servidores de metadatos***

  Paper utiliza los mismos servidores de metadatos que se describen en el diagrama de infraestructuras de Dropbox para procesar la información relacionada con los documentos de Paper, como el historial de revisión de archivos de documentos de Paper y la membresía de las carpetas compartidas. Dropbox gestiona directamente los servidores de metadatos, que se encuentran en centros de datos independientes compartidos.

- ***Bases de datos de metadatos***

  Paper usa las mismas bases de datos de metadatos que se describen en el diagrama de 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 con copia de seguridad de MySQL y se comparten y replican según sea necesario, para cumplir con los requisitos de rendimiento y alta disponibilidad.

- ***Servidores de almacenamiento de imágenes en Paper***

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

- ***Servidores de vistas previas***

  Los servidores de vistas previas brindan vistas previas de imágenes cargadas en los documentos de Paper y de hipervínculos incrustados en los documentos de Paper. Para las imágenes cargadas en los documentos de Paper, los servidores de vistas previas hacen uso de los datos de imagen almacenados en los servidores de almacenamiento de imágenes de Paper por medio de un canal cifrado. Para los hipervínculos incrustados en los documentos de Paper, los servidores de vistas previas hacen uso de los datos de imagen y brindan una vista previa de la imagen mediante cifrado, según se especifique en el vínculo de origen. Finalmente, los servidores de bloques proporcionan 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 vistas previas de imágenes almacenadas en caché. Las porciones de previas almacenadas en caché se almacenan en un formato cifrado en los servidores de almacenamiento de vistas previas.

Almacenamiento de documentos de Paper

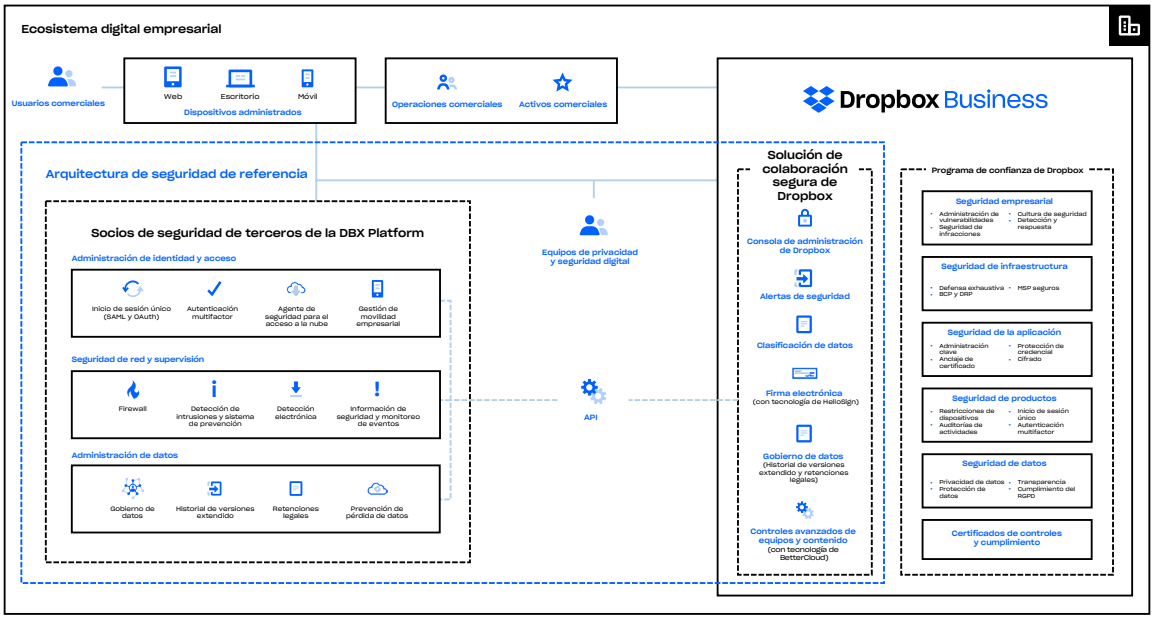
Dropbox almacena principalmente los siguientes tipos de datos en los documentos de Paper: metadatos sobre los documentos de Paper (tales como permisos compartidos de documentos) y el contenido efectivo de los documentos de Paper cargado por el usuario. A estos datos se les conoce como "datos de documentos de Paper", y las imágenes cargadas a los documentos de Paper se conocen como "datos de imagen de Paper". Cada uno de estos datos se almacena en los Amazon Web Services (AWS). Los documentos de Paper se cifran en los AWS, y los AWS cumplen con altos estándares de fiabilidad. Para obtener más detalles, consulta la sección de Fiabilidad a continuación.

Programa de confianza de Dropbox

La confianza es la base de nuestra relación con millones de personas y de empresas en todo el mundo. Valoramos la confianza que depositas en nosotros y asumimos la responsabilidad de proteger tu información con total seriedad. Para hacernos merecedores de tu confianza, desarrollamos y continuaremos desarrollando Dropbox con énfasis en la seguridad, la privacidad, la transparencia y el cumplimiento.

La política del Programa de confianza de Dropbox establece un proceso de análisis de riesgos, diseñado para abordar los problemas relacionados con los entornos, la estructura física, los usuarios, las normas y leyes aplicables, los requisitos contractuales y cualquier otro riesgo que pudiera afectar la seguridad del sistema, así como la confidencialidad, integridad, disponibilidad o privacidad de los datos. Para obtener más información acerca del Programa de confianza de Dropbox, visita dropbox.com/business/trust.

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



Seguridad de nivel empresarial

Dropbox estableció un marco de administración de seguridad de la información que describe el propósito, la dirección, los principios y las reglas básicas acerca de cómo mantenemos la confianza. Esto se logra mediante la evaluación de los riesgos y la mejora continua de la seguridad, la confidencialidad, la integridad, la disponibilidad y la privacidad de los sistemas de Dropbox Business. Revisamos y actualizamos a intervalos regulares las políticas de seguridad, brindamos capacitación en seguridad, llevamos a cabo pruebas de seguridad de la aplicación y la red (incluidas pruebas de penetración), controlamos el cumplimiento con las políticas de seguridad y llevamos a cabo evaluaciones de riesgo internas y externas.

Nuestras políticas

Hemos redactado un estricto conjunto de políticas de seguridad y el equipo de Seguridad y abusos de Dropbox verifica su cumplimiento. Todas las políticas de seguridad se revisan y aprueban al menos una vez por año. Los empleados, pasantes y contratistas participan en sesiones obligatorias de capacitación sobre seguridad al unirse a la empresa, así como en programas continuos de educación sobre seguridad.

- ***Seguridad de la información***

  Cómo protegemos la información de Dropbox y de los usuarios.

- ***Autenticación***

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

- ***Seguridad de los dispositivos***

  Los requisitos mínimos de seguridad para dispositivos móviles que se utilizan para acceder a la información empresarial.

- ***Control de acceso lógico***

  Cómo protegemos el acceso a los sistemas, usuarios e información de Dropbox. Incluye el control de acceso a entornos empresariales y de producción.

- ***Seguridad de datos***

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

- ***Seguridad de viaje***

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

- ***Pautas de seguridad para ventas y experiencia del cliente (CX)***

  Cómo mantenemos segura la información de los usuarios, protegemos a nuestros empleados y proveemos soporte a nuestros usuarios.

- ***Seguridad física***

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

- ***Pautas de seguridad física de producción***

  Cómo gestionamos el acceso físico a las instalaciones de producción.

- ***Respuesta ante incidentes***

  Describe la forma en que Dropbox gestiona los eventos notificados de seguridad, privacidad y de sitio, y registra planes de respuesta ante incidentes para cada uno.

- ***Materiales con derechos de autor no autorizados***

  Cómo se prohíbe a los empleados usar Dropbox o sistemas de Dropbox para almacenar o compartir contenido no autorizado.

- ***Administración de cambios***

  Cómo se administran los cambios en los sistemas de producción. Dirigido a todos los empleados de Dropbox, contratistas y pasantes con acceso a sistemas.

- ***Privacidad de datos del usuario***

  Cómo protegemos y administramos la información de usuarios y los datos de usuarios en Dropbox en cumplimiento con nuestra política de privacidad.

- ***Política de continuidad empresarial y gestión de emergencias***

  Describe a todas las personas (empleados de Dropbox), propiedades y procesos (procesos empresariales) relacionados con la conservación, la protección y la seguridad.

- ***Programa de privacidad de Dropbox***

  El propósito, los principios y la responsabilidad del Programa de privacidad de Dropbox.

- ***Programa de confianza de Dropbox***

  Describe cómo trabaja Dropbox y por qué es digno de tu confianza.

- ***Seguridad del entorno de pagos***

  Cómo protegemos y mantenemos el entorno para pagos dedicado que utiliza Dropbox a la hora de aceptar pagos con tarjetas de crédito.

Política y acceso de los empleados

Después de la contratación, se requiere que cada empleado de Dropbox complete una comprobación de antecedentes, firme una aceptación de las políticas de seguridad y un acuerdo de confidencialidad, y reciba capacitación sobre seguridad. Solamente las personas que hayan completado estos procedimientos tienen acceso físico y lógico a los entornos empresariales y de producción, según se requiera, para llevar a cabo sus asignaciones. Además, todos los empleados deben completar la capacitación de seguridad anual, y reciben capacitación de conciencia sobre la seguridad periódicamente a través de correos electrónicos informativos, charlas y presentaciones, así como recursos disponibles en nuestra intranet.

El acceso de los empleados al entorno de Dropbox se mantiene mediante un directorio central y se autentica a través de una combinación de potentes contraseñas, claves SSH protegidas por frases de contraseñas, y autenticación de dos factores. El acceso remoto requiere el uso de una VPN protegida con autenticación de dos factores; además, el equipo de seguridad verifica y autoriza los accesos especiales. El acceso a las redes corporativas y de producción está limitado estrictamente en función de políticas definidas. Por ejemplo, el acceso a las redes de producción está basado en claves SSH y se limita a los equipos de ingeniería que solicitan acceso como parte de sus obligaciones. La configuración del firewall está controlada y limitada a una cantidad pequeña de administradores.

Además, nuestras políticas internas exigen a los empleados acceder a entornos de producción y corporativos para cumplir con las prácticas recomendadas de creación y almacenamiento de claves privadas SSH. El acceso a otros tipos de recursos, incluidos los centros de datos, las aplicaciones de configuración de los servidores, los

servidores de producción y las aplicaciones de diseño de código fuente se concede a través de una aprobación explícita por parte del gerente que corresponda. Los gerentes llevan un registro de las solicitudes de acceso, las justificaciones y las autorizaciones, y las personas correspondientes conceden el acceso.

Dropbox usa controles técnicos de acceso y políticas internas para prohibir a los empleados acceder arbitrariamente a los archivos de los usuarios y para limitar el acceso a los metadatos y otros tipos de información relacionada con las cuentas de los usuarios. A fin de proteger la privacidad y la seguridad del usuario final, solamente un número reducido de ingenieros responsables de programar los servicios principales de Dropbox tiene acceso al entorno en el que se almacenan los archivos de los usuarios. Todo tipo de acceso por parte de los empleados se elimina oportunamente cuando un empleado abandona la empresa.

Debido a que Dropbox es una extensión de la infraestructura de nuestros clientes, estos pueden tener la seguridad de que somos custodios responsables de sus datos. Consulta la sección Privacidad a continuación para obtener más información.

Control de las vulnerabilidades

Nuestro equipo de seguridad realiza frecuentemente versiones de pruebas de seguridad automatizadas y manuales, así como administración de correcciones, además de trabajar con especialistas de terceros para identificar y resolver cualquier posible error o infracción de seguridad.

Como un componente necesario de nuestro sistema de administración de seguridad de la información, los resultados y las recomendaciones que surgen de estas actividades y evaluaciones se comunican a la gerencia de Dropbox, y luego se analizan y se adoptan las medidas que se consideren necesarias. Se documentan los problemas más graves, se les hace un seguimiento y los ingenieros de seguridad asignados los resuelven oportunamente.

Administración de cambios

Todos los procesos de desarrollo, resolución de problemas y correcciones siguen la política de administración de cambios formal definida por el equipo de ingeniería de Dropbox, a fin de garantizar que los cambios al sistema se hayan probado y autorizado antes de su implementación en los entornos de producción. Los programadores que desean hacer una mejora en la aplicación o el servicio de Dropbox son quienes inician los cambios en el código fuente. Los cambios se almacenan en un sistema de control de versiones y deben someterse a procedimientos automatizados de pruebas de aseguramiento de la calidad (QA) para verificar que se cumplan los requisitos de seguridad. Una vez que se completan correctamente los procedimientos de QA, es posible implementar el cambio. Los cambios autorizados por QA se implementan automáticamente en el entorno de producción. Nuestro ciclo de vida de programación de software (SDLC) exige que se cumplan las pautas de codificación segura, así como un filtrado de cambios en los códigos, para detectar potenciales problemas de seguridad, a través de nuestros procesos de QA y de revisión manual. Los cambios enviados a producción se registran y archivan, y, automáticamente, se envían alertas a la gerencia del equipo de ingeniería de Dropbox.

Los cambios en la infraestructura de Dropbox están restringidos al personal autorizado únicamente. El equipo de seguridad de Dropbox es responsable de mantener la seguridad de la infraestructura y de asegurar que la configuración relacionada con los servidores, los firewalls y otros parámetros inherentes a la seguridad se mantengan al día con los criterios de la industria. Los conjuntos de reglas de firewall y las personas con acceso a los servidores de producción se revisan a intervalos regulares.

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

Nuestro equipo de seguridad lleva a cabo pruebas de seguridad de aplicaciones manuales y automatizadas a intervalos regulares para identificar y corregir los posibles errores y vulnerabilidades de seguridad en nuestras aplicaciones para escritorio y para dispositivos móviles (Dropbox y Paper), y en nuestro sitio web (Dropbox y Paper).

Además, Dropbox contrata proveedores externos para que lleven a cabo pruebas de penetración y vulnerabilidad a intervalos regulares en los entornos de producción. A fin de proteger nuestras aplicaciones, trabajamos con especialistas externos, otros equipos de seguridad del sector y la comunidad de investigación de seguridad. También utilizamos sistemas de análisis automático para identificar vulnerabilidades. Este proceso incluye sistemas que desarrollamos internamente, sistemas de código abierto que modificamos para que se adapten a nuestras necesidades y proveedores externos que contratamos para llevar a cabo análisis continuos y automatizados.

Cómo mantenemos el contenido perjudicial fuera de Dropbox

Contamos con capacidades de escaneo que tienen el objetivo de impedir el almacenamiento y la distribución de contenido perjudicial en Dropbox. Nuestros escáneres utilizan tecnologías desarrolladas localmente, junto con capacidades de vanguardia de socios como Microsoft y Google, para hacer de Dropbox un lugar seguro para nuestros clientes.

Recompensas por detección de errores

Si bien trabajamos con organizaciones profesionales con las que celebramos acuerdos de pruebas de penetración y llevamos a cabo nuestras propias pruebas internas, las recompensas por detección de errores (o programas de premios por detección de vulnerabilidades) permiten aprovechar al máximo la pericia de una comunidad más amplia especializada en seguridad. Nuestro programa de recompensa por detección de errores brinda un incentivo a los investigadores para que identifiquen y divulguen de forma responsable los errores del software. Este compromiso con la comunidad externa ofrece a nuestro equipo de seguridad una evaluación independiente de nuestras aplicaciones para contribuir a la seguridad de los usuarios. Queremos ser líderes en el sector de recompensas ante vulnerabilidades, así como en tiempos de reparación y respuesta.

Establecimos el alcance de las presentaciones que reúnan los requisitos y de las aplicaciones de Dropbox, así como una política de divulgación responsable que promueva la detección y el informe de las vulnerabilidades de seguridad, lo que contribuye a proteger más eficientemente la seguridad de los usuarios. En esta política, se estipulan las siguientes pautas:

- Comunícanos el problema de seguridad en detalle.
- Te pedimos que respetes nuestras aplicaciones. Enviar formularios no deseados de manera masiva a través de los escáneres automatizados de vulnerabilidad no te hará ganar ninguna recompensa o premio, ya que estos están explícitamente fuera de alcance.
- Danos un tiempo razonable para responder antes de hacer pública la información acerca del problema de seguridad.
- No accedas a los datos de los usuarios ni los modifiques sin el permiso del propietario de la cuenta.
- No visualices, alteres, guardes, almacenes, transfieras o ni siquiera accedas a los datos, y purga inmediatamente cualquier información local después de informar a Dropbox de la vulnerabilidad.
- Actúa de buena fe y evita violaciones de privacidad, destrucción de datos e interrupción o degradación de nuestros servicios (incluida la denegación de servicio).

Para advertir sobre un problema, es posible enviar un informe a Bugcrowd a través del sitio bugcrowd.com/dropbox.

Seguridad física

Modernización

El acceso físico a las instalaciones de la organización de subservicios donde residen los sistemas de producción está restringido al personal autorizado por Dropbox, según se requiera para realizar sus funciones laborales. Las personas que requieran acceso adicional a instalaciones del entorno de producción reciben acceso a través de la aprobación explícita de la administración correspondiente.

Los gerentes llevan un registro de las solicitudes de acceso, las justificaciones y las autorizaciones, y las personas correspondientes conceden el acceso. Una vez recibida la aprobación, un miembro responsable del equipo de infraestructura se comunicará con la organización de subservicios correspondiente para solicitar acceso para la persona aprobada. La organización de subservicios ingresa la información del usuario en su propio sistema y otorga al personal de Dropbox aprobado acceso de insignia y, de ser posible, acceso de escaneo biométrico. Una vez otorgado el acceso a personas aprobadas, el centro de datos es responsable de garantizar que el acceso se restrinja a personas autorizadas solamente.

Oficinas corporativas

- ***Seguridad física***

  El equipo de seguridad física de Dropbox es responsable de exigir el cumplimiento con la política de seguridad física y de supervisar la seguridad de nuestras oficinas.

- ***Política de visitas y acceso***

  El acceso físico a instalaciones corporativas, diferentes de las entradas públicas y los pasillos, está restringido a personal autorizado de Dropbox y visitas registradas, acompañadas por personal de Dropbox. Un sistema de acceso de insignia garantiza que solo las personas autorizadas tengan acceso a áreas restringidas dentro de las instalaciones corporativas.

- ***Acceso a servidores***

  El acceso a las áreas donde se encuentran los servidores corporativos y equipo de redes está restringido al personal autorizado a través de roles de importancia concedidos a través del sistema de acceso con tarjeta de identificación. La lista de personas autorizadas para el acceso físico a los entornos corporativos y de producción se revisa al menos trimestralmente.

Respuesta ante incidentes

Contamos con políticas y procedimientos de respuesta ante incidentes para resolver cuestiones relacionadas con la disponibilidad, integridad, seguridad, privacidad y confidencialidad del servicio. Como parte de nuestros procedimientos de respuesta ante incidentes, tenemos equipos especializados que están capacitados para:

- Responder con rapidez a las alertas de posibles incidentes.
- Determinar la gravedad del incidente.
- De ser necesario, poner en práctica medidas de mitigación y contención.
- Comunícate con las partes interesadas correspondientes a nivel interno y externo; por ejemplo, informa a los clientes afectados para satisfacer las obligaciones contractuales de notificación de incidentes o incumplimientos y para cumplir con las leyes y reglamentaciones pertinentes.

- Recopilar y preservar evidencia para investigaciones.
- Documentar posteriormente un balance de resultados y desarrollar un plan para establecer prioridades de forma permanente.

Las políticas y los procedimientos de respuesta ante incidentes se controlan en nuestras auditorías de SOC 2+, ISO/IEC 27001 y otras evaluaciones de seguridad.

Seguridad de infraestructura

Seguridad de la red

Dropbox preserva diligentemente la seguridad de nuestra red de datos back-end. Nuestras técnicas de seguridad y de supervisión de redes se diseñaron para brindar múltiples capas de protección y defensa. Aplicamos técnicas de protección estándar en la industria, incluidos firewalls, exploración de vulnerabilidades de la red, supervisión de seguridad de redes y sistemas de detección de intrusiones para asegurar que solamente pueda llegar a nuestra infraestructura el tráfico que cumpla con los requisitos y que no sea malintencionado.

Nuestra red privada interna está segmentada conforme al uso y a los niveles de riesgo. A continuación, se indican las redes principales:

- DMZ accesible desde Internet
- DMZ de infraestructura de prioridad
- Red de producción
- Red corporativa

El acceso al entorno de producción está restringido a las direcciones IP autorizadas únicamente y exige una autenticación de varios factores en todos los puntos de extremo. Las direcciones IP con acceso están asociadas con la red corporativa o con el personal de Dropbox autorizado. Las direcciones IP autorizadas se revisan trimestralmente para asegurar un entorno de producción seguro. El acceso para modificar la lista de direcciones IP se limita a las personas autorizadas.

Varias capas de firewall y proxy protegen el tráfico de Internet destinado a nuestra red de producción.

Se mantiene una estricta limitación entre la red interna de Dropbox y la Internet pública. Todo el tráfico de Internet hacia la red de producción y desde ella se controla exhaustivamente a través de un servicio dedicado de servidores proxy que, a su vez, están protegidos por reglas de firewall restrictivas.

Dropbox dispone de conjuntos de herramientas sofisticadas para supervisar las computadoras portátiles y de escritorio con sistemas operativos Mac y Windows, y sistemas de producción destinados a los eventos malintencionados. Todos los registros de seguridad se recopilan en una ubicación centralizada para permitir una respuesta forense y ante incidentes, de conformidad con la política de conservación estándar en la industria.

Dropbox identifica y mitiga los riesgos a través de auditorías y pruebas de seguridad de la red a intervalos regulares que llevan a cabo equipos de seguridad internos y especialistas en seguridad externos.

Puntos de presencia (PoP)

Para optimizar el rendimiento del sitio web para los usuarios, Dropbox aprovecha las redes de entrega de contenido (CDN) de terceros y los puntos de presencia (PoP) de Dropbox en 31 ubicaciones alrededor del mundo. No se almacenan en la caché datos del usuario en estas ubicaciones, y todos los datos de usuarios transferidos se cifran con SSL/TLS. El acceso físico y lógico a PoP alojados por Dropbox está restringido al personal autorizado de Dropbox solamente. Dropbox realiza optimizaciones en la capa de transporte (TCP) y la capa de aplicación (HTTP).

Emparejamiento

Dropbox tiene una política de emparejamiento abierto, y se recomienda a todos los clientes realizar el emparejamiento con nosotros. Para obtener más información, visita dropbox.com/peering.

Fiabilidad

Un sistema de almacenamiento solo tiene buenos resultados si es fiable. Por eso, desarrollamos Dropbox con múltiples capas de redundancia para ofrecer protección contra la pérdida de datos y para asegurar la disponibilidad.

Metadatos de archivo

Las copias redundantes de los metadatos están distribuidas en dispositivos independientes en un centro de datos en al menos un modelo de disponibilidad N+2. Las copias de seguridad progresivas se realizan cada hora y las copias de seguridad completas, cada 36 horas. Los metadatos se almacenan en servidores alojados y administrados por Dropbox en Estados Unidos.

Bloques de archivo

Las copias redundantes de los bloques de archivos se almacenan independientemente en al menos dos regiones geográficas separadas y se replican de forma confiable dentro de cada región. (**Nota:** para los clientes que eligen tener los archivos almacenados en nuestra infraestructura alemana, australiana, japonesa o la de Reino Unido, los bloques de archivos se replican solo dentro de sus respectivas regiones. Para obtener más información, consulta la sección Centros de datos y proveedores de servicios administrados a continuación). Tanto Magic Pocket como AWS están diseñados para brindar una durabilidad de datos anual de al menos un 99,999999999 %.

La arquitectura, las aplicaciones y los mecanismos de sincronización de Dropbox trabajan juntos para proteger los datos de los usuarios y volverlos altamente disponibles. En el extraño caso de la interrupción de la disponibilidad del servicio, los usuarios de Dropbox aún pueden acceder a las últimas copias de archivos que se hayan sincronizado con la carpeta de Dropbox local en las computadoras vinculadas. Las copias de los archivos sincronizados en la carpeta del escritorio o la carpeta local de Dropbox del cliente están disponibles en el disco duro de un usuario durante períodos de inactividad y cortes del servicio, así como cuando no hay conexión a Internet. Los cambios en los archivos y carpetas se sincronizarán con Dropbox una vez que se haya restaurado el servicio o la conectividad.

Documentos de Paper

Las copias redundantes de los datos de los documentos de Paper están distribuidas en dispositivos independientes en un centro de datos en un modelo de disponibilidad N+1. También se realizan copias de seguridad completas de los datos de los documentos de Paper todos los días. Para el almacenamiento de los documentos de Paper, Dropbox usa una infraestructura AWS en Estados Unidos, la cual está diseñada para brindar una durabilidad de datos anual de por lo menos un 99,999999999 %. En el extraño caso de una interrupción de la disponibilidad del servicio, los usuarios aún pueden acceder a las últimas copias sincronizadas de sus documentos de Paper en el modo "sin conexión" de la aplicación móvil.

Sincronización de archivos

Dropbox ofrece la mejor sincronización de archivos en su clase, con reconocimiento del sector. Nuestros mecanismos de sincronización garantizan transferencias de archivos rápidas y flexibles, y permiten acceder a los datos estés donde estés, en cualquier dispositivo. La sincronización de Dropbox también es elástica. En caso de error en la conexión al servicio de Dropbox, un cliente reanuda correctamente el funcionamiento al restablecerse la conexión. Los archivos solamente se actualizan en el cliente local si se sincronizaron completamente y se validaron de forma correcta con el servicio de Dropbox. El equilibrio de cargas en múltiples servidores asegura la redundancia y una experiencia de sincronización uniforme para el usuario final.

Sincronización delta

Con este método de sincronización, solo se cargan/descargan las partes modificadas de los archivos. Dropbox almacena cada archivo cargado en bloques cifrados discretos y solo actualiza aquellos bloques en los que se realizaron cambios.

Sincronización por secuencias

En lugar de esperar que se complete la carga de un archivo, la sincronización con transmisión por secuencias comienza a descargar los bloques sincronizados a un segundo dispositivo antes de que terminen de cargarse desde el primero. Este método se emplea automáticamente cuando se vinculan varias computadoras a la misma cuenta de Dropbox o cuando distintas cuentas de Dropbox comparten una carpeta.

Ahorrar espacio en el disco duro

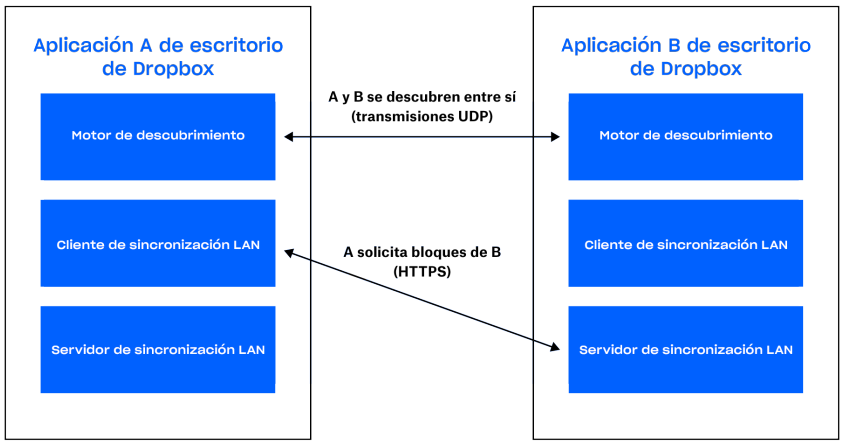
Los usuarios pueden liberar espacio de almacenamiento en la computadora al dejar disponibles sin conexión únicamente los archivos que desean en sus discos rígidos. Esto libera espacio en la computadora al mantener todo lo demás solo online en dropbox.com.

Sincronización LAN

Al habilitarse, esta función descarga archivos nuevos y actualizados de otras computadoras en la misma Red de área local (LAN), lo que permite ahorrar tiempo y ancho de banda en comparación con la descarga de archivos de servidores de Dropbox.

Arquitectura

Hay tres componentes principales del sistema de sincronización LAN que se ejecutan en la aplicación para escritorio: el motor de descubrimiento, el servidor y el cliente. El motor de descubrimiento es responsable de buscar máquinas en la red con las que llevar a cabo la sincronización. Esto se limita a máquinas que tienen acceso autorizado al mismo personal o carpeta(s) compartida(s) de Dropbox. El servidor maneja solicitudes de otras máquinas en la red y sirve a bloques de archivos solicitados. El cliente es responsable de solicitar bloques de archivos de la red.



Motor de descubrimiento

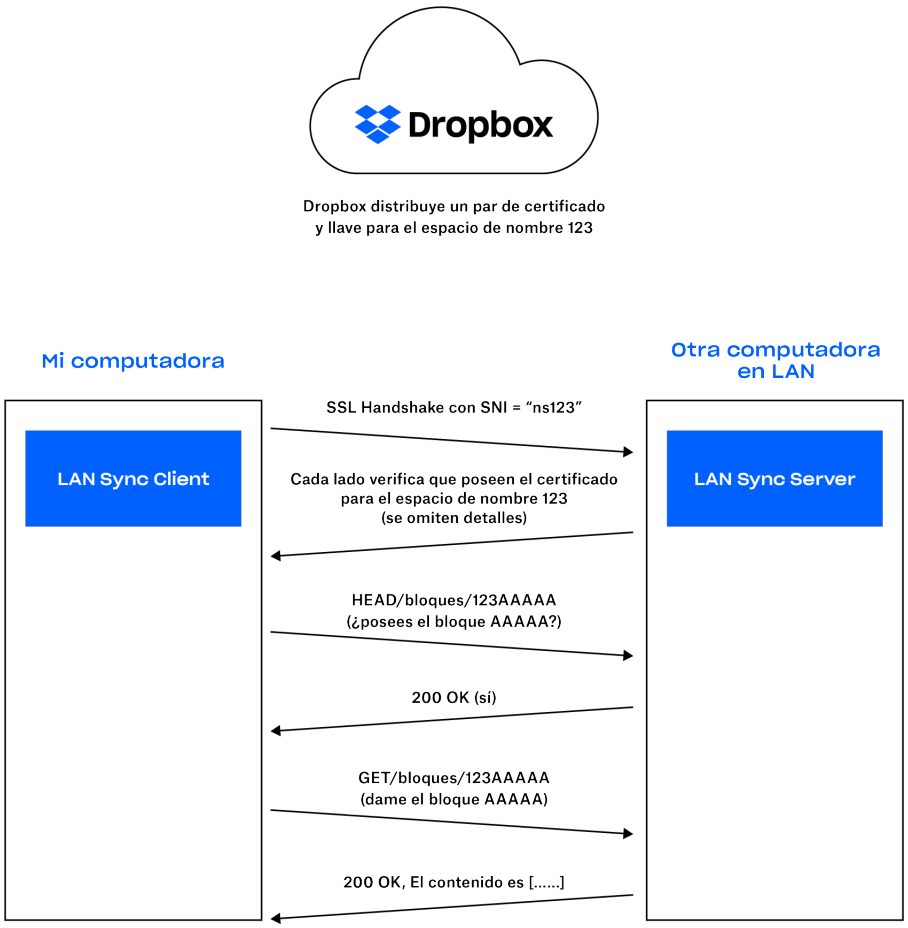
Cada máquina en la LAN envía y escucha periódicamente paquetes de difusión UDP a través del puerto 17500 (reservado por IANA para la sincronización LAN). Estos paquetes incluyen la versión del protocolo usada por esa computadora, las carpetas de Dropbox personales y compartidas compatibles; el puerto TCP que se usa para ejecutar el servidor (que puede ser diferente de 17500 si ese puerto no está disponible); y un identificador aleatorio para la máquina. Cuando se observa un paquete, la dirección IP de la máquina se agrega a una lista para cada carpeta personal o compartida, que indica un posible objetivo.

Protocolo

La transferencia de los bloques de archivos reales se realiza a través de HTTPS. Cada computadora ejecuta un servidor HTTPS con terminales. Un cliente sondeará varios pares par ver si tienen los bloques, pero solo descarga los bloques de un servidor.

Para proteger todos sus datos, garantizamos que solo los clientes autenticados para una carpeta determinada puedan solicitar bloques de archivos. También garantizamos que las computadoras no pretendan actuar como servidores para carpetas que no controlan. Para solucionar esto, generamos pares de claves/certificados SSL para cada carpeta Dropbox personal o compartida. Estas se distribuyen desde servidores de Dropbox a las computadoras del usuario autenticadas para la carpeta. Los pares de claves/certificados rotan cuando se producen cambios en la membresía (por ejemplo, cuando se elimina a alguien de una carpeta compartida). Requerimos que los extremos de la conexión HTTPS se autentiquen con el mismo certificado (el certificado para la carpeta Dropbox o compartida). Esto demuestra que ambos extremos de la conexión están autenticados.

Al establecer una conexión, indicamos al servidor la carpeta personal de Dropbox o la carpeta con la que estamos intentando establecer la conexión usando la Indicación de nombre de servidor (SNI) de modo que el servidor use el certificado correcto.



Servidor/cliente

Con el protocolo descrito anteriormente, el servidor solo debe conocer los bloques que están presentes y dónde encontrarlos.

En función de los resultados del motor de descubrimiento, el cliente mantiene una lista de pares para cada carpeta personal de Dropbox o compartida. Cuando el sistema de sincronización LAN recibe una solicitud para descargar un bloque de archivos, este envía una solicitud a una muestra aleatoria de pares que se ha descubierto para la carpeta Dropbox personal o compartida y, a continuación, solicita el bloque del primero que responde que tiene el bloque.

Para evitar latencias, usamos grupos de conexión que nos permitan volver a conexiones ya iniciadas. No abrimos una conexión hasta que sea necesario y, una vez abierta, la mantenemos activa en caso de necesitarla otra vez. También limitamos la cantidad de conexiones a cualquier par individual.

Si no se encuentra ni descarga correctamente el bloque de archivos, o si la conexión se torna demasiado lenta, el sistema regresa a obtener el bloque de los servidores de Dropbox.

Centros de datos y proveedores de servicios administrados

Los sistemas corporativos y de producción de Dropbox están alojados en centros de datos de organizaciones de subservicios externos y son administrados por proveedores de servicios que residen en los Estados Unidos. Los informes SOC de los centros de datos de organizaciones de servicios subsidiarios o los cuestionarios de seguridad para proveedores y sus obligaciones contractuales se revisan como mínimo una vez al año para garantizar los controles de seguridad necesarios. Estos proveedores de servicios externos son responsables de los controles de seguridad físicos, ambientales y operativos en los límites de la infraestructura de Dropbox. Dropbox es responsable de la seguridad lógica, de red y de la aplicación de nuestra infraestructura alojada en los centros de datos externos.

Nuestro proveedor de servicios administrados para procesamiento y 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 a través de su firewall, que se configura en un modo predeterminado de denegar todo. 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 los bloques de archivos en regiones fuera de los Estados Unidos para los clientes calificados. Amazon Web Services (AWS) aloja nuestra infraestructura 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 metadatos de archivos se almacenan en los Estados Unidos en servidores exclusivos de Dropbox. Los documentos de Paper y las vistas previas se almacenan actualmente en los Estados Unidos para todos los clientes.

Continuidad de las operaciones

Dropbox ha establecido un sistema de administración de continuidad de las operaciones (BCMS) para determinar cómo reanudar o continuar la prestación de servicios a los usuarios (y el funcionamiento como empresa) ante interrupciones en actividades y procesos críticos. Realizamos un proceso cíclico que comprende las siguientes fases:

- ***Impacto comercial y evaluaciones de riesgo***

  Realizamos una evaluación del impacto comercial (BIA) al menos una vez al año para identificar procesos críticos para Dropbox, evaluar el posible impacto de las interrupciones, establecer marcos temporales priorizados para recuperación, e identificamos nuestras dependencias críticas y proveedores. También realizamos una evaluación de riesgos de la compañía al menos una vez al año. La evaluación de riesgo nos ayuda a identificar, analizar y evaluar sistemáticamente el riesgo de incidentes disruptivos en Dropbox. Juntas, la evaluación de riesgo y la BIA brindan información sobre prioridades de continuidad, además de estrategias de mitigación y recuperación para planes de continuidad de las operaciones (BCP).

- ***Planes de continuidad de las operaciones***

  Los equipos identificados por la BIA como críticos para la continuidad de Dropbox usan esta información para desarrollar BCP para sus procesos críticos. Estos planes ayudan a los equipos a saber quién es responsable de reanudar los procesos si existe una emergencia, quién en otra oficina de Dropbox o ubicación puede asumir el control de sus procesos durante una interrupción, así como los métodos para comunicaciones que deben usarse durante un evento de continuidad. Estos planes también ayudan a prepararnos para un incidente de interrupción mediante la centralización de nuestros planes de recuperación y otra información importante, tal como cuándo y cómo se debe usar el plan, información de contacto y reunión, aplicaciones importantes y estrategias de recuperación. Los planes de continuidad de Dropbox están vinculados al plan de administración de crisis (CMP) de la compañía, que establece equipos de administración de crisis y respuesta a incidentes de Dropbox.

- ***Pruebas/ejercicios del plan***

  Dropbox realiza pruebas en elementos seleccionados de sus planes de continuidad de las operaciones al menos una vez al año. Estas pruebas son coherentes con el alcance y los objetivos de BCM, están basadas en situaciones adecuadas y están bien diseñadas con objetivos claramente definidos. Las pruebas pueden tener un alcance diverso, desde ejercicios prácticos hasta simulaciones a gran escala de incidentes de la vida real. En función de los resultados de las pruebas, además de la experiencia de incidentes reales, los equipos actualizan y mejoran sus planes para abordar problemas y fortalecer sus capacidades de respuesta.

- ***Revisión y aprobación de BCMS***

  Al menos una vez al año, nuestro personal ejecutivo revisa el BCMS como parte de la revisión del Programa de confianza de Dropbox.

Recuperación ante desastres

Para abordar los requisitos de seguridad de la información durante una crisis o un desastre de gran magnitud que afecte el funcionamiento de Dropbox Business, establecemos un plan de recuperación ante desastres. El equipo de ingeniería de Dropbox revisa anualmente este plan y realiza pruebas de elementos seleccionado al menos una vez al año. Los hallazgos relevantes se documentan y registran hasta su resolución.

Nuestro Plan de recuperación ante desastres (DRP) aborda desastres de durabilidad y disponibilidad, que se definen de la siguiente manera.

- Un desastre de durabilidad comprende uno o más de los siguientes:
  - Una pérdida completa o permanente de un centro de datos primario que almacena metadatos, o de múltiples centros de datos que almacenan los bloques de archivo.
  - La pérdida de la capacidad de comunicar o publicar datos desde un centro de datos que almacena metadatos, o desde múltiples centros de datos que almacenan el contenido de archivos.
- Un desastre de disponibilidad comprende uno o más de los siguientes:
  - Una interrupción en la energía de más de 10 días de duración.
  - Pérdida de capacidad para comunicar o publicar datos desde un servicio de almacenamiento/centro de datos que almacena metadatos, o desde múltiples servicios de almacenamiento/centros de datos que almacenan los bloques de archivo.

Definimos un "tiempo de recuperación objetivo" (RTO), que es el lapso de tiempo y el nivel de servicio en los que se deben restaurar los procesos operativos o el servicio después de un desastre, así como un "punto de recuperación objetivo" (RPO), que es el período máximo tolerable durante el cual puede haber datos perdidos por una interrupción del servicio. Además, medimos el "tiempo de recuperación real" (RTA) durante las pruebas de recuperación ante desastres, que se llevan a cabo al menos una vez al año.

Los planes de respuesta ante incidentes, de continuidad de las operaciones y de recuperación ante desastres de Dropbox pueden evaluarse a intervalos planificados y ante cambios considerables en la organización y el entorno.

Seguridad de las aplicaciones

Interfaces del usuario de Dropbox

Es posible usar el servicio de Dropbox y acceder a él a través de diferentes interfaces. Cada una de ellas cuenta con configuraciones y características de seguridad que procesan y protegen los datos del usuario a la vez que garantizan un fácil acceso.

- ***WEB***

  Es posible acceder a esta interfaz a través de cualquier explorador web moderno. Permite a los usuarios cargar, descargar, ver y compartir archivos. La interfaz web también permite que los usuarios abran las versiones locales existentes de los archivos a través de la aplicación predeterminada de su computadora.

- ***Escritorio***

  La aplicación de Dropbox para escritorio es un poderoso cliente de sincronización que almacena archivos localmente para acceder a ellos sin conexión. Le concede al usuario acceso total a sus cuentas de Dropbox y se ejecuta en los sistemas operativos Windows y Mac. Los archivos pueden visualizarse y compartirse directamente en los respectivos exploradores de archivos de cada sistema operativo.

- ***Móvil***

  La aplicación Dropbox está disponible para dispositivos con iOS y Android, lo que permite a los usuarios acceder a todos sus archivos desde cualquier lugar. La aplicación para dispositivos móviles también habilita a los usuarios a elegir archivos para acceder sin conexión.

- ***API***

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

Interfaces de usuario de Paper

Es posible usar el servicio de Paper y acceder a él a través de diferentes interfaces. Cada una de ellas tiene configuraciones y características de seguridad que procesan y protegen los datos del usuario a la vez que garantizan un fácil acceso.

- ***Web***

  Es posible acceder a esta interfaz a través de cualquier buscador web moderno. Permite a los usuarios crear, ver, editar, descargar y compartir sus documentos de Paper.

- ***Móvil***

  La aplicación móvil de Paper está disponible para dispositivos móviles y tablets iOS y Android, lo que permite a los usuarios acceder a todos los archivos desde cualquier lugar. La aplicación móvil está integrada como una aplicación híbrida compuesta por un código nativo (iOS o Android) que envuelve un buscador de vista web interna.

- ***API***

  La API de Dropbox descrita anteriormente contiene terminales y tipos de datos para administrar documentos y carpetas en Dropbox Paper, entre los que se encuentra un soporte de funcionalidad, como la administración de permisos, almacenamiento y borrado permanente.

Cifrado

Datos en tránsito

Para proteger los datos en tránsito entre las aplicaciones de Dropbox y nuestros servidores, Dropbox aplica el protocolo de capa de sockets seguros (SSL)/seguridad de la capa de transporte (TLS) para la transferencia de datos, lo que crea un túnel seguro protegido por el estándar de cifrado avanzado (AES) de 128 bits o superior. Los datos de archivos en tránsito entre un cliente de Dropbox (actualmente la aplicación para escritorio, la aplicación para dispositivos móviles, la API o el sitio web) y el servicio alojado están cifrados a través de SSL/TLS. Asimismo, los datos de documentos de Paper en tránsito entre un cliente de Paper (de la API, móvil o web) y los servicios alojados están igualmente cifrados a través de SSL/TLS. Para los puntos de extremo que nosotros controlamos (escritorio y dispositivos móviles) y los exploradores modernos, usamos cifrados potentes y admitimos confidencialidad directa total y fijación de certificados. Además, en la Web marcamos todas las cookies de autenticación como seguras y habilitamos la seguridad de transporte HTTP estricta (HSTS) con la directiva para incluir todos los subdominios activada.

Nota: Dropbox usa TLS exclusivamente y ha dado por obsoleto el uso de SSLv3 a causa de vulnerabilidades conocidas. No obstante, el TLS se conoce con frecuencia como "SSL/TLS", de modo que aquí usamos esta designación.

Para evitar los ataques del tipo "attacker-in-the-middle", la autenticación de los servidores front-end de Dropbox se ejecuta a través de certificados públicos en poder del cliente. Antes de la transferencia de cualquier archivo, se negocia una conexión cifrada que garantiza la entrega segura de archivos o documentos de Paper a los servidores front-end de Dropbox.

Datos en reposo

Los archivos de Dropbox cargados por usuarios se cifran a través del estándar de cifrado avanzado (AES) de 256 bits. Los archivos se almacenan en varios centros de datos en bloques de archivos discretos. Cada bloque se fragmenta y cifra mediante un cifrado seguro. Solamente se sincronizan los bloques que se modificaron entre revisiones. Los documentos de Paper en reposo también se cifran por medio del estándar de cifrado avanzado (AES) de 256 bits. Los documentos de Paper se almacenan a lo largo de múltiples áreas de disponibilidad usando sistemas de terceros.

Administración de claves

La infraestructura de administración de claves de Dropbox está diseñada con controles de seguridad operativa, técnica y de procedimientos con un acceso directo a las claves muy limitado. La generación de claves de cifrado, el intercambio y almacenamiento se distribuyen para permitir el procesamiento descentralizado.

- ***Claves de cifrado de archivos***

  Dropbox se diseñó para administrar las claves de cifrado de archivos en nombre de los usuarios a fin de quitar las complejidades y habilitar las características avanzadas del producto y un potente control criptográfico. Las claves de cifrado de archivos se crean, almacenan y protegen mediante controles de seguridad y políticas de seguridad de la infraestructura del sistema de producción.

- ***Claves SSH internas***

  El acceso a los sistemas de producción está restringido con pares únicos de claves SSH. Las políticas y los procedimientos de seguridad requieren la protección de las claves SSH. Un sistema interno administra el proceso de intercambio seguro de las claves públicas, y las claves privadas se almacenan de forma segura. Las claves SSH internas no pueden usarse para acceder a los sistemas de producción sin un segundo factor de autenticación independiente.

- ***Distribución de claves***

  Dropbox automatiza la administración y distribución de las claves confidenciales a los sistemas necesarios para las operaciones.

Fijación de certificados

Dropbox realiza fijación de certificados en los exploradores modernos que admiten la especificación de fijación de claves públicas para HTTP, así como en nuestros clientes para escritorio y para dispositivos móviles. La fijación de certificados es un control adicional para asegurar que el servicio al que te conectas sea realmente quien dice ser y no un impostor. La usamos para protegerte contra otras formas en que los piratas informáticos más experimentados pueden intentar controlar tu actividad.

Protección de datos de autenticación

Dropbox va más allá de la aplicación regular de algoritmos hash para proteger las credenciales de inicio de sesión de los usuarios. Al mantener las prácticas recomendadas del sector, se aplica un resumen criptográfico de cada contraseña con un algoritmo único por usuario generado aleatoriamente, a la vez que usamos algoritmos hash iterativos para desacelerar el cálculo. Estas prácticas ayudan a brindar protección contra fuerza bruta, diccionario y ataques arcoíris. Como precaución adicional, ciframos los algoritmos hash con una clave almacenada de manera individual de la base de datos, que ayuda a mantener protegidas las contraseñas en el caso de un riesgo de la base de datos solamente.

Escaneo de malware

Hemos desarrollado un sistema automatizado que escanea malware en el punto en que cualquier contenido se comparte fuera de la cuenta del usuario de origen. El sistema aprovecha la tecnología exclusiva y los motores de detección estándar del sector, y está diseñado para impedir el avance del malware.

Seguridad del producto

Dropbox proporciona las características de control administrativo y de visibilidad que potencian al equipo de informática y a los usuarios finales para administrar y proteger de forma eficaz los negocios y los datos. Con Dropbox, obtienes todo lo que necesitas para trabajar (tus herramientas, contenido y colaboradores) en un solo lugar. Dropbox es más que un almacenamiento seguro: es una forma inteligente y constante de optimizar tu flujo de trabajo existente.

A continuación, se destacan algunas de las características disponibles para los administradores y los usuarios, así como las integraciones con herramientas de terceros para administrar los procesos informáticos fundamentales.

Nota: la disponibilidad de características varía según el plan de suscripción. Visita dropbox.com/business/plans para obtener más información.

Controles de contenido

La protección de activos empresariales confidenciales (como la propiedad intelectual y la información de identificación personal o PII) es crucial para los equipos de seguridad de TI y de datos. Desde permisos detallados a políticas de retención de datos y retenciones legales, Dropbox provee soluciones de vanguardia en la industria para gestionar, monitorear y proteger tu contenido. A continuación, se presentan los productos y características principales de Dropbox que permiten el control del contenido.

Permisos de contenido granular y permisos de archivos y carpetas compartidos

- ***Permisos para archivos compartidos***

  Un miembro del equipo que es propietario de un archivo compartido puede restringir el acceso a usuarios específicos e inhabilitar los comentarios para el archivo.

- ***Permisos para archivos compartidos***

  Un miembro del equipo que es propietario de una carpeta compartida puede quitar el acceso a la carpeta para usuarios específicos, cambiar permisos de lectura/edición para usuarios específicos y transferir la propiedad de carpetas. En función de los permisos de uso compartido globales del equipo, el propietario de cada carpeta compartida también puede controlar si se puede compartir con personas fuera del equipo, si otros con permisos de edición pueden administrar la membresía y si se pueden compartir los vínculos con personas fuera de la carpeta.

- ***Contraseñas para vínculos compartidos***

  Cualquier vínculo compartido puede protegerse con una contraseña definida por el propietario. Antes de transmitir datos de un archivo o carpeta, una capa de control de acceso verifica que se haya enviado la contraseña correcta y que se hayan cumplido todos los demás requisitos (como ACL de equipo, grupo o carpeta). De ser así, se almacena una cookie segura en el explorador del usuario para recordar que la contraseña se verificó anteriormente. Con los controles de uso compartido, los administradores también pueden establecer contraseñas predeterminadas, en lugar de tenerlas como opcionales, para proteger mejor el contenido de su equipo.

- ***Caducidad de vínculos compartidos***

  Los usuarios pueden definir una fecha de caducidad para cualquier vínculo compartido, a fin de proporcionar un acceso transitorio a los archivos o las carpetas. Con los controles de uso compartido, los administradores también pueden establecer vencimientos predeterminados, en lugar de tenerlos como opcionales, para proteger mejor el contenido de su equipo.

Permisos de 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 restringir el acceso a usuarios específicos e inhabilitar la edición para el documento de Paper.

- ***Permisos para documentos de Paper***

  Un miembro del equipo que es propietario de un documento de Paper puede quitar el acceso de usuarios específicos que aparecen explícitamente en el panel de recursos compartidos. 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 vínculos del documento. La política de vínculos rige qué usuarios pueden abrir el documento y los permisos que se les conceden. El administrador del equipo puede establecer políticas para todo el equipo para los enlaces y el uso compartido de documentos.

- ***Permisos para carpetas de Paper***

  Un miembro del equipo que sea miembro de la carpeta puede cambiar la política de uso compartido y quitar el acceso a usuarios específicos que hayan sido agregados explícitamente a la carpeta.

Acciones para archivos y carpetas

- ***Carpetas del equipo por archivos***

  Los administradores pueden crear carpetas del equipo que automáticamente otorgan a los grupos y a los demás colaboradores el nivel de acceso correcto (ver o editar) al contenido que necesitan.

- ***Controles de acceso detallado y uso compartido***

  Los controles de uso compartido permiten que los administradores gestionen las membresías y los permisos en el primer nivel o en el nivel de subcarpetas, para que las personas y los grupos dentro y fuera de la empresa tengan acceso solo a carpetas específicas.

- ***Gestor de la carpeta del equipo***

  Los administradores pueden ver todas las carpetas del equipo y personalizar las políticas de uso compartido desde un lugar central para ayudar a prevenir la mala distribución de materiales confidenciales.

- ***Carpetas compartidas para documentos de Paper***

  Los administradores pueden crear carpetas compartidas de Paper que automáticamente otorguen a los demás colaboradores el nivel de acceso correcto (comentar o editar) al contenido que necesitan.

- ***Borrado remoto***

  Cuando los empleados abandonan el equipo o extravían un dispositivo, los administradores pueden eliminar de forma remota los datos de Dropbox y las copias locales de los archivos. Los archivos se borrarán de las computadoras y de los dispositivos móviles cuando estos se conecten a Internet y se ejecute la aplicación de Dropbox.

- ***Transferencia de cuenta***

  Después de la desactivación de un usuario (ya sea manualmente o a través de los servicios de directorio), los administradores pueden transferir archivos desde la cuenta de ese usuario a otro usuario del equipo. Es posible usar la característica de transferencia de cuentas cuando se elimina a un usuario o en cualquier momento después de borrar la cuenta de un usuario.

Las siguientes capacidades están disponibles como características de complemento (comunicarse con el equipo de ventas para obtener más información).

- ***Análisis de contenido***

  Con el complemento de Controles avanzados de equipos y contenido, los clientes de Dropbox Business Advanced y Enterprise pueden escanear el contenido existente o nuevo en Dropbox para encontrar y evitar vulnerabilidades de los datos.

- ***Configurar y activar flujos de trabajo personalizados***

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

- ***Configurar alertas***

  Los administradores pueden monitorear los riesgos de seguridad en tiempo real y evitar vulnerabilidades de los datos. Recibe alertas sobre los archivos compartidos de manera externa y la información confidencial escaneada.

Visibilidad del contenido

Alertas y notificaciones de seguridad

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

- Eliminaciones masivas
- Movimientos masivos de datos
- Contenido sensible compartido externamente
- Malware compartido desde fuera de tu equipo
- Malware compartido dentro de tu equipo
- Demasiados intentos fallidos de inicio de sesión
- Iniciar sesión desde un país de alto riesgo
- Detección de ransomware

Dropbox también proporciona la capacidad de configurar umbrales de alerta, ajustar los destinatarios de las notificaciones y activar alertas cuando las carpetas con archivos confidenciales se comparten externamente. Los administradores también pueden marcar las alertas como revisadas, resueltas u omitidas. Además, un widget de panel muestra estadísticas de las alertas del equipo y las tendencias de la semana pasada.

Informe y página de uso compartido externo

Dropbox ofrece visibilidad adicional con el informe y la página de uso compartido externo. Los administradores pueden crear un informe desde la página de estadísticas o desde la página de uso compartido externo. En el informe se enumeran todos los archivos y 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 compartió, configuración de vínculos y muchos más) a través de los archivos y carpetas que se comparten directamente fuera del equipo y los vínculos compartidos.

Controles de uso compartido

La configuración de uso compartido brinda a los administradores de equipo más control sobre el uso compartido y el acceso al contenido de su equipo. Los administradores pueden establecer vencimientos predeterminados en el equipo, restricciones de contraseña o ambos. Estas restricciones reducen el riesgo de pérdida de datos al quitar la responsabilidad de los usuarios de establecer restricciones.

Clasificación de los datos

Los equipos de Dropbox Enterprise pueden etiquetar automáticamente los datos personales y confidenciales para protegerlos mejor contra la exposición. 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 carpetas compartidas y personales de 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 general de procesos, tecnologías y equipos que se unen para administrar y proteger los activos de datos de una organización. Se incluye la capacidad de almacenar, identificar, descubrir y recuperar datos corporativos según sea necesario.

El complemento Gobierno de datos de Dropbox combina un conjunto de características que permitirán a las organizaciones controlar y proteger mejor sus datos, al tiempo que reduce los riesgos y costos asociados con la satisfacción de las necesidades reglamentarias y de cumplimiento. Actualmente, este complemento incluye cuatro características clave para administradores de equipo y administradores de cumplimiento.

- ***Historial de versiones extendido***

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

- ***Retenciones legales***

  Colocar una retención legal sobre un miembro del equipo permite a los administradores de equipos y de cumplimiento ver y exportar todo el contenido que dicho miembro haya creado o modificado. Los miembros afectados por una retención legal no recibirán notificaciones sobre la retención y conservarán sus permisos para crear, editar y eliminar archivos.

- ***Retención de datos***

  La retención de datos permite a los administradores de equipos y de cumplimiento evitar la eliminación accidental de contenido que las regulaciones requieren que se mantenga durante determinada cantidad de tiempo. Esta característica permitirá a los clientes conservar los datos de los últimos 10 años a partir de la fecha de “revisión” más reciente.

- ***Disposición de datos***

  La disposición de los 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 disposición de los datos. Los administradores pueden supervisar la actividad al recibir informes que les avisan sobre las próximas eliminaciones de archivos.

Recuperación y control de versiones

Los clientes de Dropbox Business tienen la capacidad de restaurar archivos borrados y documentos de Paper, así como de recuperar versiones anteriores de archivos y documentos de Paper, lo que asegura la posibilidad de rastrear y recuperar los cambios realizados en datos importantes.

Seguridad de los datos en los dispositivos móviles

- ***Borrar datos***

  Para mejorar la seguridad, el usuario puede habilitar la opción que permite borrar todos los datos de Dropbox en el dispositivo al cabo de 10 intentos fallidos de ingreso del código de acceso.

- ***Almacenamiento interno y archivos guardados***

  De manera predeterminada, los archivos no se almacenan en el almacenamiento interno de los dispositivos móviles. Los clientes móviles Dropbox tienen la capacidad de guardar archivos y carpetas individuales en el dispositivo para la visualización sin conexión. Cuando un dispositivo se desvincula de una cuenta de Dropbox a través de la interfaz móvil o la interfaz web, los archivos y carpetas se borran automáticamente del almacenamiento interno del dispositivo.

- ***Documentos de Paper sin conexión***

  Cuando un dispositivo no está vinculado con Paper, la página de seguridad de la cuenta de Dropbox se encarga de cerrar la sesión activa del usuario y los documentos de Paper sin conexión se borran automáticamente del almacenamiento interno del dispositivo.

Controles de equipo

Debido a que no existen dos organizaciones que sean exactamente iguales, desarrollamos una cantidad de herramientas que permiten a los administradores personalizar Dropbox Business, de acuerdo con las necesidades particulares de sus equipos. Dropbox Business incluye herramientas para usuarios finales que permiten agregar una capa de seguridad a sus cuentas y datos. La autenticación, la recuperación, el inicio de sesión y otras características de seguridad que se detallan a continuación están disponibles a través de las distintas interfaces del usuario de Dropbox.

A continuación, se incluyen distintas características de control y visibilidad disponibles a través de la consola de administración de Dropbox Business.

Permisos detallados de contenido

- ***Roles con niveles de administrador***

  Dropbox ofrece roles de administrador por niveles que brindan una gestión del equipo más efectiva. A los administradores de cuenta se les puede asignar uno de los tres niveles de acceso. No existe un límite en el número de administradores que puede tener un equipo, y a cualquier miembro de equipo se le puede asignar un rol de administrador.

- ***Administrador de equipo***

  Este puede establecer permisos de seguridad y uso compartido en todo el equipo, crear administradores y administrar miembros. El administrador del equipo tiene todos los permisos de administrador disponibles. Únicamente los administradores del equipo pueden asignar o cambiar los roles de administrador. Debe haber siempre al menos un administrador del equipo por cuenta de Dropbox Business.

- ***Administrador de usuarios***

  Se puede ocupar de la mayoría de las tareas de administración del equipo, como agregar y quitar miembros del equipo, administrar grupos y consultar la fuente de actividades del equipo.

- ***Administrador de soporte***

  Puede abordar solicitudes de servicio comunes de miembros del equipo, como restaurar archivos eliminados o asistir a los miembros del equipo bloqueados a partir de la verificación de dos pasos. Los administradores de soporte también pueden restablecer contraseñas no administrativas y exportar un registro de actividades para un miembro específico del equipo.

- ***Administrador de la 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 de seguridad.

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

  Puede administrar páginas de gobierno de datos (retenciones legales, retención de datos y disposición de datos) y también acceder al administrador de contenido.

- ***Grupos***

  Los equipos pueden crear y administrar listas de miembros dentro de Dropbox, y fácilmente darles acceso a carpetas específicas. Dropbox también puede sincronizar grupos de Active Directory mediante el conector de Active Directory.

- ***Grupos administrados por la empresa***

  Solo los administradores pueden crear, eliminar y administrar la membresía para este tipo de grupo. Los usuarios no pueden solicitar unirse o abandonar un grupo administrado por la empresa.

- ***Grupos administrados por los usuarios***

  Los administradores pueden elegir si los usuarios pueden crear y administrar sus propios grupos. Para asumir el control, los administradores también pueden cambiar de un grupo administrado por el usuario a un grupo administrado por la empresa en cualquier momento.

- ***Restricción de múltiples cuentas en computadoras***

  Los administradores pueden bloquear que miembros del equipo vinculen una segunda cuenta de Dropbox a computadoras que están vinculadas a su cuenta de Dropbox de trabajo.

- ***Estado de usuario suspendido***

  Los administradores tienen la posibilidad de inhabilitar el acceso de un usuario a su cuenta mientras conservan sus datos y relaciones de uso compartido para mantener protegida la información de la compañía. Los administradores pueden reactivar o eliminar más adelante la cuenta.

- ***Inicio de sesión como usuario***

  Los administradores del equipo pueden iniciar sesión como miembros de sus equipos. Esto proporciona a los administradores acceso directo a los archivos, carpetas y documentos de Paper en cuentas de miembro del equipo de modo que pueden realizar cambios, compartir en nombre de los miembros del equipo o realizar auditorías de eventos de archivos. Los eventos "Iniciar sesión como usuario" se registran en el registro de actividad del equipo, y los administradores pueden determinar si los miembros reciben notificación de estos eventos.

- ***Permisos para compartir***

  Los administradores de equipos tienen control completo de las capacidades de uso compartido del equipo mediante Dropbox, incluso en los siguientes casos:

  - Si los miembros del equipo pueden compartir archivos y carpetas con personas fuera del equipo.
  - Si los miembros del equipo pueden editar carpetas de propiedad de personas fuera del equipo.
  - Si los vínculos compartidos creados por miembros del equipo funcionarán para las personas fuera del equipo.
  - Si los miembros del equipo pueden crear solicitudes de archivo y recolectar archivos de miembros del equipo o personas fuera del equipo.
  - Si las personas pueden ver y realizar comentarios en archivos de propiedad del equipo.
  - Si los miembros del equipo pueden compartir documentos y carpetas de Paper con personas fuera del equipo.
  - Si se otorgan permisos para eliminar de manera permanente.

El administrador del equipo de una cuenta Dropbox Business puede limitar la capacidad de eliminar de manera permanente archivos y documentos de Paper a administradores del equipo solamente.

Incorporación y aprovisionamiento de usuarios

Aprovisionamiento de usuarios y métodos de administración de identidad

- ***Invitación por correo electrónico***

  Una herramienta en la Consola de administración de Dropbox Business 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 existente de Active Directory mediante nuestro conector de Active Directory o a través de un proveedor de identidad independiente. Una vez integrado, Active Directory puede usarse para administrar la membresía.

- ***Inicio de sesión único (SSO)***

Dropbox Business puede configurarse para permitir que los miembros del equipo accedan a sus cuentas al registrarse en un proveedor central de identidad. Gracias a la implementación de nuestro SSO, que usa el lenguaje de marcado de aserciones de seguridad 2.0 (SAML 2.0), el proceso de aprovisionamiento es más fácil y seguro, puesto que se asigna un proveedor de identidad de confianza como responsable de la autenticación y se concede a los miembros del equipo acceso a Dropbox sin que deban administrar una contraseña adicional. Dropbox también se ha asociado con líderes proveedores de administración de identidades para automatizar la activación y desactivación de usuarios. Consulta la sección de integraciones de API de Dropbox Business a continuación.

- ***API***

  Los clientes pueden usar la API de Dropbox Business para crear soluciones de administración de aprovisionamiento de usuarios e identidades personalidades. Consulta la sección de integraciones de API de Dropbox Business a continuación.

Verificación de dos pasos

Esta característica de seguridad, ampliamente recomendada, agrega una capa adicional de protección a la cuenta de Dropbox del usuario. Una vez que la verificación de dos pasos está habilitada, Dropbox solicita un código de seguridad de seis dígitos, además de una contraseña, al iniciar sesión o al vincular una nueva computadora, un nuevo teléfono o una nueva tablet.

- Los administradores pueden decidir si desean que la verificación de dos pasos sea obligatoria para todos los miembros del equipo o solo para algunos.
- Los administradores de cuenta pueden controlar qué miembros del equipo tienen habilitada la verificación de dos pasos.
- Los códigos de autenticación de dos pasos de Dropbox pueden recibirse a través de mensaje de texto o aplicaciones que cumplen con el criterio de algoritmo de la contraseña única basada en el tiempo (TOTP).
- En el caso de que un usuario no pueda recibir códigos de seguridad a través de estos métodos, puede optar por usar un código de copia de seguridad de emergencia de 16 dígitos para usar una vez. Como opción, puede usar un número de teléfono secundario para recibir un código de copia de seguridad a través de mensaje de texto.
- Dropbox también admite el criterio estándar abierto Segundo factor universal (U2F) FIDO, que habilita a los usuarios autenticar con una clave de seguridad USB configurada en lugar de un código de seis dígitos

Instalador empresarial

Los administradores que necesiten realizar el aprovisionamiento a escala pueden usar nuestro instalador empresarial para Windows a fin de instalar el cliente de escritorio de Dropbox de forma silenciosa y remota mediante soluciones de software administrado y otros mecanismos de implementación.

Dispositivos gestionados y acceso

- ***Administración de movilidad empresarial (EMM)***

  Dropbox se integra con un proveedor de EMM externo para otorgar mayor control a los administradores de equipos de Dropbox Business que cuenten con el plan Enterprise sobre la forma en que los miembros del equipo utilizan Dropbox en sus dispositivos móviles. Los administradores pueden restringir el uso de la aplicación móvil para las cuentas Dropbox Enterprise a solo dispositivos administrados (ya sean proporcionados por la empresa o personales), obtener visibilidad en el uso de la aplicación (incluidos el almacenamiento disponible y las ubicaciones de acceso) y borrado remoto de un dispositivo perdido o robado. Ten en cuenta que la aplicación para dispositivos móviles de Paper no se puede manejar por medio de EMM.

- ***Aprobaciones de dispositivos***

  Dropbox habilita a los administradores de equipos de Dropbox Education y Dropbox Business que cuenten con los planes Advanced y Enterprise a establecer límites en la cantidad de dispositivos que un usuario puede sincronizar con Dropbox y elegir si el usuario o el administrador gestionan las aprobaciones. Los administradores también pueden crear una lista de excepciones de usuarios que no estén limitados a una cierta cantidad de dispositivos. Ten en cuenta que la aplicación para dispositivos móviles de Paper no está incluida en las aprobaciones de dispositivos.

- ***Verificación de dos pasos obligatoria***

  Los administradores pueden elegir si desean que la verificación de dos pasos sea obligatoria para todos los miembros del equipo o solo para algunos. También se pueden imponer otros requisitos de autenticación multifactorial mediante la implementación del inicio de sesión único (SSO) del equipo.

- ***Control de contraseña***

  Los administradores de los equipos de Dropbox Education, Advanced y Enterprise pueden requerir que los miembros establezcan y mantengan contraseñas seguras y complejas para sus cuentas. Cuando se habilita esta característica, se finalizará la sesión de los miembros del equipo en cualquier sitio web. Luego, se les solicitará crear contraseñas nuevas cuando inicien sesión. Una herramienta incorporada analiza la seguridad de las contraseñas al compararlas con las bases de datos de palabras, nombres, patrones y números más usados. Si un usuario introduce una contraseña común, se le recomendará crear una más única y difícil de adivinar. Los administradores también pueden restablecer contraseñas para el equipo completo o para un usuario nada más.

- ***Administración de dominios***

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

  - **Verificación de dominio**
    Las compañías pueden reclamar la propiedad de sus dominios y desbloquear las otras herramientas de administración de dominio.

  - **Imposición de invitaciones**
    Los administradores pueden requerir que los usuarios de Dropbox individuales que hayan sido invitados al equipo de Dropbox de la compañía migren al equipo o cambien la dirección de correo electrónico en su cuenta personal.

  - **Estadísticas del dominio**
    Los administradores puede ver información clave como la cantidad de cuentas individuales Dropbox que utilizan direcciones de correo electrónico de la empresa.

  - **Captura de cuentas**
    Los administradores pueden obligar a todos los usuarios de Dropbox que utilizan la dirección de correo electrónico empresarial a unirse al equipo de la empresa o cambiar dicha dirección en su cuenta personal.

- ***Control de sesión web***

  Los administradores pueden controlar durante cuánto tiempo los miembros del equipo pueden permanecer con una sesión activa en dropbox.com. Los administradores pueden limitar la duración de todas las sesiones web y las sesiones que están inactivas. Se cerrará automáticamente la sesión en todos aquellos casos que alcancen estos límites. Los administradores también pueden rastrear y dar por finalizadas las sesiones web de usuarios individuales.

- ***Acceso a las aplicaciones***

  Los administradores tienen la capacidad de ver y denegar el acceso de las aplicaciones de terceros a las cuentas de usuarios.

- ***Desvinculación de dispositivos***

  El administrador puede desvincular las computadoras y los dispositivos móviles conectados a las cuentas de los usuarios a través de la Consola de administración, o puede hacerlo el usuario mediante la configuración

de seguridad de la cuenta personal. En las computadoras, la desvinculación borra los datos de autenticación y brinda la opción de eliminar las copias locales de archivos la próxima vez que la computadora se conecte a Internet (consultar **Borrado remoto).** En los dispositivos móviles, la desvinculación quita los archivos marcados como favoritos, los datos en caché y la información de inicio de sesión. La desvinculación también quita de la aplicación móvil de Paper los documentos de Paper sin conexión. Si se habilita la verificación de dos pasos, los usuarios deben volver a autenticar cualquier dispositivo al volver a vincularse. Además, la configuración de las cuentas de los usuarios proporciona la opción de enviar automáticamente un correo electrónico de notificación cuando se vincula cualquier dispositivo.

- ***Control de la red***

  Los administradores de los equipos de Dropbox Business que cuenten con el plan Enterprise pueden limitar el uso de Dropbox en la red de la empresa únicamente a la cuenta del equipo Enterprise. Esta característica se integra con el proveedor de seguridad de la red de la empresa para bloquear cualquier tráfico que exista fuera de la cuenta depurada en computadoras. Ten en cuenta que Paper no se administra por medio del control de la red.

Seguridad para dispositivos móviles

- ***Escaneado de huellas dactilares***

  Los usuarios pueden habilitar Touch ID o Face ID en dispositivos iOS y el desbloqueo por huellas dactilares (cuando sea compatible) en dispositivos Android como método de desbloquear la aplicación móvil de Dropbox.

Visibilidad de acceso

- ***Verificación de identidad de soporte técnico***

  Antes de que el equipo de soporte de Dropbox proporcione cualquier tipo de información sobre resolución de problemas o sobre la cuenta, el administrador de la cuenta debe suministrar un código de seguridad de un solo uso, generado aleatoriamente, para validar su identidad. Este PIN solamente está disponible a través de la Consola de administración.

Actividad de la cuenta del usuario

Cada usuario puede ver las siguientes páginas en la configuración de su cuenta para obtener información actualizada acerca de la actividad en ella.

- ***Página de uso compartido***

  Esta página muestra las carpetas compartidas disponibles actualmente en la cuenta Dropbox del usuario, además de las carpetas compartidas que el usuario puede agregar. Un usuario puede dejar de compartir carpetas y archivos, y establecer permisos de uso compartido.

- ***Página de archivos***

  Esta página muestra los archivos que se han compartido con el usuario y la fecha en la que se compartió cada archivo. El usuario tiene la opción de restringir su acceso a estos archivos. Para ver los documentos de Paper que otros han compartido con el usuario, el usuario puede navegar a la página "Compartidos conmigo" en la interfaz de navegación de documentos de Paper.

- ***Página de vínculos***

  Esta página muestra todos los vínculos compartidos activos que el usuario ha creado y la fecha de creación de cada uno. También muestra todos los vínculos compartidos con el usuario a través de otros. El usuario puede inhabilitar vínculos o cambiar permisos.

- ***Notificaciones por correo electrónico***

  Un usuario puede optar por recibir una notificación por correo electrónico inmediatamente cuando un nuevo dispositivo o una aplicación se vincula a su cuenta de Dropbox.

Permisos de la cuenta del usuario

- ***Dispositivos vinculados***

  En la **sección Dispositivos** en la configuración de seguridad de la cuenta de un usuario, se muestran todas las computadoras y todos los dispositivos móviles vinculados a la cuenta del usuario. Para cada computadora, se muestra la dirección IP, el país y la hora aproximada de la actividad más reciente. Un usuario puede desvincular cualquier dispositivo, con la opción de eliminar los archivos en las computadoras vinculadas la próxima vez que se conecte a Internet.

- ***Sesiones web activas***

  En la **sección Sesiones,** se muestran todos los exploradores web vinculados actualmente a la cuenta de un usuario. Para cada uno, se muestra la dirección IP, el país y la hora de conexión de la sesión más reciente, así como la hora aproximada de la actividad más reciente. El usuario puede cancelar una sesión de forma remota en la configuración de seguridad de la cuenta del usuario.

- ***Aplicaciones vinculadas***

  La sección **Aplicaciones vinculadas** ofrece una lista de todas las aplicaciones de terceros que tienen acceso a la cuenta del usuario y el tipo de acceso que tiene cada una de ellas. El usuario puede denegar los permisos de cualquier aplicación para acceder al Dropbox del usuario.

Fuente de actividad

Las acciones sobre archivos son registradas por Dropbox Business en la fuente de actividad del equipo, a la cual se puede acceder desde la Consola de administración. La fuente de actividad ofrece opciones de filtrado flexibles que habilitan a los administradores a realizar investigaciones dirigidas de la actividad de la cuenta, los archivos o los documentos de Paper. Esto incluye, por ejemplo, ver el historial completo de un archivo o un documento de Paper y cómo los usuarios han interactuado con este, o ver toda la actividad para el equipo en un período de tiempo específico. La fuente de actividad se puede exportar como un informe descargable en formato CSV y además integrarse directamente a un producto SIEM (administración de eventos e información de seguridad) u otra herramienta de análisis a través de soluciones de terceros. Los siguientes eventos de contenido se registran en la fuente de actividad:

- ***Uso compartido de archivos, carpetas y vínculos***

  Si corresponde, los informes especifican si las acciones involucraron a personas no pertenecientes al equipo.

  Archivos compartidos

  - Se agregó o quitó a un miembro del equipo o un miembro ajeno al equipo.
  - Se cambiaron los permisos de un miembro del equipo o miembro ajeno al equipo.
  - Se agregó o eliminó un grupo.
  - Se agregó un archivo compartido a la cuenta Dropbox del usuario.
  - Se mostró el contenido de un archivo que se compartió a través de una invitación de archivo o carpeta.
  - Se copió el contenido compartido en la cuenta Dropbox del usuario.
  - Se descargó contenido compartido.

- Se comentó en un archivo.
- Se resolvió o no un comentario.
- Se borró un comentario.
- Se realizó la suscripción o se anuló la suscripción de notificaciones de comentarios.
- Se reclamó una invitación a un archivo de propiedad del equipo.
- Se solicitó el acceso a un archivo de propiedad del equipo.
- Se canceló el uso compartido de un archivo.

Se compartieron carpetas

- Se creó una nueva carpeta compartida.
- Se agregó o quitó a un miembro del equipo, miembro ajeno al equipo, o grupo.
- Se agregó una carpeta compartida en la cuenta Dropbox del usuario o el usuario quitó su propio acceso a una carpeta compartida.
- Se agregó una carpeta compartida desde un vínculo.
- Se cambiaron los permisos de un miembro del equipo o miembro ajeno al equipo.
- Se transfirió la propiedad de la carpeta a otro usuario.
- Se dejó de compartir una carpeta.
- Se reclamó la membresía de una carpeta compartida.
- Se solicitó el acceso a una carpeta compartida.
- Se agregó el usuario solicitante a una carpeta compartida.
- Se activó o desactivó la opción de que los miembros ajenos al equipo sean agregados a una carpeta.
- Se permitió que un miembro del equipo agregara personas a una carpeta o solo el propietario.
- Se cambió el acceso de grupo a una carpeta compartida.

Vínculos compartidos

- Se creó o quitó un vínculo.
- Se mostró el contenido de un vínculo a cualquier persona que tuviera el vínculo o solo a los miembros del equipo.
- Se protegió mediante contraseña el contenido de un vínculo.
- Se estableció o quitó la fecha de caducidad de un vínculo.
- Se vio un vínculo.
- Se descargó el contenido de un vínculo.
- Se copió el contenido de un vínculo en la cuenta Dropbox del usuario.
- Se creó un vínculo a un archivo a través de una aplicación API.
- Se compartió un vínculo con un miembro del equipo, miembro no perteneciente al equipo o grupo.
- Se activó o desactivó la opción de que los miembros ajenos al equipo vean vínculos a archivos en una carpeta compartida.
- Se compartió un álbum.

Solicitudes de archivos

- Se creó, cambió, eliminó o cerró una solicitud de archivo.
- Se agregaron usuarios a una solicitud de archivo.
- Se agregó o quitó una fecha límite de solicitud de archivos.
- Se cambió una carpeta de solicitud de archivos.
- Se recibieron archivos a través de una solicitud de archivos.
- Archivos recibidos por correo electrónico en Dropbox.

Eventos individuales de archivos y carpetas.

- Se agregó un archivo a Dropbox.
- Se creó una carpeta.
- Se vio un archivo.
- Se editó un archivo.
- Se descargó un archivo.
- Se copió un archivo o carpeta.
- Se movió un archivo o carpeta.
- Se cambió el nombre de un archivo o de una carpeta.
- Se revirtió un archivo a la versión anterior.
- Se revirtieron los cambios en los archivos.
- Se restauró un archivo eliminado.
- Se eliminó un archivo o carpeta.
- Se eliminó de manera permanente un archivo o carpeta.

Inicios de sesión exitosos y fallidos.

- Intento de inicio de sesión exitoso o fallido.
- Intento de inicio de sesión fallido o error a través de inicio de sesión único (SSO).
- Error en intento de inicio de sesión o error por EMM.
- Se cerró la sesión.
- Cambio de dirección IP para sesión web.

Contraseñas

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

- Se cambió o restableció la contraseña.
- Se habilitó, restableció o deshabilitó la verificación de dos pasos.

- Se configuró o cambió la verificación de dos pasos para usar SMS o una aplicación para dispositivos móviles.
- Se agregó, editó o quitó un teléfono de copia de seguridad para la verificación de dos pasos.
- Se agregó o quitó una clave de seguridad para la verificación de dos pasos.

Membresía

Incorporaciones al equipo y eliminaciones de miembros.

- Se invitó a un miembro del equipo.
- Se unió al equipo.
- Se eliminó un miembro del equipo.
- Se suspendió o anuló la suspensión de un miembro del equipo.
- Se recuperó un miembro del equipo eliminado.
- Se solicitó la incorporación al equipo en función del dominio de la cuenta.
- Se aprobó o rechazó una solicitud de incorporación al equipo en función del dominio de la cuenta.
- Se enviaron las invitaciones de dominio a las cuentas de dominio existentes.
- El usuario se unió al equipo en respuesta a la captura de cuentas.
- El usuario abandonó el dominio en respuesta a la captura de cuentas.
- Se activó o desactivó la opción de que los miembros del equipo sugieran nuevos miembros del equipo.
- Se sugirió un nuevo miembro del equipo.

Aplicaciones

Vinculación de aplicaciones de terceros a las cuentas de Dropbox.

- Se autorizó o eliminó una aplicación.
- Se autorizó o quitó una aplicación del equipo.

Dispositivos

Vinculación de computadoras o dispositivos móviles a las cuentas de Dropbox

- Se vinculó o desvinculó un dispositivo.
- Se usó el borrado remoto y se eliminaron todos los archivos correctamente o no se pudieron eliminar algunos archivos.
- Cambio de dirección IP para computadora de escritorio o dispositivo móvil.

Acciones de administrador

Cambios de configuración en la consola de administración, por ejemplo, cambios en los permisos de las carpetas compartidas.

- ***Autenticación e inicio de sesión único (SSO)***
  - Se restableció la contraseña de un miembro del equipo.

- Se restablecieron las contraseñas de todos los miembros del equipo.
- Se activó o desactivó la opción de que los miembros del equipo inhabiliten la verificación de dos pasos.
- Inicio de sesión único habilitado o desactivado.
- Se exigió el inicio de sesión a través del SSO.
- Se cambió o quitó la URL del SSO.
- Se actualizó el certificado SSO.
- Se cambió el modo de identidad SSO.

- ***Membresía***
  - Se activó o desactivó la opción de que los usuarios soliciten incorporarse al equipo en función del dominio de cuentas.
  - Se establecieron solicitudes de membresía del equipo para su aprobación automática o para requerir la aprobación de administración manual.

- ***Administración de cuentas del miembro***
  - Cambiar el nombre de un miembro del equipo.
  - Se cambió la dirección de correo electrónico de un miembro del equipo.
  - Se otorgó o quitó el estado de administrador, o se cambió el rol administrativo.
  - Se inició o cerró la sesión como miembro del equipo.
  - Se transfirió o eliminó el contenido de la cuenta de un miembro quitado.
  - Se eliminó de manera permanente el contenido de la cuenta de un miembro quitado.

- ***Configuración de uso compartido global***
  - Se activó o desactivó la opción de que los miembros del equipo agreguen carpetas compartidas de propiedad de miembros ajenos al equipo.
  - Se activó o desactivó la opción de que los miembros del equipo compartan carpetas con miembros ajenos al equipo.
  - Se activaron advertencias que se muestran a usuarios antes de compartir carpetas con miembros ajenos al equipo.
  - Se activó o desactivó la opción de que los miembros ajenos al equipo vean vínculos compartidos.
  - Se establecieron vínculos compartidos para que sean solo del equipo de manera predeterminada.
  - Se activó o desactivó la opción de que las personas hagan comentarios en archivos.
  - Se activó o desactivó la opción de que los miembros del equipo creen solicitudes de archivos.
  - Se agregó, cambió o quitó un logotipo para páginas de vínculos compartidos.
  - Se activó o desactivó la opción de que los miembros del equipo compartan documentos o carpetas de Paper con miembros ajenos al equipo.

- ***Administración de la carpeta del equipo para archivos***
  - Se creó una carpeta del equipo.
  - Se cambió el nombre de una carpeta del equipo.
  - Se archivó o desarchivó una carpeta del equipo.

    - Se eliminó la carpeta del equipo de forma permanente.
    - Se bajó de categoría una carpeta del equipo a una carpeta compartida.

- ***Gestión de dominios***
    - Se intentó verificar o se verificó correctamente un dominio, o se quitó un dominio.
    - Soporte de Dropbox verificó o quitó un dominio.
    - Se habilitó o inhabilitó el envío de invitaciones de dominio.
    - Se activó o desactivó "Invitar automáticamente a nuevos usuarios".
    - Se cambió el modo de captura de cuentas.
    - Se proporcionó Soporte de Dropbox o se revocó la captura de cuentas.

- ***Administración de movilidad empresarial (EMM)***
    - EMM habilitada para modo de prueba (opcional) o modo de implementación (obligatorio).
    - Se actualizó el token de EMM.
    - Miembros del equipo agregados o quitados de la lista de usuarios excluidos de EMM.
    - Se desactivó el EMM.
    - Se creó un informe de la lista de excepciones de EMM.
    - Se creó un informe de uso de la aplicación para dispositivos móviles de EMM.

- ***Cambios en otra configuración del equipo***
    - Se fusionaron equipos.
    - Se subió de categoría el equipo a Dropbox Business o se bajó de categoría a un equipo gratuito.
    - Se cambió el nombre de un miembro del equipo.
    - Se creó un informe de actividad del equipo.
    - Se activó o desactivó la opción de que los miembros del equipo tengan más de una cuenta vinculada a una computadora.
    - Se permitió a todos los miembros del equipo o solo administradores para crear grupos.
    - Se activó o desactivó la opción de que miembros del equipo eliminen permanente los archivos.
    - Se inició o finalizó la sesión de soporte de Dropbox para un revendedor.

Grupos

Información sobre la creación, la eliminación y los miembros de grupos.

- Se creó, cambió el nombre, movió o eliminó un grupo.
- Se agregó o eliminó un miembro.
- Se cambió el tipo de acceso de un miembro del grupo.
- Se cambió el grupo a administrado por el equipo o administrado por el administrador.
- Se cambió la ID externa de un grupo.

Registro de actividad de Paper

Los administradores pueden seleccionar un tipo de actividad de Paper en la fuente de actividad o descargar un informe de actividad completo. Los eventos de Paper se registran para lo siguiente:

- Paper habilitado o deshabilitado.
- Creación, edición, exportación, almacenamiento, borrado permanente y restauración de documentos de Paper.
- Comentarios y resolución de comentarios en documentos de Paper.
- Documentos de Paper compartidos o no compartidos con miembros del equipo y miembros ajenos al equipo.
- Solicitudes de acceso a los documentos de Paper por parte de miembros del equipo y miembros ajenos al equipo.
- Menciones a los documentos de Paper para miembros del equipo y miembros ajenos al equipo.
- Documento de Paper visto por miembros del equipo y miembros ajenos al equipo.
- Se siguió un documento de Paper.
- Cambios en los permisos de miembros (editar, comentar o solo lectura) de documentos de Paper.
- Cambios en la política de uso compartido externo de documentos de Paper.
- Creación, almacenamiento y borrado permanente de carpetas de Paper.
- Se agregó o quitó un Documento de Paper de una carpeta.
- Se cambió el nombre de la carpeta de Paper.
- Transferencias de documentos y carpetas de Paper.

Dropbox Passwords

Dropbox Passwords es una forma segura y simple de almacenar, sincronizar y autocompletar nombres de usuario, contraseñas y tarjetas de crédito/débito en todos los dispositivos, protegiendo tus credenciales en línea. Dropbox Passwords protege nombres de usuario, contraseñas y tarjetas de crédito/débito de cuentas en línea con un cifrado de cero conocimiento, en la nube y en tus dispositivos. Nuestros productos están diseñados para el uso diario y seguros por diseño.

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 nunca tiene acceso a ellos.** Estas claves son largas, aleatorias y se generan en tu dispositivo. Nunca dejan tu dispositivo excepto cuando decides emparejar o inscribir un nuevo dispositivo. Esta transferencia utiliza criptografía de clave pública tanto para firmar criptográficamente como para proteger las claves durante la transferencia para que puedas estar seguro de que nadie más puede descifrarlas mientras también verifica que son auténticas. Esta propiedad se llama frecuentemente cifrado de conocimiento cero porque los datos cifrados son inútiles para cualquiera que no tenga las claves, incluido Dropbox. Esto significa **que solo tú puedes mirar tu información** y en el improbable caso de que Dropbox fuera pirateado, tu información seguiría estando segura. Los datos cifrados se segregan de las carpetas visibles de Dropbox y no se pueden atravesar con clientes de Dropbox o API.

Detalles de cifrado

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

Cada operación de cifrado genera un nonce aleatorio de 192 bits, que se almacena con la carga útil cifrada para su posterior descifrado. A diferencia de AES-GCM, XChacha20-Poly1305 admite nonces aleatorios. Al descifrar, el nonce de 192 bits se lee desde la carga útil y se usa para descifrar la carga útil cifrada. Cualquier cifrado posterior genera un nonce aleatorio de 192 bits independiente del nonce anterior. Dropbox Passwords genera números aleatorios usando libsodium, que por defecto 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, permanece en el almacenamiento más seguro al que tenemos acceso en esos dispositivos. Por ejemplo, en iPhones almacenamos la clave de cifrado en el llavero de iOS.

Utilizamos 128 bits de entropía como nuestra fuente porque ofrece suficiente seguridad al tiempo que solo requiere 12 palabras de recuperación utilizando el estándar BIP-39 para la copia de seguridad. BIP-39 proporciona una forma amigable para los humanos de representar grandes claves aleatorias al transformar esas claves en una lista de 12 palabras. Cualquier clave de 128 bits tiene una lista correspondiente de palabras y cada lista de 12 palabras identifica de manera única 128 bits. La única advertencia es que las 12 palabras corresponden realmente a 132 bits por lo que los cuatro bits adicionales se utilizan como suma de comprobación para identificar errores. Las palabras de recuperación proporcionan una forma de recuperar su clave de cifrado en caso de pérdida o robo de tu dispositivo. Recomendamos imprimirlas y guardarlas en un lugar seguro. También puedes considerar dárselas a un amigo o familiar de confianza o almacenarlas en una unidad de disco.

Inscripción de dispositivos

Cuando un usuario ingresa a Dropbox Passwords en un nuevo dispositivo, ese dispositivo debe completar un procedimiento de inscripción segura para acceder a los datos de contraseñas del usuario. Este procedimiento ayuda a garantizar que la clave secreta de un usuario y los datos de 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 ocurre de la siguiente manera.

Un nuevo dispositivo de inscripción genera aleatoriamente un par de claves de dispositivo pública/privada de 256 bits y carga la clave pública en el servidor de Dropbox. Entonces, se produce cualquiera de los escenarios **A**, **B** o **C.**

A: si el usuario no ha inscrito previamente un dispositivo, entonces el dispositivo de inscripción genera aleatoriamente una clave de usuario secreta de 128 bits. Tanto la clave de usuario como el par de claves de dispositivo se almacenan en una ubicación segura específica del sistema OS-como se describe en la siguiente sección de Almacenamiento de claves. El dispositivo inicializa los datos de contraseñas del usuario, los cifra y carga la carga útil cifrada en el servidor de Dropbox.

B: si el usuario tiene dispositivos inscritos previamente, se envía una solicitud de aprobación de inscripción a cada uno de esos dispositivos. La clave pública del dispositivo de inscripción se adjunta a la solicitud. El usuario deberá entonces aprobar la solicitud en uno de sus dispositivos inscritos. Si se aprueba, el dispositivo inscrito cifra la clave de usuario usando su clave privada y la clave pública del dispositivo de inscripción a través de X25519 ECDH con XSalsa20-Poly1305. El dispositivo inscrito carga la clave de usuario cifrada en el servidor de Dropbox para enviarla al dispositivo que se inscribe. El dispositivo de inscripción descarga y descifra la clave de usuario utilizando su clave privada y la clave pública del dispositivo inscrito. Luego, el dispositivo de inscripción descarga los datos de carga útil de Passwords cifrados y los descifra con la clave de usuario.

C: si el usuario ha inscrito previamente un dispositivo, pero ya no puede acceder a ellos, puede ingresar sus 12 palabras de recuperación para reconstruir localmente la clave de usuario. Luego, el dispositivo de inscripción descarga los datos de carga útil de Passwords cifrados y los descifra con la clave de usuario.

Almacenamiento de claves

Extensiones del explorador

En los navegadores web, la clave de usuario se almacena en el área de almacenamiento local de la extensión del explorador. Los valores de almacenamiento local de la extensión del explorador solo son accesibles desde la extensión. Ningún código que se ejecute en sitios web que el usuario visita se puede leer desde el área de almacenamiento local de la extensión del explorador. Además, las extensiones del explorador no permiten la ejecución de ningún código que no esté incluido en el paquete de extensión firmado, eliminando 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. Ejemplos de tales amenazas incluyen un atacante con acceso físico al dispositivo o un atacante que ejecuta malware malicioso en el dispositivo. Para protegerse contra estos escenarios, el usuario puede configurar una frase de contraseña del dispositivo local.

Cuando se configura una frase de contraseña, la clave de usuario se cifra en reposo en el almacenamiento local de la extensión del explorador. La clave de cifrado se deriva de la frase de contraseña a través del hash de contraseña Argon2, y el método de cifrado utilizado es XChaCha20-Poly1305. Cada vez que se reinicia la extensión del explorador, el usuario debe proporcionar su contraseña para descifrar la clave de usuario y desbloquear sus datos. En consecuencia, un atacante sin la frase de contraseña no puede 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 iOS, que es un archivo de base de datos cifrado en el disco. Este archivo se cifra con una clave secreta que se almacena en el módulo de hardware Secure Enclave, utilizando AES256-GCM como método de cifrado. Solo la aplicación de Dropbox Passwords para iOS firmada puede acceder a los elementos que tiene almacenados en el llavero. Esto evita que otro código que se ejecuta 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 se cifra con una clave maestra que se almacena en el hardware seguro Android Keystore, utilizando AES256-GCM como método de cifrado. Solo la aplicación de Dropbox Passwords para Android firmada puede acceder a la clave maestra utilizada 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 aplicaciones móviles, se puede reutilizar el gesto de autenticación del SO local (es decir, un código de acceso con autenticación biométrica complementaria). Para extensiones de explorador, se puede configurar una frase de contraseña opcional. Estos mecanismos proporcionan una capa adicional de seguridad de la aplicación cuando el OS del dispositivo del usuario está desbloqueado. Esto permite al usuario asegurar sus datos de Contraseñas cuando otro usuario puede estar accediendo a su dispositivo, como un familiar o compañero de trabajo.

Sugerencia de solidez de contraseña

Dropbox construyó la herramienta zxcvbn de código abierto que es utilizada por varios administradores de contraseñas para estimar la solidez de la contraseña. La herramienta compara contraseñas con una base de datos de 30 mil contraseñas comunes, nombres y apellidos comunes según datos del censo de Estados Unidos, palabras populares en inglés de Wikipedia y televisión y películas estadounidenses, y otros patrones comunes como fechas, repeticiones (aaa), secuencias (abcd), patrones de teclado (qwertyuiop) y Leet (1337) Speak. Si la contraseña que un usuario intenta ingresar es común, la herramienta le solicita ingresar algo más único y difícil de adivinar. El uso de la configuración **Muy fuerte** ayuda a garantizar el más alto nivel de seguridad de la cuenta para los usuarios.

Seguridad, privacidad y transparencia de los datos

Diariamente, personas y organizaciones confían a Dropbox sus archivos de trabajo más importantes. Por esta razón, es nuestra responsabilidad proteger esa información y conservar su privacidad.

Política de privacidad

Nuestra política de privacidad está disponible en dropbox.com/privacy. La Política de privacidad, el Acuerdo de negocios, las Condiciones del servicio y la Política de uso aceptable de Dropbox estipulan los siguientes términos:

- Qué datos recopilamos y por qué.
- Con quiénes podemos compartir la información.
- Cómo protegemos los datos y durante cuánto tiempo los conservamos.
- Dónde conservamos tus datos y cómo los transferimos.
- Qué sucede si cambia la política o si tienes preguntas.

Transparencia

Dropbox se compromete a procesar apropiadamente las solicitudes de aplicación de la ley respecto de la información del usuario, así como la cantidad y los tipos de solicitudes. Verificamos estrictamente todas las solicitudes de datos para asegurarnos de que cumplan con la ley y nos comprometemos a notificar a los usuarios cuando sus cuentas se incluyan en solicitudes de entidades de aplicación de la ley, a menos que la ley lo prohíba.

Estos esfuerzos destacan nuestro compromiso por proteger la privacidad de nuestros usuarios y sus datos. A este fin, mantenemos un informe de transparencia y establecimos un conjunto de principios para solicitudes del gobierno. Los siguientes principios rigen nuestras acciones al recibir, analizar y responder a las solicitudes del gobierno relacionadas con los datos de nuestros usuarios:

- ***Ser transparentes***

  Creemos que los servicios en línea deberían tener permitido publicar el número y los tipos de solicitudes gubernamentales recibidas, así como notificar a los individuos cuando se solicita información sobre ellos. Este tipo de transparencia fortalece a los usuarios, ya que los ayuda a entender mejor las instancias y patrones de abuso gubernamentales. Continuaremos publicando información detallada sobre estas solicitudes y abogaremos por el derecho a proveer más información relevante como esta.

- ***Lucha contra las solicitudes extralimitadas***

  Las solicitudes de datos por parte del Gobierno deberían limitarse a individuos específicos e investigaciones legítimas. Abogaremos en contra de las solicitudes extralimitadas y generalizadas.

- ***Proteger a todos los usuarios***

  Las leyes que otorgan a los individuos diferentes tipos de protección con base en el lugar donde viven o su ciudadanía son obsoletas y no reflejan la naturaleza global de los servicios en línea. Continuaremos abogando por la reforma de dichas leyes.

- ***Prestar servicios de confianza***

  Los gobiernos nunca deben instalar software de puerta trasera en los servicios en línea ni poner en riesgo la infraestructura para obtener datos de usuario. Continuaremos trabajando para proteger nuestros sistemas y modificar las leyes a fin de dejar en claro que este tipo de actividad es ilegal.

Nuestros informes de transparencia pueden verse en dropbox.com/transparency.

Certificaciones de privacidad, atestaciones y cumplimiento normativo

Todos los días, personas y organizaciones confían sus archivos de trabajo más importantes a Dropbox. Por esta razón, es nuestra responsabilidad proteger esos archivos y mantener su privacidad. Nuestro compromiso con tu privacidad está en el centro de cada decisión que tomamos.

ISO/IEC 27018 Código de prácticas para la protección de datos personales en la nube e ISO/IEC 27701 Ampliación por ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información sobre la privacidad

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

La ISO/IEC 27018 es una norma mundial 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.

La ISO/IEC 27701 es la primera norma mundial certificable para la gestión de la información sobre la privacidad y se publicó en 2019 con el fin de proporcionar un marco para ampliar el sistema de gestión de la seguridad de la información (ISMS) de la ISO/IEC 27001 por un sistema de gestión de la información sobre la privacidad (PIMS) mediante la inclusión de consideraciones sobre la privacidad de los datos.

Las normas estipulan varios requisitos sobre cómo Dropbox usará y no usará la información de tu organización:

- ***Tu organización tiene el control de los datos***

  Solamente usamos la información personal para prestarte los servicios a los que te suscribes. Puedes agregar, modificar o eliminar y documentos de Paper los archivos de Dropbox en cualquier momento.

- ***Ofrecemos transparencia***

  Te indicamos dónde residen tus datos en nuestros servidores. También te informamos quiénes son nuestros socios de confianza. Te indicamos qué sucede cuando cierras una cuenta o eliminas un archivo o un documento de Paper. Por último, te advertimos si se modifica alguno de estos procesos.

- ***Tus datos están seguros***

  Las normas ISO/IEC 27018 e ISO/IEC 27701 fueron diseñadas como mejoras y extensiones de la ISO/IEC 27001, una de las normas de seguridad de la información más aceptadas en el mundo. Recibimos la renovación del certificado de la norma ISO/IEC 27001 en octubre de 2021.

- ***Nuestras prácticas se revisan de forma periódica***

  Como parte del cumplimiento de las normas ISO/IEC 27018 e ISO/IEC 27701, e ISO/IEC 27001, nos sometemos a auditorías externas independientes anuales para conservar las certificaciones. Consulta aquí nuestros certificados de ISO.

Transferencias de datos

Cuando se transfieren datos desde la Unión Europea, el Área Económica Europea, el Reino Unido y Suiza, Dropbox usa diversos mecanismos legales, incluidos contratos con nuestros clientes y filiales, cláusulas contractuales estándares y las decisiones de aptitud de la Comisión Europea sobre determinados países, según corresponda.

Dropbox cumple con los Marcos de Privacy Shield entre los EE. UU. y la UE, y entre los EE. UU. y Suiza, según las estipulaciones del Departamento de Comercio de los EE. UU. acerca de la recopilación, el uso y la retención de datos personales transferidos desde la Unión Europea, el Espacio Económico Europeo, el Reino Unido y Suiza a los Estados Unidos, aunque Dropbox no usa los marcos de Privacy Shield entre los EE. UU. y la

UE, y entre los EE. UU. y Suiza, como base legal para las transferencias de datos personales. Dropbox declaró ante el Departamento de Comercio que él, y su subsidiaria JN Projects Inc. d/b/a Dropbox Sign cumplen con los Principios de Privacy Shield respecto de esos datos. También puedes obtener más información sobre el marco Privacy Shield en https://www.privacyshield.gov.

Los reclamos y controversias relacionados con el cumplimiento de nuestro Escudo de privacidad se investigan y resuelven a través de JAMS, un agente externo independiente. Para obtener más información, lee nuestra Política de privacidad (dropbox.com/privacy).

El Reglamento General de Protección de Datos (RGPD) de la UE

El Reglamento de Protección de Datos General, o RGPD, es un reglamento de la Unión Europea de 2018 que establece un marco integral para el manejo y protección de los datos personales.

Dropbox está comprometido con la seguridad y protección de los datos de nuestros usuarios de acuerdo con los requisitos legales y las mejores prácticas en todo momento. De acuerdo con nuestro compromiso con nuestros usuarios, hemos trabajado arduamente para garantizar que Dropbox cumpliera con el RGPD, incluidos el nombramiento de un responsable de protección de datos, el rediseño de nuestro programa de privacidad para garantizar que los usuarios puedan ejercer sus derechos, la documentación de nuestras actividades de tratamiento de datos y el refuerzo de nuestros procesos internos en caso de una brecha de seguridad. Seguimos haciendo ajustes para garantizar que, a medida que continúen surgiendo orientaciones adicionales de las autoridades de protección de datos, nuestro proceso y prácticas cumplan con elementos específicos de las nuevas normas o los superen.

Código de Conducta en la Nube de la UE

El código de Conducta de la Nube de la UE es un instrumento voluntario que permite a un proveedor de servicios en la nube como Dropbox demostrar nuestro compromiso con el cumplimiento del RGPD. Dropbox Business, que se compone de los planes para equipos Standard, Advanced, Enterprise y Education, ha sido declarado adherente al Código de Conducta de la Nube de la UE y ha recibido una marca de cumplimiento de "Nivel 2", lo que significa que estos servicios han implementado medidas técnicas, organizativas y contractuales en línea con los requisitos del Código. Para obtener más información sobre el Código de Conducta en la Nube de la UE y el cumplimiento del código por parte de Dropbox, visita el sitio web oficial del código.

Para obtener más información sobre nuestras prácticas y políticas de privacidad, consulta el informe blanco de Protección de privacidad y datos de Dropbox.

Conformidad

Existen diversos requisitos normativos y específicos de cada industria relacionados con la seguridad y la privacidad que tu organización podría tener la obligación de cumplir. Nuestro abordaje implica combinar las normas más aceptadas con medidas de cumplimiento orientadas a las demandas específicas de las industrias y las empresas de nuestros clientes.

ISO

La Organización Internacional de Normalización (ISO) ha desarrollado una serie de estándares de clase mundial para la seguridad de la información y las sociedades para ayudar a las organizaciones a desarrollar productos y servicios confiables e innovadores. Dropbox ha certificado sus centros de datos, sistemas, aplicaciones, personas y procesos por medio de una serie de auditorías realizadas por una entidad independiente externa, la neerlandesa EY CertifyPoint, que cuenta con sus acreditaciones ISO del Raad voor Accreditatie (Consejo Holandés de Acreditación).

ISO/IEC 27001 (Seguridad de la información)

ISO/IEC 27001 es reconocido como el estándar principal de sistema de gestión de la seguridad de la información (ISMS) en el mundo, que hace uso de las prácticas recomendadas detalladas en ISO/IEC 27002. Para ser dignos de tu confianza, en Dropbox gestionamos de manera continua e integral nuestros controles físicos técnicos y legales.

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

ISO/IEC 27017 (Seguridad en la nube)

ISO/IEC 27017 es un estándar internacional para la seguridad en la nube que proporciona pautas para los controles de seguridad aplicables al aprovisionamiento y uso de servicios en la nube. Nuestra Guía de responsabilidad compartida explica los requisitos de seguridad, privacidad y cumplimiento a los que Dropbox y sus clientes pueden responder juntos.

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

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

La norma ISO/IEC 27018 es una norma internacional de privacidad y protección de datos que se aplica a proveedores de servicio en la nube, como Dropbox, que procesan información personal en nombre de sus clientes y ofrece un fundamento para los requisitos o las consultas de los clientes respecto a la normativa y contratos.

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

ISO/IEC 22301 (Continuidad de las operaciones)

ISO/IEC 22301 es un criterio internacional de continuidad de operaciones que orienta a las organizaciones sobre cómo reducir la probabilidad de eventos disruptivos y responder a ellos de manera apropiada en caso de que ocurrieran, mediante la minimización del daño potencial. El sistema de gestión de continuidad de las operaciones de Dropbox Business (BCMS) forma parte de nuestra estrategia de riesgos general para proteger a las personas y las operaciones en tiempos de crisis.

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

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

La ISO 27701 es una norma internacional para la gestión de la información sobre la privacidad. La norma proporciona un marco para mejorar y ampliar el sistema de administración de la seguridad de la información según la ISO 27001 por un sistema de administración de la información sobre la privacidad (PIMS). Dropbox Business y Dropbox Education han recibido esta certificación como procesador de PII.

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

SOC

Los informes del control de organización de servicio (SOC), conocidos como SOC 1, SOC 2 o SOC 3, son marcos establecidos por el Instituto Estadounidense de Contadores Públicos Certificados (AICPA) para informar sobre los controles internos implementados dentro de una organización. Dropbox ha validado sus sistemas, aplicaciones, personas y procesos a través de una serie de auditorías realizadas por un auditor independiente externo, Ernst & Young LLP.

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

El informe de seguridad SOC 3 cubre los cinco criterios de servicios de confianza de seguridad, confidencialidad, integridad, disponibilidad y privacidad (TSP Section 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 el diseño y el funcionamiento efectivo de nuestros controles.

Consulta la auditoría SOC 3 de Dropbox Business y Dropbox Education.

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

El informe SOC 2 brinda a los clientes un nivel detallado de seguridad hecha con controles, que cubre los cinco criterios de servicios de confianza de seguridad, disponibilidad, integridad de procesamiento, confidencialidad y privacidad (TSP Section 100). El informe SOC 2 incluye una descripción detallada de los procesos de Dropbox y más de 100 controles con los que contamos para proteger tus cosas. Además de la opinión de nuestro auditor externo independiente sobre el diseño y el funcionamiento efectivo de nuestros controles, el informe incluye los procedimientos de prueba del auditor para cada control. Nuestro informe SOC 2 (a veces llamado informe SOC 2+) también incluye una evaluación auditada de nuestros controles de los estándar ISO mencionados anteriormente, donde se proporciona transparencia adicional con nuestros clientes. La auditoría SOC 2 de Dropbox Business y Dropbox Education está disponible a petición.

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

El informe SOC 1 proporciona seguridades específicas para los clientes que determinan que Dropbox Business o Dropbox Education sea un elemento clave de sus controles internos sobre el programa de informes financieros (ICFR). Estas seguridades específicas se usan principalmente para el cumplimiento de la ley Sarbanes-Oxley (SOX) de nuestros clientes. La auditoría independiente de terceros se lleva a cabo de acuerdo con la Declaración sobre las normas para los compromisos de certificación n.º 18 (Statement on Standards for Attestation Engagements No. 18, SSAE 18) y la Norma internacional de compromisos de seguridad n.º 3402 (International Standard on Assurance Engagements No. 3402, ISAE 3402). Estas normas han reemplazado las obsoletas Declaración sobre las normas para los compromisos de certificación n.º 16 (Statement on Standards for Attestation Engagements No. 16, SSAE 16) y Declaración sobre las normas de auditoría n.º 70 (Statement on Auditing Standards No. 70, SAS 70). La auditoría SOC 1 de Dropbox Business y Dropbox Education está disponible a petición.

CSA

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

El registro de seguridad, confianza y cumplimiento de CSA (STAR) es un registro gratuito y accesible al público que ofrece un programa de garantía de seguridad para los servicios en la nube, y ayuda así a los usuarios a evaluar la posición de seguridad de los proveedores de servicio en la nube que actualmente usan en la actualidad o a los que están considerando contratar.

Dropbox Business y Dropbox Education recibieron el certificado de nivel 2 y la atestación de nivel 2 de CSA STAR. El nivel 2 de CSA STAR requiere de una evaluación externa independiente de nuestros controles de seguridad realizada por EY CertifyPoint (para certificación) y Ernst & Young LLP (para atestación), regida por los requisitos de la ISO 27001, los principios de servicios de confianza de SOC 2 y la matriz de controles de la nube (Cloud Controls Matrix, CCM) v.4.0.1 de CSA.

Accede a nuestro certificado de nivel 2 y atestación de CSA STAR en el sitio web de CSA.

HIPAA/HITECH

Dropbox firmará acuerdos de socios de negocios (Business Associate Agreements, BAA) con aquellos clientes de Dropbox Business y Dropbox Education que los requieren para cumplir con la Ley sobre la Transferibilidad y Responsabilidad de los Seguros Médicos (Health Insurance Portability and Accountability Act, HIPAA) y la Ley de Tecnología de Información de Salud para la Salud Económica y Clínica (Health Information Technology for Economic and Clinical Health Act, HITECH). Consulta Dropbox e HIPAA/HITECH para obtener más información.

Dropbox pone a disposición un informe externo de garantía que evalúa nuestros controles para las reglas de seguridad, privacidad y notificación de infracción de seguridad de HIPAA/HITECH, así como una evaluación de nuestras prácticas internas y recomendaciones a clientes que buscan cumplir con los requisitos de Seguridad HIPAA/HITECH y Reglas de Privacidad en Dropbox Business o Dropbox Education.

Los clientes interesados en solicitar estos documentos u obtener más información sobre la compra de Dropbox Business o Dropbox Education, pueden comunicarse con nuestro equipo de ventas. Si cuentas con un administrador de equipo de Dropbox Business o Dropbox Education, puedes firmar un BAA electrónicamente en la página de la Cuenta en la Consola de administración.

Ten en cuenta que la posibilidad de firmar un BAA electrónico por medio de la Consola de administración solo está disponible para clientes ubicados en Estados Unidos.

NIST 800-171

El Instituto Nacional de Normas y Tecnología (NIST) promueve y mantiene normas y pautas para ayudar a proteger los sistemas de información. La Publicación Especial del NIST (SP) 800171 Revisión 2 (R2) proporciona pautas sobre cómo proteger la información no clasificada controlada (CUI) en los sistemas y organizaciones de información no federales. Toda entidad que procese o almacene CUI del gobierno de los Estados Unidos, como las instituciones de investigación y el sector de la educación, debe cumplir la norma NIST SP 800-171 R2. Los sistemas, procesos y controles de la CUI de Dropbox fueron validados por un auditor externo independiente, Ernst & Young LLP.

El informe del NIST SP 800-171 R2 para Dropbox Business y Dropbox Education está disponible previa solicitud a través de nuestro equipo de ventas o del soporte (para clientes actuales de Dropbox Business).

Ten en cuenta que Dropbox Paper no se incluye en el alcance del informe del NIST SP 800-171 R2.

FERPA y COPPA (estudiantes y niños)

Dropbox Business y Dropbox Education permiten a los clientes usar los servicios de conformidad con las obligaciones del proveedor impuestas por la Ley de Derechos Educativos y de Confidencialidad de la Familia de los EE. UU. (FERPA). Las instituciones educativas con estudiantes menores de 13 años también pueden usar Dropbox Business o Dropbox Education en el marco de la Ley de Protección de la Privacidad Infantil en Internet (COPPA), siempre y cuando acepten disposiciones contractuales específicas que exigen que la institución obtenga el consentimiento de los padres para el uso de nuestros servicios.

FDA 21 CFR Parte 11

Título 21 del Código de Reglamentos Federales (CFR) rige los alimentos y medicamentos dentro de los Estados Unidos para la Administración de Alimentos y Medicamentos (FDA), la Administración de Control de Drogas y la Oficina de Política Nacional de Control de Drogas. La Parte 11 del Título 21 establece los criterios conforme a los cuales la FDA considera que los registros y firmas electrónicos son confiables y generalmente equivalentes a registros impresos y firmas estampadas a mano en papel.

Lee nuestro documento técnico de Dropbox y FDA 21 CFR Parte 11 y el artículo del Centro de ayuda para obtener más información sobre cómo Dropbox puede ayudar en tus esfuerzos por cumplir con el Título 21 Parte 11 del CFR.

PCI DSS

Dropbox es un comerciante que cumple con el Estándar de Seguridad de Datos para la Industria de las Tarjetas de Pago (PCI DSS). Sin embargo,Dropbox Business, Dropbox Education y Dropbox Paper no tienen como finalidad procesar o almacenar transacciones con tarjetas de crédito. La Certificación de Conformidad (AoC) de PCI relacionada con nuestro estado como comerciante está disponible a petición.

Más información sobre el cumplimiento normativo de Dropbox Business y Dropbox Education en dropbox.com/business/trust/compliance.

Aplicaciones para Dropbox

La plataforma DBX está conformada por un amplio ecosistema de programadores que desarrollan nuestras interfaces de programación de aplicaciones (API) flexibles. Más de 750 000 desarrolladores han creado aplicaciones y servicios en la plataforma para la productividad, la colaboración, la seguridad, la administración y otros aspectos.

Componentes prediseñados

Chooser, Saver y Embedder son componentes web y móviles preconstruidos que permiten un acceso fácil a Dropbox en aplicaciones/sitios de terceros con solo una pocas líneas de código.

- Chooser permite seleccionar archivos desde 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 obtienen el acceso a los archivos seleccionados por Chooser a través de vínculos compartidos o vínculos de descarga de corta duración de Dropbox. Estos componentes preconstruidos se pueden utilizar de manera independiente o en conjunto con la API, que se describe a continuación.

Integraciones de la API de Dropbox Business

La API pública de Dropbox permite a los desarrolladores de terceros acceder a Dropbox e interactuar con él dentro de sus aplicaciones. Esto incluye la interacción con archivos y metadatos, uso compartido y funcionalidad de equipos.

Autorización

Dropbox usa OAuth, un protocolo estándar en la industria diseñado para conceder autorización, a fin de que los usuarios puedan conceder a las aplicaciones acceso a las cuentas sin divulgar las credenciales. Admitimos OAuth 2.0 para autenticar solicitudes de la API; las solicitudes se autentican a través del sitio web de Dropbox o de la aplicación de Dropbox para dispositivos móviles. Dropbox soporta las prácticas recomendadas de OAuth, incluidos los tokens de acceso de corta duración y PKCE para aplicaciones distribuidas.

Permisos de usuario

Las aplicaciones que usan la API de Dropbox se pueden integrar con el siguiente nivel de acceso a contenido para usuarios finales de Dropbox:

- ***Carpeta de aplicaciones.***
  Se crea una carpeta dedicada, con el nombre de la aplicación, en la carpeta de aplicaciones de la cuenta Dropbox del usuario. La aplicación tiene acceso de lectura y escritura a esta carpeta únicamente, y los usuarios pueden aportar contenido a la aplicación si mueven archivos a la carpeta. Además, la aplicación podría solicitar acceso a archivos o carpetas a través de Chooser o Saver.

- ***Dropbox completo.***
  La aplicación recibe acceso pleno a todos los archivos y las carpetas en Dropbox de un usuario, y también puede solicitar acceso a archivos o carpetas a través de Chooser o Saver.

Las aplicaciones también pueden solicitar alcances específicos y restringir su comportamiento según el acceso a subconjuntos de terminales de la API. Por ejemplo, las aplicaciones pueden estar limitadas al acceso de solo lectura de archivos, o a la capacidad de cargar contenido, pero no compartirlo.

Permisos del equipo

Los administradores de Dropbox Business pueden autorizar a las aplicaciones a usar la funcionalidad de administración que se encuentra en la consola de administración del equipo. Las acciones que las aplicaciones vinculadas a los equipos pueden realizar están limitadas por su alcance, que especifica qué configuración del equipo la aplicación puede leer o administrar.

Las combinaciones de alcances más comunes incluyen lo siguiente:

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

- ***Auditorías del equipo***
  Acceso de solo lectura a la información del equipo y al registro detallado de eventos.

- ***Acceso a los archivos de los miembros del equipo***
  La capacidad de realizar acciones en nombre de los usuarios del equipo, como administrar sus archivos y carpetas.

- ***Administración de los miembros del equipo***
  Agregar y quitar miembros del equipo.

Webhooks

Los webhooks permiten a las aplicaciones web obtener notificaciones en tiempo real sobre los cambios efectuados en el Dropbox de un usuario. Cuando se registre un identificador de recursos uniforme (URI) para recibir webhooks, se enviará una solicitud HTTP a ese URI cada vez que se efectúe un cambio referente a cualquiera de los usuarios registrados en la aplicación. Con la API de Dropbox Business, los webhooks también pueden usarse para generar notificaciones sobre cambios en la membresía del equipo. Muchas aplicaciones de seguridad usan webhooks para ayudar a los administradores a rastrear y gestionar las actividades del equipo.

Extensiones

Las aplicaciones pueden registrar el URI de extensiones, lo que permite que las acciones aparezcan en los menús "Compartir" y "Abrir" en la interfaz de usuario de Dropbox. Las extensiones permiten a los usuarios iniciar flujos de trabajo personalizados de terceros directamente desde un archivo en una superficie de Dropbox. Cuando se dispara una acción, Dropbox redirige a los usuarios a la URI especificada, a través de un identificador de archivos que puede utilizarse con la API para realizar cualquier tipo de operación con archivos. Las aplicaciones deben estar autorizadas antes de que la extensión registrada pueda ser visible para los usuarios. Podemos promover un conjunto selecto de integraciones de extensiones desde los menús "Compartir" y "Abrir", aunque estas aplicaciones no tendrán acceso al contenido hasta que lo autorice el usuario.

Guías para el desarrollador de Dropbox

Ofrecemos una serie de pautas y prácticas para ayudar a los programadores a crear aplicaciones de API que respeten y protejan la privacidad del usuario a la vez que mejoren la experiencia de los usuarios en Dropbox.

- ***Claves de la aplicación***

  Para cada aplicación diferente que cree un programador, debe usarse una clave de aplicación de Dropbox exclusiva. Si una aplicación ofrece servicios o software que incorporen la plataforma DBX para que la usen otros programadores, cada programador también debe suscribirse para tener su propia clave de la aplicación de Dropbox.

- ***Permisos de la aplicación***

  Se indica a los desarrolladores que una aplicación debe usar el permiso menos privilegiado posible. Cuando un desarrollador envía una aplicación para la aprobación del estado de producción, revisamos que la aplicación no solicite un permiso general innecesario en función de la funcionalidad proporcionada por ella.

- ***Proceso de revisión de aplicaciones***

  - **Estado de desarrollo**
    Cuando una aplicación de la API de Dropbox se crea por primera vez, se le proporciona un estado de desarrollo. La aplicación funciona de la misma forma que cualquier aplicación de estado de producción, excepto que solo se puede vincular con hasta 500 usuarios de Dropbox en total. Una vez que la aplicación vincula 50 usuarios de Dropbox, el desarrollador tiene dos semanas para solicitar y recibir la aprobación del estado de producción antes de que se congele la capacidad de la aplicación de vincular usuarios de Dropbox adicionales.

  - **Estado de producción y aprobación**
    Para recibir la aprobación para el estado de producción, todas las aplicaciones de API deben cumplir con las pautas sobre personalización de marcas y con las Condiciones del servicio, incluso los usos prohibidos de la plataforma DBX, entre ellos, promover la infracción de IP o de copyright, crear redes de uso compartido de archivos y descargar contenido de forma ilegal. Los programadores deben ingresar información adicional acerca de la funcionalidad de la aplicación y sobre la forma en que usan la API de Dropbox antes de enviarla a revisión. Una vez que se autoriza la aplicación y pasa al estado de producción, todos los usuarios de Dropbox que deseen hacerlo podrán vincularse a la aplicación.

Administración de aplicaciones del equipo

Dentro de la consola de administración del equipo, los administradores de equipos de Dropbox Business pueden administrar las integraciones y aplicaciones vinculadas para sus equipos.

Asociaciones de la API

Dropbox ha trabajado estrechamente con sus socios de tecnología para permitirles desarrollar integraciones con sus paquetes de software más populares. Estos socios desarrollan aplicaciones con las API de Dropbox y trabajan estrechamente con los arquitectos de Dropbox para seguir las mejores prácticas de seguridad y experiencia de usuario. Estas incluyen diversas aplicaciones de productividad para usuarios finales, así como también herramientas de seguridad y administración, como las siguientes:

- ***Administración de eventos e información de seguridad (SIEM) y analíticos***

  Conecta tu cuenta de Dropbox Business a herramientas de SIEM y de análisis para supervisar y evaluar el uso compartido de archivos por parte de los usuarios, los intentos de inicio de sesión, las acciones de los administradores y más. Accede a registros de actividad de los empleados y datos relevantes para la seguridad y adminístralos mediante tu herramienta de administración de registros central.

- ***Prevención de pérdida de datos (DLP)***

  Explora automáticamente el contenido y los metadatos de los archivos para desencadenar alertas, informes y acciones cuando se realizan cambios importantes en tu cuenta de Dropbox Business. Aplica las políticas de la organización a tu implementación de Dropbox Business y cumple con los requisitos normativos.

- ***eDiscovery y retención legal***

  Responde a litigios, mediaciones e investigaciones de las autoridades normativas con datos de tu cuenta de Dropbox Business. Busca y recopila información relevante guardada en formato electrónico y preserva los datos mediante el proceso de eDiscovery para ahorrarle tiempo y dinero a tu empresa.

- ***Administración de derechos digitales (DRM)***

  Incorpora protección de contenido de terceros para los datos confidenciales o protegidos por derechos de autor que estén almacenados en las cuentas de los empleados. Accede a potentes características de DRM, como cifrado del lado del cliente, aplicación de marcas de agua, pistas de auditoría, revocación de accesos y bloqueo de usuarios o dispositivos.

- ***Migración de datos y copias de seguridad in situ***

  Migra a Dropbox los datos almacenados en servidores existentes u otras soluciones en la nube para ahorrar tiempo, dinero y esfuerzo. Automatiza la creación de copias de seguridad desde tu cuenta de Dropbox Business a los servidores in situ.

- ***Administración de identidades e inicio de sesión único (SSO)***

  Automatiza el proceso de activación y desactivación, además de agilizar la incorporación de nuevos empleados. Optimiza las tareas de administración y refuerza la seguridad mediante la integración de Dropbox Business con un sistema de identidades existente.

- ***Flujos de trabajo personalizados***

  Desarrolla aplicaciones internas para integrar Dropbox a los procesos empresariales existentes a fin de mejorar los flujos de trabajo internos.

Consulta la página Integraciones de aplicaciones de Dropbox para ver una lista de estos socios de tecnologías. Los usuarios finales pueden descubrir aplicaciones e integraciones selectas de primera y tercera parte en el Centro de aplicaciones.

Integraciones de Dropbox

También hemos trabajado con algunos de nuestros principales socios de tecnologías para desarrollar integraciones que aparecen en superficies de Dropbox. Dropbox y los socios desarrollan en conjunto estas integraciones más profundas. Estos incluyen lo siguiente:

Dropbox Extensions

Estas integraciones te permiten usar diversos tipos de extensiones de aplicaciones para realizar acciones de manera fluida, como publicar videos, agregar archivos a correos electrónicos y chats, enviar un archivo para su firma electrónica y más, sin salir de Dropbox. Las aplicaciones están desarrolladas por nuestros socios, mientras que Dropbox facilita la búsqueda de socios de extensiones selectas a través de los menús “Abrir con” y “Compartir con”.

Slack, Zoom y Trello

Dropbox ha desarrollado estas integraciones en primera parte y permiten a los usuarios iniciar conversaciones de Slack, iniciar reuniones y crear tareas sin salir de Dropbox. Los usuarios finales se autentican en estas herramientas a través de OAuth.

Microsoft Office para dispositivos móviles y en la Web

Nuestras integraciones con Microsoft Office permiten a los usuarios abrir archivos de Word, Excel y PowerPoint almacenados en Dropbox; realizar cambios en las aplicaciones de Office para dispositivos móviles o en la Web; y volver a guardar esos cambios directamente en Dropbox. La primera vez que los usuarios intentan abrir un archivo de Dropbox en cada aplicación para dispositivos móviles de Office o en cualquier aplicación de Office en la Web, se les solicita que autoricen el acceso. Para los usos posteriores, se conservan esos vínculos.

Adobe Acrobat y Acrobat Reader

Nuestras integraciones con las versiones de escritorio y móvil (Android e iOS) de estas aplicaciones permiten que los usuarios vean, editen y compartan PDF almacenados en su Dropbox. Se solicita a los usuarios otorgar acceso en el primer intento de abrir un archivo Dropbox en cada aplicación. Los cambios en los PDF se guardan en Dropbox automáticamente.

Resumen

Dropbox Business ofrece herramientas fáciles de usar para ayudar a los equipos a colaborar eficientemente a la vez que proporciona medidas de seguridad y las certificaciones de conformidad que exigen las organizaciones. Con un enfoque de múltiples capas que combina una infraestructura back-end sólida con un conjunto de políticas personalizables, ofrecemos a las empresas una potente solución que puede adaptarse a sus demandas exclusivas. Para obtener más información acerca de Dropbox Business, comunícate con nosotros a sales@dropbox.com.