Dropbox Business

Responsabilidad compartida: trabajemos juntos para mantener a salvo tus datos

Dropbox colabora con sus clientes con planes Business y Education para mantener sus datos a salvo. Adoptamos medidas exhaustivas para proteger nuestra infraestructura, nuestra red y nuestras aplicaciones; formamos a nuestros empleados en las prácticas de seguridad y privacidad; creamos una cultura en la que ser digno de confianza es la máxima prioridad; y sometemos nuestros sistemas y nuestras prácticas a rigurosas pruebas y auditorías externas.

Aunque Dropbox tiene la responsabilidad de proteger todos y cada uno de los aspectos del servicio que estén bajo nuestro control, los clientes desempeñan un rol fundamental para garantizar la protección y seguridad de sus equipos y datos. Como administrador de un equipo de Dropbox Business o Education, puedes configurar, usar y supervisar tu cuenta de una forma que cumpla los requisitos de seguridad, privacidad y cumplimiento normativo de tu organización.

Hemos elaborado esta guía para ayudarte a comprender lo que hace Dropbox para preservar la seguridad de tu cuenta, así como lo que puedes hacer para mantener la visibilidad y el control de los datos de tu equipo.

Responsabilidades de Dropbox

Integrar la seguridad en nuestra arquitectura

Miles de empresas de todo el mundo confían en nosotros para proteger sus archivos más importantes. Para ganarnos dicha confianza, nos esforzamos por crear productos seguros en los que los administradores como tú podáis confiar. Estas son algunas de las formas en que protegemos nuestra arquitectura y nuestras redes.

Arquitectura distribuida

La arquitectura de Dropbox distribuye distintos niveles de información en varios servicios. Esto no solo hace que la sincronización sea más rápida y fiable, sino que también mejora la seguridad. La naturaleza de la arquitectura de Dropbox impide que se pueda usar el acceso a cualquier servicio individual para volver a crear archivos o documentos de Paper.

Redes seguras

Mantenemos estrictas limitaciones entre la red interna de Dropbox y la red pública con acceso a Internet. El tráfico de red se controla cuidadosamente mediante un servicio de proxy específico que, a su vez, está protegido por las restricciones del cortafuegos. El acceso al entorno de producción está restringido a las direcciones IP autorizadas y requiere autentificación en todos los terminales.

Cifrar los datos de los usuarios

Los clientes de Dropbox Business y Education interactúan con nuestros sistemas por medio de nuestras aplicaciones para móviles, escritorio y web, así como mediante nuestras API. Independientemente de la aplicación que uses, protegemos tus archivos y documentos de Paper tanto en tránsito como en reposo.

Datos en tránsito

Para proteger los datos en tránsito entre las aplicaciones de Dropbox y nuestros servidores, Dropbox emplea las tecnologías Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para la transferencia de datos, creando un túnel seguro protegido por un cifrado con Advanced Encryption Standard (AES) de 128 bits o superior. Los datos de archivos en tránsito entre un cliente de Dropbox (actualmente para escritorio, dispositivos móviles, API o web) y el

servicio alojado se cifran mediante SSL/TLS. Los datos de documentos Paper en tránsito entre un cliente de Paper (actualmente para dispositivos móviles, API o Web) y el servicio alojado siempre están cifrados mediante SSL/TLS. En los puntos de destino que controlamos (escritorio y dispositivos móviles) y los navegadores actuales, usamos un cifrado robusto compatible con mecanismos de confidencialidad directa total ("perfect forward secrecy") y comprobación de certificado ("certificate pinning"). Además, en el sitio web identificamos todas las cookies de autenticación como seguras y habilitamos la tecnología HTTP Strict Transport Security (HSTS) con includeSubDomains habilitado.

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

Datos en reposo

Los archivos estáticos se cifran mediante el estándar Advanced Encryption Standard (AES) de 256 bits y se almacenan en varios centros de datos en bloques de archivos independientes. Cada bloque se fragmenta y se encripta mediante un potente cifrado. Solo se sincronizan los bloques que se hayan modificado desde la versión anterior. Los documentos de Paper en reposo también se cifran mediante Advanced Encryption Standard (AES) de 256nbspbits y se almacenan en diferentes zonas de disponibilidad mediante sistemas de terceros.

Mantener la fiabilidad del servicio

Un sistema de almacenamiento solo es bueno si es fiable. Hemos desarrollado Dropbox con varias capas de redundancia con este fin, para proteger el servicio contra pérdidas de datos y garantizar la disponibilidad. Se distribuyen copias redundantes de los metadatos entre dispositivos independientes dentro de un centro de datos con, al menos, un modelo de disponibilidad N+2. Se realizan copias de seguridad incrementales de los metadatos cada hora y copias de seguridad totales cada tres días. Los metadatos se almacenan en servidores alojados y gestionados por Dropbox. Para almacenar bloques de archivos, Dropbox utiliza sistemas internos y externos diseñados para ofrecer una durabilidad anual de los datos de, al menos, un 99,999999999 %.

En el caso poco probable de que el servicio se interrumpa, los usuarios de Dropbox siguen teniendo acceso a la última copia de sus archivos sincronizada en la carpeta de Dropbox local de los ordenadores vinculados. Se podrá acceder a las copias de los archivos sincronizados en la carpeta de Dropbox local o en el cliente de Dropbox para escritorio desde el disco duro de un usuario durante la interrupción del servicio o cuando no haya conexión.

Distribuimos copias redundantes de datos de documentos de Paper entre dispositivos independientes dentro de un centro de datos con un modelo de disponibilidad N+1. También se realizan copias de seguridad completas de datos de documentos de Paper a diario. Para almacenar documentos de Paper, Dropbox utiliza sistemas de terceros diseñados para ofrecer una durabilidad anual de los datos de, al menos, un 99,999999999 %. En el caso poco probable de la interrupción del servicio, los usuarios seguirán teniendo acceso a las últimas copias sincronizadas de sus documentos de Paper en el modo sin conexión dentro de la aplicación móvil.

Limita el acceso de los empleados a los sistemas back-end

Somos plenamente conscientes de que, cuando almacenas los archivos en Dropbox o creas documentos de Paper, ya sea como cliente de Dropbox Business o Education, esperas que administremos tus datos de forma responsable. Dentro de esta responsabilidad, nos aseguramos de que el acceso por parte de los empleados de Dropbox a nuestros sistemas internos esté sujeto a un control riguroso. Para empezar, el acceso entre nuestras redes corporativas y de producción está estrictamente limitado. Por ejemplo, el acceso a la red de producción se basa en una clave SSH y está restringido a los equipos de ingenieros que necesitan acceder para cumplir con sus obligaciones. La configuración del cortafuegos está estrechamente controlada y limitada a un reducido número de administradores. El acceso a otros recursos, como centros de datos, servicios de configuración de servidores, servidores de producción y servicios de desarrollo de código fuente se autoriza mediante la aprobación explícita por parte de los gestores pertinentes. Los supervisores mantienen un registro de la solicitud de acceso, su justificación y aprobación, y el acceso lo autoriza el personal pertinente.

Mantener la concienciación de los empleados con la seguridad y la privacidad

Parte del trabajo de mantener la seguridad del servicio consiste en asegurarnos de que el personal que trabaja en Dropbox sabe cómo ser concienzudo con la seguridad y reconocer las actividades sospechosas. Para tal fin, los empleados de Dropbox deben aceptar las políticas de seguridad antes de que se les autorice el acceso a los sistemas. Asimismo, los empleados participan en cursos obligatorios en materia de seguridad y privacidad y se someten a una formación anual de seguimiento. Además, reciben periódicamente formación de concienciación con la seguridad a través de mensajes de correo informativos, charlas, presentaciones y los recursos disponibles en nuestra intranet.

Validar nuestras prácticas

Para asegurarnos de que nuestras prácticas de seguridad funcionan según lo previsto, recurrimos a terceros para que evalúen su eficacia. Estos especialistas realizan pruebas periódicas de infiltración y vulnerabilidades en los entornos corporativos y de producción de Dropbox. Si se identifica algún problema, nuestro equipo de ingenieros de seguridad le da la máxima prioridad y lo soluciona. Además, los auditores externos evalúan nuestras prácticas de seguridad conforme a las normas internacionales y del sector. Para que puedas obtener más información sobre las prácticas de Dropbox y evaluarlas, hemos puesto a tu disposición nuestro informe SOC 3 y los certificados ISO 27001, 27017, 27018 y 22301 en línea. También puedes solicitar nuestro informe SOC 2, un informe de evaluación, una evaluación e informe BSI C5 (disponible en inglés y alemán) y asignación de requisitos de la HIPAA, así como resúmenes de los resultados de las pruebas de infiltración bajo las condiciones de confidencialidad.

Comunicarte los problemas

Estado del servicio

Dropbox pone a tu disposición un sitio externo que comunica el estado de nuestro servicio a los clientes de Dropbox Business y Education. Si eres cliente, puedes visitar status.dropbox.com en cualquier momento para consultar el estado actual del sitio, así como las interrupciones y el mantenimiento anteriores.

Notificación de infracciones

Dropbox te enviará una notificación en el caso de que se produzca una filtración de datos, conforme a lo exigido por la legislación vigente. Mantenemos políticas y procedimientos de respuesta ante incidencias, lo que incluye un proceso de notificación de filtraciones que nos permite avisar a los clientes afectados según sea preciso. Si has firmado un acuerdo de asociación comercial de la HIPAA (HIPAA Business Associate Agreement) o un acuerdo de procesamiento de datos de la UE, recibirás estas notificaciones conforme a lo detallado en dichos acuerdos.

Las herramientas que necesitas para garantizar la seguridad de la empresa

Queremos que tanto tú como los demás administradores de Dropbox Business y Education dispongáis de las herramientas que necesitáis para tomar decisiones responsables sobre la seguridad de vuestros equipos. Para ayudarte a configurar, usar y supervisar tu cuenta de una forma que cumpla tus requisitos, el panel de administración está equipado con funciones de seguridad que puedes habilitar en nombre de tu equipo. A través de guías como esta, nuestro informe técnico de seguridad de Dropbox Business, el Centro de ayuda y nuestro equipo de asistencia, ofrecemos información que te ayudará a comprender cómo pueden ayudarte estos parámetros a configurar tu cuenta de forma responsable.

Responsabilidades del cliente

Informarse sobre nuestras prácticas

Determinar si Dropbox Business o Education se ajusta adecuadamente a las necesidades de tu empresa es un proceso importante. Te animamos a que dediques tiempo a validar nuestras prácticas, del mismo modo que lo harías con cualquier otra aplicación. Para brindarte las herramientas que necesitas para verificar nuestras prácticas de seguridad, nuestros certificados ISO 27001, 27017, 27018 y 22301, el informe de control SOC 3 y la autoevaluación CSA STAR Nivel 1 y la certificación CSA STAR Nivel 2 están disponibles en línea. También proporcionamos acceso a documentación adicional bajo las condiciones de un acuerdo de confidencialidad para ayudarte a tomar una decisión fundamentada. Entre dicha documentación, se encuentran nuestros informes de evaluación SOC 1 y SOC 2, nuestro informe de evaluación C5 (disponible en inglés y alemán), una asignación de nuestras prácticas internas y recomendaciones para los clientes que desean cumplir los requisitos de las normas de seguridad y privacidad HIPAA/HITECH, requisitos de de la notificación de privacidad y vulneración, además de resúmenes de nuestras últimas pruebas de infiltración en la aplicación. Las Condiciones del servicio, la Política de uso aceptable y el Acuerdo empresarial estándar están disponibles en línea para que los consultes y te asegures de que Dropbox Business o Education se ajustan correctamente a tu equipo.

Configurar el uso compartido y ver permisos

Dropbox Business y Education te ofrecen la flexibilidad de configurar tu cuenta para respaldar tus requisitos de seguridad, colaboración y privacidad. Los administradores pueden revisar y modificar esta configuración mediante la Consola de administración para reflejar su entorno normativo o de uso compartido. Por ejemplo, las cuentas se pueden configurar de forma que las carpetas, los enlaces y los documentos de Paper no se puedan compartir con personas ajenas a tu equipo. Cuando los miembros del equipo crean carpetas compartidas para sus archivos de Dropbox, pueden personalizar su configuración aún más y elegir el nivel adecuado de acceso (edición o solo lectura).

Consolidar la autenticación

Las prácticas de autenticación sólidas contribuyen a mantener la seguridad de los datos de tu equipo. Los administradores deben revisar la configuración de autenticación disponible y habilitar la más adecuada para proteger sus cuentas. Las cuentas de Dropbox Business y Education incluyen las siguientes opciones:

Verificación en dos pasos

Los administradores de equipo pueden obligar a los miembros a usar la verificación en dos pasos para iniciar sesión en sus cuentas. Esta función de seguridad que recomendamos encarecidamente incorpora una capa de protección adicional para las cuentas de Dropbox de los usuarios. Una vez habilitada, Dropbox solicitará un código de seguridad de seis dígitos o una clave de seguridad, además de una contraseña, para iniciar sesión o vincular un ordenador, teléfono o tablet nuevos.

Inicio de sesión único

Si tu empresa ya gestiona políticas y autenticación de contraseñas con un proveedor de identidades centralizado, puede que te interese configurar un inicio de sesión único para tu equipo de Dropbox Business o Dropbox Education. Al utilizar el proveedor de inicio de sesión único existente, los miembros del equipo se ahorrarán el tener que recordar una contraseña más. Y lo que es más importante, la autenticación del acceso a Dropbox se gestionará con las mismas políticas de contraseñas que el resto de los servicios de tu empresa.

Llevar a cabo revisiones periódicas del acceso

El acceso a la cuenta de tu equipo debe evolucionar a medida que los miembros del equipo, los roles internos y los dispositivos cambien. Debes realizar comprobaciones con frecuencia para asegurarte de que solo puedan acceder a tu cuenta el personal, los dispositivos y las aplicaciones apropiados y, de este modo, mantener tu información en las manos adecuadas. Se puede modificar o eliminar el acceso fácilmente a través del panel de administración.

Miembros del equipo

En la Consola de administración se pueden añadir, eliminar y revisar miembros del equipo con facilidad. Para garantizar que solo las personas adecuadas puedan acceder a los datos confidenciales de tu cuenta de Dropbox Business o Education, recomendamos que revises con frecuencia esta lista De este modo, podrás eliminar el acceso si alguien deja la organización o si ya no tiene que acceder por un cambio en su rol profesional. Del mismo modo, puedes modificar los roles de los miembros del equipo en la Consola de administración para que todas las cuentas de usuario tengan el nivel de acceso adecuado.

Dispositivos

Los miembros del equipo y tú debéis revisar con frecuencia los dispositivos vinculados a tu cuenta, así como eliminar los dispositivos sin usar o no autorizados. Tanto los miembros del equipo como los administradores de equipo pueden desvincular dispositivos. También tenéis la opción de borrar de forma remota contenido de Dropbox del dispositivo al desvincularlo. Gracias a la desvinculación y el borrado de dispositivos, podrás mantener tus datos seguros en caso de pérdida o robo, o si alguien deja el equipo.

Aplicaciones de terceros

Hay un sólido ecosistema de aplicaciones externas que puedes vincular a tu cuenta de Dropbox Business o Education para conseguir una mayor funcionalidad. Las integraciones que aportan servicios tales como la administración de eventos e información de seguridad (SIEM), la prevención de la pérdida de datos (DLP) y la gestión de identidades pueden ser herramientas eficaces para consolidar las prácticas de seguridad existentes. Aunque estas integraciones y aplicaciones externas pueden ser complementos estupendos para tu cuenta, debes recordar que no forman parte de los servicios que incluimos. Por lo tanto, no están cubiertos por los términos del servicio de Dropbox ni por el acuerdo comercial (lo que incluye los acuerdos de asociación comercial o los acuerdos de procesamiento de datos) que hayas firmado con Dropbox. Las aplicaciones pueden pedirte varios niveles de acceso a tu información en función de los servicios que ofrezcan. Como administrador, puedes vincular o eliminar aplicaciones del equipo (que se aplican a toda la cuenta), así como eliminar las aplicaciones individuales que los miembros del equipo hayan podido añadir a sus propias cuentas. Las aplicaciones externas y el acceso se pueden revisar y modificar a través de la Consola de administración.

Supervisar en busca de actividad inusual

Como administrador de equipo, puedes ver y exportar informes que detallan las actividades de archivo de tu equipo, el uso compartido, la autenticación y las actividades del administrador. Los administradores deben revisar periódicamente estos informes de actividad para estar alerta ante cualquier actividad inusual y contribuir a preservar la seguridad del equipo. Es posible que también debas plantearte el uso de una integración de SIEM externa u otra integración de supervisión para mejorar tus capacidades.

Determinar las necesidades de cifrado

De forma predeterminada, Dropbox almacena una copia local de los archivos en tu ordenador para garantizar que tengas los archivos que necesitas al alcance de la mano. Las copias locales de tus archivos están igual de protegidas que cualquier otro archivo de tu ordenador. Para preservar su seguridad, recomendamos que habilites el cifrado de discos en tus dispositivos siempre que sea posible, y que, para acceder a tu portátil, teléfono, tablet o cualquier otro dispositivo que permita acceder a tu cuenta de Dropbox, haya que introducir una contraseña única y segura. Al utilizar este tipo de contraseña, también protegerás el acceso a tus documentos de Paper.

Dropbox protege los archivos que subes a tu cuenta dividiéndolos automáticamente en bloques independientes y cifrando cada uno de dichos bloques mediante el estándar Advanced Encryption Standard (AES) de 256 bits. De forma similar, Dropbox protege los documentos de Paper cifrándolos en reposo en un almacenamiento persistente mediante el estándar Advanced Encryption Standard (AES) de 256 bits Dropbox gestiona las claves de cifrado en nombre de nuestros clientes para facilitar este proceso a los usuarios y habilitar unas funciones concretas.

Los miembros de Dropbox Business y Education también pueden optar por cifrar los archivos antes de subirlos a Dropbox por su cuenta o mediante una integración externa. No obstante, los usuarios que cifren los datos antes de subirlos a Dropbox serán responsables de la gestión de las correspondientes claves de cifrado. Cifrar los archivos antes de subirlos a Dropbox también puede reducir la funcionalidad de algunas funciones.

Animamos a los clientes que estén interesados en obtener más información sobre los métodos de seguridad de Dropbox a que consulten el informe técnico de seguridad o visiten nuestro sitio web: dropbox.com/business/trust. Para obtener más información sobre Dropbox Business o Dropbox Education y solicitar los informes de las auditorías externas bajo las condiciones de un acuerdo de confidencialidad, ponte en contacto con sales@dropbox.com.