Dropbox Business

Responsabilidad compartida: Trabajamos juntos para mantener tus datos seguros

Dropbox trabaja con los clientes de Dropbox Business y Dropbox Education para proteger sus datos. Tomamos medidas abarcativas para proteger nuestra infraestructura, nuestra red y nuestras aplicaciones; capacitamos a nuestros empleados en prácticas de seguridad y privacidad; construimos una cultura en la que ser confiable es la máxima prioridad; y sometemos los sistemas y las prácticas a pruebas y auditorías rigurosas de terceros.

Si bien Dropbox es responsable de asegurar cada aspecto del servicio que esté bajo nuestro control, los clientes tienen un rol clave en asegurarse de que sus equipos y sus datos estén protegidos y seguros. Como administrador de un equipo de Dropbox Business o Dropbox Education, puedes configurar, utilizar y controlar tu cuenta para que satisfaga las necesidades de seguridad, privacidad y cumplimiento normativo de tu organización.

Hemos armado esta guía para ayudarte a comprender lo que hace Dropbox para mantener tu cuenta segura y lo que puedes hacer tú para mantener la visibilidad y el control de los datos de tu equipo.

Responsabilidades de Dropbox

Crear seguridad en nuestra arquitectura

Miles de empresas del mundo confían en nosotros para proteger su trabajo más importante. A fin de ganar esa confianza, trabajamos arduamente para crear productos seguros, en los que los administradores como tú pueden confiar. A continuación, detallamos algunas de las formas en las que protegemos nuestra arquitectura y nuestras redes.

Arquitectura distribuida

La arquitectura de Dropbox distribuye diferentes niveles de información en múltiples servicios. Esto no solo ayuda a que la sincronización sea más ágil y más segura, sino que también aumenta la seguridad. La naturaleza de la arquitectura de Dropbox hace que el acceso a cualquier servicio individual no pueda utilizarse para recrear archivos ni documentos de Paper.

Redes seguras

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. 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.

Cifrar datos de usuario

Los clientes de Dropbox Business y Education interactúan con nuestros sistemas a través de nuestras API y nuestras aplicaciones móviles, de escritorio y web. Sin importar qué aplicación utilices, protegemos tus datos en archivos y documentos de Paper en tránsito y en almacenamiento.

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.

Para evitar los ataques del tipo "man-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 en reposo se cifran con un cifrado de 256nbspbits a través del estándar de cifrado avanzado (AES). Los archivos se almacenan en varios centros de datos en bloques de archivos separados. Cada bloque se fragmenta y cifra mediante un potente cifrado. 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 256nbspbits. Los documentos de Paper se almacenan en diferentes áreas de disponibilidad usando sistemas de terceros.

Mantener un servicio confiable

Un sistema de almacenamiento solamente 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. 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, una vez cada tres días. Los metadatos se almacenan en servidores alojados y administrados por Dropbox. Para el almacenamiento de bloques de archivos, Dropbox utiliza sistemas de almacenamiento internos y de terceros que están diseñados 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 de Dropbox aún pueden acceder a las últimas copias sincronizadas de sus archivos en la carpeta local de Dropbox de 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 los períodos de inactividad y los cortes del servicio, así como cuando no hay conexión a Internet.

De manera similar, las copias redundantes de los datos de los documentos de Paper se distribuyen en dispositivos independientes en un centro de datos en un modelo de disponibilidad N+1 y hemos configurado copias de seguridad completas diarias de los datos de los documentos de Paper. Para el almacenamiento de documentos de Paper, Dropbox utiliza sistemas de almacenamiento de terceros que están diseñados 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.

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

Sabemos que cuando almacenas archivos como cliente de Dropbox Business o Dropbox Education, esperas que administremos tus datos con responsabilidad. Como parte de esta responsabilidad, nos aseguramos de controlar estrictamente el acceso de los empleados de Dropbox a nuestros sistemas internos. Para empezar, el acceso entre nuestras redes corporativas y de producción está estrictamente limitado. 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 estrictamente controlada y limitada a una cantidad reducida de administradores. 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.

Mantener a los empleados informados sobre la seguridad y la privacidad

Parte de la seguridad del servicio consiste en asegurarnos de que quienes trabajan en Dropbox comprendan cómo ser conscientes de la seguridad y cómo reconocer actividades sospechosas. Para eso, los empleados de Dropbox deben conocer las políticas de seguridad antes de obtener acceso a los sistemas. Los empleados también participan en capacitaciones obligatorias sobre seguridad y privacidad cuando ingresan, y de capacitaciones de seguimiento anuales. Además, reciben capacitación regular relativa a la seguridad a través de correos electrónicos, charlas, presentaciones y recursos disponibles en nuestra intranet.

Validar nuestras prácticas

Para ayudarnos a garantizar que nuestras prácticas de seguridad funcionen según lo previsto, recurrimos a terceros que evalúan su eficacia. Los especialistas realizan pruebas periódicas de penetración y vulnerabilidad en los entornos corporativos y de producción de Dropbox. Nuestro equipo de ingeniería de seguridad prioriza y soluciona los problemas identificados. Además, los auditores externos evalúan nuestras prácticas de seguridad en función de las normas internacionales y del sector. Para ayudarte a conocer más las prácticas de Dropbox y a evaluarlas, ponemos a tu disposición el informe SOC 3, y los certificados ISO 27001, 27017, 27018 y 22301 que puedes consultar en línea. También puedes solicitar nuestro informe SOC 2, el informe de evaluación y el mapa de los requisitos de la HIPAA, una evaluación y un informe BSI C5 (disponible en inglés y en alemán) y los resúmenes de los resultados de pruebas de penetración de conformidad con un acuerdo de confidencialidad (NDA).

Comunicarte los problemas

Estado del servicio

Dropbox pone a tu disposición un sitio de un tercero que comunica el estado de nuestro servicio a los clientes de Dropbox Business y Dropbox Education. Como cliente actual, puedes ingresar a status.dropbox.com en cualquier momento para ver el estado actual del sitio, así como también las interrupciones y el mantenimiento previos.

Notificación de violación de seguridad

Dropbox te notificará si hay una violación de seguridad de datos, como lo establece la ley en vigencia. Contamos con políticas y procedimientos de respuesta ante incidentes, incluido un proceso de notificación de violación de seguridad que nos permite notificar a los clientes afectados, según sea necesario. Si ingresaste en un Acuerdo de Socio Empresarial de HIPAA o en un Acuerdo de Procesamiento de Datos de la UE, recibirás una notificación como se detalla en esos acuerdos.

Brindarte las herramientas que necesitas para estar seguro

Queremos que tú y otros administradores de Dropbox Business y Dropbox Education cuenten con las herramientas necesarias para poder tomar decisiones responsables e informadas sobre la seguridad de su equipo. Para configurar, utilizar y controlar tu cuenta de forma tal que cubra tus necesidades, tu consola de administración cuenta con funciones de seguridad que puedes habilitar en nombre de tu equipo. A través de guías como esta, nuestro Documento Técnico sobre Seguridad de Dropbox Business, el Centro de Ayuda y nuestro equipo de soporte, te brindamos información para que comprendas cómo estas configuraciones pueden ayudarte a configurar tu cuenta de forma responsable.

Responsabilidades del cliente

Aprender sobre nuestras prácticas

Determinar si lo que tu compañía necesita es Dropbox Business o Dropbox Education es un proceso importante. Te invitamos a dedicar algún tiempo a validar nuestras prácticas, como lo harías con cualquier otra aplicación. Con el fin de brindarte las herramientas necesarias para verificar nuestras prácticas de seguridad, los certificados ISO 27001, 27017, 27018, 22301; el informe de control de calidad SOC 3; y la Autoevaluación CSA STAR Nivel 1 y la Certificación de Nivel 2 están disponibles en línea. Además, brindamos acceso a documentación adicional de conformidad con nuestro acuerdo de confidencialidad para ayudarte a tomar una decisión informada. Esto incluye nuestros informes de evaluación SOC 1 y SOC 2, nuestro informe de evaluación C5 (disponible en inglés y alemán), un mapa de nuestras prácticas internas y recomendaciones para los clientes que buscan cumplir con los requisitos de la Reglamentación de Notificación de Seguridad, Privacidad y Violaciones de HIPAA/HITECH, así como resúmenes de nuestras últimas pruebas de penetración de aplicaciones. Nuestras Condiciones de servicio, la Política de Uso Aceptable y el Acuerdo Empresarial Estándar están disponibles en línea para que los revises y determines si la opción adecuada para tu equipo es Dropbox Business o Dropbox Education.

Configurar permisos de uso compartido y de visualización

Dropbox Business y Dropbox Education te brindan flexibilidad para configurar tu cuenta de manera que cubra tus necesidades de seguridad, colaboración y privacidad. Los administradores pueden revisar y modificar estas configuraciones desde la consola de administración para reflejar su uso compartido o su entorno regulatorio. Por ejemplo, las cuentas se pueden configurar de forma tal que las carpetas, los enlaces y los documentos de Paper no se puedan compartir con personas que no sean de tu equipo. Cuando los miembros del equipo crean carpetas compartidas de archivos de Dropbox, pueden personalizar la configuración de las carpetas y elegir el nivel de acceso apropiado: edición permitida o de solo lectura.

Fortalecer la autenticación

Las prácticas de autenticación sólidas ayudan a mantener seguros los datos de tu equipo. Los administradores deben revisar las configuraciones de autenticación disponibles y habilitar aquellas que mejor se adecuen a la protección de sus cuentas. Las cuentas de Dropbox Business y de Dropbox Education cuentan con las siguientes opciones:

Verificación de dos pasos

Los administradores del equipo pueden solicitar que los miembros utilicen una verificación de dos pasos para iniciar sesión en sus cuentas. Esta función de seguridad recomendada agrega una capa extra de protección a las cuentas de Dropbox de los usuarios. Una vez habilitada, Dropbox solicitará un código o una clave de seguridad de seis dígitos, además de una contraseña para iniciar sesión o para vincular computadoras, teléfonos o tablets nuevos.

Inicio de sesión único (SSO)

Si tu compañía ya administra las políticas de contraseñas y la autenticación con un proveedor de identidad central, quizás desees elegir configurar un inicio de sesión único para tu equipo de Dropbox Business o Dropbox Education. Al utilizar tu proveedor de SSO existente, los miembros del equipo no necesitan recordar otra contraseña. Lo más importante es que se puede administrar la autenticación del acceso a Dropbox con las mismas políticas de contraseña que utilizas para otros servicios en tu compañía.

Realizar revisiones de acceso periódicas

El acceso a las cuentas de tu equipo debe evolucionar a medida que la membresía, los roles internos y los dispositivos del equipo cambian. Debes controlarlo con frecuencia y asegurarte de que solo las personas, los dispositivos y las aplicaciones adecuados tengan acceso a la cuenta para mantener la información en las manos correctas. Modificar o eliminar el acceso es simple desde la consola de administración.

Miembros del equipo

Desde la consola de administración, se pueden agregar, eliminar y revisar fácilmente los miembros del equipo. Para asegurarte de que solo las personas correctas puedan acceder a la información confidencial en la cuenta de Dropbox Business o Dropbox Education, te recomendamos que revises con frecuencia esta lista. Puedes eliminar un acceso cuando alguien abandone la organización o ya no necesite acceso porque cambió su rol de trabajo. De manera similar, puedes modificar los roles de los miembros del equipo desde la consola de administración para que cada cuenta de usuario tenga el nivel de acceso apropiado.

Dispositivos

Tú y los miembros del equipo deben revisar con frecuencia los dispositivos conectados con la cuenta y eliminar los que no se utilicen o los que no estén autorizados. Tanto los miembros como los administradores del equipo pueden desvincular dispositivos. Tú y los miembros del equipo también tienen la opción de borrar de sus dispositivos en forma remota el contenido de Dropbox al desvincularlos. Desvincular y borrar los dispositivos puede mantener la seguridad de los datos en caso de pérdida o robo, o si alguien abandona el equipo.

Aplicaciones de terceros

Existe un sólido ecosistema de aplicaciones de terceros que puedes vincular a tu cuenta de Dropbox Business o Dropbox Education para obtener más funcionalidades. Las integraciones que brindan servicios, como SIEM, DLP y administración de identidad, pueden convertirse en herramientas poderosas para fortalecer tus prácticas de seguridad existentes. Si bien estas aplicaciones e integraciones de terceros pueden ser complementos perfectos para tu cuenta, es importante que recuerdes que no son parte de los servicios incluidos. Por lo tanto, no están cubiertas por las Condiciones de Uso de Dropbox ni por un acuerdo empresarial, incluidos un acuerdo de asociación empresarial o de procesamiento de datos, que puedas haber firmado con Dropbox. Las aplicaciones pueden pedir varios niveles de acceso a tu información según el servicio ofrecido. Como administrador, puedes vincular o eliminar aplicaciones de equipo, que se aplican a toda tu cuenta, y eliminar aplicaciones individuales que pueden haber agregado los miembros del equipo en sus propias cuentas. Se pueden revisar y modificar las aplicaciones y el acceso de terceros desde la consola de administración.

Controlar la actividad inusual

Como administrador del equipo, puedes ver y exportar informes que detallan los eventos de archivos, el uso compartido, la autenticación y las actividades del administrador. Los administradores deben revisar de forma periódica estos informes de actividad para detectar cualquier actividad inusual y para ayudar a mantener el equipo seguro. También puedes utilizar un SIEM de terceros u otra integración de control para aumentar tus capacidades.

Determinar las necesidades de cifrado

Dropbox almacena de forma predeterminada una copia local de tus archivos en tu computadora para asegurarse de que tienes los archivos que necesitas al alcance de tu mano. Las copias locales de tus archivos están protegidas como cualquier otro archivo de tu computadora. Para mantenerlas protegidas, te recomendamos que, cuando sea posible, habilites el cifrado de disco en tus dispositivos y que solicites una contraseña segura y única para acceder a tu computadora portátil, teléfono o tablets, o a cualquier dispositivo que permita acceder a tu cuenta de Dropbox. Tener contraseñas seguras y únicas en tus dispositivos también ayudará a proteger el acceso a los documentos de Paper.

Dropbox protege los archivos que subes a tu cuenta al dividirlos automáticamente en bloques independientes y cifrarlos con el estándar de cifrado avanzado (AES) de 256 bits. De manera similar, Dropbox protege los documentos de Paper al cifrarlos en reposo en almacenamiento a largo plazo con el estándar de cifrado avanzado (AES) de 256 bits . Dropbox administra las claves de cifrado por sus clientes para simplificar este proceso y habilitar ciertas características.

Los miembros de Dropbox Business y de Dropbox Education pueden cifrar los archivos antes de subirlos a Dropbox, ya sea por sí mismos o a través de una integración de un tercero. Sin embargo, los usuarios que cifren datos antes de subirlos a Dropbox son responsables de la administración de esas claves de cifrado. Cifrar los archivos antes de subirlos a Dropbox también puede reducir la funcionalidad de algunas características.

Los clientes que estén interesados en conocer más sobre la forma en que Dropbox maneja la seguridad pueden leer el Documento Técnico sobre Seguridad o revisar nuestro sitio web: dropbox.com/business/trust. Para obtener más información sobre Dropbox Business o Dropbox Education y solicitar informes de auditorías de terceros de conformidad con el acuerdo de confidencialidad, puedes escribir a sales@dropbox.com.