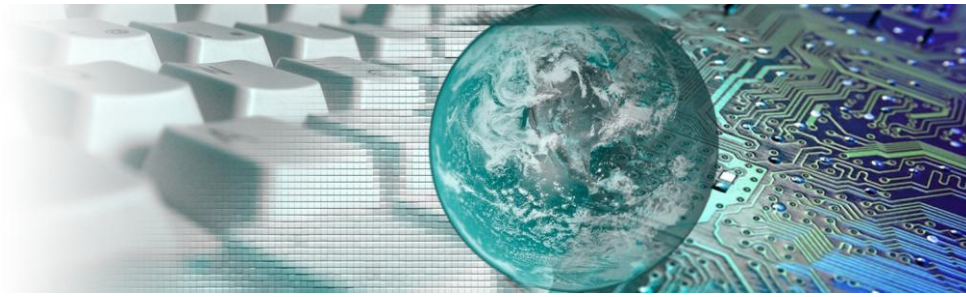
Guía de utilización segura de Dropbox

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana



GENERALITAT VALENCIANA
CONSELLERIA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Sobre CSIRT-cv

CSIRT-cv es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, englobado dentro del III Programa de Servicios de Telecomunicaciones Avanzados Corporativos y de Comunicación con los Ciudadanos incluido en el Plan Estratégico Valenciano de Telecomunicaciones Avanzadas (PEVTA) del programa Avantic, como una apuesta de la **Generalitat de la Comunitat Valenciana** por la seguridad en la red.

Se trata de una iniciativa pionera al ser el primer centro de estas características que se crea en España para un ámbito autonómico.

Datos de contacto

CSIRT-cv Centro de Seguridad TIC de la Comunitat Valenciana
http://www.csirtcv.gva.es/
Generalitat de la Comunitat Valenciana,
C/Cardenal Benlloch, 69 Entlo
46021 Valencia, España

Teléfono: +34-96-398-5300
Telefax: +34-96-196-1781
Email: csirtcv@gva.es
https://www.facebook.com/csirtcv
https://twitter.com/csirtcv

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Índice de contenido

Acerca de Dropbox

A grandes rasgos, Dropbox es un servicio que permite **almacenar ficheros en Internet**.

Su gran expansión y fama se debe principalmente a la facilidad con la que se pueden compartir ficheros entre distintos dispositivos (PC's, portátiles, tabletas, móviles…), o almacenarlos online directamente desde su propia web sin necesidad de instalar ninguna aplicación.

Generalmente se utiliza para almacenar material multimedia como fotos, música o pequeños videos, además de para guardar documentos ofimáticos, o copias de seguridad personales.

Otra de sus carácteristicas más interesantes es la posibilidad de poder compartir carpetas entre diferentes usuarios, lo cual elimina los problemas habituales que tiene el correo electrónico a la hora de enviar ficheros grandes.

Si bien es un servicio muy práctico y útil, debemos tener ciertas **precauciones** a la hora de utilizarlo, algunas comunes a cualquier otra aplicación web y otras específicas de este servicio.

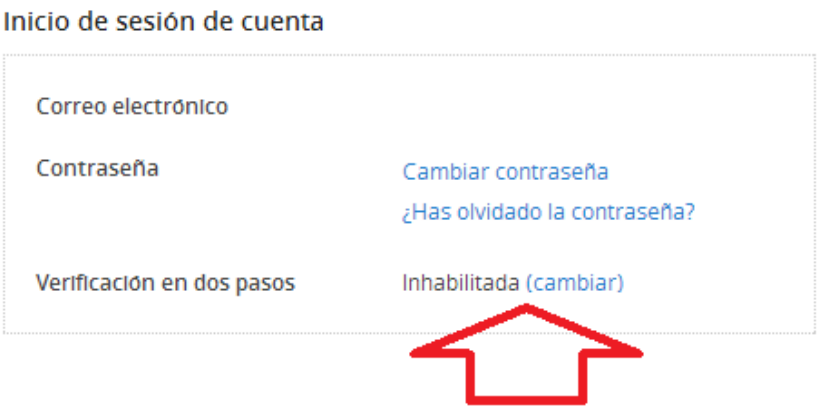
Accediendo a nuestra cuenta

Como casi todos los servicios que utilizamos a través de Internet, Dropbox controla el acceso a la plataforma mediante una combinación de correo electrónico y contraseña.

Para asegurarnos que nuestros datos están a buen recaudo debemos utilizar una **contraseña robusta** mayor de 8 caracteres, a ser posible con números, letras, caracteres especiales y combinando mayúsculas y minúsculas, además de cambiarla periódicamente. Con esto evitaremos que puedan adivinar nuestra contraseña, ya sea por ser demasiado sencilla o por sufrir un ataque de fuerza bruta (probar todas las combinaciones posibles) hasta encontrar nuestra contraseña.

La elección de nuestra **contraseña de acceso al correo electrónico,** además de tener que ser una contraseña distinta, es incluso más importante que la de Dropbox, ya que si se consiguiera acceder al correo se podría obtener una contraseña nueva para nuestra cuenta de Dropbox y acceder a nuestros ficheros.

Para aquellos usuarios que deseen seguridad extra en el acceso a su cuenta de Dropbox, existe la posibilidad de activar la llamada ***"verificación en dos pasos"***. Al activar esta característica, cuando se accede al servicio o se intenta enlazar un nuevo dispositivo (ver apartado siguiente), además de la contraseña de acceso se nos pedirá un código que recibiremos en el móvil o directamente en una aplicación aparte, evitando así que nadie que no seamos nosotros pueda acceder a los datos almacenados. Se trata de una funcionalidad bastante desconocida y poco utilizada ya que complica ligeramente el acceso a la cuenta, pero es necesaria si los datos que almacenamos son especialmente sensibles. Para activarla y obtener más información al respecto se debe acceder a la pestaña de seguridad, dentro de la configuración de la cuenta de Dropbox.



Accediendo desde distintos dispositivos

El acceso a los datos se puede hacer desde la propia página web de Dropbox o desde la aplicación instalada en un equipo. Si el uso que le vamos a dar es esporadico, o estamos utilziando un equipo que no es nuestro y solo queremos cargar o descargar algún fichero, lo más seguro es utilizarlo desde el **navegador web** con el fin de dejar el menor rastro posible de información en el equipo. Recordemos que siempre que accedemos a algún servicio online desde ordenadores o dispositivos ajenos, debemos cerrar la sesión web antes de cerrar la página.

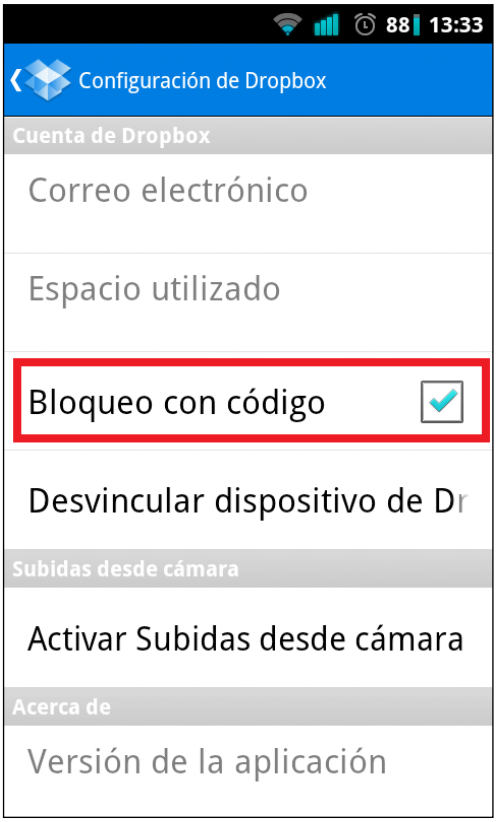
Por otro lado, uno de los principales usos que se le da a Dropbox es el de sincronización de ficheros entre distintos dispositivos, es decir, tener carpetas con los mismos documentos en distintos equipos y que se actualicen automáticamente. Para ello solo hace falta instalar la **aplicación de Dropbox** en cada dispositivo e introducir el correo electrónico y la contraseña. A partir de ese momento el equipo quedará "enlazado" y se podrá acceder a todos los datos de la cuenta.

Cabe destacar una diferencia importante entre la utilización en dispositivos móviles (tabletas o móviles) y ordenadores: cuando un ordenador se enlaza a una cuenta de Dropbox, automáticamente se descargan todos sus datos en el equipo, mientras que si se hace desde un dispositivo móvil los datos siguen en Internet, y solo se descargan de uno en uno si se indica expresamente. Esta diferencia es importante ya que si desinstalamos Dropbox de un ordenador **los datos permanecerán guardados** en el equipo, mientras que si se hace desde un dispositivo móvil, solo quedarán los que hayamos dicho expresamente que se descarguen. En cualquier caso es recomendable asegurarse de eliminar los ficheros descargados una vez desinstalada la aplicación.

Pérdida de dispositivos y medidas de protección

Es posible que tengamos Dropbox enlazado con distintos dispositivos y que uno de ellos se pierda, sea robado, o tengamos que enviarlo al servicio técnico por que no funciona.

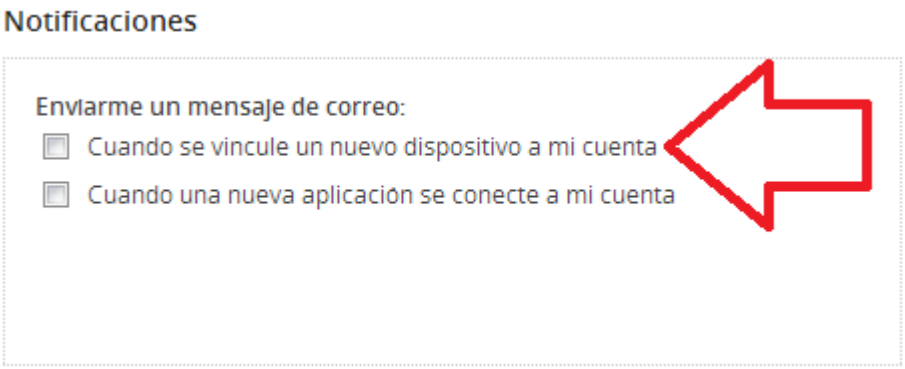
Si hemos sido previsores, nuestro dispositivo tendrá un código de desbloqueo por lo que a priori nuestros datos estarán a salvo. No obstante hay usuarios reacios a estos códigos por lo que Dropbox permite activar un código de desbloqueo propio que solo será necesario introducir al acceder a la aplicación. Para ello bastará con acceder a la configuración de la aplicación, marcar "*Bloqueo con código*" e introducir el código que queramos. Podremos también marcar la opción de que si se introduce el código mal 10 veces los datos de Dropbox almacenados en el dispositivo se eliminen automáticamente (solo se borran del dispositivo, no de la web):



Se puede dar también la situación de que por descuido no hayamos activado el código de bloqueo y que nuestro terminal se pierda o sea robado. Ante estas situaciones en las que no queremos que se pueda acceder a nuestros datos, pero no podamos acceder directamente a nuestro dispositivo para borrar los datos, podemos acceder a la web de Dropbox y desde *Configuración → Seguridad*, pulsar "*Desvincular*" sobre el dispositivo que queremos que deje de sincronizarse. Tengamos en cuenta que al hacer esto, los datos que hubiese en el dispositivo no se eliminarán, pero conseguiremos que no puedan volver a sincronizarse (bastante útil con dispositivos móviles, aunque no con portátiles y PCs).

Si en lugar de haber perdido el dispositivo hemos olvidado **cerrar la sesión en un navegador web**, desde la ventana anterior (*configuración → seguridad*) también podremos cerrar las distintas sesiones web que estén abiertas en ese momento.

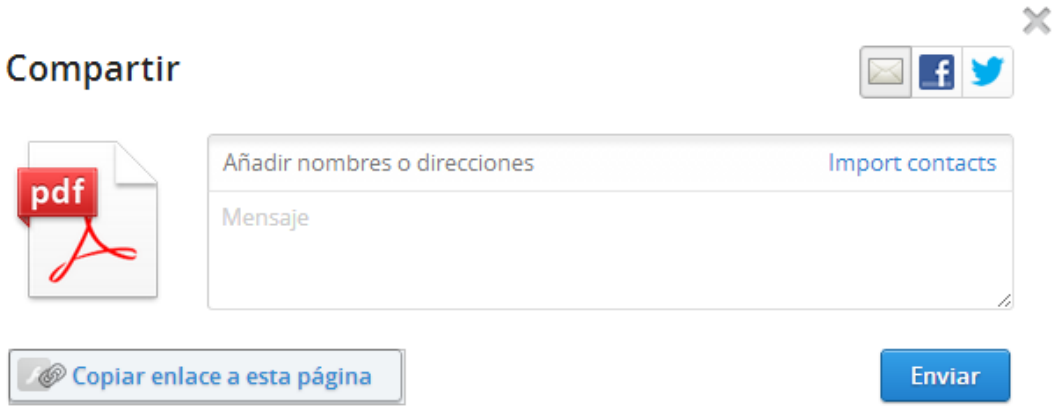
Adicionalmente podemos activar la opción de **notificar** "*cuando se vincule un nuevo dispositivo a mi cuenta*", para que en caso de que alguien conozca nuestra contraseña, el sistema nos avise si se intenta vincular un nuevo dispositivo a nuestra cuenta.



De cualquier forma, recordemos que ante la pérdida de un dispositivo, o la detección de un dispositivo desconocido que se haya vinculado o cualquier otro indicio de acceso no autorizado a nuestra cuenta es necesario **cambiar la contraseña** de acceso.

Compartiendo ficheros

Dropbox dispone de dos posibilidades a la hora de compartir ficheros: **crear un enlace público**, o **compartir ficheros únicamente con algunos usuarios**. Debemos ser cautelosos a la hora de decidir qué metodo utilizar, ya que si nos decantamos por el enlace, aunque este se lo hagamos llegar únicamente a algún contacto, si el enlace es interceptado el fichero será accesible por cualquier usuario de Internet sin que nos enteremos. Es pues recomendable utilizar en la medida de lo posible la compartición de ficheros con usuarios de Dropbox, ya que, aunque es menos cómodo, asegura que únicamente ese usuario tendrá acceso.



CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Protegiendo nuestros datos

En principio, Dropbox protege nuestros datos cifrándolos con una contraseña para que en caso de que atacasen sus servidores, los ficheros que se pudiesen robar no sean legibles.

Decimos "en principio" porque a pesar de que es una buena práctica esta medida **no garantiza que nuestros datos sean 100%** privados ya que los propios empleados de Dropbox podrían tener acceso a nuestros ficheros. Además, ante un posible ataque, estas contraseñas de cifrado podrían ser tambien robadas con lo que los atacantes podrían tener acceso a toda nuestra información almacenada en su servicio.

Para proteger nuestra información frente a ataques o empleados curiosos, debemos ser nosotros quienes **cifremos nuestros datos antes de cargarlos** en Dropbox. Para ello podemos utilizar herramientas como TrueCrypt, o ficheros comprimidos con contraseñas robustas. Si bien este sistema es el más sencillo y el que más control sobre nuestros ficheros proporciona, tiene el inconveniente que cada vez que queramos acceder a un fichero hay que descifrarlo, y si queremos modificarlo, volverlo a cifrar y subirlo de nuevo.

Para evitar este problema existen otras alternativas como BoxCryptor, la cual cifra de forma automática cualquier fichero que carguemos en cierta carpeta de nuestro Dropbox con una contraseña diferente de la de acceso al servicio. Si deseamos acceder a nuestros datos cifrados bastará con iniciar la aplicación la cual nos montará una nueva unidad de disco en "Mi Pc" con nuestros documentos cifrados. También dispone de versiones para las principales plataformas, como pueden ser Android, Linux, Mac, iOS o Windows RT.

Así pues, si bien el servicio de **Dropbox no es recomendable para almacenar información confidencial o sensible**, aplicándose medidas de seguridad compensatorioas como es el cifrado de información en contenedores seguros (TrueCrypt o similares) podría considerarse adecuado.

Metadatos, o información oculta

Según las condiciones de privacidad de Dropbox, solo una pequeña parte de sus empleados tienen permiso para acceder a los ficheros de los usuarios y siempre de forma justificada (peticiones legales, incidencias técnicas y similares), pero existe una cláusula según la cual **pueden acceder a los metadatos de los ficheros**. Como sabemos, los metadatos son información semi-oculta en los ficheros que indican carácteristicas del mismo: mientras que un documento de texto puede almacenar datos como el autor, la versión, o nombres anteriores del fichero, una foto puede guardar el modelo de la cámara, la velocidad de disparo o incluso las coordenadas GPS de donde fue tomada. Estos datos pueden ser relativamente sensibles ya que pueden dar información de donde está nuestro domicilio, datos personales, o incluso revelar información confidencial en forma de comentario, por lo que su publicación debe ser controlada.

Al respecto las indicaciones de Dropbox son muy claras y les citamos textualmente: "*Si no desea compartir archivos integrados con su información de ubicación geográfica con nosotros, no los cargue.*"

Si se desea más información sobre cómo eliminar los metadatos se puede acceder a la siguiente campaña informativa de CSIRT-cv.

Conclusiones

Este documento ha sido una breve guia de utilización segura de Dropbox. Como acostumbra a ser frecuente con todos los servicios de Internet, cualquier medida de seguridad o curso de formación no sirve de nada si el usuario no actúa con **sentido común**. Antes de utilizar un servicio es recomendable familiarizarse con él y aplicar las normas básicas de seguridad comunes a cualquier aplicación online. Estas recomendaciones deben siempre aplicarse de forma proporcional a lo privados y confidenciales que sean los datos que se están exponiendo, por lo que se han propuesto medidas desde lo más genérico y simple, hasta las más estrictas.

A modo de conclusión final, **desde CSIRT-cv se desaconseja la utilización de Dropbox para compartir información sensible** ya que existen alternativas para almacenar y compartir datos sin necesidad de ceder los datos a un tercero. La utilización de Dropbox sin las medidas de seguridad adecuadas pueden conllevar la difusión de información confidencial o la perdida sobre el control de la misma.