8 Prácticos Consejos Para Proteger Tus Datos En La Nube

Servicios como Dropbox, OneDrive, Drive, entre otros, son una gran herramienta para aquellas personas que deseen tener al alcance sus datos, proyectos, trabajos y quieran usarlos cuando los deseen y donde los deseen, claro, con la facilidad de no cargar ya sea una USB, portátil ó Disco Duro Externo.

Aunque los **servicios Cloud** presten un gran servicio, no debemos de dejar de lado las preocupaciones en cuanto a la seguridad de los datos, es por esto que deseamos compartir con ustedes, algunos **prácticos consejos para proteger tus datos en la nube**.

La comodidad que nos brinda este tipo de servicios **parece tentador**, pero la carga de tus datos personales a un proveedor de servicios, sin duda plantea un par de problemas de seguridad. Por un lado, nunca se puede estar seguro de que nadie mas puede acceder a tus datos. Dicho esto, siempre podemos proteger nuestros datos contra el ingreso a los datos que deberían de ser personales.

1. Los Datos En La Nube, De Forma Local

Regla **N º 1,** cuando se trata de la gestión de datos, tener siempre un respaldo es lo primordial. En términos generales, es una buena práctica crear **copias electrónicas** de cualquiera de sus datos, para que seas capaz de tener tu información a la mano en caso de perdida, borrado accidental o cualquier otro evento ajeno que pueda afectar la seguridad de tus datos. Existe una cantidad de servicios Cloud para empresas, y para usuarios que no necesiten servicios grandes, puedes usar respaldos entre estos servicios para asegurar tus datos.

Aunque es bien cierto que estos servicios nos proveen la facilidad de dejar de lados las unidades de almacenamiento de la información, no debemos de dejar totalmente de lado estos dispositivos. Como buena practica deberás de usar al menos dos dispositivos para tener tus respaldos en caso de una eventualidad.

2. Almacenar

Información Importante, Tu Ultima Opción

Este punto es algo confuso, pero vamos a ver como nos va :D Como hemos dicho, los **servicios Cloud** nos sirven para almacenar nuestros datos mas importantes, pero, ¿Que tan seguro estarán estos datos? Puede ser paranoia ó delirios de persecución, pero digamos, tienes un proyecto realmente importante, el tener estos **datos en la Cloud** no te puede asegurar que están a salvo ;)

Mi consejo es mantener sólo aquellos archivos que necesitas para **acceder con frecuencia** y evitar la poner los documentos que contienen contraseñas y en definitiva datos sensibles que no deberian ser accedido por alguien mas.

Si tiene que incluir esta información en sus archivos, asegúrese de cifrarlos antes de subirlo.

3. Usa

Servicios Que Cifren Tus Datos

Una de las manera más fácil para **proteger tu privacidad cuando utilice los servicios de almacenamiento en la nube**, es buscar uno que ofrezca el cifrado local para tus datos. Esto proporciona un nivel adicional de seguridad, ya que será necesario el descifrado antes de poder tener **acceso a los datos.**

Si bien los datos de mantenimiento de cifrados en la nube pueden ser lo suficientemente bueno, sería aún mejor si el servicio en la nube también asegura el cifrado durante las fases de carga y descarga. Esto puede hacerse usando de grado militar Advanced Encryption Standard (AES) (256 bits), como el que usa el servicio de DrivePop.

Con el paso adicional de cifrar y descifrar los datos, es posible darse cuenta de que la sincronización de sus archivos con la unidad de nube tarda un poco. Dicho esto, este es un dolor necesario que tendrás que pasar, si deseas que los documentos sean accesibles solo para tu uso personal.

4. Cifra Tus Datos Antes De Almacenarlos

El tener un servicio de almacenamiento que no cifre tus datos, no será un inconveniente para usar tal servicio, ya que podrás usar un servicio de terceros para que tu mismo cifres tus datos. Todo lo que tienes que hacer es descargar una aplicación de protección de nube que le permitirá aplicar contraseñas y generar secuencias de teclas secretas para sus archivos antes de que realmente subirlos a la nube.

Incluso si usted ya está optando por un **servicio en la nube encriptado**, no estaría de más que pasar por una ronda preliminar de cifrado para los archivos de conseguir un poco de garantía adicional.

5. Letra Pequeña,

Enemiga De La Privacidad

Además de almacenar tus datos, algunos servicios en la nube le permiten compartir sus fotos y archivos con otros usuarios. Sin duda suena bastante atractivo, pero a veces estos servicios vienen con una pequeña trampa. Puede haber alguna letra pequeña que no verás en sus Términos de Servicio (TOS) para que sea legítima.

Por ejemplo, ya en 2011, **Twitpic escribió en su TOS** que podía compartir sus fotografías en su servicio les da el derecho de «usar ó distribuir» las imágenes. Más tarde se disculparon por tal derecho que se atribuían, pero aclaro que podían seguir haciendo uso de ellos al igual que los afiliados, y aun así, los derechos de autor recaían sobre el usuario.

Aunque Twitpic no es exactamente un **servicio dedicado de almacenamiento en la nube**, presenta un buen caso para que debas ser consciente de lo que puedes esperar de tu proveedor de cloud, especialmente con respecto a sus políticas de seguridad y privacidad.

6.

Verificación De Dos Pasos, Para Estar Seguros

Como primera línea de defensa contra los usuarios maliciosos que andan en la Web, es mejor asegurar tu contraseña para que pueda **soportar un intento de hacking o cracking**. Hay un montón de consejos en Internet sobre lo que puedes hacer para tener una buena contraseña.

Como alternativa, puedes hacer uso de la verificación de dos pasos para el inicio de sesión si tu servicio en la nube ofrece la opción. En el caso de Google Drive, los usuarios tienen que iniciar sesión en su cuenta de **Google** en primer lugar con el fin de usar el **servicio de almacenamiento en la nube**. La **verificación de dos pasos** se puede activar para las cuentas de Google, un código de verificación será enviado al teléfono móvil, con el cual podrás verificar que eres tu, cuando se trata de acceder a tus datos.

7. Cuidado Donde Navegas

A veces, la **seguridad para proteger tus datos en la nube** depende de lo que haces en la web, sobre todo en equipos ó conexiones públicas. Cuando se utiliza un equipo público, y almacenas tu contraseña por accidente, le habrás dado el poder a otra persona para ingresar y manipular los datos que tan precavidamente has guardado en la nube.

¿Tiendes a conectar tu dispositivo a puntos de acceso Wi-Fi abiertos y no garantizados en lugares públicos para acceder a tus cuentas? Tales conexiones no se cifran, lo que significa que todo lo que hagas mientras estás conectado puede ser «rastreado» por un hacker en la misma red.

8. Asegurar Tu PC, Dá Mas Seguridad A Tus Datos

Puede que estés usando un proveedor de **servicio Cloud bastante seguro**, pero a veces el eslabón más débil resulta ser el Sistema Operativo del usuario que se está conectando. Sin la protección adecuada para su sistema, te expones a bugs y virus que proporcionan puntos de penetración a piratas informáticos para acceder a tu cuenta.

Tomemos por ejemplo la presencia de un Keylogger troyano que intenta realizar un seguimiento de todas las pulsaciones del teclado. Al incorporar este software malicioso aparentemente como un archivo legítimo, los hackers podrán hacerse con su nombre de usuario y contraseña si el sistema no está lo suficientemente protegido para detectarlo.

Finalmente

Las anteriores solo son medidas de seguridad que debemos tener, en anteriores artículos hemos hablado bastante sobre el Ataque de Hombre en el Medio ó MITM según sus siglas en ingles. ¿Añadirías algún otro consejo para proteger los datos que se almacenan en un servicio Cloud? Compártelo en un comentario.