(https://www.welivesecurity.com/la-es/) (https://www.eset.com)

6 formas de hacer backup de tu información

USB, Time Machine, discos externos, la nube... hay muchas opciones para quienes estén buscando hacer backup de los datos, y todas tienen pros y contras.



(https://www.welivesecurity.com/la-es/author/staffwriter/)
Alan Martin (https://www.welivesecurity.com/la-es/author/staffwriter/)

Hoy es el Día Internacional del Backup y ya vimos una interesante infografía (/la-es/2015/03/31/deberias-hacer-copia-de-backup/) que te ayudará a determinar en qué casos debes hacer copias de respaldo de tus archivos. De más está decir que esta es una práctica importante para llevar adelante a modo de hábito.

No solo tiene sentido en caso de que tu *laptop* sea robada, o tu disco rígido falle, sino también si tu computadora se infecta con *ransomware* (/la-es/2014/06/10/todo-sobre-ransomware-guia-basica-preguntas-frecuentes/). Este es un tipo particularmente desagradable de *malware* que cifra tus archivos y amenenaza con borrarlos si no pagas un

rescate en un cierto período de tiempo. ESET recomienda no pagar (/la-es/2013/10/29/no-pagues-como-evitar-combatir-amenazas-ransomware/) por muchos motivos, tanto éticos como prácticos -y además de que te marcarías como un posible objetivo de futuros ataques. Pero si tus archivos están respaldados en forma segura, ni siquiera te sentirás tentado de negociar en primer lugar.

Hay muchas opciones disponibles para quienes estén buscando hacer copias de seguridad de los datos, y todas tienen pros y contras. Aquí hay algunas opciones, pero recuerda: es mejor tener más de un backup para estar seguro.

1. Dispositivo USB



Pequeños, económicos y convenientes, los dispositivos USB están en todos lados, y su portabilidad significa que son fáciles de guardar en forma segura, pero al mismo tiempo fáciles de perder. Hay interrogantes en relación al número de ciclos de lectura y escritura que pueden realizar, por lo que deberían ser considerados junto a otros métodos de backup.

(https://www.welivesecurity.com/la-es/) (https://www.welivesecurity.com/la-es/)

Pros:

+ Sumamente portátil

+ Muy económico

+ Puede transferir datos fácilmente

Contras:

– La portabilidad significa que son pequeños y fáciles de perder

–Preguntas sobre duración de ciclos de lectura y escritura

2. Disco externo

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)



Los discos duros externos, justamente, viven fuera de tu computadora, lo que significa que pueden ser conectados a otras fuentes. Si se usan para backup, es mejor no usarlos como dispositivos de cabecera para copias diarias.

Pros:

+ Relativamente económico

+ Mucho espacio para almacenar grandes archivos

Contras:

– Potencialmente abierto a problemas que hicieron perder los archivos en primer lugar (un corte de electricidad o *malware*)

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)

3. Time Machine



Para los usuarios de Mac, Time Machine es una opción que hace backup automático a discos externos. Apple vende su propia marca de Time Capsules (http://es.wikipedia.org/wiki/Time_Capsule) inalámbricos, pero puedes usar cualquier otro. Con este método, se harán copias de respaldo cada hora en forma automática para el último día, y cada día para el último mes, y luego semanales hasta que la máquina esté llena.

Pros:

+ Automatizado, por lo que no te olvidarás de estar al día

+ Por la frecuencia de los backups, nunca deberías estar atrasado

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)

+ Respalda todo el disco, no solo los archivos importantes

Contras:

– La máquina inalámbrica dedicada es costosa

– Solo para Mac

4. NAS (Network-attached storage)



Las organizaciones tienden a hacer backup de sus archivos en redes en las que se comparte la capacidad de almacenamiento de un servidor (tecnología llamada NAS (http://es.wikipedia.org/wiki/Network-attached_storage)). Pero con más y más

hogares teniendo múltiples computadoras, la idea tiene cierto atractivo en niveles hogareños, especialmente para aquellos que buscan guardar archivos de más de una fuente.

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)

Con los precios bajando, una solución de almacenamiento inalámbrico dedicada es una opción conveniente que requiere menos análisis.

Pros:

+ Los backups automáticos no se interrumpirán por que te olvides

+ Las soluciones inalámbricas también funcionan en teléfonos y tablets

Contras:

– Puede ser costoso

– Puede ser incómodo para configurar y mantener

5. Almacenamiento en la nube



Si bien la opción anterior es, en escencia, tu propio servidor en la nube, hay muchas otras opciones de terceras partes: gratuitas, de pago, o gratuitas con extras pagos. iCloud, Dropbox, Google Drive y OneDrive son conocidos, pero hay otros disponibles.

Pros:

+ Puede hacerse automáticamente

+ Cierta cantidad de espacio es usualmente gratuita

+ Recomendable para los que no confíen en dispositivos físicos

Contras:

– Requiere una conexión a Internet para funcionar

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)

– No puedes dar cuenta de las brechas de seguridad

– Las compañías no están obligadas a mantener estos servicios activos

6. Imprimir



A primera vista, puede sonarte chistoso. A pesar de ser considerablemente menos avanzadas técnicamente, las impresoras te ofrecen una copia dura de tus documentos más importantes, la cual

sobrevivirá cortes de suministro eléctrico y será fácil de guardar, con acceso rápido aunque la computadora esté fuera de servicio por unos días.

Claro que es difícil guardar archivos de esta forma hoy en día, y no funciona para video o audio, pero para esa novela que te devastaría perder, vale la pena cosiderarla.

Pros:

+ Un backup que no se verá afectado por problemas técnicos

+ Acceso imposible para los cibercriminales

Contras:

– Imposible para ciertos tipos de archivos

– Incómodo de manejar

– Menos práctico para documentos largos

– No amigable con el medio ambiente

Sin importar cómo decidas hacer backup de tus datos, es importante que lo hagas -y que consideres usar más de una opción al menos para tus archivos más sensibles.

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)

Los usuarios no piensan muy seguido es qué pasaría si se perdieran sus archivos valiosos, o no lo hacen hasta que no es tarde. No cometas ese error, y usa el Día Mundial del Backup para asegurarte de que tus archivos están a salvo. Accede a nuestra Guía de Backup (/wp-content/uploads/2014/01/documento_guia_de_backup_baja.pdf) para más información y consejos para llevar adelante esta práctica.



(https://www.welivesecurity.com/wp-content/uploads/2017/03/guia-backup.pdf)

Alan Martin (https://www.welivesecurity.com/la-es/author/staffwriter/)

31 Mar 2015 - 08:12 PM

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)

Newsletter

Correo electrónico... **Enviar**

Artículos similares



(https://www.welivesecurity.com/la-es/2021/06/23/como-saber-sitio-web-es-seguro-o-no/)

Cómo saber si un sitio web es seguro (https://www.welivesecurity.com/la-es/2021/06/23/como-saber-sitio-web-es-seguro-o-no/)



(https://www.welivesecurity.com/la-es/2021/06/03/5-estafas-comunes-dirigidas-a-los-adolescentes-y-como-protegerse/)

5 estafas comunes dirigidas a los adolescentes y cómo protegerse (https://www.welivesecurity.com/la-es/2021/06/03/5-estafas-comunes-dirigidas-a-los-adolescentes-y-como-protegerse/)

Discusión

2 Comments WeLiveSecurity.com Disqus' Privacy Policy 1 Login

Recommend Tweet Share Sort by Best

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)



Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name



Erwin Osbel • a year ago

muy Buenas sugerencias

^ | v • Reply • Share ›

Yolanda • 4 years ago

En la empresa donde trabajo utilizamos Dataprius. Una solución de gestión documental, almacenamiento y trabajo directo en la nube para empresas y profesionales, que incluye para mayor seguridad de los datos un backup gratuito semanal en la nube. Además firman contratos de protección de datos.

^ | v 2 • Reply • Share ›

welivesecurity™ BY eset®

(https://www.welivesecurity.com/la-es/) (https://www.eset.com)

Inicio (/la-es)

Acerca de (https://www.welivesecurity.com/la-es/acerca-de/)

Contáctanos (https://www.welivesecurity.com/la-es/contactanos/)

Mapa del Sitio (https://www.welivesecurity.com/la-es/mapa-del-sitio/)

Investigaciones (https://www.welivesecurity.com/la-es/category/investigaciones/)

Tutoriales (https://www.welivesecurity.com/la-es/category/tutoriales/)

Categorías (https://www.welivesecurity.com/la-es/categorias-2/)

Nuestros Expertos (https://www.welivesecurity.com/la-es/nuestros-expertos/)

RSS (https://www.welivesecurity.com/la-es/configurar-rss/)

(https://www.welivesecurity.com/la-es/)

ESET (https://eset.com)

(https://www.eset.com)

Noticias (https://www.welivesecurity.com/la-es/news-widget-generator-la-es/)

Política de Privacidad (https://www.welivesecurity.com/la-es/politica-de-privacidad/)

Información Legal (https://www.welivesecurity.com/la-es/informacion-legal/)

Copyright © ESET, Todos Los Derechos Reservados