ENJOY SAFER TECHNOLOGY™

GUÍA DE

Backup

Introducción

Imagina que tienes almacenada en tu computadora información personal e irrecuperable como fotografías o trabajos para la universidad; o en el caso de los servidores corporativos, información sensible que ayuda al negocio a operar correctamente, y que cuando llega el momento en que deseas utilizar esta información importante, te das cuenta de que está inutilizable.

¿La causa? Un desperfecto en los dispositivos de almacenamiento de tu equipo como un disco duro, la interrupción del suministro eléctrico, el robo del dispositivo, o una infección por un código malicioso del tipo ransomware.

Pese a que algunos usuarios subestiman este tema y piensan que es poco probable que les suceda alguna de las situaciones mencionadas anteriormente, si se tiene en cuenta cuánto han crecido los casos de ransomware en la región ya nos da una idea del alcance de esta problemática.

Por tal razón, la presente guía tiene como objetivo ayudar a los usuarios a que puedan adoptar las medidas necesarias para resguardar información importante a través de los respaldos de datos.

Índice

¿Qué es un respaldo o backup?

Es el proceso en el que se crea una copia de los archivos importantes con el fin de poder recuperarlos en caso de una pérdida de la información. Esto es muy importante debido a que existen múltiples causas por las cuales un usuario podría experimentar este problema. Por ejemplo, la limitada vida útil de los discos duros, los robos o extravíos de los dispositivos y los ya mencionados códigos maliciosos.

Hay que tener en cuenta que los respaldos corren los mismos peligros. Por este motivo, no es recomendable que las unidades de respaldo estén conectadas a la misma red de producción todo el tiempo ya que, de esta manera, en caso de una infección de dicha red podrían verse afectados. Por otro lado, es importante que los usuarios no tengan en su poder el disco duro donde guardan el backup de su información junto con el dispositivo respaldado, puesto que de sufrir robos o extravíos también perderían su respaldo.

Códigos maliciosos y pérdida de información

Dentro de las múltiples causas por las cuales un usuario podría perder su información, se encuentran los códigos maliciosos, particularmente los del tipo **ransomware**, es decir, malware que infecta al equipo, cifra archivos y, luego, pide un rescate monetario para que el usuario pueda volver a acceder a ellos.

Esta metodología convirtió al ransomware en una de las amenazas más prolíficas de los últimos años. Actualmente, no solo encontramos casos en computadoras, sino que también atestiguamos una migración hacia equipos móviles, y hasta dispositivos bien diferentes a los informáticos, aquellos que forman parte de la Internet de las Cosas.

A raíz de esta complejización del ransomware, es vital contar con un backup, puesto que es una de las herramientas ideales para recuperar la información en el desafortunado caso de ser víctima de una infección.

¿Qué información se debe respaldar?

No toda la información posee el mismo valor, por ende, antes de comenzar con el proceso de backup, es fundamental determinar qué información será respaldada. Esto se puede lograr valorando los datos y estableciendo cuáles tienen mayor relevancia según las preferencias personales, el tipo de trabajo que se haga con dichos datos, o incluso el objetivo o utilidad que tengan.

Una consideración importante recae en establecer si el backup necesita elementos de hardware o si simplemente el recuperar los datos es suficiente. Esto se refiere a que, en algunos casos, respaldar solo los datos puede generar un esfuerzo mayor para restablecerlos, ya que la situación puede requerir, incluso, la reinstalación manual de todo un sistema operativo y sus aplicaciones.

Además, no se puede perder de vista la frecuencia con la cual se modifican los datos. Puede existir información tan dinámica y/o de uso único que seguramente no valga el esfuerzo respaldar.

Por último, no se debe olvidar hacer un respaldo de archivos de configuración y otra documentación importante que ayude a que las operaciones normales de un sistema se puedan poner en funcionamiento fácilmente. Esto se debe hacer, sobre todo, cuando se evalúan situaciones, como el posible caso de padecer un incidente que genera la pérdida de archivos de sistema.

Medios de almacenamiento

El siguiente paso consiste en elegir el medio de almacenamiento de las copias de seguridad. En este punto, el espacio físico en donde se guarde el soporte de respaldo también debe estar protegido.

Tal como se mencionó al comienzo, de nada sirve ir por la calle con una laptop y con el disco rígido externo donde está alojado el backup, ya que en el potencial caso de un robo, se perdería la información original y su copia.

Disco rígido

Es buena idea utilizar uno exclusivamente con este propósito para evitar un desgaste innecesario. Asimismo, si el disco es interno debe ser uno físicamente distinto al que se utiliza para iniciar el sistema operativo.

Dispositivo de almacenamiento USB

Es recomendable utilizar uno exclusivamente para respaldos y evitar transportarlo fuera de donde se lo guarde para evitar extravíos.

Medios ópticos (CD/DVD/ Blue-Ray)

Son más susceptibles a sufrir daños físicos como rayas que pueden corromper los datos. Se recomienda almacenar la información en más de un medio óptico por si alguno falla.

La Nube

Posee la ventaja de facilitar el acceso a la información desde prácticamente cualquier lugar con una conexión a Internet, sin embargo, es importante considerar las políticas de uso del servicio elegido y los sistemas de protección que utiliza para resguardar los datos.

Frecuencia de respaldo

Luego de haber seleccionado qué información será respaldada y el medio de almacenamiento, es importante establecer la periodicidad con la que se debe realizar la copia de seguridad.

Esta decisión debe adoptarse en base a la frecuencia con que se modifican, eliminan y crean archivos. Si se trabaja todos los días en un proyecto, será necesario realizar una copia de seguridad a diario. En el caso opuesto, una carpeta con fotos debe ser nuevamente respaldada solo cuando se agreguen fotografías.

Una vez que también está determinada la frecuencia, se puede elegir entre **3 tipos diferentes de copias de seguridad**:

Completa

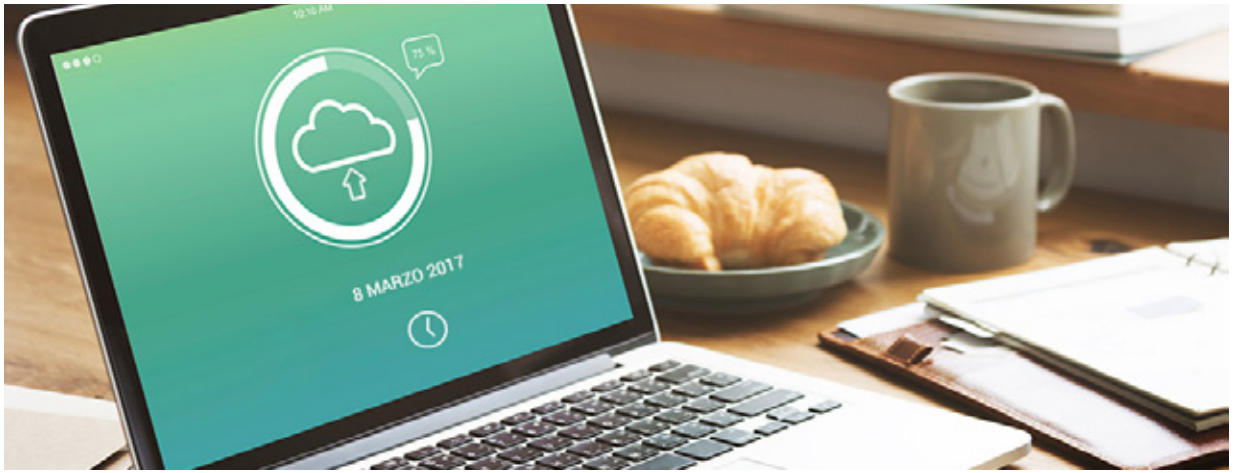
Este tipo de backup hace un respaldo completo de todos archivos del equipo. Abarca la totalidad de los datos por lo que va a llevar más tiempo y espacio de almacenamiento. Se puede elegir esta opción en un primer momento, y luego utilizar una de las siguientes opciones.

Diferencial

Contiene solamente los archivos que han cambiado en el sistema desde la última vez que se hizo una copia de seguridad completa. Son copias acumulativas, es decir que cada copia que se realiza, respalda lo que es diferente desde la última copia seguridad completa. Se recomienda cuando se establece una frecuencia diaria de backup.

Incremental

Respalda los archivos que se han modificado desde la última copia de seguridad diferencial o incremental. Una diferencia importante con respecto a las copias diferenciales es que las incrementales al hacer las copias de seguridad con menor cantidad de datos, se realizan más rápido y requiere un espacio menor de almacenamiento.



¿Se debe respaldar la información de un dispositivo móvil?

Los dispositivos móviles como teléfonos inteligentes y tabletas suelen almacenar información sensible e importante. Por este motivo, realizar copias de seguridad de estos equipos es igual de necesario que con las computadoras, sobre todo al considerar que se utilizan para manejar información igual de crítica.

Existe la posibilidad de respaldar manualmente dichos archivos conectando el dispositivo a una computadora. También se pueden utilizar servicios de almacenamiento en la Nube como iCloud en iPhone y una cuenta de Google en el caso de Android.

Cómo respaldar en distintos sistemas operativos

Windows

Si necesitamos respaldar la información personal en nuestras computadoras, el sistema operativo de Microsoft desde la versión Windows 7 ha incorporado una herramienta nativa que permite crear copias de seguridad de los archivos personales.

Para acceder a este recurso se debe ingresar al Panel de Control, luego hacer clic en la opción de Sistema y mantenimiento, y por último ingresar en Copias de seguridad y restauración. Asimismo, a partir de Windows 8 se incluyó una característica de respaldo denominada Historial de Archivos. Activando esta opción, el sistema mantiene una copia de los archivos personales del usuario que se encuentren almacenados en el escritorio, las librerías de archivos y contactos, entre otros.

Para acceder a este recurso se debe buscar Historial de archivos en el menú Inicio. Luego ingresar en Configuración y, por último, hacer clic en la opción Historial de archivos para activarla.

Para más información, se puede ingresar al sitio de **Soporte de Microsoft.**

macOS

A partir de la versión 10.5, el sistema operativo de Apple cuenta con una herramienta denominada Time Machine que permite crear copias de seguridad y restaurarlas en caso de ser necesario. Para acceder a este recurso se debe insertar un medio de almacenamiento externo USB u otro y macOS automáticamente le preguntará al usuario si desea utilizarlo con Time Machine. Si no, también es posible configurar esta aplicación de forma manual.

Para acceder a este recurso manualmente se debe ir a la Utilidad de Discos, seleccionar el disco a utilizar, hacer clic en la pestaña borrar y, por último, abrir las preferencias de Time Machine en Preferencias del Sistema.

Se puede encontrar más información en el sitio de **Soporte de Apple.**

¿Qué características debe tener una aplicación de backup óptima?

Algunos usuarios podrían requerir de otro software de respaldo por necesidades particulares que los aplicativos nativos no pueden ofrecer. Por ello, a continuación, se mencionan cinco características a considerar en la elección de programas de este tipo:

- ✓ Que ofrezca la posibilidad de seleccionar manualmente la información a respaldar.
- ✓ Que permita crear una imagen del equipo para poder restaurar el sistema operativo, los programas y archivos de forma completa desde un disco de arranque.
- ✓ Que se pueda establecer una contraseña de protección para acceder a los datos y que cifre la información.
- ✓ Que comprima los archivos copiados para ahorrar espacio de almacenamiento.
- ✓ Que permita seleccionar la frecuencia de respaldo de los archivos.

Antivirus + Backup: dos soluciones complementarias

Es importante considerar que un programa para respaldar información es complementario a una solución de seguridad, por lo tanto, ninguno reemplaza al otro.

Un software antivirus permite proteger la computadora de las amenazas informáticas y, así, evitar infecciones con ransomware, por nombrar un caso, que cifren la información.

Por otro lado, una solución de backup permite mantener una copia de seguridad de la información para poder restaurarla ante cualquier inconveniente, tal como se vio en esta guía.

Al cumplir objetivos distintos y complementarios, la recomendación es implementar ambos programas para lograr un nivel de protección óptimo.

Conclusión

La información es uno de los activos más importantes para las empresas y las personas, por lo tanto, realizar respaldos periódicos es una tarea que debe considerarse prioritaria y en ningún caso hay que subestimarla. Esto se debe, principalmente, a las múltiples causas por las que podría ocurrir una situación de pérdida de información.

Para garantizar la seguridad de tu información recuerda realizar este procedimiento de la forma correcta, es decir, considerando la información a resguardar, los tipos de respaldos existentes, los medios de almacenamiento y la frecuencia de los procesos.


ENJOY SAFER
TECHNOLOGY™