VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Septiembre 2013

Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

En esta edición...

Copias de seguridad y recuperación personal

Visión general

Hacer copias de seguridad es una de las medidas más importantes que debes tomar en cuenta para proteger tu información. Éstas permiten que recuperes datos cuando algo va mal, como fallas en el disco duro, eliminación accidental de archivos, dispositivos robados o extraviados, o infección por malware. En este número encontrarás los criterios para realizar copias de seguridad de información y la manera de desarrollar una estrategia adecuada para ti.

Editor Invitado

El Dr. Eric Cole es el editor invitado para esta edición. Es un experto reconocido por la industria de la seguridad. Es autor de varios libros. Entre otros, el Dr. Cole escribió “Advanced Persistent Threat, Hackers Beware y Network Security Bible”. También es fundador de Secure Anchor Consulting, miembro del profesorado del SANS y autor de varios cursos. Encuentra al Dr. Cole en **www.securityhaven.com** o en Twitter: **@drericcole**.

¿Qué incluir y cuándo hacerla?

Hay dos enfoques básicos para decidir qué incluir en la copia de seguridad: el primero consiste en elegir los datos específicos que sean importantes, tales debe incluirse, imágenes o videos; el segundo incluye todo, es decir, el sistema operativo y todos los programas que has instalado, además de tus datos exclusivos. El primer enfoque simplifica el proceso de la copia de seguridad, sin embargo, el segundo es más simple y fiable si se tiene que recuperar de un fallo completo del sistema. Si no estás seguro de qué incluir en la copia de seguridad, entonces haz una copia general.

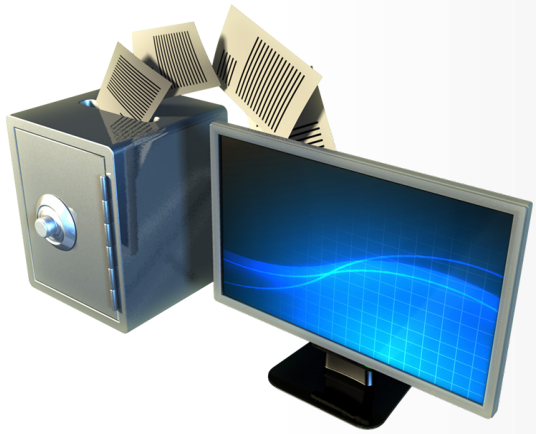
Después, tendrás que decidir con qué frecuencia realizarás las copias de seguridad. Puedes hacerlas cada hora, diario, semanalmente, etc. En el hogar, los programas de copia de seguridad personal, como Time Machine de Apple o Respaldos y Recuperación de Microsoft Windows, pueden crear copias de seguridad simples y automáticas, es decir puedes “configurarlas y olvidarte de realizarlas”. Estas soluciones realizan una copia de seguridad silenciosa de tus datos mientras trabajas o te encuentras lejos de tu computadora. Otras soluciones ofrecen “protección continua” en la que los archivos nuevos o modificados se copian inmediatamente tan pronto como se cierran.

¿Cómo hacer una copia de seguridad?

En general, hay dos maneras de realizar copias de seguridad: una es utilizando medios físicos; y la otra, empleando almacenamiento basado en la nube. Los medios físicos incluyen DVD, memorias USB o discos duros externos. Al utilizar las copias de seguridad físicas, asegúrate de no hacer una copia de seguridad en el mismo dispositivo que contiene los archivos originales, además, etiqueta tus medios externos para que puedas

Copias de seguridad y recuperación personal

identificar fácilmente una copia de seguridad de una fecha y hora determinadas. La ventaja de los medios físicos para copias de seguridad y recuperación es que son mucho más rápidos. La desventaja es, que si se ubican en donde tal vez ocurra un desastre (como un incendio), no solo perderás tu computadora, sino las copias de seguridad. Como tal, debes tener un plan de contingencia para almacenar copias de la copia de seguridad fuera del sitio. Al almacenarlas fuera del sitio, no olvides cifrarlas, pues de esa manera si se pierden o se roban los datos, estos aún estarán protegidos. Si cifras las copias de seguridad, almacena de forma segura las contraseñas, para que no se pierdan u olviden con el tiempo.



Usa la verificación en dos pasos siempre que sea posible, es una solución mucho más segura que usar solo contraseñas.

Las soluciones basadas en la nube son diferentes, este es un servicio donde los archivos se almacenan en la nube (en alguna parte de Internet). Dependiendo de la cantidad de información que desees respaldar, el servicio podría ser de paga. La acción consiste en instalar un programa en tu computadora que automáticamente sube las copias de seguridad. La ventaja es que no tienes que preocuparte por el almacenamiento de archivos, pues esta solución se adapta conforme a tu necesidad. La desventaja es que las copias de seguridad basadas en la nube (y su recuperación) pueden ser mucho más lentas, especialmente si tienes una gran cantidad de información.

Tampoco olvides hacer copias de seguridad de los dispositivos móviles. Mientras que la mayoría de la información en el dispositivo móvil ya está almacenada en la nube, como por ejemplo, el correo electrónico o los eventos del calendario, algunos de los datos del dispositivo móvil son únicos, como fotos o videos que hayas tomado recientemente. Un iPhone o iPad puede realizar copias de seguridad de cualquier computadora que tenga instalado iTunes o iCloud de Apple. Para Android u otros tipos de dispositivos móviles, las opciones de copia de seguridad dependen del fabricante o del proveedor del servicio. En algunos casos puede que tengas que comprar aplicaciones móviles diseñadas específicamente para las copias de seguridad.

Recuperación

La copia de seguridad de información es sólo la mitad de la batalla, hay que estar seguro de que puede recuperarse. Revisa mensualmente que el programa de copia de seguridad está funcionando. Si no es así, trata de recuperar un archivo y verificar su contenido. Además, asegúrate de hacer una copia de seguridad del todo sistema antes de una actualización importante (como moverse a un equipo nuevo) o una reparación mayor (como el reemplazo de una unidad de disco duro) y comprueba que se puede restaurar.

Copias de seguridad y recuperación personal

Puntos clave

- Automatiza el proceso de copia de seguridad tanto como sea posible, pero comprueba que funciona correctamente.
- Al reconstruir un sistema completo desde la copia de seguridad, asegúrate de volver a aplicar los últimos parches de seguridad y actualizaciones antes de ponerlo de nuevo en servicio.
- Las copias de seguridad de fechas anteriores u obsoletas pueden convertirse en un riesgo, y deben ser destruidas con el fin de evitar que usuarios no autorizados accedan a ellas.
- Si estás utilizando una solución en la nube, investiga las políticas y la reputación de la organización y cerciórate de que cumplen con tus requisitos. Por ejemplo, ¿Se cifran los datos cuando se almacenan? ¿Quién tiene acceso a las copias de seguridad? ¿Son compatibles con la autenticación fuerte?
- El método más seguro para realizar copias de seguridad de información es combinando ambos medios, físicos y de servicios en la nube.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Recursos

Apple Time Machine:	https://support.apple.com/kb/HT1427?viewlocale=es_ES
Windows 7 Backup and Restore:	http://windows.microsoft.com/es-xl/windows7/products/features/backup-and-restore
Cloud Backup:	http://www.arkeia.com/es/solutions/backup-to-cloud
Cloud Backup Services:	http://www.rackspace.com/es/cloud/backup/
Backup Apps for Android:	http://bitelia.com/2013/04/aplicaciones-copias-de-seguridad-de-android

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Sarahí Díaz, Pedro Guerrero, Nora Cozaya