# PREVENIR ES SALUD – CUIDE SU INFORMACIÓN

Javier García Gómez

El presente artículo tiene como objetivo crear conciencia entre los usuarios de equipo de cómputo sobre la importancia de realizar respaldos de información periódicamente. Además pretende dar a conocer algunos aspectos para prevenir la pérdida de datos.

Utilizar un adecuado esquema de seguridad para mantener a salvo la información le ahorrará un buen dolor de cabeza y muchas horas de trabajo. Alguna vez se ha preguntado ¿Qué pasaría si perdiera todos los documentos, imágenes, archivos que lleva almacenando durante mucho tiempo en la computadora portátil o de escritorio? ó tal vez ya le sucedió.

Imagine un día en el que enciende su equipo de cómputo y se tarda mucho tiempo en cargar el sistema operativo y se vuelve lento muy lento, sorpresa su equipo esta infectado por un virus. ¿Qué es en lo primero que piensa? ¡MI INFORMACIÓN!, si corre con buena fortuna y el virus aún no hace de las suyas tendrá oportunidad de rescatar algo; pero suponga que ya no enciende, que por azares del destino el disco duro sufre un daño (falla más común en los equipos de cómputo) y simplemente ya no tiene acceso a la carpeta “Mis documentos” no hay manera de recuperarlos ¡Oh por Dios me quiero morir! mi proyecto de Tesis para maestría, mi agenda, entre otras cosas.

Los equipos son traicioneros y no por nuevos y caros están exentos de sufrir una falla o descompostura. No ponga en riesgo su información considere que son horas de mucho trabajo y dedicación y que igual como se cuida el dinero guardándolo en bancos o cajas de seguridad y no atesorándolo debajo del colchón o enterrándolo; sus archivos deben mantenerse bien seguros. Día con día la información esta más expuesta ya que cada vez es mayor el número de equipos conectados a Internet, accesos a redes inalámbricas, el intercambio de datos con dispositivos como teléfonos celulares, computadoras de mano o la conexión de memorias USB y el uso de cualquier dispositivo de almacenamiento la hacen más vulnerable.

Internet, hoy por hoy es el medio de propagación más frecuente de programas dañinos como los “virus informáticos”, es casi común el mantener una conexión a este servicio y para entrar a esta carretera denominada www se debe proteger, asegurar bien las puertas del auto e instalar una alarma anti-asalto (antivirus), dar un mantenimiento periódico al automóvil (actualizaciones de sistema operativo y programas) y no olvide colocarse el cinturón de seguridad (respalde sus archivos) le puede salvar la vida.

## 1. ¿Qué hacer para prevenir esta situación?

### 1.1. *Proteger el equipo con una herramienta antivirus*

Virus, troyanos y gusanos ¿suena familiar?, cualquiera que pase un cierto tiempo en Internet o intercambie archivos con otras personas está expuesto al ataque de un usuario malicioso (hacker) o a ser infectado por uno de estos programas maliciosos; para protegerse debe obtener un buen software anti-virus, mucha gente lo tiene pero lo más importante es mantenerlo actualizado y realizar un escaneo periódico. Existe una gran oferta en el mercado de productos muy completos e interesantes. Normalmente podrá descargar una versión de prueba gratuita por treinta días; cada uno de ellos tiene sus pros y sus contras, pero la mayoría están homologados por los estándares establecidos por la comunidad internacional y poseen una sólida reputación en cuanto a calidad y fiabilidad.

Estás son páginas de los principales desarrolladores de programas anti-virus; en ellas encontrará a detalle la forma de instalación, actualización e información general.

`www.symantec.com` `www.hauri.com` `www.pandasoftware.es` `www.macafee.com`

### 1.2. *Actualizar periódicamente el sistema operativo y las aplicaciones*

Los hackers o programadores maliciosos se dedican al análisis de los sistemas operativos y aplicaciones para encontrar las vulnerabilidades que estos presentan (errores de programación) y explotarlas creando virus informáticos. Es por ello que los programadores de empresas desarrolladoras de software se dedican a corregir estas vulnerabilidades y a emitir parches o programas que eliminen los problemas.

La empresa de software Microsoft número uno en ventas, tiene en su portal `www.microsoft.com` una opción para realizar actualizaciones de seguridad tanto para aplicaciones como sistemas operativos; ahí explican paso a paso las acciones a seguir para mantener su equipo al día.

Todos los sistemas operativos Windows tienen una opción llamada Windows Update (actualizaciones automáticas) al hacer clic en esta nos enlaza a una página de Internet que analiza el equipo e indica las actualizaciones pendientes, ahí se puede decidir si se realizan o no.

Todas las empresas desarrolladoras de software emiten boletines en sus portales web o cuentan con un área para descargar actualizaciones de seguridad o parches.

### 1.3. *Lo más importante respaldar*

No deje las copias de seguridad para luego, un archivo de copia de seguridad actualizado puede salvar su actividad productiva. Su información es vital, pero también frágil. Recuerde las primeras líneas de este artículo, el bloqueo de un disco duro, un virus o un desastre natural podría provocar en un instante la pérdida de toda su información.

Puede crear fácilmente un archivo de copia de seguridad de modo que sea posible restaurar información crítica. No obstante, también requiere planeación y un esfuerzo constante.

1. Decida qué hay que guardar. El primer paso consiste en decidir qué datos deben protegerse. Probablemente no será necesario que haga una copia de seguridad de ninguno de sus programas o aplicaciones, estos los puede reinstalar con el juego de medios que le entregaron cuando los adquirió. Lo que tiene que preocuparle es todo aquello que genere. Esto incluiría:
   - Información de contacto de clientes, proveedores, amistades, etc.
   - Hojas de cálculo.
   - Documentos, como la tesis, notas, documentos de trabajo y todo lo relacionado con su actividad productiva.
   - Correo electrónico; sobre todo, mensajes que contienen datos importantes.
   - Cualquier otro dato cuya pérdida pueda suponer un serio contratiempo.
2. Antes de seguir adelante, asegúrese de contar con una lista de carpetas que contienen archivos de los que debe realizar una copia de seguridad. (Copia de seguridad y recuperación de datos)
3. Uso de software de copia de seguridad. Ahora que sabe lo que necesita guardar, deberá empezar a realizar copias de seguridad con regularidad. Aunque es posible realizar copias de seguridad copiando manualmente archivos importantes, el proceso puede resultar laborioso si hay muchos archivos o carpetas. Existen programas dentro del mismo sistema operativo que ayudan a la realización de copias de seguridad.
4. Conozca las opciones de almacenamiento. Las herramientas de copia de seguridad crearán un archivo con todos los documentos importantes, pero tendrá que indicar dónde debe guardarse ese archivo. De forma predeterminada, deseará guardar ese archivo en un disquete, pero si hay mucha información, quizá necesite docenas o, incluso, centenares de discos. Otra opción sería guardar la copia de seguridad en alguna ubicación de la red o en una segunda unidad de disco duro del equipo. Aunque este tipo de copias de seguridad proporciona protección en caso de error del disco duro o por infección de virus, si se produce un incendio o un desastre natural, es posible que pierda el equipo y, por lo tanto, todos los datos. Por ese motivo debe copiar periódicamente su archivo de copia de seguridad en un CD, un DVD o una unidad externa que pueda almacenar en una ubicación protegida, lejos del lugar de trabajo.
5. Aténgase a un calendario. No olvide que la seguridad de los datos está determinada por la última copia de seguridad. Haga respaldos periódicos.
6. Practique la restauración de datos. Lo ideal es que no se vea nunca en la necesidad de utilizar una copia de seguridad, pero es bueno saber que la restauración de los datos exige poco más

esfuerzo del que supuso realizar las copias. Las copias de seguridad constituyen un excelente seguro contra desastres y errores del sistema, pero sólo si se dedica el tiempo necesario a realizar copias periódicas del sistema.