

Computadora, información y ¿pérdida?

Cuando la información se pierde

*Por Yves Godbout, CA-IT.



Es un hecho. Estamos usando las Computadoras Personales (PCs) más que nunca y tenemos muchos datos almacenados en ellas. Considerando el número de computadoras robadas diariamente, toda esa información puede estar comprometida.

Según los analistas, la información personal tiene más valor que la programación. Tomamos toda clase de precauciones para poder proteger los datos en nuestras PCs; aplicamos actualizaciones de

seguridad y usamos programación antivirus y antiespionaje. Una PC bien protegida puede casi asegurar que nadie tenga acceso a nuestros datos, a menos que tenga acceso físico a nuestro equipo. Cada año miles de PCs se pierden o son robadas. Aunque el blanco primario es usualmente una computadora portátil (laptop), las computadoras de escritorio, en el hogar o la oficina, pueden también ser atractivas para los ladrones. En vista de que llevamos las llamadas laptops a todas partes son más vulnerables al robo.

El valor económico del equipo de una PC puede ser significativo si usted tiene una máquina nueva de alto rendimiento, pero ésta, quizá, no sea la razón única por la cual un ladrón

Hay formas de protegerse de responsabilidades con sus clientes, así como también contra robos o abusos. Todas las PCs deberían tener un mecanismo para protegerlas contra pérdidas.

se fije en su equipo; la información que contiene puede ser más atractiva, dependiendo del calibre del ladrón.

Considere los datos que puede tener su PC:

- ⊗ Información personal: de tarjetas de crédito, cuentas bancarias, contraseñas basadas en Internet.
- ⊗ Información personal de amigos o familiares: nombres, direcciones, fechas de nacimientos.
- ⊗ Datos personales de clientes: nombres, direcciones, números de teléfonos, números de seguridad social.
- ⊗ Información confidencial de clientes: de negocios, archivos de auditoría e información fiscal.

Aunque la pérdida del equipo es una molestia, especialmente si usted no tiene respaldo, puede reemplazarse. El seguro del domicilio o del negocio probablemente cubra el costo del equipo en caso de tal pérdida. Pero el robo de información es mucho más intimidante. Además de exponerlo a usted o a sus clientes a pérdidas enormes, también podría usted estar valorando la ley de protección de información personal de Canadá y la ley de protección de documentos electrónicos que protege la información personal colectada electrónicamente.

Hay cientos de casos de pérdida de información o historias de horror de robos. (Un listado de algunos de ellos y enlaces adicionales se puede ver en www.CAmagazine.com/technology/lostnews). Existen servicios para ayudarle a recuperar su PC. Algunos usan programación para avisarle al propietario de la PC sobre su paradero cuando es extraviada o robada, tan pronto como se establece una conexión a Internet. Tales productos incluyen *Computrace de Absolute Software* o *PC Home Home de Brigadoon*.

Pero la recuperación del equipo es sólo parte de la solución. Los ladrones sofisticados están buscando la información y no el equipo. De acuerdo con los expertos, el valor de la información personal básica como el nombre, la dirección, fecha de nacimiento y el número del seguro vale aproximadamente 20 dólares en el mercado negro. Imagine lo que puede valer la laptop de un corredor de seguros. Si usted piensa que *Windows Security* es todo lo que necesita para proteger su información, especialmente con sistemas operativos seguros tales como *Windows*

XP o *Vista*, está equivocado. La información puede leerse si el ladrón tiene el equipo y la programación adecuada.

Hace pocas semanas, la hija de un amigo olvidó su contraseña Windows y su tarea escolar universitaria estaba en la computadora, y no había forma de obtener esa información en ese momento. Todo lo que necesitó fue llamarme. Me aparecí con unos pocos CDs, pusimos a trabajar la computadora con un sistema operativo basado en *Linux*, recuperamos el archivo y lo escribimos en un disco USB. Ella quedó sorprendida.

Pero eso no fue todo. Trabajamos con un CD nuevo y cambiamos la contraseña del administrador dentro de Windows. Entonces fue capaz de usar la PC como lo había hecho antes e incluso podría haber hecho su trabajo si le hubieran robado la PC, ya que toda la información estaba clara y disponible.

Hay formas de protegerse de responsabilidades con sus clientes, así como también contra robos o abusos. Todas las PCs deberían tener un mecanismo para protegerlas contra pérdidas.

Hay varias formas de proteger su información:

- ⊗ Contraseña para conectar las computadoras. Podemos odiar las contraseñas, pero son una forma efectiva de neutralizar a un ladrón de PCs. Si una máquina es robada, queda virtualmente inútil a menos que el ladrón tenga acceso a la información contenida en una contraseña maestra o pueda ponerse en contacto con apoyo técnico del fabricante.

En muchos casos un ladrón que sólo está buscando tener la máquina, se cansará y la tirará a menos que tenga la contraseña para conectarla. Sin embargo, si el ladrón es también un ladrón de datos, simplemente puede remover el disco duro e instalarlo en otro sistema haciendo que toda la información esté disponible. ⊗ Técnicas y aparatos de identificación por biometría. Estas son muy efectivas porque garantizan que los usuarios sean quienes dicen que son, pero estas técnicas tienen el mismo problema que las contraseñas para conectar: Un ladrón podría remover el disco duro, instalarlo en otro sistema y acceder a la información. ▶▶

⦿ No existe información en la PC. Aunque puede parecer radical, es posible almacenar la mayor parte de la información en discos flash USB, disco duros portátiles USB o tarjetas SD. Sin embargo, esto no protege completamente los datos, ya que el aparato de la información podría fallar o perderse o ser robado, resultando otra vez en pérdida de la información.

Igualmente, si los datos no están protegidos, pueden leerse en otra PC. También puede usted usar una computadora de escritorio o *Citrix* para acceder a sus datos, pero esto no resulta siempre práctico para las personas que viajan.

⦿ Codificación de archivo. Puede elegir codificar toda la información sensible. Esto es efectivo para proteger la información, pero es un proceso manual que puede resultar engorroso. Igualmente, sus aplicaciones quizá no soporten la codificación de los archivos y usted tendría que codificar todos los archivos para conservarlos. Otro problema es que si aun el archivo está codificado, a menos que tome medidas especiales, la “huella” de su archivo original puede quedar en su disco duro o en un espacio de archivo temporal.

⦿ Codificación del sistema de archivos. Comenzando con Windows 2000, Windows ha proporcionado el sistema de codificación de archivos, *EFS*. Simplemente archive su carpeta *My Documents* y cualquier otro archivo que usted guarde ahí será codificado.

Sin embargo, si alguien tiene el equipo adecuado, puede cambiar su contraseña y ganará acceso a todos los datos. Igualmente, el *EFS* puede causar problemas si usted está enviando adjuntos por correos, use equipo especial para almacenar archivos en discos de la red (*network*). Así, podrá terminar con datos tan seguros que ni usted, ni sus colegas, leerán.

⦿ Codificación del disco. Con codificación completa del disco nadie puede ganar acceso a los datos sin tener acceso a la contraseña y a la clave de codificación. Las soluciones de calidad actualmente en el mercado proporcionan algoritmos de codificación que no pueden ser fácilmente violados y la mayor parte son aprobados para su uso por el Departamento de Defensa de los Estados Unidos de América.

Los productos más recientes proporcionan fuerte autenticación usando el Módulo de Plataforma confiable (*TPM*)1.2., que es un microprocesador incrustado en la PC y es exclusivo para esa máquina. Si su computadora es robada, la información no puede accederse moviendo el disco a otra máquina y usando herramientas de programación, ya que los datos y las claves de codificación forman parte de la máquina específica.

Hay fabricantes para este tipo de codificaciones, la mayor parte tiene muy buenas credenciales y productos sólidos.

Microsoft tiene un producto que maneja codificación en volumen completo en Vista, *BitLocker* que proporciona codificación de disco completo y está disponible en *Windows Vista Ultimate* y *Windows Vista Enterprise*; no está disponible en Windows XP.

También hay otros fabricantes en el mercado. WinMagic, compañía canadiense, tiene un producto llamado *SecureDoc*, que codifica discos, así como también medios removibles. Su producto es robusto y el módulo administrativo ayuda con los movimientos del negocio y la administración clave. Otros nombres bien conocidos en codificación de discos son *PointSec* para PC y *Ultimaco's SafeGuard Easy*.

⦿ Codificación en disco duro. Un fabricante importante de discos duros, *Scagate* vende un disco duro para anotaciones llamado *Momentum * 5400 FDE.2*. Estos discos están basados en la computadora y son productos de codificación en disco completo que ofrecen protección avanzada de datos al personal y usuarios corporativos de laptops. La codificación está lanzada a la máquina pero todo se hace por el disco mismo. Usa *TPM 1,2* y codificación *AES*.

Usted no puede permitirse la pérdida. No puede arriesgar datos comprometedores. Hay soluciones efectivas para asegurar que la información esté segura. Es algo de sentido en los negocios proteger los datos inteligentemente. ❁

Valor estimado de la información personal (en dólares)

Dirección	0.50
Código Postal	0.50
Dirección anterior	9.95
Fecha de nacimiento	2.50
Número teléfono publicado	0.25
Número teléfono no publicado	17.50
Número teléfono celular	10.00
Lista nombres de familiares	3.00
Número del Seguro Social Norteamericano	8.00
Información Licencia de Manejo	3.00
Información Registro Vehículo	3.00

Fuente: Calculador data Swipe y GeekZone.

Texto original: What have you got to lose? CA Magazine Agosto 2007. Traducción para el Colegio de Contadores Públicos de México por Antonio Berges Carus.

*Por Yves Godbout, Preside la CICA Alliance for Excellence Information Technology.