Cómo eliminar toda tu información personal de tu computadora (formatear no basta)

¿Sabías que formatear no es la solución definitiva para borrar todos tus datos?

BBC MUNDO.- A la hora de vender, prestar o reciclar una computadora que ya no utilizas, es fácil pasar por alto todos los datos personales que permanecen almacenados en ella.

Uno podría pensar que formatear la máquina es suficiente para eliminar para siempre esa información. Sin embargo, muchas veces los datos se quedan guardados en la memoria, y en ocasiones terminan en la red oscura, a disposición de hackers

malintencionados.

Según un estudio publicado este martes por la firma de software estadounidense Rapid7, hay mucha información privada que permanece en los aparatos tecnológicos que se donan.

“Para comprobarlo, estuve seis meses extrayendo todos los datos que pude de los dispositivos disponibles en empresas que venden computadoras restauradas o aceptan artículos donados para venderlos luego de, supuestamente, haber borrado los datos”, explicó Josh Frantz, consultor de seguridad de la compañía.

Pasaportes, tarjetas de crédito y mucho más
“Al final del experimento, esta investigación reveló que muchas de esas empresas no cumplen con su garantía de borrar los datos de los dispositivos que la gente les entrega”.

La información personal puede ser muy valiosa. Frantz cuenta que pudo averiguar cosas como direcciones de email: fechas de nacimiento, números de seguridad social, tarjetas de crédito, licencias de conducir o números de pasaporte.

Las tarjetas de crédito y los pasaportes provenían de imágenes escaneadas o fotografías de los documentos.

En total, Frantz extrajo más de 200.000 datos en imágenes, unos 3.400 en documentos y casi 149.000 de un centenar de aparatos.

El experto recuerda lo que dicen varios especialistas en decenas de blog de ciberseguridad: que formatear -aunque sea varias veces- o restablecer una computadora no basta para borrar esa información.

Y enviar tus archivos a la Papelera y vaciarla o restaurar Windows o iOS tampoco es lo más adecuado. Con el software adecuado y ciertas habilidades informáticas es posible recuperar los archivos borrados sin gran dificultad.

La explicación es muy sencilla: para la computadora, “borrar” en ese caso significa “volver a escribir” sobre esos datos… pero estos siguen ahí.

Enviar archivos a la papelera y borrarlos no equivale a deshacernos de ellos por completo/ GETTY IMAGES

“Realísticamente hablando, a menos que destruyas el dispositivo físicamente, los expertos forenses pueden extraer potencialmente datos de él”, señala Frantz.

“Es mejor pecar de precavido y destruirlos. Hacer una limpieza del dispositivo suele ser suficiente y puede ser un proceso muy sencillo”.

“Si te preocupa que tus datos puedan acabar en manos equivocadas, destrúyelos”, declara.

“Y si vas a donar tu tecnología, asegúrate de que al menos borraste los datos a un nivel aceptable. Incluso aunque te confirmen por escrito que tus datos serán borrados, no hay forma de saber si es cierto… a no ser que los borres tú mismo”.

Tus datos personales quedan almacenados en la memoria de tu computadora/ GETTY IMAGES

¿Cómo borrar toda esa información?

Una opción para deshacerte eficazmente de los datos es usar un

software especializado para limpiar la unidad de almacenamiento de tu computadora o un disco duro. Es lo que se conoce como “wiping” o borrado seguro. Hay muchos gratuitos. Por ejemplo:

- DBAN
- Disk Wipe
- MHDD
- KillDisk
- FreeEraser
- Eraser

Esos programas funcionan llenando de datos inútiles los espacios en donde antes hubo información útil para que se ocupe ese espacio.

Para ello, borran y repiten varias veces el proceso, de manera que no quede “ni rastro” de los datos originales, explica la Asociación Colombiana de Seguridad (AOSEC).

En cualquier caso, y pese a que estos métodos suelen ser eficaces, siempre existe una posibilidad, aunque sea muy pequeña, de que alguien encuentre la manera de recuperar los datos.

“Técnicamente, la única manera de que los datos sean definitivamente inaccesibles es con el uso de hardware forense”, dice la AOSEC. Ese sistema consiste en escribir numerosas veces sobre la información con datos aleatorios. Pero requiere de alta tecnología.

Otra opción es dañar físicamente el disco duro o el aparato… aunque entonces ya no podrás ni venderlo ni reciclarlo.
Ten en cuenta que el agua no es la mejor opción: no solo deja inservible la computadora o el disco duro, sino que los datos siguen ahí.

Los imanes suelen ser más eficaces porque desmagnetizan el disco. Y en varios sitios de ciberseguridad hablan de soluciones más radicales, como golpear la computadora o el disco duro o prenderle fuego.

“Si tienes datos muy comprometedores y definitivamente quieres hacerlos desaparecer, la mejor opción es tomar este dispositivo y golpearlo con un mazo hasta dejarlo totalmente pulverizado”, explica el organismo colombiano.

Fuente: BBC MUNDO