Reutilización y sustitución de dispositivos de almacenamiento de datos y seguridad de la información

En las próximas semanas numerosos usuarios domésticos aprovecharán los regalos navideños para cambiar de teléfono móvil, adquirir un nuevo ordenador o sustituir su disco duro por otro de más capacidad de memoria, o incluso tirar a la basura todos esos diskettes y cd´s que ya no nos sirven y hemos acumulado durante el año. Asimismo, muchas empresas aprovechan el comienzo de un nuevo año para deshacerse de sus terminales más obsoletos y renovar su equipamiento informático.

Traduciendo la idea anterior a cifras, se estima que los españoles tiran a la basura entre 3 y 4 millones de ordenadores y 12 millones de teléfonos móviles al año, a los que habría que añadir una cantidad desconocida de dispositivos informáticos que se dona a instituciones o se vende en el mercado de segunda mano. Así, por ejemplo, de los cerca de los 45 millones de terminales de telefonía móvil que existen en España, unos 20 millones se renuevan anualmente.[1]

¿Por qué debemos ser cuidadosos a la hora de deshacernos o reciclar nuestros dispositivos de almacenamiento de datos?

El problema de fondo que aborda este artículo es que, con demasiada frecuencia, los usuarios – tanto domésticos como empresas – se deshacen de sus antiguos equipos informáticos y soportes digitales sin haberse asegurado que los datos que pueden contener los mismos han sido completamente y definitivamente eliminados. Así, actos tan comunes como deshacerse de un CD o un DVD, reciclar un teléfono móvil o vender un disco duro usado pueden representar una fuga importante de información desde dichos equipos a terceras personas. Esta circunstancia ha cobrado mayor importancia para las empresas conforme ha aumentado la práctica de la periódica renovación tecnológica y devolución al proveedor-arrendador de los antiguos equipos gracias a un contrato de leasing o renting.

El borrado de archivos e incluso el formateo de los dispositivos de almacenamiento no siempre es suficiente para garantizar el borrado irreversible de la información almacenada. De este modo, estas conductas ponen en peligro la confidencialidad de los datos, facilitando su uso fraudulento o malintencionado, lo que afecta a la seguridad de

1 INE: Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los hogares, 1º semestre 2006.

los sistemas de las empresas y equipos informáticos, así como a la privacidad del usuario.

¿Qué tipo de información podría ser recuperable?

Recientes trabajos de investigación tanto del Instituto Tecnológico de Massachussets (EEUU) como de la Universidad de Glamorgan (Gales, Reino Unido) y la Universidad Edith Cowan (Australia), han constatado la necesidad de seguir unas buenas prácticas de gestión de la seguridad de la información no solo en la utilización de los dispositivos electrónicos de almacenamiento, sino también cuando nos deshagamos de estos aparatos y soportes.

El objeto de análisis de los estudios anteriormente mencionados fueron discos duros de segunda mano adquiridos a través de Europa, América y Australia. Dichos discos fueron sometidos a un proceso de recuperación de datos, pudiéndose obtener información a partir de más del 50% de los discos duros; pero lo que es aún más significativo, de los datos recuperados, un 70%, eran datos de naturaleza privada o confidencial.

El tipo de información que puede ser recuperada desde un dispositivo que no ha sufrido un proceso eficiente y depurado de eliminación de la información viene dado por el contenido y utilización del equipo antes de su reciclado. Así, de tomar las medidas adecuadas son susceptibles de recuperarse desde datos personales del usuario, direcciones IP, listados de direcciones de correo electrónico, hasta números de cuenta bancarios y números de tarjetas de crédito, contraseñas de todo tipo, números de teléfono fijo y móvil, datos empresariales, nóminas, fotografías, y un largo etcétera de información que no solo puede comprometer la confidencialidad y seguridad informática de los antiguos usuarios, sino que en manos inadecuadas puede llegar a utilizarse fraudulentamente.

¿A qué dispositivos reciclables nos estamos refiriendo?

En la actualidad, la seguridad en el reciclado ha adquirido una mayor relevancia ya que en los últimos años ha aumentado enormemente el número de terminales, equipos y componentes que son objeto de recuperación y reutilización. Así, nos referimos tanto a aquellos equipos capaces de almacenar información y ser objeto de reciclaje (teléfonos móviles, ordenadores personales, PDA o agenda electrónica, etc.), y los componentes de los mismos que contienen efectivamente dicha información (discos duros internos y externos, así como a cualquier otro componente o soporte capaz de almacenar datos (disquetes, CDs, DVDs, tarjetas de memoria, memorias USB, memorias flash, etc.).

El denominado “reciclado” de los equipos se lleva acabo a través de la venta del dispositivo a un tercero en el mercado de segunda mano, bien donándolo a organizaciones o a conocidos, o simplemente deshaciéndose de él en la basura.

En estos casos, si no se ponen los medios adecuados o estos son insuficientes, en ocasiones, el traspaso en la propiedad de uno de estos aparatos o soportes conlleva la posible transmisión o fuga de información sensible, sin que el usuario sea consciente del peligro que esto supone. Por ello, el reciclado de un dispositivo debe estar precedido de una serie de medidas de seguridad para evitar que sea posible la extracción de información de dicho dispositivo.

Cuando se recicla un disco duro una conducta habitual es efectuar un borrado de los datos que contiene el disco e, incluso, un formateo de la unidad para borrar toda la información contenida en el mismo. Sin embargo este proceso, ejecutado de modo ineficiente, no efectúa un borrado físico total de los datos, que permanecen todavía residentes en el soporte sin ser mostrados en los directorios. Esta circunstancia da pie a que dichos datos puedan ser recuperados desde el dispositivo. Hoy en día existe software que rescata dicha información de los distintos soportes. Para evitar esta posibilidad es necesario efectuar un borrado completo y total de los datos contenidos en la unidad de almacenamiento. En la actualidad existen métodos avanzados de borrado, mediante los cuales, además, se realiza una sobre-escritura, en varias ocasiones, de la información contenida en la unidad soporte. Este proceso graba en la unidad otros datos de carácter aleatorio o pseudoaleatorio, los cuales tienen un valor informativo nulo. Existe también, por otro lado, la posibilidad de recurrir a alguna herramienta de borrado que certifique que la información ha sido eliminada totalmente del soporte.

La información contenida en los distintos soportes puede ser recuperada más fácilmente si el dispositivo se encuentra en buen estado, mediante herramientas de todo tipo, incluido software. En aquellos dispositivos en los que se ha producido una avería o deterioro de carácter físico, la recuperación de la información se complica considerablemente. En este caso se deben aplicar previamente procedimientos de manipulación física sobre el elemento dañado y posterior tratamiento informático a nivel de software para recuperar la información.

Recomendaciones de INTECO con relación al reciclado de dispositivos

Como hemos apuntado anteriormente, en ocasiones, el borrado o formateo de la unidad es insuficiente para garantizar que los datos han sido eliminados definitivamente de nuestro equipo o soporte de almacenamiento de datos. Por ello, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) recomienda realizar un análisis previo de necesidades y seguir los siguientes pasos según se trate del un reciclado con o sin reutilización, posterior de los dispositivos:

- Si se pretende el **reciclado del dispositivo para su posterior reutilización por otros usuarios**, como ocurriría tras su venta o donación, se recomienda un borrado total de la información contenida en el soporte.

Así, existen programas que eliminan los datos del soporte y sobrescriben en dicha unidad con información de valor nulo para el usuario que utilice dicho elemento. El borrado puede efectuarse a distintas velocidades, en función del objetivo que se pretenda.

Los métodos de borrado serán de distinto de nivel en función del grado de seguridad que se desee obtener y la velocidad a la que se produce el borrado. Por lo general, los métodos de borrado lento ofrecen mayor fiabilidad y seguridad en sus resultados.

1. En un primer nivel se encuentran las técnicas que ofrecen una mayor velocidad pero que proporcionan un menor índice de seguridad. Dentro de éstas se sitúa el método "*Super Fast Zero Write*".

2. En un segundo nivel aparecen técnicas que efectúan un borrado más lento, con un nivel medio de seguridad, entre las cuáles estaría el método "*Random and Zero Write*".

3. En el tercer nivel se sitúan los métodos avanzados de borrado de datos con un alto nivel de seguridad. Estos métodos se caracterizan porque sobrescriben hasta en 35 ocasiones el soporte, insertando números aleatorios o pseudoaleatorios generados por cada pasada de grabación sobre el elemento. En este caso se aplican modelos matemáticos avanzados para la generación e inserción de información de valor nulo para el usuario, como el "*método Gutmann*" o el "*DoD 5220.22-M*".

- En el caso de que lo que se pretenda es que **los dispositivos de almacenamiento no puedan reutilizarse**, aunque ello sea posible, es recomendable la destrucción física e integral del soporte físico donde se almacenan dichos datos para convertir la información que contienen en irrecuperable. Dentro de este grupo se encuentran:

  1. Soportes no regrabables, como son los DVD o CD no regrabables: el procedimiento de seguridad es relativamente sencillo, por ejemplo cortándolos en fragmentos.

  2. Si se trata de soportes regrabables, como son también DVD, CD o disquetes: el procedimiento a seguir no solo pasa por el borrado de la información que contienen, sino además la destrucción del soporte físico (en el caso de disquetes extrayendo previamente el disco interno de la carcasa).

  3. Soportes como discos duros, tanto internos como externos, o de unidades externas de memoria: el medio de destrucción del soporte se complica, tanto en ejecución, como en coste. La destrucción de estos dispositivos es posible

llevarla a cabo en empresas especializadas que ofrecen este servicio. Uno de los métodos más utilizados incluye el borrado definitivo por magnetización del dispositivo y su posterior destrucción física.

A continuación, ofrecemos una recopilación de enlaces a **herramientas y soluciones gratuitas** que pueden encontrarse en la Red y que pueden ser de utilidad para el borrado seguro de datos:

BiteByBite: www.potentialsys.com/potential

Eraser: www.tolvanen.com/eraser/

NecroFile: www.necrocosm.com/nfinfo.html

Smart Data Scrubber: www.smartpctools.com/es/data_scrubber/index.html

Asimismo, se indican algunas **empresas españolas** que ofrecen servicios de recuperación de datos y borrado seguro:

Datarecsa: www.datarecsa.com/

Infodata: www.infodata.es

Ondata International: www.ondata.es/

Onretrieval: www.onretrieval.com/

Recovery labs: www.recoverylabs.com/

Serman: www.serman.com/