

Reuse and substitution of data storage devices and information security

In the next weeks, numerous home users will use the Christmas season to change their mobile phone, purchase a new computer, change their hard disk for another one with more memory capacity or even throw away the useless floppy disks or CDs they have been accumulating during the year. Likewise, many companies will use the beginning of the year to dispose of their obsolete terminals and update their computer equipment.

If we translate this previous idea into figures, it is estimated that Spaniards throw away between 3 and 4 million computers and 12 million mobile phones a year. To this, we should add an unknown amount of computer devices that are donated to institutions or sold on second-hand markets. For example, about 20 million mobile telephony terminals in Spain are reused every year from the roughly 45 million ones existing¹.

Why should we be careful when getting rid of or recycling our data storage devices?

The background problem, which this article tackles, is that users (both home users and companies) frequently dispose of their old computer equipments and digital supports, without making sure that the data contained in them have been completely erased. Therefore, common proceedings, such as getting rid of a CD or DVD, recycling a mobile phone or selling a used hard disk may pose an important information leak from these equipments and this information may get to third parties. This circumstance has gained greater importance among companies, as the practice of periodical technological updates and returns to the provider or leaser of old equipments (thanks to a leasing or renting contract) have increased.

File deletion or even formatting storage devices is not always sufficient to guarantee the irreversible deletion of stored information. Limiting oneself to these procedures jeopardises the confidentiality of data and allows for its fraudulent and malicious use, which affects the security of company's systems and computer equipments, as well as users' privacy.

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

Which type of information could be recovered?

Recent research works from the Technological Institute of Massachusetts (USA), the University of Glamorgan (Wales, United Kingdom) and the University of Edith Cowan (Australia) have shown the need of following good practices of information security management, not just in the use of electronic storage devices, but also when we dispose of them.

The object of analysis of the aforementioned studies was second-hand hard disks, which were acquired in Europe, America and Australia. These disks were subjected to a data recovery process, which permitted to obtain information from over 50% of hard disks. However, the most important fact is that 70% of the recovered data were private or confidential.

The type of information that can be recovered from a device that has not undergone an efficient and pure process of information deletion depends on the content and usage of the equipment before it was recycled. So, if proper measures are not taken, different types of data can fall into wrong hands, such as users' personal details, IP addresses, e-mail address lists, bank account numbers, credit card numbers, passwords, fixed and mobile phone numbers, business details, salaries or photographs. This cannot only jeopardise the confidentiality and information security of old users, but the information could also be illegally used for fraudulent purposes.

Which recyclable devices are we referring to?

Currently, security in recycling has acquired greater importance, since the number of terminals, equipments and components that can be recovered and reused has greatly increased in the last years. In this way, we are referring to those equipments that can store information and be recycled (mobile phones, personal computers, PDAs or electronic agendas, etc.) and their components, which effectively contain this information (internal and external hard disks or another type of component or support that can store data, such as floppy disks, CDs, DVDs, USB memory sticks or flash memories).

The “recycling” of equipments is carried out by selling the device to a third party on the second-hand market, by giving it to organisations or private individuals or by throwing it away.

In these cases, if proper measures are not taken or if they are insufficient, the transfer of these devices or supports sometimes entails the possible transmission or leak of sensitive information, without the user being aware of the danger involved. Therefore, when recycling a device, a series of security measures must be taken in order to avoid the possible extraction of information from the device.

When a hard disk is recycled, people frequently erase the data on the disk and even format the unit, in order to delete all the information. However, if this process is inefficiently executed, the physical deletion of data is not completely carried out. Indeed, the data will remain in the support without appearing in the directories. This means the information can be recovered from the device. Nowadays, there is software that recovers information from the different supports. In order to avoid this possibility, it is necessary to completely erase the data contained in the storage unit. Currently, there are advanced deletion methods, through which the information in the support unit is also overwritten, on some occasions. This process records other random or pseudorandom null value data in the unit. On the other hand, there is the possibility of using other erasure tools that certify the information has been totally erased from the support.

The information contained in the different supports can be recovered more easily when the device is in good condition. This can be done through all types of tools, including software. Indeed, it is considerably more difficult to recover the information from those devices that have suffered a breakdown or are damaged. In this case, physical manipulation processes should be previously applied on the damaged element and, subsequently, computer processing should be used at a software level, in order to recover the information.

Recommendations of INTECO regarding the recycling of devices

As mentioned before, deleting or formatting the unit is insufficient to guarantee the data have been completely erased from our equipment or data storage support. Therefore, the National Institute of Communication Technologies (INTECO) recommends to conduct a previous analysis of the needs and to follow the next steps depending on the subsequent recycling of the devices (with or without reuse):

- In case of **recycling devices for its subsequent use by other users**, as would happen after being sold or given, the total erasure of the information contained in the support is recommended.

For example, there are programs that erase data from the support and overwrite it with null value data. The erasure can be carried out at different speeds depending on the pursued objective.

The erasure methods will have a different level according to the degree of security we wish to obtain and the speed at which the erasure is carried out. On the whole, slow erasure methods are more reliable and secure in their results.

1. At a first level, we find techniques which offer more speed but a lower security level. Within these techniques, we find the method “*Super Fast Zero Write*”.

2. At a second level, we find techniques that have a slow erasure speed and an average security level. Among these techniques, we find the method “*Random and Zero Write*”.
 3. At the third level, we find advanced methods for the erasure of data with a high security level. These methods overwrite up to 35 times the support by inserting random or pseudorandom numbers, generated by each rec run, on the element. In this case, advanced mathematical processes for the generation and insertion of null value information, such the “*Gutmann method*” or the “*DoD 5220.22-M*” method are applied.
- If we do **not want the storage devices to be reused** – even if this is technically possible – we recommend the physical and total destruction of the physical support where the data are stored, in order to make the information irretrievable. Within this group we find:
 1. Non-rewritable supports, such as non-rewritable DVDs or CDs: the security process is relatively simple, for example, we can cut them into fragments.
 2. In case of rewritable supports, such as DVDs, CDs or floppy disks, the process consists not only of deleting the contained information, but it also includes the physical destruction of the physical support (in the case of floppy disks, you need to previously extract the internal disk from the plastic shell).
 3. Supports, such as internal and external hard disks and external memory units: the way of destructing the supports is more complicated to execute and more costly. The destruction of these devices is carried out by specialised companies that offer this service. One of the most used methods is the total erasure by the magnetization of the device and its subsequent physical destruction.

Next, we offer a series of links to **free tools and solutions** that can be found on the Internet, which are very useful to securely erase data:

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

Furthermore, we list some **Spanish companies** that offer services of data recovery and secure erasure:

Datareca: www.datareca.com/

Infodata: www.infodata.es

Ondata International: www.ondata.es/

Onretrieval: www.onretrieval.com/

Recovery labs: www.recoverylabs.com/

Serman: www.serman.com/