Los soportes de información

Cuando hablamos de **soportes de información** nos referimos a todos aquellos dispositivos que nos permiten almacenar información en formato electrónico y que en general, son fáciles de transportar.

Existe una gran variedad de dispositivos en los que se puede almacenar información, y que han proliferado durante los últimos años a medida que los volúmenes de información iban creciendo.

Como sucedió con los diskettes, a medida que las necesidades de almacenamiento crecen, los soportes con menor capacidad y versatilidad van cayendo en el desuso.

Entre los soportes más utilizados encontramos los siguientes:

- Discos duros (internos y externos).
- Cintas y discos de copias de seguridad.
- Unidades USB o *pendrives*.
- Tarjetas de memoria (SD, *microSD*, etc.)
- Discos ópticos (CD/DVD).

Además de estos soportes, debemos tener en cuenta que un ordenador portátil, un *smartphone* o una *tablet* también puede ser considerado un soporte, al ser fácilmente transportable y disponer de una capacidad significativa para el almacenamiento de información. En este caso, también deben aplicarse las medidas de la píldora de dispositivos móviles.

1. Riesgos

Los soportes de información, especialmente los de pequeño tamaño, como USBs o tarjetas de memoria y dispositivos móviles, pueden ser objeto de pérdida, robo o rotura y/o avería.

Aunque podamos estar hablando de soportes de cierto importe económico, debemos tener en cuenta que estos riesgos repercuten de manera directa en un activo mucho más importante que el propio dispositivo: la información que almacena.

Dicho de otra forma, los riesgos de los soportes se trasladan de manera directa a la información que contienen, cuya importancia y valor puede ser mucho más alto, tanto en el caso de rotura (por ejemplo, una copia de seguridad cifrada) como en el de robo (por ejemplo, un USB).

Por tanto, la mejor manera de proteger la información que contienen es proteger los propios soportes.

2. Cifrado

La principal medida a aplicar sobre los soportes que utilizamos para evitar que la información se vea comprometida en el caso de robo o pérdida, es la de **cifrar la información**. De este modo nos aseguramos de que la información no es accesible por una persona no autorizada.

Existen múltiples herramientas para el cifrado de la información y la mayor parte de los fabricantes de herramientas de seguridad disponen de aplicaciones específicas para ello. Existen incluso dispositivos que incorporan en su propio hardware medidas para cifrar la información y hacerla irrecuperable en el caso de que se intente acceder a ella de manera no autorizada.

Además de estas herramientas, muchas aplicaciones de compresión y suites de ofimática disponen de funcionalidades específicas para el cifrado de los documentos, que en ciertas circunstancias y cuando no se requiere el cifrado de todo el dispositivo es una medida muy útil para el intercambio y almacenamiento de información. Siempre, evidentemente, que la clave utilizada para el cifrado sea robusta.

3. Destrucción segura

Cualquier soporte tiene una vida útil determinada, ya sea por quedarse obsoleto, tener poca capacidad en comparación con otros soportes, o mostrar fallos en su funcionamiento (que no obstante, pueden permitir a una persona con conocimientos recuperar parte de la información que contiene).

Una vez llegado el final de esta vida útil, debemos destruir el soporte de una manera adecuada, para evitar que alguien pueda obtener la información que éste almacena. En seguridad llamamos a eso un proceso de **destrucción segura**.

Para garantizar que nadie podrá acceder a la información que hubiera contenido el soporte, lo más frecuente es realizar una destrucción física del soporte.

Dependiendo del tipo de soporte que utilicemos, es posible que seamos capaces de realizar una destrucción segura con medios propios. Por ejemplo, si se trata de un USB, un CD/DVD o de una tarjeta de memoria, podemos destruirlos fácilmente con el uso de, por ejemplo, un martillo. Algunas destructoras de papel también permiten la destrucción de discos ópticos de manera segura.

Sin embargo, la destrucción de discos duros de los equipos, o cuando el volumen de soportes es muy grande (por ejemplo, tres docenas de cintas de seguridad), puede requerir que necesitemos delegar la destrucción en un tercero. En este caso, es necesario que el proveedor firme con nosotros un compromiso de confidencialidad y requiramos un certificado de destrucción.

Debemos recordar que no estamos hablando de un proceso de reciclaje, sino de destrucción, con independencia que posteriormente, cuando es imposible la recuperación de la información, se reciclen los materiales.

4. Borrado seguro

En el punto anterior hablábamos de destrucción segura, pero debemos tener en cuenta que no siempre un soporte es desechado, sino que a menudo es reutilizado.

Por ejemplo, un portátil que inicialmente pertenecía a un usuario de RRHH y que luego es utilizado por un usuario de marketing, o un PC que donamos a un colegio para las clases de informática.

En estos ejemplos se muestra que es necesario, antes de donar o reutilizar un soporte, aplicar medidas de **borrado seguro**. Para esta finalidad existen múltiples herramientas que nos permiten realizar un borrado seguro sobre nuestros soportes, muchas de ellas de software libre.

También podemos aplicar esto a aquellos USBs que utilizamos de manera esporádica y que podemos prestar a compañeros, usuarios o proveedores, pensando que con borrar la información de la manera habitual es suficiente.

Además, es necesario tener en cuenta que el formateo de un soporte no implica necesariamente el borrado seguro de su información.

Algunas de las medidas de seguridad que debemos aplicar para evitar confusiones en el uso de soportes son:

- Marcar o etiquetar los soportes de las distintas áreas o propietarios para que no sean intercambiados por error.
- Evitar en la medida de lo posible el uso de memorias USB. En lugar de esto, podemos establecer carpetas departamentales con control de acceso lógico basado en perfiles y puestos.
- Documentar el procedimiento a seguir para realizar un borrado seguro.