Els suports d'informació

Quan parlem de **suports d'informació** ens referim a tots aquells dispositius que ens permeten emmagatzemar informació en format electrònic i que en general, són fàcils de transportar.

Existeix una gran varietat de dispositius en els quals es pot emmagatzemar informació, i que han proliferat durant els últims anys a mesura que els volums d'informació han anat creixent.

Com va passar amb els disquets, a mesura que les necessitats d'emmagatzemat creixen, els suports amb menor capacitat i versatilitat van caient en desús.

Entre els suports més utilitzats trobem els següents:

- Discs durs (interns i externs).
- Cintes i discs de còpies de seguretat.
- Unitats USB i memòries USB.
- Targetes de memòria (SD, microSD, etc.)
- Discs òptics.

A més d'aquests suports, hem de tenir en compte que un ordinador portàtil, un telèfon intel·ligent o una tauleta també poden ser considerats un suport, en ser fàcilment transportables i disposar d'una capacitat significativa per l'emmagatzemat d'informació. En aquest cas, també han d'aplicar-se les mesures de la píndola de dispositius mòbils.

1. Riscs

Els suports d'informació, especialment de mida petita, com USBs o targetes de memòria i dispositius mòbils, poden ser objecte de pèrdua, robatori o trencament i/o avaria.

Tot i que podem estar parlant de suports de cert import econòmic, hem de tenir en compte que aquests riscs repercuteixen de manera directa a un actiu molt més important que el mateix dispositiu: la informació que emmagatzemen.

Dit d'una altra manera, els riscs dels suports es traslladen de manera directa a la informació que contenen, amb una importància i valor que pot ser molt més alta, tant en forma de trencament (per exemple, una còpia de seguretat xifrada) com en el de robatori (per exemple, un USB).

Per tant, la millor manera de protegir la informació que contenen és protegir els mateixos suports.

2. Xifrat

La principal mesura a aplicar sobre els suports que utilitzem per evitar que la informació es vegi compromesa en el cas de robatori o pèrdua, és la de **xifrar la informació**. D'aquesta manera ens assegurem que la informació no sigui accessible per una persona no autoritzada.

Existeixen moltes eines pel xifrat d'informació i la major part dels fabricants d'eines de seguretat disposen d'aplicacions específiques per fer-ho. Existeixen fins i tot dispositius que incorporen en el seu propi hardware, mesures per a xifrar la informació i fer-la irrecuperable en el cas que s'intenti accedir a ella de manera no autoritzada.

A més d'aquesta eina, moltes aplicacions de compressió i suites d'ofimàtica disposen de funcionalitats específiques pel xifrat de documents, que en certes circumstàncies i quan no es requereix el xifrat de tot el dispositiu és una mesura molt útil per a l'intercanvi i emmagatzematge d'informació. Sempre, evidentment, que la clau utilitzada pel xifrat sigui robusta.

3. Destrucció segura

Qualsevol suport té una vida útil determinada, ja sigui per quedar-se obsolet, tenir poca capacitat en comparació amb altres suports, o mostrar errors en el seu funcionament (que tot i això, poden permetre a una persona amb coneixements recuperar part de la informació que contenen).

Un cop arribat al final de la vida útil determinada, hem de destruir el suport de manera adequada, per evitar que algú pugui obtenir la informació que emmagatzema. En seguretat és el que s'anomena un procés de **destrucció segura**.

Per garantir que ningú pugui accedir a la informació que havia contingut el suport, el més freqüent és realitzar una destrucció física del suport.

Depenen del tipus de suport que utilitzem, és possible que siguem capaços de realitzar una destrucció segura amb medis propis. Per exemple, si es tracta d'un USB, un CD/DVD o de una targeta de memòria, podem destruir-los fàcilment amb l'ús de, per exemple, un martell. Algunes destructores de paper també permeten la destrucció de discs òptics de manera segura.

Tot i això, la destrucció de discs durs dels equips, o quan el volum de suports és molt gran (per exemple, tres dotzenes de cintes de seguretat), pot requerir que necessitem delegar la destrucció en un tercer. En aquest cas, és necessari que el proveïdor firmi amb nosaltres un compromís de confidencialitat i necessitem un certificat de destrucció.

Hem de recordar que no estem parlant d'un procés de reciclatge, sinó de destrucció, amb independència que posteriorment, quan sigui impossible la recuperació d'informació, es reciclin els materials.

4. Esborrat segur

En el punt anterior parlàvem de la destrucció segura, per hem de tenir en compte que no sempre un suport és rebutjat, sinó que molts cops és reutilitzat.

Per exemple, un portàtil que inicialment pertanyia a un usuari de RRHH i que després és utilitzat per un usuari de màrqueting, o un PC que donem a una escola per a les classes d'informàtica.

En aquests exemples es mostra que és necessari, abans de donar o reutilitzar un suport, aplicar les mesures d'esborrat segur. Per aquesta finalitat existeixen múltiples eines que ens permeten realitzar un esborrat segur sobre els nostres suports, moltes d'elles de software lliure.

També podem aplicar això a aquells USBs que utilitzem de manera esporàdica i que podem deixar a companys, usuaris o proveïdors, pensant que amb la informació esborrada de la manera habitual és suficient.

A més, és necessari tenir en compte que el formatat d'un suport no implica necessàriament l'esborrat segur de la seva informació.

Algunes de les mesures de seguretat que hem d'aplicar per evitar confusions en l'ús de suports són:

- Marcar o etiquetar els suports de les diferents àrees o propietaris perquè no siguin intercanviats per error.
- Evitar en la mesura del possible l'ús de memòries USB. En lloc d'aquests, podem establir carpetes departamentals amb control d'accés lògic basats en perfils i llocs de treball.
- Documentar el procediment a seguir per a realitzar un esborrat segur.