# La informació

## 1. Confidencialitat de la Informació

**Que és la confidencialitat?** Una norma de seguretat reconeguda internacionalment defineix la confidencialitat com la propietat de la informació "per la que la informació no es posa a disposició o es revela a individus, entitats o processos no autoritzats". Es a dir, la informació confidencial és aquella que hem de protegir de l'accés a persones no autoritzades.

Però, **que considerem informació confidencial?** Doncs és tota aquella que hem de protegir de l'accés d'altres persones. No importa el suport, el tipus d'informació o fins i tot si es comunica verbalment. En l'altre extrem tenim la informació d'ús públic, com per exemple, qualsevol material publicitari que utilitzem amb els nostres usuaris.

**Per què diem que una informació és confidencial?**

1. Perquè és **informació crítica** de la nostra feina.
2. Perquè és **informació "sensible"** i poden haver-hi altres organitzacions interessades.
3. Perquè està **protegida per la legislació**, com per exemple les dades personals.
4. Perquè ens hem compromès **amb un tercer** a mantenir la informació en secret: un usuari, un soci, un proveïdor...

**Què hem de fer en gestionar informació confidencial?**

- Signar un acord de confidencialitat amb qualsevol persona o organització a qui li donem accés a la informació.
- Evitar que persones no autoritzades tinguin accés a la informació confidencial que utilitzem, no deixant-la a la vista ni en directoris o sistemes en els quals pot ser accedida per a altres persones.
- Aplicar mesures de xifrat quan la informació sigui espacialment sensible.

# 2. Les dades personals

Segons la legislació espanyola en protecció de dades, una dada de caràcter personal és "qualsevol informació concernent a persones físiques identificades o identificables".

És a dir, el DNI és una dada de caràcter personal, una fotografia és una dada de caràcter personal, i l'estatura d'algú és una dada de caràcter personal si podem d'alguna manera saber a qui pertany.

Hem de tenir en compte que la legislació de protecció de dades és d'obligatori compliment per a qualsevol organització espanyola, i complir amb ella és tan senzill com portar a terme una sèrie de tràmits administratius i posar en marxa algunes mesures bàsiques de seguretat senzilles.

En el nostre cas, hem d'evitar l'accés de persones no autoritzades a les dades personals que tinguem en la nostre organització, gestiona-les sempre de la manera adequada i informar-nos quan tinguem qualsevol dubte.

Tot i que a Internet existeixen nombrosos recursos, per qualsevol dubte podem recorre a l'Agència Espanyola de Protecció de Dades, sent l'adreça web http://www.aepd.es

# 3. Xifrat de la informació

A l'hora de protegir la informació en format electrònic, una de les mesures més eficaces és el xifrat d'informació. Mitjançant aquesta tècnica podem codificar qualsevol fitxer i fer-lo inaccessible a altres persones que no sàpiguen la clau per a desxifrar-lo.

**Quina informació hem de xifrar?**

- Tota aquella que sigui de vital importància en la nostra feina i sobretot, si la seva difusió pot ser un problema.
- Si treballem amb dades personals d'alt nivell com dades de salut, la legislació requereix que l'emmagatzemen xifrat en certes circumstàncies.
- També és recomanable xifrar un fitxer si l'hem d'enviar a usuaris i/o proveïdors. Així, encara que algú capturi el fitxer, no podrà accedir al seu contingut.

Tot i que existeixen múltiples eines pel xifrat d'informació, moltes aplicacions de compressió de fitxers i ofimàtica disposen de la possibilitat de comprimir amb contrasenya, cosa que pot ser suficient en la majoria de casos.

# 4. Còpies de seguretat

Les còpies de seguretat són un dels principals elements per evitar la pèrdua d'informació quan tenim un problema.

Tot i que en general aquest tipus de sistemes les gestiona el personal informàtic, hi ha diversos aspectes que s'han de tenir en compte:

- **Informació:** Hem d'assegurar-nos que s'està realitzant una còpia de seguretat de tota la informació que utilitzem en la nostra feina. Per exemple, de la informació que guardem en "Els meus documents".
  És necessari que emmagatzemem la informació en els sistemes i directoris del que sabem que es fa una còpia. Si tenim dubtes, podem parlar amb el personal d'informàtica.

- **Suports externs:** Si per treballar utilitzem suports com discs durs externs, hem d'assegurar-nos que es fa una còpia de la informació que emmagatzemem. Si les còpies de seguretat les fem en suports com CDs o DVDs o fins i tot llapis USBs, hem de desar-los sempre en llocs protegits.

- **Freqüència:** Si fem còpies periòdiques de la nostra informació, hem de definir la periodicitat adequada per què un problema en el nostre equip no suposi una pèrdua de les últimes setmanes o mesos de treball.

- **Sortida de còpies:** Si hem de traslladar les còpies fora de l'organització (per exemple, fins una altra oficina o domicili), hem de xifrar-les, per evitar que si les perdem, algú pugui accedir al contingut.

UB: Si necessites ajuda amb les teves còpies de seguretat, contacta amb el personal d'informàtica per a conèixer les solucions de backup disponibles a la teva universitat i quina d'elles s'adapta millor a les teves necessitats.

# 5. Classificació de la informació

Qualsevol de nosaltres gestiona informació de diferent índole durant la seva feina diària: tarifes, propostes a usuaris, dades personals, plans estratègics, comptabilitat, etc.

És normal que no tota la informació amb la qual es treballa tingui la mateixa importància. En alguns casos serà informació pública, en altres casos serà per ús intern i en altres serà molt crítica.

Per tant, és normal que tots aquests tipus d'informació necessitin mesures de seguretat diferents. Per exemple, la informació pública té poques restriccions d'accés, mentre que l'accés a la informació confidencial estarà molt restringida.

En el cas que la nostra organització tingui definits els diferents tipus d'informació segons la importància, hem d'aplicar les mesures que ens hagin indicat. Entre altres, hem de tenir en compte el següent:

- **Marcar els documents** que utilitzem amb el nivell de seguretat que ens hagin dit en cada cas.
- **Aplicar xifrat** als tipus d'informació més sensible.
- Tenir en compte quin tipus d'informació pot ser emmagatzemada en **suports externs** o distribuir-se per correu electrònic. Si necessites fer-ho, que sigui sempre utilitzant xifrat.
- **No imprimir** aquella informació la qual la impressió no està permesa.
- **No intentar accedir** a informació a la què no es té accés.

# 6. Metadades

Una "metadada" és aquella informació que inclou fitxers digitals però que no forma part del contingut. Alguns exemples són la data de creació, la data de modificació o l'autor del fitxer.

Hem de tenir en compte que cada tipus de fitxer tindrà les seves pròpies metadades. Per exemple, mentre que un fitxer d'ofimàtica pot contenir l'autor del document, una imatge pot contenir a més a més les seves dimensions i una fotografia informació d'on es va fer o fins i tot el model de la càmera que es va utilitzar.

Tot i que poden ser molt útils, en alguns casos aquesta informació pot proporcionar informació valuosa sobre nosaltres: nom d'usuari, dates dels documents, ubicació de les fotografies, aplicacions utilitzades, etc.

Per això, hem d'eliminar qualsevol metadada abans d'enviar un fitxer a una altra persona o organització. Per això, alguns programes d'ofimàtica incorporen funcionalitats per eliminar informació i també és possible eliminar algunes metadades mitjançant l'opció de botó dret -> Propietats -> Detalls.