@ctitud digit@l

Enric Bruguera Payà

P08/04506/01694

Universitat Oberta de Catalunya
www.uoc.edu

Índex

1. Utilitzem dispositius electrònics

Els ordinadors i els dispositius informàtics ens permeten treballar amb informacions digitals, comunicar-nos amb altres usuaris i interactuar-hi. En el seu interior emmagatzemen dades i documents que per a nosaltres són importants. Dels seus manteniment i cura dependrà sempre el nivell d'eficiència amb què podrem utilitzar-los individualment i el grau de convivència raonable amb què podrem moure'ns en els diferents àmbits socials electrònics.

1.1. L'ordinador

L'ordinador és la principal eina que us permet treballar amb la informació digital, comunicar-vos amb fonts de dades i interactuar amb els altres usuaris. És, per tant, un instrument fonamental de la utilització raonable del qual dependrà la major, menor o nul·la eficàcia de les vostres accions de treball, lleure i interacció en el món electrònic. I és, alhora, la vostra eina bàsica de comunicació i convivència amb la resta d'usuaris de les xarxes i dels dispositius digitals.

Si utilitzeu l'ordinador personal, recordeu que hi heu anat dipositant dades i informacions que no haurien de quedar a disposició d'altres usuaris. Per a això és convenient que sigueu molt estrictes amb les persones que deixeu accedir al vostre terminal i que tracteu amb els màxims respecte i prudència els dispositius electrònics aliens.

Si compartiu l'ordinador amb altres usuaris, és aconsellable que elimineu regularment la informació i les dades innecessàries i que traslladeu a altres dispositius d'emmagatzematge –unitats portàtils de memòria com discos durs externs, llapis USB, CD...– les dades i les informacions que voleu preservar de mirades indiscretes. També podeu xifrar mitjançant contrasenya la part del disc dur a la qual no vulgueu que ningú més pugui accedir. Quan utilitzeu ordinadors d'altres usuaris o terminals instal·lats en espais públics (biblioteques, cibercafès, etc.) podeu millorar la seguretat i la privacitat de les dades amb unes senzilles mesures de precaució:

- Si heu navegat per Internet, tanqueu el navegador quan acabeu la sessió i abans elimineu l'historial de navegació (**Eines>Opcions>Privacitat**).

- No automatitzeu el record de les contrasenyes ni en el sistema operatiu ni en el navegador.

- Eviteu introduir dades personals, realitzar operacions comercials o efectuar transaccions bancàries des d'ordinadors i xarxes que no siguin de total confiança.

- En tots els casos, preserveu la privacitat de les dades personals (telèfon, adreça postal, etc.) amb especial atenció als nombres del document nacional d'identitat i de les targetes de crèdit.

1.2. La contrasenya

Les contrasenyes són un instrument fonamental bàsic per a controlar i restringir l'accés als dispositius electrònics i a la informació que contenen. Un ús raonable i acurat de les contrasenyes ens evitarà intrusions indesitjades en els equips, intromissions en la nostra privacitat i la captura de dades personals per terceres persones. Encara que existeixen individus i programes informàtics capaços de rebentar qualsevol contrasenya digital, en una aclaparadora majoria de casos el robatori o el desxifratge de les claus personals són deguts a una gestió deficient o descuidada de l'usuari. Per a un ús eficient i raonable de les contrasenyes, us anirà bé tenir en compte el següent:

- Idear contrasenyes de vuit caràcters com a mínim, que combinin nombres i lletres, i que aquestes combinin majúscules i minúscules.

- No utilitzar com a contrasenya dades personals fàcils d'esbrinar, com la data de naixement, el nom, els cognoms, el número de telèfon o l'adreça electrònica.

- Evitar escriure les contrasenyes en paper o en documents electrònics emmagatzemats al mateix dispositiu.

- Com a mesura de precaució resulta molt efectiu canviar amb regularitat les contrasenyes que tenim establertes per a cada sistema i cada fitxer.

- També és recomanable evitar l'ús de paraules del diccionari en qualsevol idioma, ja que alguns programes informàtics basen el seu mètode d'atac en la morfologia de les paraules.

- No enviar mai contrasenyes en missatges de correu electrònic ni incloure-les en converses de missatgeria instantània.

- És aconsellable no utilitzar les mateixes contrasenyes en tots els sistemes o fitxers i disposar de claus d'alta seguretat per a accedir en aquells enclavaments d'Internet que no ens ofereixin garantia absoluta de seguretat.

És imprescindible que mantinguem, respecte a les contrasenyes alienes, el mateix grau de discreció i de respecte que exigim per a les nostres pròpies claus personals.

1.3. Programes

Dels programes informàtics depèn la gestió i la conservació de les dades, els documents i la capacitat d'interacció a la Xarxa.

Podem utilitzar programes comercials de pagament (programari de propietat), programes oberts d'ús lliure (*freeware*), programes d'ús limitat (*shareware*)... Qualsevol opció pot ser legítima i adequada, sempre que:

- Ens assegurem d'utilitzar programes informàtics legals (siguin comercials o d'ús lliure i obert). La informàtica il·legal pot ser una font de virus, intrusions il·lícites i problemes jurídics.

- Ens presentin opcions d'actualització regular.

- Fem un petit esforç permanent d'informació sobre el seu funcionament, les actualitzacions i les opcions de seguretat.

El millor programa per a una funcionalitat determinada pot ser-nos absolutament inútil si descuidem la nostra responsabilitat en la informació, bàsica però constant, sobre els seus maneig segur i actualització. I en la mateixa mesura un ús cívic dels programes informàtics ens ajudarà a contribuir a una millor convivència entre els usuaris i a frenar fenòmens antisocials com la pirateria i la còpia indiscriminada de programes comercials, la manipulació i l'alteració il·lícita de programes oberts o les iniciatives massives de frau, extensió de virus i programes maliciosos i captura indesitjada de dades personals privades.

1.4. Seguretat

Els temuts virus informàtics constitueixen una amenaça important en la societat digital. Però el primer perill és no prendre mesures per a garantir la integritat dels dispositius informàtics i de la informació que hi emmagatzemem. Per això, és imprescindible usar **sempre** un bon antivirus per a detectar i neutralitzar qualsevol programa que pugui contaminar o fer malbé els fitxers, així com programes de seguretat que impedeixin que qualsevol intrús pugui accedir a l'ordinador o a les nostres dades. Així, en usar programes de seguretat actualitzats:

- preservem els ordinadors i la informació,

- garantim la privacitat de les nostres dades personals,

- evitem convertir-nos en distribuïdors d'infeccions informàtiques a altres usuaris i ser còmplices involuntaris d'intrusions danyoses als seus ordinadors,

- contribuïm a una major fluïdesa de comunicació en els entorns digitals i ajudem a optimitzar el funcionament col·lectiu de les xarxes i dels àmbits de convivència que generen.

1.5. Antivirus

Els programes antivirus són eines informàtiques específicament dissenyades per a detectar, neutralitzar i eliminar qualsevol altre programa informàtic que pugui introduir-se a l'ordinador o als arxius amb la finalitat de danyar-los, capturar la nostra informació i dades personals o donar ordres als nostres dispositius sense que nosaltres puguem detectar o controlar aquesta activitat oculta.

L'ús normalitzat i quotidià d'informació digital i de xarxes telemàtiques fa **imprescindible** la utilització de programes antivirus per al següent:

- Evitar l'entrada de programes danyosos a través de fitxers que podem introduir a l'ordinador mitjançant còpies o transferències d'arxius procedents d'unitats de memòria com CD, DVD, llapis de memòria, discos durs externs, etc.

- Detectar i destruir programes maliciosos que poden colar-se en l'equip des d'Internet, a través de missatges de correu electrònic, fitxers adjuntats a correus o a la missatgeria electrònica, codis maliciosos ocults en programes dels web que visitem en el nostre recorregut per la Xarxa o arxius i continguts que ens baixem d'Internet mitjançant qualsevol dels seus canals de subscripció, captura lliure o intercanvi.

- Garantir que els nostres equips, dispositius i fitxers estan nets i que no es convertiran en focus difusors d'infecció per codis maliciosos de tots aquells usuaris amb qui interactuem a la Xarxa o a través de l'intercanvi de fitxers entre dispositius informàtics o de memòria.

Evitar-nos problemes i costos, ja que la millor inversió en seguretat ens la proporcionarà un bon programa antivirus que:

- Ens garanteixi actualització i protecció permanent davant dels centenars de noves amenaces víriques que diàriament sorgeixen i s'expandeixen a través dels dispositius i xarxes electròniques globals.

- Ens permeti configurar i personalitzar les opcions de detecció, rastreig i eliminació de codis maliciosos.

1.6. Hàbits clau

L'ús quotidià de les tecnologies i xarxes digitals pot aportar a la nostra vida diària molts més avantatges que inconvenients. Per a aconseguir-ho n'hi ha prou d'aplicar en la seva utilització els criteris raonables i de sentit comú que ens resulten efectius en els altres àmbits de la vida personal, social, laboral i professional.

Com a usuaris de dispositius i xarxes electròniques, tenim al nostre abast l'opció d'adoptar uns senzills hàbits quotidians que resulten clau a l'hora de facilitar-nos l'activitat i les accions digitals amb el màxim de seguretat, privacitat i sentit cívic:

- Mantenir l'ordinador i els programes actualitzats amb els últims elements de seguretat i operativitat que els seus fabricants –si utilitzem informàtica comercial– o la Xarxa –si som usuaris de programes oberts– ofereixen regularment al conjunt d'usuaris.

- Utilitzar habitualment programes informàtics legals, tant si són comercials i de pagament, com si són oberts i gratuïts.

  Programes informàtics

  L'important és conèixer-ne la procedència, que mereixin la nostra confiança –per contracte de compra o pels coneixements i referències que hem obtingut d'altres usuaris– i que presentin garanties de suport tècnic comercial o de caràcter obert.

- Convé estar permanentment informat sobre novetats relatives als programes que utilitzem i els que ens poden interessar. I, sobretot, assegurar-nos de conèixer permanentment les alertes de seguretat que puguin produir-se per a poder identificar les que poden afectar-nos.

- És aconsellable utilitzar de manera quotidiana i normal eines de seguretat com **antivirus** i **tallafocs** (***firewalls***).

  Cost econòmic

  El cost econòmic que poden tenir pot arribar a representar un estalvi incalculable de temps i diners davant de l'entrada d'intrusos i virus en els nostres equips.

- Cal realitzar regularment còpies seguretat de tots aquells elements (programes, arxius, fotografies, dades, etc.) que vulguem posar fora de perill d'eventuals errors o intrusions en qualsevol de les màquines que utilitzem.

- Hem de recordar que, com a usuaris de xarxes, les accions individuals de cada un de nosaltres repercuteixen en el conjunt de la comunitat d'usuaris: un ús personal segur i sostenible dels dispositius electrònics té una dimensió social i cívica decisiva perquè el col·lectiu d'usuaris pugui utilitzar la Xarxa amb més confiança, fluïdesa i seguretat.

2. Gestionem informació digital

Els dispositius i programes informàtics ens faciliten la creació, la captura i l'emmagatzemament de grans quantitats de fitxers, dades i documents.

Un ventall d'opcions per al qual és convenient que tinguem clar el següent:

- on i com emmagatzemem la informació,
- de quina manera ens n'assegurem la recuperació en casos d'emergència,
- com ens fem entendre mitjançant codis bàsics de comunicació virtual,
- com protegim els documents de text,
- quines normes hem de respectar quan utilitzem informació aliena, i
- per què no hauríem de plasmar en paper una rèplica del nostre ús d'informació digital.

2.1. Les memòries

Memòries

Discos durs externs, unitats de memòria flaix USB, discos DVD..., els dispositius per emmagatzemar dades cada vegada presenten més i millors prestacions amb costos cada vegada més raonables.

La proliferació de dispositius digitals de memòria creix en proporció a l'augment de la seva capacitat d'arxivament de dades i a la progressiva disminució dels seus preus.

Un ús raonat d'aquestes unitats de memòria ens permetrà:

- Duplicar dades i arxius que vulguem preservar de les incidències dels ordinadors d'ús diari (arxius de fotografies, de vídeos, de dades personals...).

- Efectuar còpies de seguretat de tot allò que no volem mantenir a l'ordinador personal, exposat eventualment a la mirada d'altres usuaris amb qui compartim terminal o obert a possibles accessos indesitjats des de la Xarxa.

Els dispositius d'emmagatzematge de memòria contenen dades i objectes digitals que són importants per a nosaltres, així que haurem de tractar-los amb la mateixa cura amb què tractem:

- Les claus del nostre domicili, ja que els nostres dispositius també contenen claus i contrasenyes per a accedir a les possessions més valuoses.

- El nostre vehicle, ja que el seu contingut ens permet manejar la nostra informació i dades digitals i moure'ns per la Xarxa.

- La nostra documentació personal, ja que amb moltes de les dades que guarda qualsevol altra persona es podria suplantar la nostra identitat i efectuar tot tipus d'operacions econòmiques i socials en el nostre nom.

2.2. Gestió del text

El tractament de la informació textual sobre suports digitals ens permet treballar constantment sobre aquesta informació, introduir-hi canvis i millores i generar totes les còpies que necessitem sense més límit que la capacitat de memòria dels dispositius d'emmagatzematge. Tot això ens reporta avantatges evidents sobre les limitacions dels textos manuscrits o fotocopiats, però també ens obliga a adoptar criteris eficients perquè les grans quantitats de documents digitals que podem crear no ens facin del tot impossible l'ús ràpid de la informació que contenen.

Quan elaborem, modifiquem i reproduïm continguts textuals, ens hi ajudarà aplicar hàbits d'higiene digital tan senzills com els que segueixen:

- Anomenar els documents de manera clara i concisa. Així podrem identificar-los fàcilment quan necessitem localitzar la informació que contenen.

- Ordenar els fitxers correctament.
  - Per nom, versió i data.
  - Utilitzant les carpetes de manera eficient. De manera similar als fitxers, l'arbre de carpetes ens permetrà una localització més ràpida i eficient dels documents si les estructurem amb noms clars i representatius i realitzem un esforç continuat d'ordenació de cada arxiu a la carpeta corresponent.

Localització de documents

Un document anomenat "currículum_versió7_2008_08_27" ens permet localitzar la versió del currículum que elaborem el 27 d'agost de 2008 i ens permet fer-ho amb més rapidesa que si hem de buscar entre la llista de documents "currículum", "curric", "curricul", "curri", etc.

- Eliminar documents obsolets que ja no presenten cap utilitat. Acumular-los al disc dur i als dispositius de memòria no farà més que ocupar espai i interferir en la localització d'informació rellevant.

Localitzar documents

Un currículum ben presentat, un treball escolar excel·lentment elaborat o la millor memòria anual de l'empresa són textos absolutament inútils si estan perduts a les entranyes de l'ordinador sense que siguem capaços de localitzar-los amb rapidesa i eficiència quan els necessitem.

2.3. Còpies de seguretat

Les còpies de seguretat ens garanteixen que informacions i dades continuen sent en la nostra disposició encara que les màquines o programes sofreixin qualsevol error que els bloquegi o inutilitzi. És fonamental, doncs, fer còpies de seguretat de tots aquells fitxers i documents que vulguem mantenir sans i estalvis d'eventuals incidències. Una còpia de seguretat dels documents importants (fitxers de text, fulls de càlcul, fotografies, arxius de vídeo, etc.) ens permetrà preservar la informació:

- si perdem o ens sostreuen l'ordinador o el dispositiu que contenia el fitxer,
- si un error informàtic bloqueja o inutilitza el dispositiu,
- si una intrusió en el sistema deixa els fitxers a l'abast de terceres persones, o
- si, per error o distracció, danyem o esborrem la informació del dispositiu.

Perquè una còpia de seguretat sigui realment útil convé fer-la:

- amb un nom de fitxer diferent al del document original i guardar-la en una altra ubicació, i

- traslladant-la a un disc dur diferent al del document inicial, a un dispositiu de memòria (DVD, memòria flaix, etc.) o a una xarxa.

L'opció més bàsica i senzilla per a efectuar una còpia de seguretat és duplicar el fitxer en un altre dispositiu mitjançant una simple opció de **còpia**. Perquè aquesta còpia resulti efectiva com a opció de seguretat, haurem de tenir molt en compte el següent:

- Traslladar la còpia a un altre dispositiu diferent.

Còpies de seguretat

Les còpies de seguretat al mateix ordinador no ens seran de cap utilitat en aquells casos en els quals aquesta màquina quedi inutilitzada o bloquejada. És més recomanable fer còpies de seguretat en dispositius, unitats o xarxes externes (CD, DVD, llapis de memòria, discos durs externs, unitats compartides, etc.), que haurem de mantenir en òptimes condicions de seguretat.

- Rebatejar els arxius copiats de manera que puguem identificar-los fàcilment sense que la duplicitat de noms d'arxius dificulti eventuals recuperacions de la informació.

Fàcil identificació

Una còpia de seguretat del fitxer currículum.doc és aconsellable que la rebategem currículum_2008_10_25.doc, si l'hem feta en aquesta data (25 d'octubre de 2008).

- Hem d'assegurar-nos que realitzem còpies de seguretat actualitzades dels fitxers que volem preservar i destruir versions anteriors una vegada guardades les versions actualitzades. Això ens permetrà localitzar més fàcilment la informació i no confondre'ns amb l'actualització de les dades pròpies.

També ens convé analitzar les opcions de còpia de seguretat que ens proporciona el sistema operatiu dels nostres dispositius electrònics:

- La còpia completa a tots els directoris i fitxers prèviament seleccionats al dispositiu.
- La còpia incremental als fitxers nous o en aquells la data de modificació dels quals hagi variat.
- La còpia diferencial només duplica els arxius en el contingut dels quals detecta modificacions.

Convé analitzar les opcions de còpies automatitzades i programables que ens ofereix el sistema operatiu que utilitzem en cada equip.

Web recomanat

L'Institut Nacional de Tecnologia de Telecomunicacions ofereix, a més, accés i valoració d'algunes eines per a la còpia de seguretat disponibles a la Xarxa. Per a més informació, podeu accedir-hi a través de

http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=13&pagina=0.

2.4. Text eficient

El tractament digital de la informació que redactem ens permet nombroses i variades possibilitats de creació, organització i gestió dels continguts textuals, així com innombrables opcions de combinació amb so, imatge estàtica, vídeo i animació multimèdia.

Totes poden potenciar i amplificar la capacitat de comunicació i d'interacció dels textos, sempre que tinguem present que les funcionalitats tecnològiques no anul·len ni substitueixen les normes i convencions del text escrit, dins i fora dels àmbits digitals.

Si volem assegurar-nos un tractament digital efectiu i eficient de la informació textual, ens convé redactar continguts que:

- respectin les normes bàsiques de l'ortografia i de la sintaxi,

El llenguatge

L'ús d'un llenguatge bast, descurat o incorrecte desposseeix de tota efectivitat comunicativa el missatge millor tractat i més vistós des del punt de vista digital.

- estructurin nítidament el que volem comunicar, i

L'efectivitat comunicativa

El desordre d'idees i conceptes, les repeticions, els raonaments recurrents... resten efectivitat comunicativa a qualsevol text, encara que es faci i es presenti sobre suport digital. A més, mostren una lamentable actitud cívica de falta de respecte envers els interlocutors.

- evidenciïn la correcció i la competència de l'autor.

Correcció del text digital

El tractament digital del text permet una correcció fàcil i immediata. I precisament per això un text digital incorrecte delata un autor descurat que no s'ha pres la molèstia de realitzar una segona lectura i de corregir errors evidents. També delata un autor incompetent, que no sap utilitzar els recursos digitals mínims de tractament del text.

Per les seves opcions i versatilitat, el text digital ens defineix. De cada usuari depèn plasmar-hi el seu nivell de coneixements i de competència, no solament en el domini necessari dels mecanismes informàtics del tractament de text, sinó també de les seves capacitats en el domini bàsic de l'ortografia, la sintaxi i l'ordenació elemental d'idees i conceptes per a expressar de manera efectiva el que vol transmetre. Una competència encara més important en la mesura en què també expressa el sentit cívic del seu autor i la capacitat d'interrelació i de convivència amb el conjunt d'usuaris del text digital.

2.5. Text segur

No és aconsellable intentar un ús normalitzat de dispositius i programes digitals des d'una preocupació obsessiva per la seguretat. Resulta més pràctic i efectiu adoptar com a habituals hàbits senzills d'informació i de prevenció d'eventuals riscos elementals. Quan treballem amb programes de tractament de text, és convenient consultar les seves opcions de seguretat i de protecció de documents, de manera que puguem:

- restringir l'accés al fitxer, seleccionant mitjançant contrasenya quins usuaris podran obrir-lo, i

- determinar amb quin nivell d'intervenció podrà operar cada usuari que accedeixi al fitxer: només lectura, edició, modificació de continguts...

La majoria de programes de tractament de textos permeten personalitzar les opcions de seguretat a través de menús que solen seguir l'itinerari **d'Eines > Opcions > Seguretat**. És important analitzar les opcions de protecció de documents que ens brinda cada programa determinat de tractament d'informació textual, ja que aquesta breu i senzilla exploració inicial ens donarà el control total sobre el contingut dels fitxers.

El control dels fitxers

El control dels fitxers adquireix la màxima importància en directoris i xarxes compartides, en l'àmbit professional del treball i de l'empresa, si compartim l'ordinador personal en l'àmbit domèstic i familiar o si utilitzem ordinadors i xarxes públiques per a treballar amb els nostres documents.

La seguretat és un factor determinant per a una convivència cívica fluida en entorns digitals de comunicació i interactivitat.

2.6. Continguts i drets

Els programes de tractament digital de la informació ens ofereixen grans facilitats per a capturar, usar, inserir i manipular tot tipus de continguts, tant textuals com d'imatge o de naturalesa multimèdia. Però hem de ser conscients que no tots els continguts són a la nostra disposició perquè els utilitzem sense limitacions.

Quan manegem informació digital, hem de distingir entre els següents tipus de continguts:

- Continguts subjectes a drets de propietat intel·lectual i a drets d'autor. Són continguts l'ús dels quals està regulat per l'Organització Mundial de la Propietat Intel·lectual (OMPI) en funció de disposicions legals que permeten als seus propietaris o a titulars disposar-ne sense que cap altra persona física o jurídica pugui utilitzar-los legalment sense el seu consentiment.

- Continguts de domini públic. Són aquells els drets de propietat intel·lectual dels quals ja han expirat i que, per tant, poden ser utilitzats per qualsevol usuari. Podem treballar amb aquests continguts sense cap limitació.

- Continguts *fair use*. Es tracta de continguts els titulars de drets d'autoria i propietat intel·lectual dels quals permeten explícitament que siguin utilitzats de manera lliure en determinats casos: si s'utilitza només part de l'obra i se'n cita degudament l'origen i l'autoria, si s'usen amb finalitats educatives o de formació, si s'empren en iniciatives no comercials i sense ànim de lucre.

  El concepte de *fair use*

  Té el seu origen en la jurisprudència legislativa nord-americana i introdueix l'opció d'un "ús raonable i legítim" per qualsevol usuari de continguts protegits per drets d'autor. Podem usar aquest tipus de continguts en un treball escolar o universitari i sempre esmentant-ne l'origen, però no podem utilitzar-los per a publicar un llibre els titulars de propietat i drets del qual siguem nosaltres mateixos.

- Continguts *copyleft*. Són continguts els titulars de drets de propietat dels quals autoritzen explícitament qualsevol usuari a utilitzar-los, modificar-los i distribuir-los. És un tipus de llicència d'ús de continguts en expansió a Internet i sol presentar com a única limitació la condició que els seus usuaris mantinguin la mateixa llicència *copyleft* per als nous continguts que generin a partir de la utilització lliure dels continguts previs.

  El concepte de *copyleft*

  Podem usar continguts amb llicència *copyleft*, però haurem de mantenir aquest ús lliure en els nous continguts que nosaltres generem. No podem usar continguts *copyleft* per a escriure i publicar un llibre que pensem sotmetre a la nostra propietat intel·lectual i pel qual vulguem obtenir drets d'autor.

Atendre el tipus d'informació que manegem quan usem els diferents mecanismes de tractament de la informació digital no solament pot estalviar-nos més d'un problema legal. També evidencia el grau de coneixement, capacitat i civisme en l'ús correcte dels continguts, més enllà de les habilitats tècniques d'edició i presentació de textos. D'altra banda, incideix decisivament en un ús convivencial de la Xarxa pel conjunt dels usuaris.

2.7. Plagi

En termes generals, s'entén per *plagi* l'ús literal i deliberat de continguts aliens, sense esmentar-ne la procedència i intentant transmetre que la seva autoria ens correspon i ens pertany.

L'ús de les tecnologies digitals i la gran facilitat amb què aquestes permeten replicar continguts de tot tipus i en tots els formats (text, dibuix, fotografia, vídeo...) afavoreix i facilita la còpia amb una doble repercussió:

- la vulneració dels drets d'autoria i propietat intel·lectual de l'autèntic autor, i
- l'engany de l'interlocutor en presentar-li com a creació pròpia una còpia d'un altre original.

Però convé tenir en compte que la mateixa tecnologia que facilita el plagi, n'accelera la detecció. És fàcil buscar, localitzar, copiar, enganxar o inserir continguts aliens per fer-los passar per creacions pròpies. Però és encara més ràpid enganxar un fragment de text en un motor de cerca, localitzar una fotografia o activar un programa específic sobre plagi i verificar l'origen real d'un contingut, la qual cosa posa en descobert l'intent d'apropiació indeguda.

Plagiar continguts és

- Antisocial i incívic:
  - perquè vulnerem els drets de propietat i autoria dels autèntics creadors dels continguts que copiem, i
  - perquè intentem enganyar l'interlocutor sobre la vertadera autoria dels continguts.
- Inútil:
  - qualsevol usuari detectarà l'engany utilitzant un simple motor de cerca,
  - un interlocutor qualificat localitzarà ràpidament la impostura gràcies als programes específics de localització de còpies, i

– els usuaris de les xarxes socials (blogs, comunitats virtuals, grups de treball en entorns virtuals...) denunciaran immediatament la còpia.

L'ús no acreditat de continguts aliens pot semblar una idea pràctica a primera vista, però en realitat pot portar-nos complicacions molt greus, com les següents:

- la desqualificació del treball acadèmic i la suspensió de la seva valoració,
- problemes (advertència, sanció...) en el lloc professional,
- descrèdit públic davant de la comunitat i les xarxes socials on exposem les nostres presumptes creacions i
- reclamacions legals dels autèntics autors o propietaris dels continguts.

2.8. Citació

La facilitat de localització i tractament de la informació de text que ens ofereixen els mitjans i les eines digitals fa imprescindible adoptar uns hàbits clars i permanents de citació de les fonts de les quals hem obtingut la informació que usem i editem. Un ús correcte d'informació procedent d'altres fonts comporta:

- distingir clarament mitjançant les opcions del processador de text les frases i els paràgrafs que importem directament d'una altra font, posar-los entre cometes i utilitzar un recurs tipogràfic diferenciat (cursiva, negreta, etc.),

- utilitzar les opcions de notes a peu de pàgina per referenciar de manera completa les citacions bibliogràfiques o webgràfiques de què hem extret determinats continguts textuals, i

Web recomanat

La Norma ISO-690 de referències electròniques ens proporciona indicacions normalitzades sobre com citar correctament les fonts electròniques d'informació. Per a més informació, podeu consultar:

http://www.ugr.es/~pwlac/G00_Referencias_electronicas.html)

- incloure enllaços a les fonts electròniques de la informació que presentem, com a opció d'aval i credibilitat de les dades que manegem.

Usar informacions alienes sense fer esment de la procedència situarà els nostres textos sota la sospita immediata i sistemàtica de plagi o còpia il·lícita. A més, contribuirà a la saturació de les xarxes amb més dades i continguts insuficientment acreditats i, per tant, sense cap garantia de credibilitat.

2.9. Hàbits sostenibles

2.9.1. Codi lliure

En termes generals, s'entén com a programes de codi lliure (*free software* o programes lliures) el conjunt d'aplicacions informàtiques que poden ser usades, copiades, modificades i distribuïdes lliurement i sense restriccions entre usuaris.

Davant els programes comercials sotmesos a llicències de pagament, l'ús de programes de codi lliure incideix en una major sostenibilitat de la societat i les xarxes digitals, perquè:

- atorguen a qualsevol usuari el dret d'usar lliurement aquest tipus de programes,
- permeten l'estudi dels seus codis i la realització d'adaptacions per a noves funcionalitats,
- autoritzen la distribució oberta de tot tipus de còpies dels programes i
- estimulen a introduir millores en les aplicacions i a difondre-les lliurement i universal.

L'ús de programes de codi lliure té una important dimensió cívica i social de creació i difusió de les utilitats informàtiques, ja que:

- fa arribar aplicacions digitals gratuïtament a persones i sectors socials que no tenen accés a programes comercials de pagament,

- estén al conjunt d'usuaris l'opció de millorar els programes i accedir més fàcilment a aquestes millores,

- el seu desenvolupament repercuteix en el benefici de tota la comunitat en la mesura que millora les prestacions i la seguretat per a cada un dels seus usuaris, i

- el caràcter obert estimula el sentit de pertinença a una comunitat d'usuaris i l'intercanvi de coneixements individuals a la Xarxa col·lectiva.

2.9.2. Impressió

Els programes informàtics de tractament de text presenten grans possibilitats per a la impressió de continguts digitals en suport de paper, de manera immediata i en grans quantitats. Un ús raonable de les opcions d'impressió requereix:

- no imprimir de manera sistemàtica i compulsiva tots els continguts que capturem, tractem i emmagatzemem a l'ordinador,

- no considerar la còpia impresa com una còpia de seguretat: les úniques còpies de seguretat útils seran les realitzades sobre suports digitals,

Còpia en paper

Una còpia en paper ens obligarà a repetir manualment l'elaboració d'un document.

- realitzar proves i esborranys en pantalla i no imprimir fins a estar segurs que necessitem una prova sobre paper, i

- distingir quin ús real volem donar a la informació, ja que una impressió en paper pot ser útil per a revisar informació en llocs i moments en què no disposem d'ordinador, dispositius o xarxes, però és prescindible si llegim aquest text al costat de la pantalla de l'ordinador.

Un ús sostenible de la impressió de documents ens estalviarà:

- costos econòmics personals, derivats de la despesa en paper per a la impressora i consumibles de tinta, i

- costos socials derivats del consum de paper, dels components químics de les tintes i del reciclatge industrial de components amb diversos graus de toxicitat (tòners, cartutxos de tinta, etc.).

3. Navegació segura

La connexió que utilitzem per a accedir a Internet ens converteix en un nus més de la Xarxa planetària de xarxes. La teranyina global posa al nostre terminal grans quantitats d'informació i opcions molt eficients de comunicació, però també ens exposa a alguns riscos que ens convé prevenir.

Internet genera espais socials d'intercanvi i interacció entre persones, en els quals les mesures de seguretat no són només elements fonamentals per a preservar la integritat i la privacitat dels nostres dispositius i dades, sinó que constitueixen també un factor bàsic de convivència i civisme, perquè:

- faciliten la fluïdesa de circulació d'informacions i dades,
- eviten la proliferació i l'extensió de virus i codis maliciosos,
- frenen l'efectivitat d'iniciatives fraudulentes massives relacionades amb les trameses de missatges no sol·licitats (*spam*), captura il·lícita de dades personals o intents d'estafa econòmica, i
- ajuden a prevenir usos il·lícits d'informació privada (dades, fotografies, vídeos...) de qualsevol usuari de la Xarxa.

Ens convé fer un ús segur d'Internet, pel nostre propi interès i perquè aquest coincideix en els seus principals objectius amb l'interès social del conjunt dels usuaris. Cada un de nosaltres obté beneficis personals d'un millor funcionament global i col·lectiu de la Xarxa, en la mateixa mesura que cada un de nosaltres pot contribuir quotidianament que Internet sigui millor, més eficient i més segura.

3.1. Seguretat a la Xarxa

La seguretat en la navegació i l'ús d'Internet té el seu factor bàsic i fonamental en els programes antivirus. Un ordinador connectat a Internet (sobretot si la connexió és de banda ampla) manté sempre les portes obertes al trànsit de dades i programes, davant dels quals hem de posar una barrera potent d'anàlisi, detecció i eliminació que actuï quan no en puguem garantir l'origen i la fiabilitat.

Quan estem connectats a Internet hem d'utilitzar un antivirus solvent i fiable:

- per a preservar l'equip i les dades d'eventuals intrusions no desitjades, danyoses o fraudulentes, i

- per l'imperatiu cívic d'intentar evitar convertir-nos en còmplices involuntaris de la distribució massiva d'un codi maliciós i d'activitats il·lícites de qui vulgui utilitzar el nostre ordinador i la connexió de manera remota per a perjudicar altres usuaris.

A més del ja exposat en el capítol **Dispositius electrònics > Antivirus**, quan ens connectem a Internet ens hem d'assegurar que l'antivirus ens garanteixi:

- protecció permanent davant de qualsevol intrusió a les xarxes i equips,

- actualització constant dels virus i codis maliciosos davant dels quals pot desplegar de manera automàtica accions de rastreig, avís, neteja i desinfecció,

- informació i alertes actualitzades sobre nous riscos i amenaces, i

- opcions flexibles de configuració perquè puguem determinar nivells de seguretat adequats a l'ús quotidià que fem de les xarxes i fitxers digitals.

A més de l'antivirus personal, també podem utilitzar complementàriament programes antivirus d'ús lliure per a reforçar l'acció preventiva:

- Des de l'escriptori. Programes antivirus gratuïts que podem instal·lar en cada un dels nostres equips per a verificar la neteja d'arxius i fitxers que baixem des d'Internet o des del correu electrònic. La seva capacitat d'ús sense connexió a la Xarxa obliga que els actualitzem regularment per a assegurar-nos que el nivell de protecció no ha quedat obsolet.

- Antivirus en línia. Opcions limitades de rastreig i detecció de virus i programes maliciosos, que funcionen des de la Xarxa i que ens serveixen, fonamentalment, per a verificar la neteja de la nostra màquina i els fitxers quan l'antivirus ens ofereix resultats dubtosos.

Web recomanat

L'Institut Nacional de Tecnologia de Telecomunicacions ofereix solucions gratuïtes actualitzades sobre antivirus d'ús puntual i eines de desinfecció. Per a més informació, podeu consultar:

- antivirus d'ús puntual:
  http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=1&pagina=0

- eines de desinfecció:
  http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=8&pagina=0

3.1.1. Tallafocs

Juntament amb els imprescindibles antivirus, els anomenats *tallafocs* (*firewalls*) són programes de la màxima utilitat quan usem un ordinador connectat a Internet, ja que ens permeten controlar i restringir tot el trànsit de dades entre la nostra màquina i la Xarxa. Aquest control pot resultar vital per a impedir l'entrada de virus i codis maliciosos a l'equip i per a tallar qualsevol intent de captura i fuga de dades del nostre ordinador des de la Xarxa.

En síntesi, un programa tallafoc actua sobre les connexions TCP/IP, que regulen els protocols d'Internet mitjançant els quals l'ordinador intercanvia informació amb la Xarxa a què connectat.

Una correcta configuració ens permet:

- monitorar de seguida qualsevol intent d'entrada a l'equip i denegar-lo si convé,
- controlar les connexions sortints i evitar la fuga d'informació que programes espia o codis maliciosos instal·lats inadvertidament a l'ordinador puguin intentar enviar a la Xarxa,
- impedir que l'activitat interna de l'ordinador sigui visible a Internet, i
- navegar de manera segura, en donar entrada i sortida només a programes prèviament autoritzats per nosaltres i preguntar en cada cas si autoritzem l'accés o la sortida de programes que no hem definit explícitament.

La majoria de sistemes operatius presenten programes tallafocs, però als ordinadors personals també podem optar per eines gratuïtes com les que ofereix l'Institut Nacional de Tecnologia de Telecomunicacions a la seva seu oficial.

Web recomanat

Podeu obtenir eines gratuïtes a:
http://alerta-antivirus.red.es/utiles/ver.php?tema=U&&articulo=2&&pagina=0

Igual que en l'ús dels antivirus, la utilització raonada i raonable de tallafocs ens ajuda a millorar el maneig de la Xarxa en dos nivells fonamentals i profundament relacionats, com són:

- la seguretat personal i la integritat d'equips i dades, i
- un ús social de la Xarxa més sostenible, fluid i segur pel conjunt d'usuaris del qual formem part.

3.1.2. Les xarxes Wi-Fi

Les anomenades *xarxes Wi-Fi* (*wireless fidelity*) permeten que els dispositius electrònics (ordinador, agenda electrònica, telèfon mòbil, etc.) accedeixin sense cables a Internet o a altres xarxes de dispositius si són prou a prop d'antenes repetidores o encaminadors (*routers*) del seu senyal corresponent.

Els avantatges que ens proporciona una connexió Wi-Fi de poder utilitzar la Xarxa sense fil en qualsevol lloc i en qualsevol moment poden augmentar o disminuir segons l'ús més o menys raonable que en fem. A la Xarxa domèstica, és convenient que configurem tots els paràmetres de seguretat d'aquell encaminador sense fil per evitar l'eventual entrada d'intrusos externs. Una xarxa Wi-Fi domèstica correctament configurada i protegida:

- Evita intrusions externes que puguin connectar-se a Internet i ocupar l'amplada de banda que tenim contractat (i pel qual paguem a l'empresa proveïdora del servei).

- Evita que qualsevol usuari en el radi d'acció de la Xarxa sense fil pugui introduir-se a l'ordinador i capturar dades i informació personal.

- Evita que la Xarxa faciliti la introducció en el nostre equip de virus i programes maliciosos.

De manera recíproca a les mesures d'autoprotecció, és recomanable el màxim de cura i correcció cívica en l'ús de xarxes sense fil de connexió aliena. Així, si utilitzem xarxes públiques o privades d'accés autoritzat, convé que ens cenyim a les normes d'ús establertes i que respectem la privacitat dels altres usuaris, sense utilitzar les eventuals deficiències de seguretat que puguem detectar per capturar informacions o dades personals d'altres usuaris.

En el cas de localitzar xarxes Wi-Fi alienes amb baix nivell de protecció, és recomanable respectar-ne la privacitat i evitar-ne l'ús, ja que aquest no solament seria fraudulent, sinó que ens exposaria a les intrusions de virus i programes maliciosos que poguessin tenir els ordinadors i les xarxes sense fil a què accedim il·lícitament. El Centre de Seguretat de l'Institut Nacional de Tecnologies de la Comunicació recomana el següent:

- Establir i definir el nombre màxim d'equips que es puguin connectar al punt d'accés.

- Apagar el punt d'accés i l'encaminador quan s'hagi d'utilitzar.

- Desactivar l'opció de difusió del nom de la Xarxa sense fil per a evitar que altres usuaris externs puguin identificar de manera automàtica les dades de la Xarxa.

- Canviar la contrasenya per defecte que ja porta incorporada l'encaminador, ja que molts fabricants utilitzen la mateixa clau per a tots els equips.

- Utilitzar sistemes d'encriptació per a impedir que el trànsit de la Xarxa sigui fàcilment llegible. Es recomana utilitzar el sistema WPA, ja que el sistema WEP és insegur.

- Desactivar l'assignació dinàmica d'IP a nous dispositius que sol·licitin la connexió a la Xarxa. És més segur fer dependre qualsevol connexió a una assignació manual d'IP.

3.1.3. Antiespies

En un ús regular i normalitzat de la Xarxa és molt convenient que reforcem la seguretat de l'ordinador davant dels anomenats *programes espia* (*spyware*).

Spyware

Són aplicacions informàtiques que solen entrar i instal·lar-se en l'equip de manera oculta quan baixem de la Xarxa i instal·lem a la nostra màquina determinats programes, gratuïts o no.

L'acció d'aquests programes sol centrar-se a recopilar informació del nostre sistema per a enviar-la a través de la Xarxa a bases de dades, generalment de caràcter comercial, on s'utilitzen posteriorment per a iniciatives comercials i publicitàries. Però alguns d'aquests codis maliciosos també poden recopilar i robar amb finalitats delictives dades tan personals com les claus bancàries que teclegem quan operem en els nostres comptes. Per a prevenir l'espionatge informàtic indesitjat és aconsellable:

- restringir la baixada de programes gratuïts a pàgines que ens ofereixin les màximes garanties de fiabilitat,

- llegir acuradament les condicions d'ús de programes gratuïts que podem baixar d'Internet i instal·lar a l'ordinador, i

- instal·lar programes antiespia, que
  - són complementaris d'antivirus i tallafocs, els quals ja detecten bona part dels codis maliciosos que intenten instal·lar-se a l'ordinador i
  - actuen específicament contra codis camuflats com programes normals per evitar les alertes d'antivirus i tallafocs.

Web recomanat

Podem accedir a una àmplia oferta d'antiespies gratuïts, sempre que abans en verifiquem la solvència i l'honestedat en centres de seguretat acreditats com l'Institut Nacional de Tecnologia de Telecomunicacions:

http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=10

3.1.4. E-comerç i banca electrònica

Si la seguretat general en l'ús d'Internet és important, la precaució resulta transcendental quan utilitzem la Xarxa per a efectuar transaccions comercials o operacions bancàries. En aquests casos, el que circula per la Xarxa són les claus d'accés als nostres comptes i les contrasenyes de les nostres targetes de crèdit. La possibilitat d'accés, en definitiva, als nostres recursos econòmics.

Risc a la Xarxa

Quan el que corre per la Xarxa és l'accés als nostres diners, hem de ser conscients que no estem exposats a majors riscos que en el món presencial, com extraviar una targeta de crèdit dins d'una bossa en un taxi, sofrir un atracament en un caixer automàtic, ser víctimes d'un assalt al portal del domicili o patir una estrebada al carrer.

Però, igual que en la vida quotidiana presencial, ens convé ser previnguts. I a la Xarxa hem d'adaptar la nostra seguretat a les característiques del món digital:

- Abans que res, ens convé efectuar operacions econòmiques només en webs i pàgines que ens mereixin una confiança total.

- És necessari que verifiquem l'acreditació comercial i bancària (adreça web, adreça electrònica, adreça física, telèfon de contacte...) de la pàgina en la qual introduirem les claus.

- És imprescindible observar que l'adreça de la pàgina on introduirem claus i contrasenyes comenci per http, cosa que indica que es tracta d'una connexió segura, i que apareix un *cadenat* () en la part inferior dreta del navegador.

- Ens convé assegurar-nos de la validesa dels certificats (polsant el cadenat), que coincideixen amb l'entitat sol·licitada i que són vàlids.

- És aconsellable evitar l'ús d'equips públics (cibercafès, estacions o aeroports, xarxes sense fil insuficientment acreditades...) per a realitzar operacions comercials o bancàries.

- També convé desactivar l'opció autocompletar si s'accedeix des d'un equip diferent a l'habitual o si es comparteix equip amb altres persones.

- Sempre hem de tancar la sessió de la web i el navegador quan finalitzem l'operació per evitar que algú pugui accedir als últims moviments o recuperar les claus que hem utilitzat.

La xarxa presenta tants riscos com la vida quotidiana presencial i, com en aquesta, és necessari mantenir actituds raonables i de sentit comú per a prevenir eventuals atacs o daltabaixos econòmics. El major percentatge de robatoris

i estafes a Internet no tenen el seu origen en sofisticats artefactes tecnològics, sinó en una gestió deficient o descuidada de claus i contrasenyes dels propietaris d'aquestes.

3.1.5. Precaucions addicionals

Filtres de contingut

Els anomenats *filtres de contingut* són programes informàtics que permeten bloquejar l'accés a determinades pàgines d'Internet en funció de paraules i expressions clau que l'usuari ha definit prèviament.

Els filtres de contingut resulten útils per a controlar i restringir l'arribada a l'ordinador d'informacions i imatges que considerem inconvenients o inadequades i s'utilitzen sobretot per a prevenir que usuaris infantils de l'ordinador domèstic trobin fortuïtament continguts als quals, per edat o per nivell de formació, no haurien de tenir accés.

Web recomanat

L'Institut Nacional de Tecnologia de Telecomunicacions proporciona una guia comentada de recursos gratuïts per al control parental a la seva pàgina oficial: http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=16&pagina=0

Al costat de la prevenció i el bloqueig informàtic de determinades pàgines web per paraules clau del seu contingut, la majoria d'experts aconsellen completar el control parental de l'accés dels menors a la Xarxa fomentant hàbits educatius:

- Educar els menors sobre els eventuals riscos que poden trobar quan naveguen per Internet.

- Acompanyar-los en el seu ús de la Xarxa, sempre que sigui possible i intentant que el menor no senti envaïda la seva intimitat personal.

- Advertir molt seriosament els menors dels perills de facilitar informacions personals (noms, adreces, telèfons, contrasenyes, fotografies, claus bancàries...) a persones desconegudes a través de qualsevol mitjà, presencial o electrònic.

- Conscienciar els menors que han d'informar immediatament de qualsevol conducta o contacte de la Xarxa que els resulti incòmode o sospitós.

- Acostumar-los a crear comptes d'usuari específics i limitats per a les activitats que vulguin realitzar a la Xarxa.

P2P

Si som usuaris de xarxes d'intercanvi de fitxers amb altres usuaris, ens convé tenir en compte que els programes P2P que utilitzem s'anomenen així precisament perquè van de punt a punt (*peer to peer*), és a dir, es donen entre iguals. Això vol dir que quan ens connectem a una d'aquestes xarxes ens convertim en client i servidor, en rebre i enviar arxius alhora. Per la nostra pròpia seguretat i responsabilitat en la convivència cívica a la Xarxa, és important que:

- Analitzem amb compte tots els arxius que baixem.

- Evitem intercanviar programes o continguts que no presentin garanties de respecte als drets de propietat i autoria, ja que la distribució il·lícita d'informació o fitxers protegits podria plantejar-nos problemes legals i, fins i tot, implicar-nos en delictes.

- Executem el programa client P2P eMule, BitTorrent, Pando, Ares o Nosolodescargas(entre molts d'altres) en una sessió d'usuari amb permisos limitats per aïllar-lo d'altres components crítics del sistema.

- Prestem la màxima atenció a l'extensió dels fitxers que baixem per evitar introduir per error o distracció fitxers executables (extensión.exe) quan en realitat pensàvem baixar un altre tipus d'arxius.

- Modifiquem el nom de les carpetes de baixada.

Precaucions

Modificar el nom de les carpetes de baixada és important, ja que molts codis maliciosos busquen rutes fixes per replicar-se. També convé fer molta atenció a les caselles de les carpetes que realment estarem compartint a la Xarxa. Una mala elecció, o deixar activades les carpetes que alguns programes P2P marquen per defecte, pot exposar a les xarxes d'intercanvi arxius i continguts del disc dur que en cap cas no voldríem veure circulant per la Xarxa.

- No posar a disposició de l'intercanvi fitxers o continguts que puguin ofendre, ferir la sensibilitat o atemptar contra la convivència cívica amb la resta d'usuaris d'aquest tipus de xarxes.

3.2. Localització d'informació

3.2.1. Cerca a la Xarxa

Internet posa al nostre abast una incalculable quantitat d'informació. Però la dada que busquem no sempre és visible i localitzable de manera immediata a causa de la proliferació de fonts, de les diverses maneres d'organitzar la informació i de la seva acumulació indiscriminada. Per buscar i localitzar informació de manera eficient a la Xarxa, ens ajudarà:

- definir exactament què és el que estem buscant en cada cas,
- informar-nos amb regularitat sobre les noves eines de cerca disponibles a la Xarxa, analitzar-ne el funcionament i provar-ne les actualitzacions,
- utilitzar les eines de cerca generalista per localitzar fonts especialitzades d'informació que puguin portar-nos a les dades específiques desitjades, i
- guardar i ordenar els resultats rellevants de les localitzacions d'informació com a possibles fonts, ja localitzades, que ens facilitaran posteriors cerques d'informació.

La Xarxa conté pràcticament totes les respostes que podem necessitar. Tan sols li hem de formular les preguntes correctes i en la forma adequada. De vegades, el procés requereix cert temps, però sol ser una inversió altament rendible en resultats informatius i rapidesa de localització.

3.2.2. La localització

Abans de començar a utilitzar qualsevol motor de cerca d'informació ens pot ser molt beneficiós realitzar algunes accions prèvies que, encara que poden representar una petita inversió inicial d'atenció, acabaran estalviant temps i millorant resultats:

- Plasmar els objectius de cerca en una llista de termes concrets, representatius i definitoris que pensem que presenten les màximes possibilitats d'identificació per a l'eina de cerca.
- En la llista de termes convé incloure sinònims i paraules relacionades que puguin ajudar a delimitar l'àmbit de localització del cercador, així com noms d'empreses o institucions que pensem que poden contenir dades o informacions relacionades amb els nostres objectius de localització.

- En determinats tipus de cerca o fases de localització pot ser aconsellable també definir frases literals molt concretes que creiem que poden estar relacionades amb la informació que busquem.

- Analitzar el funcionament i els criteris sintàctics de consulta que utilitza cada eina de cerca. Per a fer-ho és aconsellable revisar les seccions d'ajuda i de preguntes més freqüents (PMF o, en anglès, FAQ) que solen presentar la majoria de cercadors.

A més de conèixer el funcionament específic de cada eina de cerca, quan desitgem formular una consulta també ens ajudarà tenir en compte:

- l'àmbit idiomàtic preferent on busquem la informació i l'idioma d'ús del cercador que utilitzem,

- en cerques molt dirigides i concretes, la utilitat de l'ús de frases textuals, normalment entre cometes,

- combinar diversos termes relacionats, ja que pot ser efectiu sempre que tots siguin molt definits i facin referència a un objectiu molt concret, i

Buscar informació

Si busqueu dades o informació que podeu preveure que hi haurà a la Xarxa en anglès, formular les consultes mitjançant termes en català, per exemple, pot provocar resultats molt distorsionats.

L'ús de les cometes

Per a localitzar, per exemple, el text d'*El Quixot* pot ser eficient formular "en un lugar de la Mancha".

- l'ús de lletres majúscules i minúscules, ja que pot fer variar els resultats de la localització.

Consultes en funció de la tipografia

Normalment, les consultes en minúscula tornen resultats sense filtrar per criteri tipogràfic, mentre que sovint la consulta de termes amb la lletra inicial en majúscula restringeix els resultats a noms propis.

3.2.3. Cerca avançada

Els motors de cerca més potents solen presentar opcions de cerca avançada que poden ser-nos molt útils per a obtenir un primer filtratge automàtic dels resultats localitzats, sempre que hàgim definit i delimitat prèviament els criteris en els quals emmarquem la cerca. Les opcions de cerca avançada presenten com a paràmetres més freqüents:

- Incloure o excloure termes: ens permet definir si els resultats de la consulta han d'incloure tots els termes introduïts en el formulari, si han de recollir tots els resultats que inclouen qualsevol dels termes plantejats o si només han de presentar resultats sense determinats termes concrets.

- Poder restringir la cerca només a una frase o formulació concreta.

- Delimitar el retorn de resultats que estiguin redactats en un idioma determinat.

- Limitar la cerca a les dates més recents d'actualització de les pàgines contingudes en la base de dades del cercador.

- Definir si els termes de consulta han d'aparèixer en el títol, en el text complet, en l'adreça electrònica de la pàgina web o en els enllaços que aquesta conté.

- Seleccionar el format de la informació de la qual ens interessa rebre resultats.

- Buscar pàgines amb enllaços a un determinat web o domini.

3.2.4. Credibilitat

La majoria de criteris que ens seran útils per a verificar la credibilitat dels resultats de cerca estan relacionats amb la font d'informació on localitzem continguts. La major o menor presència d'aquests criteris en un web, blog o motor de cerca n'avalarà més o menys la fiabilitat. Els principals criteris de credibilitat que hauríem de tenir en compte són:

- Autoria. Un autor identificat, sigui individual o col·lectiu, proporciona més fiabilitat que una font informativa anònima, sobretot si, a més d'identificar-se, el responsable dels continguts en qüestió presenta acreditacions de caràcter professional i elements de contacte, com una adreça electrònica. Es tracta d'un criteri especialment rellevant en el cas de blogs i iniciatives de publicació personal d'informació a la Xarxa.

- Filiació i autoritat. Més enllà de l'autoria personal, la credibilitat de qualsevol pàgina web requereix la menció explícita i clara de l'organisme, de la institució o de l'empresa de què depèn. La referència a l'entitat que subministra els continguts o el suport econòmic de la publicació ens permetrà no solament avaluar la fiabilitat, sinó també el grau d'autoritat de la font d'informació en el seu àmbit d'actuació o de coneixement.

- Actualització. Un nivell fonamental de valoració de la informació localitzada està vinculat a les dates de creació d'aquell contingut, de la seva presentació en una determinada web i, sobretot, de la seva última actualització.

- Crèdits i procedència. La citació explícita de l'origen de la informació és una garantia clara de credibilitat, perquè situa els continguts i ens permet acudir a la font original de la informació per contrastar i ampliar dades. És aconsellable sotmetre a la revisió crítica i a la verificació sistemàtica tots aquells continguts que localitzem si no aclareixen quina és la seva font originària d'informació.

- Objectivitat. En els casos de webs i pàgines amb publicitat, un criteri complementari de verificació de la seva credibilitat és la distinció clara i definida entre els continguts informatius i els de caràcter publicitari o propagandístic.

3.2.5. Certificacions

Encara que no hi ha una única autoritat que acrediti de manera universal la qualitat i la credibilitat dels continguts que circulen per Internet, diverses agències i entitats han creat estàndards d'anàlisi i valoració de pàgines web, la majoria dels quals estan centrats en criteris d'accessibilitat, legalitat, autocontrol i defensa dels consumidors i usuaris. Aquestes entitats tenen àmbits bastant heterogenis i fragmentats d'estudi i actuació i solen assignar les pàgines que se sotmeten voluntàriament als seus controls determinats segells de qualitat en reconeixement dels requisits que compleixen.

Malgrat que cap segell de qualitat no garanteix, ara com ara, la credibilitat dels continguts d'una determinada pàgina web, el fet que una web determinada presenti una acreditació o una altra afegeix cert grau de fiabilitat, associat almenys a la voluntat dels responsables de la pàgina de sotmetre's a determinats controls externs. Els principals segells de qualitat i control que podem trobar en pàgines web són els següents:

- ICANN (Internet Corporation for Assigned Names and Numbers). Es tracta d'una entitat que regula l'assignació de dominis a Internet.

- IQUA (Agència de Qualitat d'Internet). El seu segell verifica paràmetres sobre accessibilitat, usabilitat, seguretat, legalitat i protecció de menors. Està avalada per institucions públiques com el Consell de l'Audiovisual de Catalunya o els consells de Navarra i Andorra i l'organisme Red.es, dependent del Govern espanyol.

- W3C. Aquest consorci, format per més de 400 associacions, emet una certificació de qualitat internacional en funció, sobretot, de criteris d'accessibilitat.

- AUI (Associació Espanyola d'Usuaris d'Internet). Més que segell de qualitat, promou l'adhesió de webs respecte a criteris de defensa dels interessos i els drets dels usuaris de la Xarxa.

- AI (Associació d'Internautes). Es tracta d'un organisme de defensa dels usuaris d'Internet, sobretot respecte a operadores telefòniques, empreses i serveis relacionats amb la Xarxa.

4. Comunicació sostenible

4.1. Correu electrònic efectiu

El correu electrònic és l'instrument que fins aquest moment s'ha revelat com a més efectiu i utilitzat en la comunicació personal virtual. Milions de persones de tot el món usem constantment el correu electrònic per a comunicar-nos de manera instantània. La seva efectivitat tecnològica és fora de tot dubte. La seva eficiència com a canal de comunicació depèn de l'ús que fem cada un de nosaltres com a usuaris.

Com hem d'usar el correu electrònic amb la màxima efectivitat comunicativa?

Es pot fer amb hàbits molt senzills i sense cap complicació tecnològica:

- Escriure bé
  - La majoria de missatges que intercanviem es basen en el text. Els nostres interlocutors entendran millor i més ràpidament missatges redactats amb correcció, estructurats raonablement, que no siguin excessivament llargs i que no presentin repeticions o reiteracions innecessàries d'idees i conceptes.

  - La immediatesa de redacció i de tramesa de missatges pròpies del correu electrònic ens permet precisament prendre uns minuts per a ser correctes en l'ortografia i en la sintaxi del missatge, per a rellegir i retocar el contingut diverses vegades fins a definir amb precisió el que volem transmetre i enviar finalment només el contingut necessari.

  - Cal analitzar les regles específiques per a redactar correctament missatges de correu electrònic: no són necessàries les abreviatures pròpies dels missatges de text entre telèfons mòbils (per exemple, *xq* ('perquè') no està justificat en un missatge de correu electrònic; l'ús constant de MAJÚSCULES ÉS EQUIVALENT A CRIDAR, I A QUI LI AGRADA UNA COMUNICACIÓ FETA A CRITS?).

- Definir el missatge
  - El tema o assumpte del missatge és molt important perquè permet al receptor organitzar la seva atenció i el seu temps en funció del títol de la nostra crida.

  - Hem d'emplenar sempre el camp del tema o assumpte del missatge i hem de fer-ho condensant l'element informatiu principal del correu electrònic.

  - Com més precís i adequat sigui el tema o assumpte dels missatges que enviem, més ràpida i concreta serà la resposta del nostre interlocutor.

- Identificar el missatge
  - Les normes bàsiques de cortesia són fonamentals en l'encapçalament dels missatges. No és el mateix dirigir-nos pel nom de pila a un amic que fer-ho protocolàriament a una empresa o que ometre qualsevol encapçalament, de manera que el destinatari pugui pensar que rep un correu automàtic no sol·licitat.

  - La signatura és imprescindible perquè l'interlocutor pugui identificar l'autor del missatge. Hem de valorar amb compte en cada cas quines dades incloem en la signatura del missatge segons el grau de confiança en el nostre interlocutor: nom i cognoms complets, telèfon, adreça, altres adreces professionals de correu electrònic, etc.

La màxima efectivitat de comunicació individual en l'ús del correu electrònic coincideix sempre amb la seva màxima eficiència cívica i social: pensar en el receptor sol ser la clau fonamental per a fer el millor ús del correu electrònic.

4.2. Correu electrònic sostenible

El correu electrònic ens permet la transferència instantània de grans quantitats d'informació mitjançant l'opció d'adjuntar fitxers als missatges. Davant d'aquesta possibilitat, ens hem de preguntar **sempre**: és realment necessari? Uns consells bàsics per a una comunicació raonable i sostenible mitjançant el correu electrònic són els següents:

1) No adjunteu fitxers amb poca informació.
Si necessiteu transmetre informació que es pot condensar en deu o quinze línies de text, és millor copiar-les i enganxar-les en el text del missatge. Evitareu a l'interlocutor el temps necessari per a baixar el fitxer adjunt i li permetreu dedicar aquell temps de baixada i gestió a descobrir què voleu dir-li.

2) És millor que no adjunteu fitxers grans.
  a) Assegureu-vos que, en adjuntar un fitxer de grans dimensions, sigui de tant interès per a l'interlocutor que li compensi el temps de connexió de baixada i el temps i l'espai de gestió del fitxer en el seu ordinador.

b) Si creieu que heu d'enviar un fitxer adjuntat que supera els 500 kb, envieu abans un missatge en què demaneu permís i justifiqueu raonadament la tramesa.

3) Utilitzeu un compressor per a enviar fitxers que pesin molt o conjunts d'arxius.

a) Programes de compressió d'informació com WinZip, WinRar o 7Zip redueixen sensiblement la mida dels fitxers que enviem i n'agiliten la transmissió. També empaqueten en una sola carpeta diversos arxius, amb la qual cosa facilitem a l'interlocutor la baixada del material enviat i la seva organització en el disc dur.

b) Abans d'enviar fitxers comprimits és convenient que:

- Ens assegurem que el nostre interlocutor disposa del programa adequat per a descomprimir-los i accedir-hi o que li facilitem informació per obtenir el programa necessari.

- Hàgim acordat la tramesa amb el nostre interlocutor i tinguem la seva autorització i la seguretat que espera aquests continguts a què dedicarà temps de baixada i organització.

4) Eviteu formar part de les cadenes de missatges.

a) Analitzeu quins missatges reenvieu, a qui i per què. El reenviament compulsiu de missatges, amb fitxers adjunts, a tota la llista de contactes pot ocasionar una pèrdua de temps i de cost de connexió a tots aquells que no estiguin molt interessats a formar part de les cadenes de missatges.

b) Assegureu-vos que els missatges que reenvieu als vostres contactes no formen part de cadenes de correu electrònic dissenyades per a estafar els usuaris o per a obtenir de manera il·lícita les seves adreces electròniques o que introdueixin en els equips programes espia o virus informàtics.

4.3. Correu electrònic segur

Juntament amb els seus indubtables avantatges, l'ús intensiu del correu electrònic comporta també alguns riscos que podem prevenir de manera responsable amb senzills hàbits de seguretat, pel nostre propi interès i per la seguretat dels usuaris amb qui ens comuniquem electrònicament. La seguretat en l'ús del correu electrònic depèn fonamentalment de rutines tan senzilles com aquestes:

- No obrir fitxers adjunts de missatges de procedència desconeguda o l'aparença dels quals resulti directament sospitosa. Abans d'inspeccionar

un missatge compulsivament convé parar-se a pensar uns segons quins elements i de qui procedeixen introduirem en el nostre equip.

- Analitzar amb l'antivirus de confiança qualsevol document rebut per correu electrònic abans d'executar-lo a l'ordinador.

- Configurar correctament l'antivirus que analitzi els fitxers que obrim des del correu electrònic i que ens avisi i en paralitzi immediatament la baixada si detecta elements sospitosos.

- Utilitzar filtres contra el correu electrònic no desitjat i activar totes les opcions de bloqueig d'aquest tipus de missatges que ens ofereixi el programa de gestió de correu electrònic que utilitzem.

- No introduir l'adreça electrònica en formularis o llistes de correu que no ens mereixin una confiança raonable.

No facilitar l'adreça electrònica.

Aquesta actitud preventiva hauria d'incloure no respondre mai missatges dubtosos ni cadenes de correus per a evitar que el missatge de resposta sigui utilitzat com a confirmació que el nostre compte de correu existeix i és operatiu.

- No difondre col·lectivament les adreces electròniques que guardem a l'agenda o a la llista de contactes.

Tramesa a múltiples destinataris

Si volem enviar un missatge a un grup de contactes, convé posar la nostra adreça en el camp del destinatari i utilitzar el camp de còpia oculta (CCO) per a posar les adreces de tots els destinataris. Així, l'adreça de cada un d'ells no quedarà exposada a la vista de la resta de destinataris. De manera similar, hem d'esborrar l'historial de destinataris abans de reenviar un missatge a diverses persones.

Les claus bàsiques d'una comunicació electrònica segura són, sobretot, uns hàbits personals de maneig raonable, responsable i cívic de missatges, fitxers i programes de correu electrònic.

4.4. *Spam*

La recepció massiva de missatges de correu electrònic no sol·licitats constitueix una de les plagues digitals de més difícil solució global per les seves dimensions i conseqüències immediates. El bombardeig intensiu de l'anomenat *spam* o correu brossa provoca:

- ocupació estèril de gran part de l'amplada de banda de totes les xarxes, troncals i sectorials, d'Internet,

- àmplia pèrdua de temps dels usuaris per a gestionar i discernir degudament el correu brossa dels missatges importants i per a eliminar les missives electròniques no pertinents,

- risc d'entrada en l'equip propi de virus i codis maliciosos i la conseqüent pèrdua de temps per a detectar i eliminar eventuals infeccions, i

- perill d'extensió d'infeccions i estafes per un reenviament intens de missatges maliciosos als nostres contactes, sigui per la capacitat de codis ocults per a reenviar-se automàticament, sigui per una gestió descurada d'aquest tipus de missatges per la nostra part.

I davant d'aquest ús indegut de les xarxes telemàtiques, ens convé, per tant, respondre-hi amb contundència:

- Utilitzant diverses adreces electròniques, que ens permetin aïllar en bústies separades el correu brossa i l'intercanvi de missatges amb els nostres contactes importants.

Una manera de controlar el correu brossa

Una adreça secundària de correu electrònic per a utilitzar en formularis web o en llistes de correu ens serà molt útil, ja que podrem rebutjar-la fàcilment si es converteix en canal de distribució de missatges no desitjats.

- Evitant difondre la nostra adreça electrònica en webs de baixa fiabilitat, on pot ser fàcilment capturada pels programes i individus dedicats al trànsit d'adreces.

- Intentant no participar en cadenes de missatges que confirmaran la validesa de la nostra pròpia adreça electrònica i posaran en descobert les dels nostres contactes.

- Protegint els contactes de la nostra agenda, reenviant-los els missatges poc fiables utilitzant el camp CCO (amb còpia oculta).

- No responent mai un missatge indesitjat o poc fiable ni les instruccions que alguns d'aquests presenten per a no rebre més missatges similars: solen ser falses i confirmen a l'emissari la validesa del compte de correu electrònic.

- Denunciant a les autoritats competents la tramesa de correu brossa i participant en la creació de llistes negres.

- Utilitzant filtres *anti-spamming* (antiinundació):
  - Ens convé configurar adequadament els filtres que posa a la nostra disposició el proveïdor del compte de correu electrònic.

- Poden ser-nos molt útils els reforços *anti-spamming* (antiinundació) que presenten nombroses eines gratuïtes de protecció, sempre que prèviament n'acreditem la credibilitat amb l'aval d'organismes solvents.

Web recomanat

Un organisme solvent és l'Institut Nacional de Tecnologia de Telecomunicacions: http://alerta-antivirus.red.es/ utiles/ ver.php?tema=U&&articulo =11&&pagina=0

4.5. L'etiqueta

El 1995, en plena prehistòria d'Internet, la directiva d'Intel Sally Hambridge ja va intentar plasmar en un document tècnic el primer protocol de bones pràctiques en l'ús de la Xarxa. La seva iniciativa ha anat evolucionant en una infinitat de recomanacions que, sense arribar a cristal·litzar en codis de conducta, constitueixen un autèntic manual del bon ús dels canals digitals de comunicació.

Web recomanat

Per a més informació sobre el primer protocol de bones pràctiques en l'ús de la Xarxa podeu consultar:http:// www.rfc.net/rfc1855.html

Es coneix popularment amb el nom de *netiquette* (o etiqueta en la seva versió catalanitzada), que ha sorgit a partir de conjuntar el terme francès *etiquette* (bona educació) amb el vocable anglès *net* (xarxa). Sense que necessàriament hàgim de considerar-la i assumir-la com una normativa tancada de comportament, l'evolució de l'etiqueta ens proporciona recomanacions que convé tenir molt en compte per a aprofitar al màxim les potencialitats comunicatives dels canals digitals a partir del sentit comú i les convencions socials que els humans ja havíem anat desenvolupant abans de l'aparició i el desenvolupament d'Internet. En síntesi, l'etiqueta ens aconsella el següent:

- Els missatges de correu electrònic han de ser concisos i breus: convé recordar que és més difícil llegir en una pantalla que en paper.

- La presentació és important: escriure en majúscules, per exemple, fa la impressió de cridar.

- Igual que al món presencial, és recomanable no ser groller.

- El tema del missatge és imprescindible: fa al nostre interlocutor més fàcil catalogar, prioritzar i llegir el correu.

- Quan s'envia un mateix correu a moltes persones, és millor ocultar-les escrivint-ne les adreces en el camp BCC-CCO i posant l'adreça pròpia a TO-Per a.

- Convé organitzar les idees i pensar bé què s'escriurà. Potser us serveixi fer-ne abans un esborrany. També és bo corregir l'ortografia.

- Privacitat: el correu que s'envia és públic i permanent. No digueu res per correu de què no vulgueu que quedi constància per escrit ni de què altres s'assabentin.

- És millor no participar en cadenes de missatges.

Cadenes de missatges

Fer cartes cadena té diverses implicacions. Gasta amplada de banda que podria ser més ben utilitzat (i que costen diners a altres persones) i molt probablement algun *spammer* capturarà les adreces i enviarà molts correus no desitjats. Els acudits, els arxius adjunts de presentacions PowerPoint i altres ocurrències textuals o gràfiques també cauen dins aquesta categoria, per la qual cosa la regla pot resumir-se així: millor que no envieu correus que les altres persones no estan esperant ni desitgen especialment.

- Atenció amb els arxius adjunts: si adjunteu massa fitxers o són molt grans triguen bastant a ser transmesos per la Xarxa i en fan més difícil la recepció al destinatari. En general és recomanable que, si l'arxiu adjunt supera els 500 kb, demaneu permís per enviar-lo.

- La signatura de tots els missatges és més que recomanable: acredita la nostra personalitat, avala el contingut i marca l'acabament del contingut de la missiva electrònica. És encara més imprescindible quan intercanviem missatges relacionats amb la feina o els estudis.

Amb recomanacions més o menys vigents a través de l'evolució d'Internet, l'etiqueta ens recorda la clau fonamental de la comunicació en xarxa: formem part d'un conjunt de persones interrelacionades electrònicament. Per tant, com més cíviques siguin les nostres accions individuals a la Xarxa, millor contribuirem a la convivència en els seus diferents àmbits socials i més ens en beneficiarem individualment com un més dels seus membres.

4.6. Interactuem en xarxes socials

Més enllà de la localització d'informació i de la comunicació bidireccional, l'ús d'Internet ens permet interactuar en comunitats de diferent signe i format com la missatgeria instantània, blogs, xarxes socials... Es tracta de diferents àmbits d'actuació electrònica en què la nostra actitud digital serà decisiva per a fer més ràpida, fluida, eficient i directa la interacció immediata i permanent amb altres usuaris... o per a dificultar-la fins al punt de fer-la impossible o perillosa.

4.6.1. Missatgeria instantània

Els programes clients de missatgeria instantània ens proporcionen els indubtables avantatges de la comunicació permanent amb altres usuaris en temps real. No obstant això, també requereixen alguns hàbits d'ús raonable perquè la seva eficàcia comunicativa sigui òptima.

Programes de missatgeria instantània

El popular Messenger de Windows, però també Yahoo! Messenger, Google Talk, AIM, ICQ...

Des del punt de vista de la gestió:

- Ens convé ser selectius quan agreguem contactes: una llista extensa d'amics ens pot obligar a dedicar un temps excessiu a l'atenció de les peticions de conversa.

- Configurar correctament l'estat a les xarxes de què formem part ens ajudarà a seleccionar les converses que podem i que volem atendre en cada moment.

- La correcció sintàctica dels missatges, i el seu to, dependran en cada cas del grau de familiaritat i de confiança amb l'interlocutor o la xarxa de conversa. En converses col·lectives molt àmplies, convé mantenir una redacció i un to correctes i tan neutres com sigui possible.

I des de la perspectiva de la seguretat:

- És aconsellable evitar invitacions a la conversa que resultin sospitoses o que tinguin un origen desconegut, sobretot si ens requereixen que visitem altres pàgines web: poden ocultar una font de transmissió de virus o de programes espia.

- Quan agreguem contactes al client de missatgeria, ens convé tenir un coneixement raonable de qui és realment l'interlocutor. És aconsellable la màxima precaució davant de possibles contactes que ens resultin desconeguts.

- Davant dels fitxers adjunts, en la missatgeria instantània ens convé mantenir les mateixes prevencions que apliquem en l'ús del correu electrònic.

- En els missatges instantanis convé no incloure mai dades personals confidencials com contrasenyes, claus bancàries o números de compte, numeració de targetes de crèdit...

4.6.2. Els blogs

L'estil, el to i la correcció de les anotacions són definitoris de la identitat i credibilitat de l'autor d'un blog. Al costat de l'acceptació generalitzada d'estils personals de redacció i expressió, el tipus de llenguatge i la forma de plasmar-lo poden acreditar o desautoritzar un blog de manera global i potenciar-ne o limitar-ne les expectatives de comunicació i relació. Com a autors i com a lectors de blogs, pot ser-nos de molta utilitat tenir en compte el següent:

- Des del punt de vista de la comunicació amb lectors i usuaris, la redacció d'anotacions hauria d'anar orientada a la conversa i a l'obertura i al manteniment de diàlegs i debats.

Narracions personals

La simple projecció de pensaments subjectius i narracions personals no afavoreix l'establiment de relacions ni la creació de vincles de comunitat amb altres usuaris. Per tant, tampoc no ajuda a generar noves entrades ni circulació de comunicació.

- Des de la perspectiva de la visibilitat del blog, convé redactar les anotacions amb brevetat i amb tendència a insistir en aquells termes i conceptes que considerem clau. A més de facilitar el comentari dels lectors, convé recordar que els cercadors i sindicadors de continguts inclouen el titular i les primeres frases de les anotacions: el que aparegui en els titulars i primeres paraules serà el reclam que atraurà l'atenció de possibles lectors i les seves eventuals intervencions.

- L'actualització freqüent de continguts és fonamental per a mantenir el moviment comunicatiu en el blog i generar dinàmiques de relació, alhora que també incidirà en el grau de credibilitat, tant dels continguts, com de la mateixa intencionalitat comunicativa de l'autor.

- L'ús intensiu de l'enllaç d'hipertext és un dels elements definitoris del blog com a mitjà d'edició i de publicació i el que el diferencia d'altres canals (com els basats en el paper) i d'altres formats (com els formats electrònics tancats o fora de xarxa). Una utilització restrictiva d'enllaços en un blog és clarament contradictòria amb la seva naturalesa com a mitjà de comunicació i relació en xarxa.

Els blogs, igual que la missatgeria instantània i les xarxes socials, ens converteixen en membres de comunitats en les quals ens convé actuar amb actituds digitals bàsiques de respecte i conducta cívica. D'aquesta manera, millorarem el funcionament i la fluïdesa i la interacció entre els membres d'aquestes comunitats i ens beneficiarem de millores com a membres d'aquestes xarxes.

4.6.3. Xarxes socials

L'ús de la majoria de canals d'Internet, per la seva pròpia naturalesa, ja ens integra en xarxes socials de característiques diverses: xarxa de contactes del correu electrònic, grups de contactes en programes de missatgeria instantània, teranyines de blogs i comunitats que comparteixen vídeos, arxius d'àudio...

Comunitats virtuals

Comunitats virtuals com Facebook o MySpace han consolidat el grup d'amics per Internet com una de les xarxes socials per excel·lència, en dotar de canals tecnològics d'interacció permanent els seus usuaris i els seus amics i coneguts, i els amics i coneguts d'aquests, etc. en una teranyina pràcticament interminable de contactes, interessos i aficions compartides.

Formar part d'aquestes xarxes socials presenta innombrables avantatges, sempre que adoptem hàbits d'ús i de gestió tan sostenibles i raonables com els que exigim als altres membres de la comunitat:

- Les xarxes socials i els grups d'amics faciliten la tramesa de missatges i de recomanacions massives a tots els nostres contactes: restringir-los als casos

necessaris farà que estalviem recursos i evitarà que els nostres contactes optin per deixar de ser-ho quan es cansin d'una insistència repetitiva en assumptes que no els interessen.

- Ens convé afegir i deixar-nos ser afegits a grups de membres amb qui tenim realment interessos semblants.

- És recomanable no instal·lar aplicacions de manera generalitzada: una bona manera per a seleccionar les aplicacions que volem instal·lar és comprovar quines utilitzen més assíduament els amics de la Xarxa social.

- També convé evitar enviar sistemàticament invitacions a tots els contactes: és millor seleccionar un grup d'amics afí, interessats prèviament a la recepció de l'esmentada invitació.

- No s'ha d'afegir com a amics gent desconeguda: col·leccionar amics no fa més populars els usuaris. Tampoc no és recomanable acceptar com a amigues totes les persones desconegudes que ho sol·licitin, ja que són propenses a reenviar tot tipus de correu brossa social.

- Convé participar només en grups d'interessos afins. La quantitat de contactes en una xarxa social té una rellevància infinitament menor que el coneixement concret expressat en participacions i casos determinats.

Els contactes

Els contactes pels contactes serveixen de poc, ocupen molt temps de gestió i generen un incalculable volum de trànsit innecessari i estèril.

4.6.4. Privacitat

La proliferació de xarxes socials i d'intercanvi d'arxius entre usuaris atorga especial sensibilitat a les qüestions relacionades amb la privacitat de les persones, més enllà, fins i tot, dels drets legals explícits de propietat o autoria sobre els continguts. Davant de la multiplicitat d'arxius de so, fotografies i vídeos que podem obtenir a la Xarxa i gestionar fàcilment amb els programes de tractament digital, ens convé adoptar com a límit raonable el respecte a la intimitat i la privacitat.

Respectem la privacitat dels altres usuaris:

- No utilitzant sense un permís explícit les seves fotografies i vídeos en els nostres propis fitxers digitals i menys si pensem utilitzar-los públicament de manera presencial (presentacions, treballs, estudis...) o a la Xarxa (blogs, videoblogs, xarxes socials...).

- No distribuint aquests continguts en la nostra llista de contactes de correu electrònic, comunitats virtuals, xarxes professionals o de formació...

Respectem la nostra pròpia privacitat:

- Valorant acuradament a qui i com enviem a fitxers privats de so, imatge o vídeo, i a qui i com hi donem accés.

- Analitzant quins drets de propietat i gestió podrem mantenir sobre els nostres fitxers de so, imatge o vídeo si els allotgem en determinats servidors gratuïts d'Internet.

- Tenint en compte que els nostres fitxers d'imatge i so poden continuar circulant per la Xarxa més enllà de les previsions inicials i que aquesta projecció pot persistir en el temps molt més del que havíem previst o del que ens pugui interessar quan passin les setmanes, els mesos, els anys...