

# Internet segur per a tothom

---

## Beneficis i riscos d'Internet en els menors

<b>1. INTRODUCCIÓ</b>	<b>3</b>
1.1. Què és Internet?	
1.2. Per què cal parlar de “seguretat a la xarxa”?	
<b>2. SERVEIS QUE ENS OFEREIX INTERNET: BENEFICIS, RISCOS I RECOMANACIONS</b>	<b>4</b>
2.1. Navegació: recerca d'informació	
2.2. Correu electrònic	
2.3. Messenger	
2.4. Xats i fòrums	
2.5. Realització de tràmits i comerç electrònic	
2.6. Entreteniment a la xarxa	
<b>3. EINES DE CONTROL</b>	<b>17</b>
3.1. Pàgina d'inici	
3.2. Configurar la seguretat del navegador	
3.3. Filtrat de continguts	
3.4. Us del arxius temporals	
3.5. Definir comptes d'usuaris restringides	
<b>4. SISTEMES DE SEGURETAT</b>	<b>22</b>
4.1. Tallafocs	
4.2. Programaris antivirus	
4.3. Virus informàtic	
<b>5. ENLLAÇOS RECOMANATS</b>	<b>25</b>
<b>6. RECOMANACIONS PER A UN ÚS RESPONSABLE D'INTERNET</b>	<b>26</b>

# 1. INTRODUCCIÓ

## 1.1. QUE ÉS INTERNET?

Internet és una xarxa de comunicació i serveis, és la xarxa d'ordinadors més gran del món. Tothom pot accedir a Internet des de qualsevol punt (casa, oficina, *espainernet...*), mitjançant una simple *trucada urbana* que es fa a través de l'ordinador.



Aquesta eina permet la **comunicació** simultània amb persones per mitjà d'ordinadors que són en un altre continent les 24 hores del dia, sempre està disponible.

Podeu considerar Internet com una gran comunitat on es pot consultar qualsevol tipus d'**informació**.

És una forma molt ràpida d'**intercanviar** informació, idees i opinions sobre qualsevol tema; per això també ha estat anomenada "superautopista de la informació".

S'ha qualificat Internet com l'invent més influent des que es va inventar la impremta.

Parlant de les connexions, en podem destacar dues: RTB i ADSL. Totes dues fan servir el mateix cable telefònic. Mentre que el sistema RTB no permet l'ús conjunt d'Internet i veu alhora, l'ADSL sí que permet aquest ús simultani ja que fa servir un sistema de banda més ampla; això permet que, pel mateix canal, hi circulin tres fluxos alhora: recepció i enviament de dades i veu.

## 1.2. PER QUÈ CAL PARLAR DE "SEGURETAT A LA XARXA"?

Quan parlem d'Internet heu de pensar en una finestra oberta al món que ofereix la possibilitat d'aprendre, obtenir informació i comunicar-vos amb total llibertat d'expressió.

Igualment heu de pensar que, com a la vida real, la informació que es troba o els serveis que ofereix no són convenients a totes les edats ni sempre són de fiar.

Des de molt petits, els infants s'apropen al monitor amb la mateixa curiositat amb la qual veuen el món real. Són tantes les possibilitats que ofereix Internet –treballar, conversar amb els amics des de qualsevol part del món, informar-se de les activitats preferides, comprar, jugar, baixar música i pel·lícules– que és impossible no deixar-s'hi portar.

Actualment, molts organismes, institucions i entitats treballen per facilitar eines que ajuden a fer un ús correcte d'Internet i fer front a les situacions de risc.

Els experts coincideixen en el fet que, per sobre de la censura i la vigilància sempre inexacta que ofereixen alguns programes informàtics, les millors eines per protegir els nens a la xarxa són l'**educació** i la **informació**. Es produeix la paradoxa que "l'ordinador i Internet" són molt sovint un terreny on els pares i educadors sou els que rebeu lliçons dels vostres fills, més familiaritzats amb les noves tecnologies.

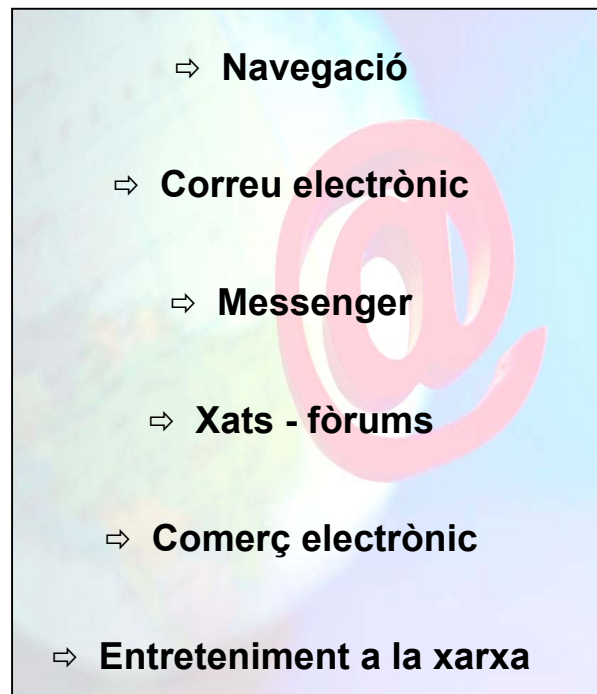
Sovint passa que deixeu els menors navegant per Internet sense involucrar-vos-hi gaire, i moltes vegades no sabeu com funciona ni sou prou conscients de les oportunitats i els riscos que això comporta. Penseu que, encara que no tingueu Internet a casa, els menors hi poden accedir en altres espais (biblioteca, *espainernet*, casa d'amics...).

Cal que els adults assumiu la **responsabilitat** d'educar i pactar conductes adequades en l'ús d'Internet. De la mateixa manera que els ensenyeu a anar sols pel carrer, de manera segura, els podeu ensenyar a navegar sols per Internet.

## 2. SERVEIS QUE OFEREIX INTERNET: BENEFICIS, RISCOS I RECOMANACIONS

---

Per entendre millor la importància de la seguretat en l'ús d'Internet, cal una formació bàsica dels serveis que es troben a la xarxa, tot i que és recomanable ampliar els coneixements amb altres cursos específics. A continuació us fem una petita exposició del que permet cada eina o servei:



Cal dir que l'objectiu d'aquest taller és incidir en els beneficis i riscos de cadascun dels serveis i aportar consells o recomanacions que us poden ajudar en la tasca educativa dels menors en l'ús responsable d'Internet i concretament en cada servei.

## NAVEGACIÓ

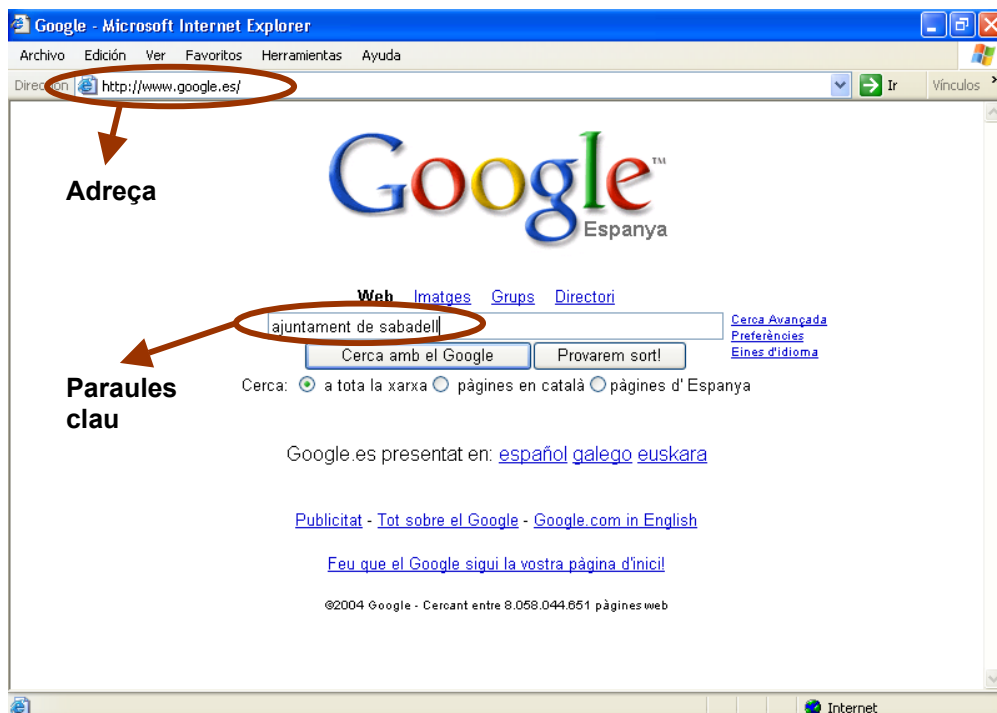
### QUÈ PERMET?

- ⇒ Permet la **recerca d'informació** de qualsevol tema (esports, viatges, música, jocs...) a través d'un navegador, un programa informàtic que serveix per entrar a Internet.
- ⇒ Els navegadors més habituals són: Internet Explorer i Netscape.

### COM FUNCIONA?

- ⇒ Cal escriure l'**adreça** de la pàgina web que es vol trobar; si no la coneixem, es fa servir un cercador (p. ex: Google) i s'escriu la **paraula** o paraules claus del tema que es vol buscar.

### COM ES VISUALITZA?



**Pràctica 1:** Recerca d'informació de tema lliure mitjançant adreça web i/o cercador/motor de cerca. Estructura d'una pàgina web; identificar publicitat subliminal, galetes. Continguts no adequats per als menors. Visualitzar i controlar l'Historial. Controlar i personalitzar els Preferits (Favoritos).

**ADSL.** Asymetrical Digital Subscriber Line. Línea de subscripció asimètrica digital. És un tipus de connexió XDSL (Sistema de transferència que permet a les línies de fils de coure tradicional una gran velocitat. És asimètrica perquè permet més velocitat de baixada que de pujada.

**Banda ampla.** Xarxa que permet la connexió de múltiples xarxes en un únic cable. Fa referència a una gran velocitat de transmissió.

**Cibernauta.** Persona que navega per Internet, navegant, timoner.

**Domini.** Els noms de domini s'utilitzen per identificar les adreces dintre d'Internet.

**Enllaç (link)** És una paraula o frase que connecta amb una altra informació. Pàgines web relacionades.

**Galetes.** Són blocs de dades que determinades pàgines envien al nostre ordinador quan ens connectem a elles, quedant-se emmagatzemades al nostre disc dur o en la memòria temporal. Les dades que podem contenir són un Login i password per connectar-se, dades per fer una compra, o per navegar per la pròpia pàgina.

**Navegador.** Programari que serveix per a connectar-se a Internet i navegar des d'un servei Internet. El servei web pot ser del tipus: www, ftp...

## BENEFICIS

- ⇒ Permet la recerca de tot tipus d'informació.
- ⇒ Facilita l'accés a recursos educatius i culturals (text, so, imatges i vídeo).
- ⇒ Es pot jugar a jocs divertits i educatius.
- ⇒ Proporciona informació actualitzada (diaris, revistes...).
- ⇒ Possibilita la realització de cursos en línia.
- ⇒ Permet accedir a llocs web d'institucions i organismes públics i privats (biblioteques, universitats...).
- ⇒ Planificar activitats d'oci (viatges, entrades de cinema, música...).

## RISCOS

- ⇒ Accedir a pàgines amb continguts no adequats a totes les edats:
  - ✓ Il·lícits (pornografia infantil o apologia del terrorisme).
  - ✓ Nocius (pornografia per adults, informació sobre violència, sectes..).
  - ✓ Falsos (informació errònia donada com a certa).
- ⇒ Baixar-se programes infectats amb virus .
- ⇒ Publicitat subliminal. Galetes.
- ⇒ Poden ser víctimes, però també responsables de conductes il·legals.
  - ✓ Distribuir, copiar o publicar informació amb copyright.
  - ✓ Posar en perill altres persones.
- ⇒ Pot provocar una dependència si no es controla el temps de connexió.

## RECOMANACIONS

- ⇒ Acompanyeu els menors quan estiguin connectats a Internet.
- ⇒ Interesseu-vos per saber què fan i manteniu una bona comunicació amb ells.
- ⇒ Pacteu amb els menors una sèrie de conductes:
  - ✓ Horari i temps de connexió.
  - ✓ Accedir a webs conegudes i de confiança.
  - ✓ Saber distingir entre els continguts que són recomanables i els que no ho són.
  - ✓ Davant qualsevol situació incòmode, han d'avisar els adults.
  - ✓ Saber reaccionar de manera responsable i resoldre per si mateixos possibles solucions de risc.
  - ✓ No donar mai dades personals ni de la seva família sense la supervisió d'un adult.
  - ✓ Quan els nens utilitzen informació d'Internet per fer els treballs escolars, que indiquin sempre la font (la pàgina web) on l'han trobat.
  - ✓ Si es connecten en un lloc públic (espainetnet) que no s'oblidin de tancar la connexió, ja que una altra persona es podria fer passar per ells.
- ⇒ Utilitzeu **eines de control**, programes informàtics que permeten:
  - ✓ Bloquejar l'accés a continguts no recomanats.
  - ✓ Controlar el temps de connexió.
  - ✓ Consultar l'historial de pàgines web visitades.

## 2.1 CORREU ELECTRÒNIC

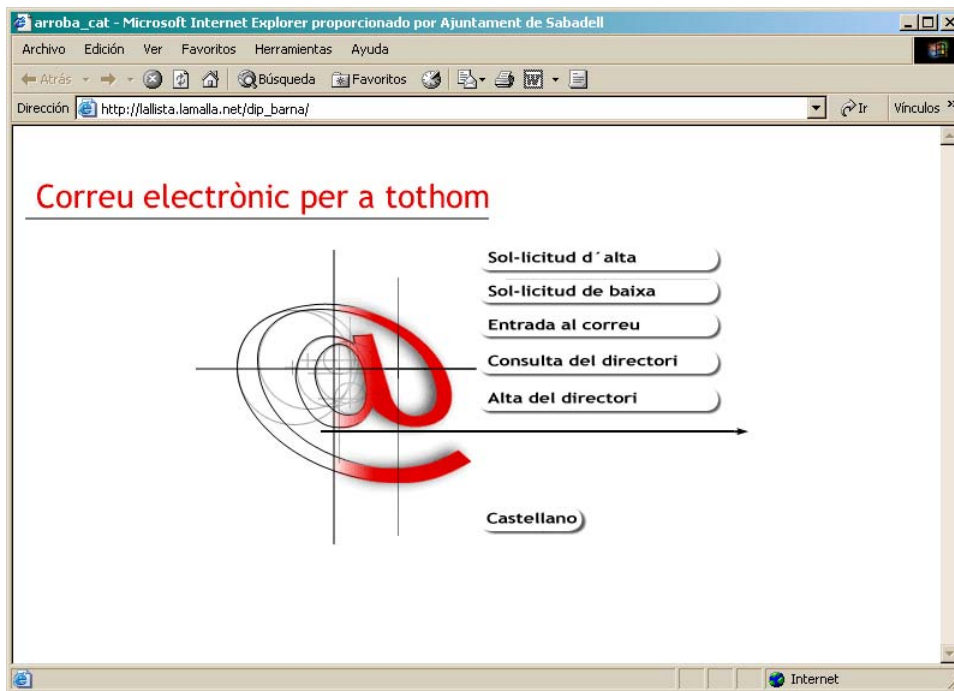
### QUÈ PERMET?

- ⇒ **Enviar i rebre informació** a través de **missatges** que poden incloure fitxers electrònics amb diferents continguts (fotos, música...).

### COM FUNCIONA?

- ⇒ Per enviar un missatge únicament cal disposar d'un compte de correu personal (**nom d'usuari i contrasenya**) que ens identifiqui i conèixer el de la persona o persones destinatàries del missatge.

### COM ES VISUALITZA?



**Pràctica 2:** Com es configura una adreça de correu electrònic, explicant quines dades demana. Enviar un missatge entre dos usuaris. Adjuntar diferents tipus d'arxiu. Explicar la funció d'un antivirus. Configurar filtres o regles de missatges per controlar els missatges no desitjats.

#### Antivirus

Són tots aquells programes que permeten analitzar la memòria i unitats del disc dur en la recerca de virus. Aplicació amb la finalitat de detenir i eliminar els virus informàtics.

#### Arxiu executable

És un arxiu que conté les instruccions necessàries perquè un determinat programa es posi en marxa.

#### Carrega destructiva.

Es la part del virus que realitza una acció sobre el Pc infectat. Pots ser de caràcter relativament inofensiu com mostrar missatges o expulsar la unitat de CD, o més destructiu com esborrar tot el disc dur.

#### Contrasenya

Conjunt de lletres, xifres i símbols, fins i tot de frases, utilitzats per autenticar usuaris en un sistema informàtic. Perquè l'ús de contrasenyes sigui efectiu cal triar-les de manera que siguin difícils de descobrir per un atacant.

#### Firma digital.

Dades xifrades de forma que el receptor faci la comprovació del transmissor.

#### Password.

Contrasenya, identificació d'usuari.

<b>BENEFICIS</b>	<b>RISCOS</b>
<ul style="list-style-type: none"><li>⇒ És molt còmode: no calen segells, ni sobres ni adreces. Només una adreça electrònica i una connexió a Internet.</li><li>⇒ Permet comunicar-se amb persones que estan lluny.</li><li>⇒ Es poden enviar i rebre documents adjunts de tota classe (textos, fotos, música) i reenviar-los a d'altres persones.</li><li>⇒ Facilita enviar el mateix missatge a més d'un destinatari.</li><li>⇒ Facilita la comunicació amb empreses, institucions, organismes i administracions respecte els serveis que ofereixen.</li></ul>	<ul style="list-style-type: none"><li>⇒ El correu electrònic és el canal més ràpid per a la propagació de virus.</li><li>⇒ <i>Spam</i>: publicitat no sol·licitada que es rep sense la nostra autorització.</li><li>⇒ Rebre missatges de desconeguts amb arxius executables que poden contenir virus.</li><li>⇒ Rebre missatges amb continguts que atemptin la intimitat personal.</li><li>⇒ Cometre certs delictes legals, sense saber-ho de vegades, per incórrer en actituds inapropiades: amenaçar, intimidar, plagiar informació.</li></ul>
<b>RECOMANACIONS</b>	
<ul style="list-style-type: none"><li>⇒ Informeu els menors de certs aspectes a tenir en compte:<ul style="list-style-type: none"><li>✓ És molt recomanable instal·lar un programari antivirus i mantenir-lo actualitzat.</li><li>✓ Han de ser respectuosos amb altres persones i no fer res que pugui ferir o perjudicar ningú:<ul style="list-style-type: none"><li>• No revelar dades personals d'altres persones.</li><li>• No ofendre ni molestar amb paraules o actituds.</li><li>• Evitar ser autor d'un delicte (amençar o assetjar algú, distribuir, copiar o publicar dibuixos, música o text amb copyright obtinguts de webs sense permís.</li></ul></li><li>✓ No han d'obrir missatges de desconeguts ni aquells dels quals no s'està segur de la fiabilitat del seu contingut.</li><li>✓ No donar mai el nom d'usuari i/o contrasenya a ningú.</li><li>✓ No donar mai dades personals ni familiars a cap desconegut.</li></ul></li></ul>	

## 2.2 MESSENGER

### QUÈ PERMET?

- ⇒ **Mantenir converses** en línia de forma instantània, en temps real.
- ⇒ **Fer videoconferències**, converses amb càmera per poder veure al nostre interlocutor.

### COM FUNCIONA?

- ⇒ Cal **registrar** una adreça de correu electrònic en Microsoft Passport. Si ja es té una adreça de Hotmail o Msn.com ja està registrat.
- ⇒ Descarregar-se el **programa** i afegir els contactes.

**Configurar.**  
Adaptar una aplicació del programari o un element del maquinari a la resta d'elements i a les necessitats del usuari.

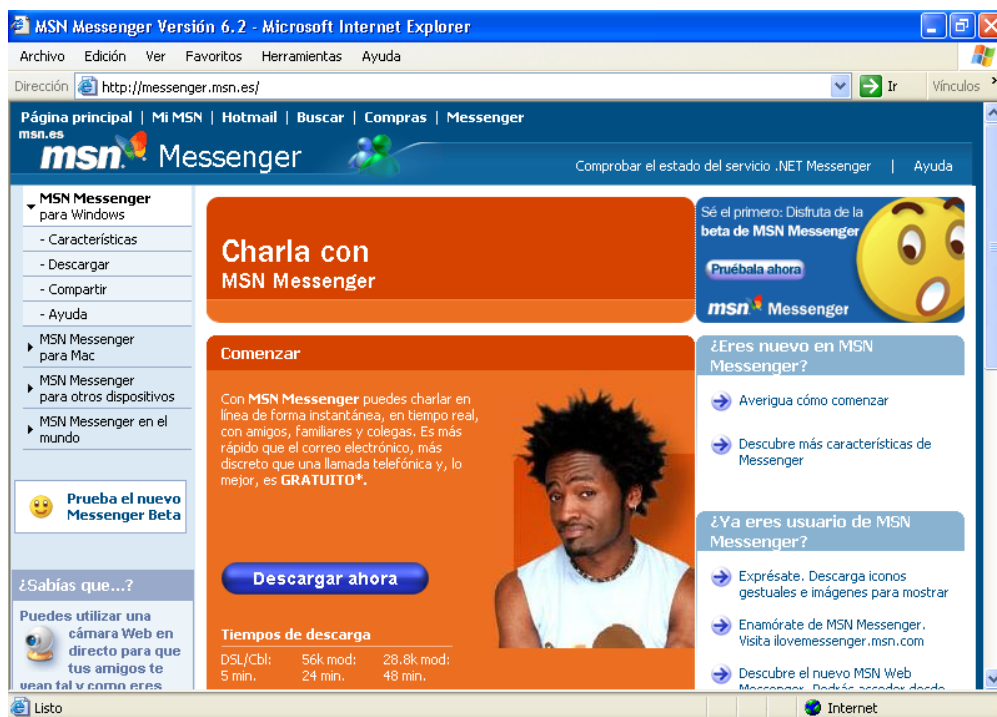
**Descarregar.**  
Copiar a través de la xarxa un element que es troba en un altre ordinador (fitxer, programari, document...) al nostre ordinador

**FTP**  
Protocol de transferència d'arxius a Internet..

**ISP (Internet Service Provider).**  
Proveïdor de serveis d'Internet.

**Lan**  
Xarxa local.

### COM ES VISUALITZA?



**Pràctica 3:** Registrar-se i descarregar el programa. Afegir contactes. Establir converses. Personalitzar el fons, els icones... Inserir arxius durant la conversa. Conversacions amb càmera web.

## BENEFICIS

- ⇒ És molt còmode. Només cal una adreça electrònica i una connexió a Internet.
- ⇒ Permet comunicar-se amb persones que estan lluny.
- ⇒ Es poden enviar i rebre documents adjunts de tota classe (textos, fotos, música) i reenviar-los a d'altres persones.
- ⇒ És més ràpid que el correu electrònic, ja que és en temps real.
- ⇒ Permet també converses amb càmera web, converses que s'anomenen de vídeo, per poder veure l'altre persona.
- ⇒ És gratuït.

## RISCOS

- ⇒ Si algú coneix la nostra contrasenya i adreça de correu, podria fer-se passar per nosaltres.
- ⇒ Cal controlar el temps de connexió. Si no es fa així, és fàcil tenir problemes de diferents tipus (trastorns de la son, dolors d'esquena, de visió...).
- ⇒ Infecció de l'ordinador a través d'un arxiu amb virus.

## RECOMANACIONS

- ⇒ Informeu els menors de certs aspectes a tenir en compte:
  - ✓ Es molt recomanable instal·lar un programari antivirus i mantenir-lo actualitzat.
  - ✓ Han de ser respectuosos amb d'altres persones i no fer res que pugui ferir o perjudicar ningú
  - ✓ No han d'obrir missatges de desconeguts ni aquells dels quals no s'està segur de la fiabilitat del seu contingut.
  - ✓ No donar mai el nom d'usuari i/o contrasenya a ningú.
  - ✓ No donar mai dades personals ni familiars a cap desconegut.

## 2.3 XATS I FÒRUMS

### QUÈ PERMET?

- ⇒ Comunicar-se de **manera instantània** amb qualsevol usuari que estigui connectat en aquell moment a la Xarxa.
- ⇒ Obtenir informació de temes diversos, experiències d'altres persones.

### COM FUNCIONA?

- ⇒ A través de les pàgines específiques, trobarem **sales temàtiques** on es pot entrar a través del nostre sobrenom o àlies.

### COM ES VISUALITZA?



**Pràctica 4:** *Participar activament en un xat temàtic (o fòrum).*

**CPU (Unitat Central de Procés).**  
Caixa o torre de l'ordinador.

**Civer.** Prefix utilitzat per referir-se a tot allò relacionat amb Internet. Prové del Hel·lènic Kibermao que vol dir pilotar una nau.

**IP, adreces.**  
És la forma estàndard d'identificar un equip que està connectat a la xarxa

**Màquina.**  
Ordinador o PC.

**News.**  
Servei d'Internet amb estructura de tauló d'anuncis, dividit per temes i països en els que els components del grup deixen o responen missatges relacionats.

**Nick.**  
Nom o pseudònim utilitzat en els fòrums, xats o serveis d'Internet en general; identitat virtual.

**Virus.**  
Programa o fragment que provoca efectes nocius en un sistema informàtic que es pot reproduir o no.

<b>BENEFICIS</b>	<b>RISCOS</b>
<ul style="list-style-type: none"><li>⇒ És ràpid, immediat, es fa en temps real.</li><li>⇒ Facilita la comunicació instantània amb una o vàries persones.</li><li>⇒ Permet trobar respostes a qüestions molt diverses (matèries escolars, música, programari...).</li><li>⇒ Facilita l'intercanvi d'informació sobre molts temes que ens poden interessar (viatges, cotxes, jocs...)</li><li>⇒ No cal donar cap dada personal per poder fer servir aquest servei. Només és necessari donar-se d'alta amb un sobrenom i tenir una contrasenya.</li></ul>	<ul style="list-style-type: none"><li>⇒ Desconeixement de la persona o persones amb les quals s'està mantenint la comunicació.</li><li>⇒ No es pot saber si realment és qui diu ser (naveguem en l'anonimat).</li><li>⇒ Prendre actituds que poden ferir altres persones (insults...).</li><li>⇒ Pèrdua de la intimitat si es donen dades personals, familiars o d'algun altre conegut a una persona desconeguda.</li><li>⇒ Intentar quedar amb desconeguts per coneixe'ls personalment.</li><li>⇒ Ser víctimes de situacions que poden fer sentir incòmode el menor (insults...).</li></ul>
<b>RECOMANACIONS</b>	
<ul style="list-style-type: none"><li>⇒ Insistiu en què els menors siguin responsables en l'ús del servei:<ul style="list-style-type: none"><li>✓ Fer servir un àlies o sobrenom per tal que no puguin ser identificats.</li><li>✓ Ser sempre respectuosos i evitar ficar-se en discussions amb altres persones. En cas que algú ho faci amb el menor, de seguida comentar-ho amb un adult.</li><li>✓ No oblidar-se de tancar la connexió si està en un lloc públic (espainternet), ja que qualsevol es podria fer passar per ell.</li><li>✓ No facilitar mai informació personal, de la família o coneguts que puguin identificar-los.</li><li>✓ No quedar amb ningú que s'ha conegut a través de la Xarxa sense demanar permís a un adult i fins i tot fer-se acompanyar.</li></ul></li></ul>	

## 2.4 REALITZACIÓ DE TRÀMITS I COMERÇ ELECTRÒNIC

### QUÈ PERMET?

⇒ Poder fer **consultes** a empreses, organismes i institucions públiques, de manera que s'estalvia molt de temps en cues i ens assegura una rapidesa i claredat en les gestions (xarxes de biblioteques, consultes d'expedients acadèmics, compra d'entrades, llibres...).

### COM FUNCIONA?

⇒ Mitjançant la pàgina web específica de l'empresa (banc o caixa, biblioteca, club esportiu, botiga virtual...) i dels seus enllaços.

⇒ En alguns casos caldrà donar-se d'alta com a client amb un codi i llavors serà necessari definir la forma de pagament.

### COM ES VISUALITZA?



**Pràctica 5:** Fer una simulació de compra. Pagaments amb targetes de crèdit. Màrqueting per atreure els menors. Publicitat enganyosa. Formularis amb recull de dades.

**Cardin.**  
1.1.1.2 Parietal targetes de crèdit o telefòniques, per a realitzar compres a través d'Internet.

**Copyright.**  
Drets de còpia, drets d'autor. Dret que té un autor de la seva obra o que crea perquè estigui prohibida la seva distribució o reproducció. El seu símbol és ©.

**Filtrat de continguts**  
Conjunt de tecnologies que permeten un control de la informació transmesa per serveis d'internet. S'utilitza per bloquejar virus enviats per correu electrònic, per controlar l'accés a internet de menors, etc.

<b>BENEFICIS</b>	<b>RISCOS</b>
<ul style="list-style-type: none"><li>⇒ Rapidesa i comoditat en els tràmits de compra i gestions.</li><li>⇒ Evitar cues innecessàries i possibilitat de fer els tràmits les 24 hores del dia.</li><li>⇒ Accés als tràmits de totes les administracions (locals, nacional i estatal) sense haver de desplaçar-se.</li><li>⇒ Comprar llibres, música, entrades per el cinema....</li><li>⇒ Comprar articles específics que són molt difícils de trobar en les botigues habituals</li><li>⇒ Col·laborar amb associacions, ONG que gestionen productes manufacturats per països en vies de desenvolupament.</li></ul>	<ul style="list-style-type: none"><li>⇒ Indueixen a comprar coses innecessàries.</li><li>⇒ Rebre publicitat abusiva per aconseguir fer la venda (vincles a formularis de compra).</li><li>⇒ Ser víctimes d'estafes per la donació de dades personals (número de targeta de crèdit) que després les empreses poden vendre a d'altres i carregar compres que no s'han realitzat.</li><li>⇒ Fer la compra sense la supervisió d'un adult o que el menor se n'adoni (a partir d'enllaços teòricament informatius).</li><li>⇒ El frau del 806: pagar addicionalment quan es visita alguna pàgina web concreta sense que ens adonem.</li></ul>
<b>RECOMANACIONS</b>	
<ul style="list-style-type: none"><li>⇒ Expliqueu els menors les pràctiques de màrqueting a Internet o les estratègies comercials adreçades a atreure els joves consumidors.<ul style="list-style-type: none"><li>✓ Pàgines infantils que inciten a comprar articles involuntàriament.</li></ul></li><li>⇒ Informeu els infants de les situacions de risc i fer-los conscients de mesures preventives:<ul style="list-style-type: none"><li>✓ No es poden facilitar mai dades personals (tarja de crèdit) sense un adult al davant</li><li>✓ No es poden donar dades personals per a concursos on prometen regals.</li><li>✓ No realitzar compres sense un adult al davant.</li><li>✓ Davant d'instruccions no gaire clares, no continuar el procés (compte amb els formularis).</li><li>✓ Desconfiar dels proveïdors que a l'hora de realitzar la compra només demanen les dades mínimes (un bon proveïdor demanaria més per fer el seguiment comercial).</li></ul></li></ul>	

## 2.5 ENTRETENIMENT A LA XARXA

### QUÈ PERMET?

- ⇒ Permet compartir recursos: música, pel·lícules, etc.
- ⇒ Ofereix una multitud de jocs d'ordinador per jugar de manera individual o amb altres usuaris.

### COM FUNCIONA?

- ⇒ Accedint als webs musicals es pot escoltar i descarregar les pistes multimèdia.
- ⇒ A través de portals educatius o pàgines web específiques sobre jocs, podem jugar i/o descarregar els jocs des de la xarxa.

### COM ES VISUALITZA?



Pràctica 6: Entrar en pàgines de jocs.

<b>BENEFICIS</b>	<b>RISCOS</b>
<ul style="list-style-type: none"><li>⇒ Ofereix un ampli ventall d'oportunitats d'oci (humor, lleure, jocs, música, vídeos, pel·lícules...).</li><li>⇒ També ofereix informació per dur a terme les activitats d'oci preferides pels usuaris (cinema, llibres, música, viatges...).</li><li>⇒ Permet compartir recursos: música, pel·lícules, programari...</li></ul>	<ul style="list-style-type: none"><li>⇒ L'ús excessiu del entreteniment pot portar problemes <b>d'addicció</b>.</li><li>⇒ L'ordinador no és cap persona, i per tant no pot mai substituir les relacions i l'entreteniment que l'infant viu amb d'altres persones.</li><li>⇒ Infecció de virus a través dels jocs, quan s'executen des de la pàgina web.</li><li>⇒ Cometre delictes legals, copiant o distribuint informació amb copyright.</li></ul>
<b>RECOMANACIONS</b>	
<ul style="list-style-type: none"><li>⇒ Tenir un antivirus actualitzat.</li><li>⇒ Cal dialogar amb els infants per comentar els següents aspectes:<ul style="list-style-type: none"><li>✓ Pactar el temps d'ús i l'horari.</li><li>✓ Anar amb compte de no distribuir i/o copiar informació amb copyright.</li></ul></li></ul>	

### 3. EINES DE CONTROL

---

#### 3.1 PÀGINA D'INICI

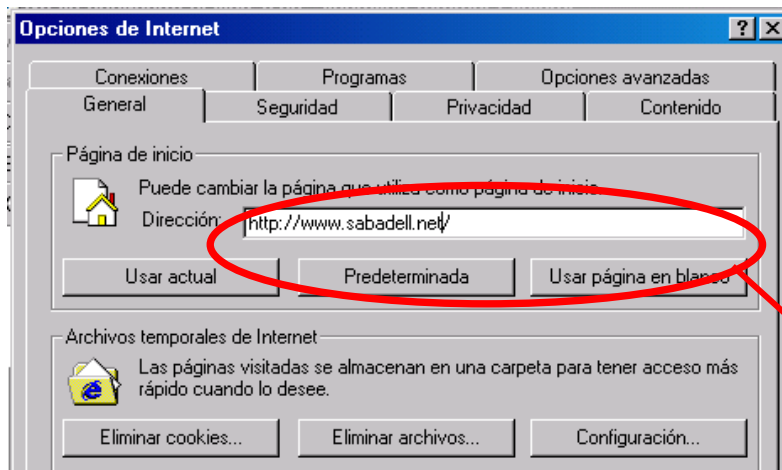
##### QUÈ PERMET?

⇒ Seleccionar la pàgina que apareixerà en el moment de fer la connexió a Internet. És recomanable predeterminar pàgines amb continguts i enllaços infantils.

##### COM FER-HO?

⇒ Al “Menú Herramientas”, opció “Opciones de Internet”, seleccioneu a la fitxa general secció de “Página de Inicio” i escriviu la pàgina escollida, per exemple [www.chaval.es](http://www.chaval.es) o [www.edu365.com](http://www.edu365.com)

##### COM ES VISUALITZA?



Escriure l'adreça de la pàgina web inicial.

**Pràctica 7:** Configurar la pàgina d'inici mitjançant les “Opciones de Internet”, a través del menú Herramientas.

## 3.2 CONFIGURAR LA SEGURETAT DEL NAVEGADOR

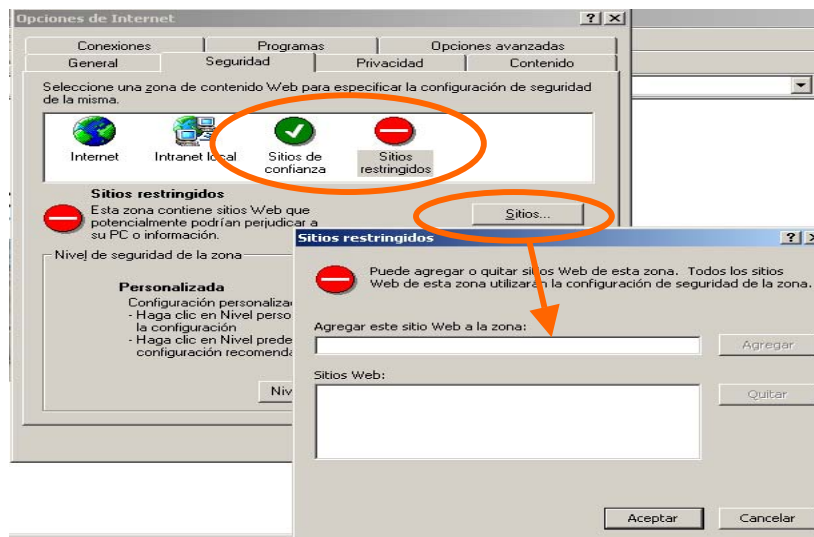
### QUÈ PERMET?

- ⇒ Assignar els nivells de seguretat als llocs
- ⇒ Ajuda a protegir la privacitat del usuari mentre està connectat.
- ⇒ Guardar a “Favoritos” pàgines web organitzades per temes en carpetes.

### COM FER-HO?

- ⇒ A la fitxa de seguretat “Menú herramientas”, opció “Opciones de Internet” seleccioneu “Sitios restringidos” per escriure adreces a les quals voleu restringir l'accés- **Fig.1**
- ⇒ Heu de crear les carpetes corresponents des del Menú Favoritos, opció “Organizar favoritos” i posteriorment buscar les pàgines i guardar-les a la carpeta corresponent a partir del menú Favoritos, opció “Agregar a favoritos” (Pràctica)

### COM ES VISUALITZA?



**Pràctica 8:** Incorporar llocs web de confiança i d'altres als quals restringim el seu accés. Treballar amb el menú Favoritos, per organitzar les pàgines web més visitades.

### 3.3 FILTRAT DE CONTINGUTS

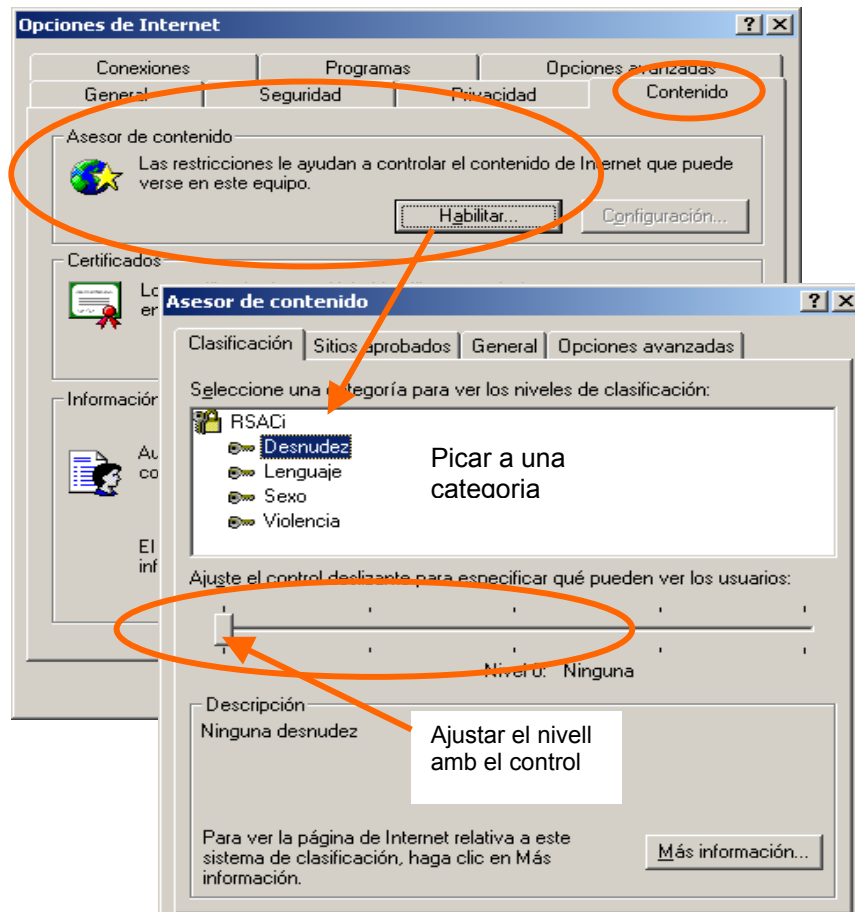
#### COM FER-HO?

#### QUÈ PERMET?

⇒ Permet restringir el accés a pàgines classificades per categories segons el seu contingut.

⇒ Habiliten el assessor de contingut, seleccionant les categories que vulgueu restringir i el seu nivell (sexe, violència...) restringireu el accés a determinades pàgines.

#### COM ES VISUALITZA?



**Pràctica 9:** *Habilitar l'assessor de contingut i ajustar el nivell de restricció per cada categoria (nuesa, llenguatge, sexe i violència).*

### 3.4 ÚS DELS ARXIUS TEMPORALS

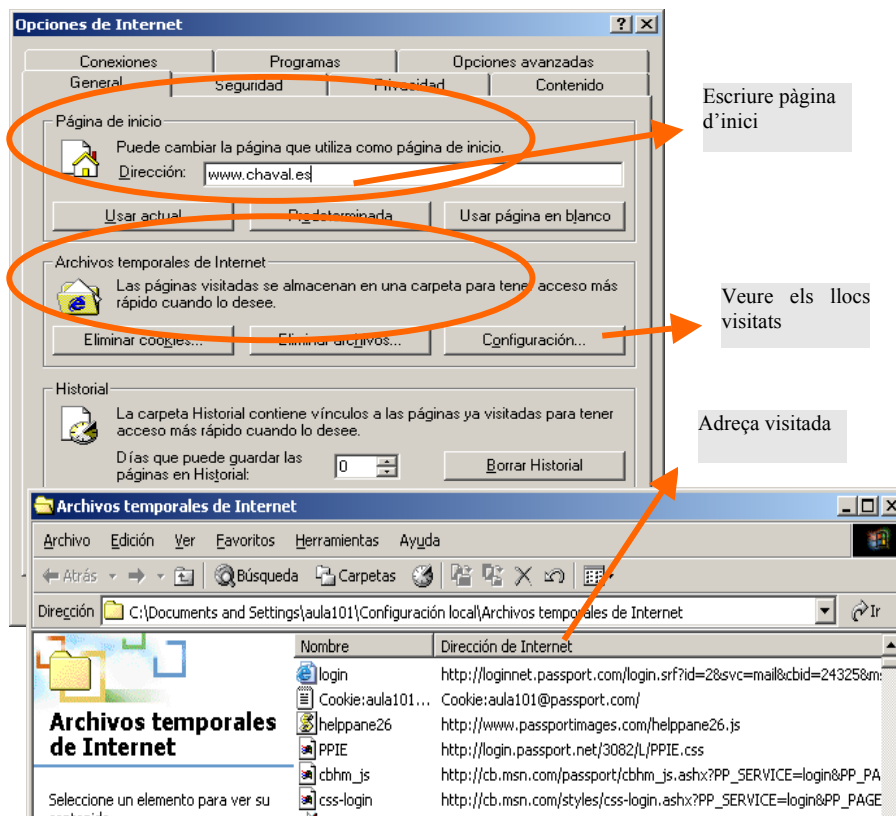
#### QUÈ PERMET?

⇒ Revisar els darrers llocs web visitats.

#### COM FER-HO?

⇒ Seleccioneu a la fitxa general i a la secció “Archivos temporales de Internet”, piqueu el botó de “configuración” i “Ver archivos”, a direcció d’Internet veureu la llista de pàgines visitades últimament.

#### COM ES VISUALITZA?



**Pràctica 10:** Revisar els llocs web que s’han visitat.

### 3.1 DEFINIR COMPTES D'USUARIS RESTRINGITS

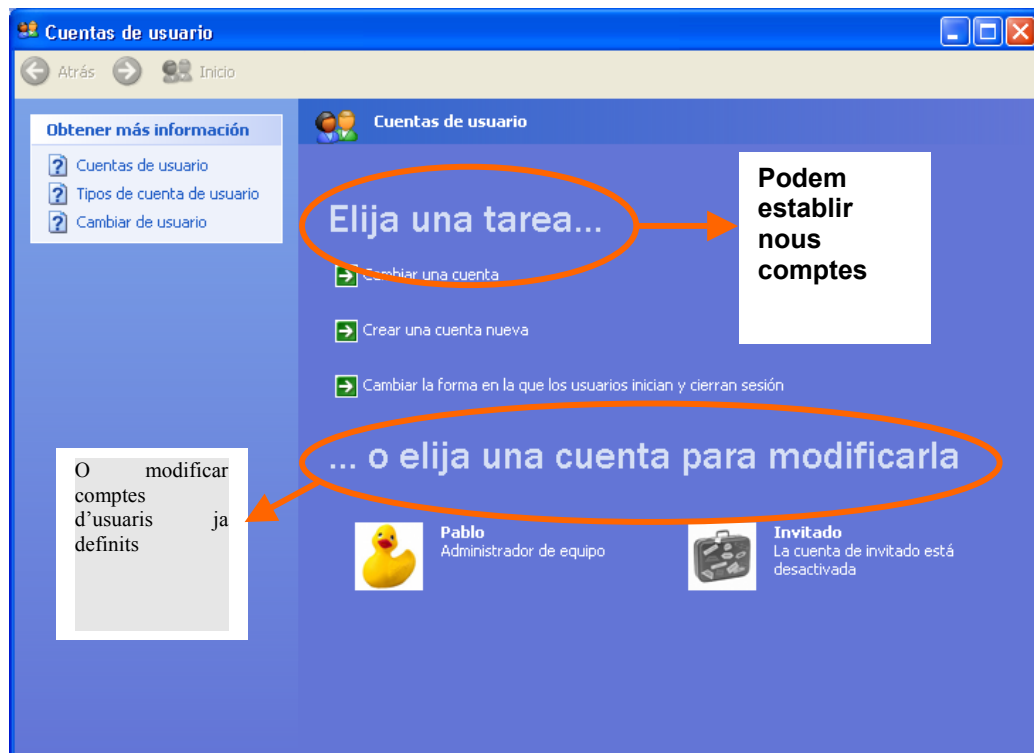
#### QUÈ PERMET?

- ⇒ Crear comptes d'usuaris per l'equip, de forma que cada usuari inicia una sessió per separat amb el seu propi perfil.
- ⇒ Es poden configurar com administrador (amb total control del equip o com a usuaris limitats (amb restriccions).

#### COM FER-HO?

- ⇒ Heu d'anar al *Panell de Control* i seleccionar la opció *Configuració*.
- ⇒ Feu doble "clic" a *Usuarios* i definiu la configuració i els permisos.

#### COM ES VISUALITZA?



**Pràctica 11:** Revisar quants usuaris tenim definits al sistema operatiu. Modificar els comptes existents; crear usuaris nous i personalitzar les seves característiques.

## 4. SISTEMES DE SEGURETAT

Totes les mesures de seguretat que podeu fer servir per evitar els riscos no són mai prou, ja que contínuament apareixen nous virus o els pirates informàtics aconseguen vulnerar els sistemes.

Tot i que els riscos els podeu minimitzar amb les eines de control bàsiques que us hem explicat, per incrementar la seguretat a Internet hi ha al mercat sistemes específics de seguretat.

### 4.1 TALLAFOCS

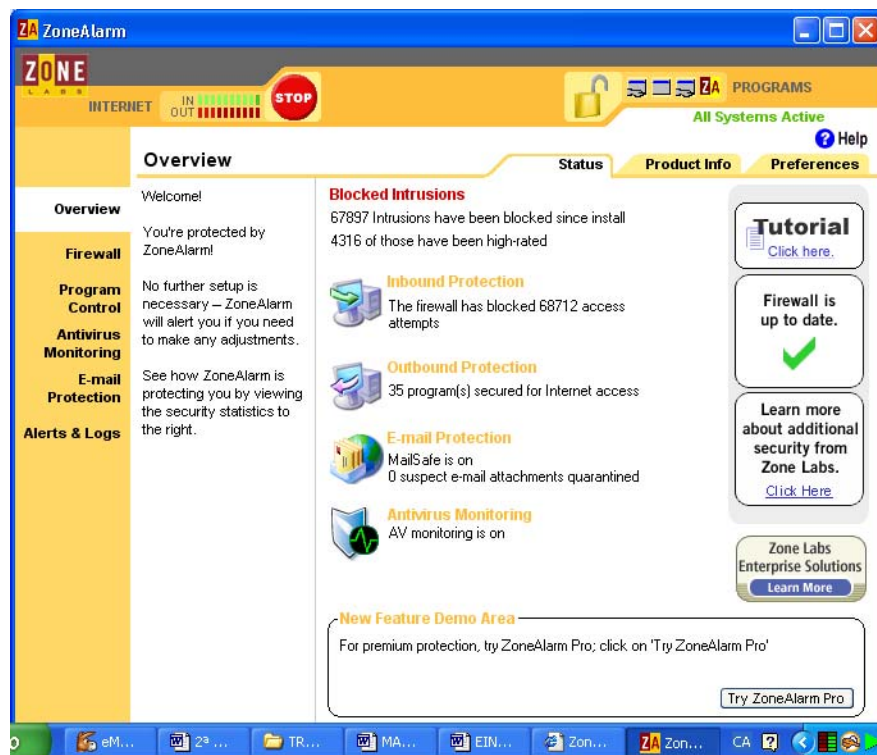
#### QUÈ ÉS?

Un tallafocs és un **sistema de defensa** que es basa en la instal·lació d'una "barrera" entre l'ordinador i la xarxa, per la qual circulen totes les dades. Aquest tràfic entre la xarxa i l'ordinador és autoritzat o denegat pel tallafocs seguint les indicacions que prèviament s'hauran de configurar.

#### COM ACTUA?

El funcionament d'aquest tipus de programes es basa en el "filtratge de paquets". Qualsevol dada o informació que circuli entre l'ordinador i la xarxa és analitzat pel programari (tallafocs) amb la missió de permetre o denegar el seu pas en ambdues direccions (Internet → PC o PC → Internet).

#### COM ES VISUALITZA?



**Pràctica 13:** Instal·lar un programa tallafocs i visualitzar-ne el funcionament.

**Hacker.**  
Pirata informàtic. Persona amb molts coneixements informàtics que per demostrar-s'ho a si mateix intenta vulnerar sistemes informàtics

**Ata.c**  
Atac electrònic (típicament no provocat) que intenta vulnerar el sistema destí, els mecanismes de xarxa i de seguretat

**Tallafocs o firewall personal.**  
Firewall instal·lat en una màquina com un programa que controla exclusivament els seus accessos. S'acostuma a fer servir en ordinadors domèstics amb connexió directa a Internet.

**Crack.**  
Programari utilitzat per eliminar les proteccions.

**Crackejador.**  
Persona amb la capacitat per entrar en un sistema sense autorització amb intencions malicioses. És una aplicació capaç de destruir claus d'accés.

**Desinfecció.**  
És l'acció que realitzen els antivirus després de detectar un virus, l'eliminen tot el possible i recuperen l'informació infectada.

**Filtrat de continguts**  
Conjunt de tecnologies que permeten un control de la informació transmesa per serveis d'Internet. S'utilitza per bloquejar virus enviats per correu electrònic o per controlar l'accés a Internet.

## 4.2 PROGRAMARIS ANTIVIRUS

Qualsevol ordinador connectat a Internet com a mínim hauria de tenir instal·lat un antivirus, perquè com veureu la major preocupació és combatre l'efecte de ser infectat per un virus informàtic.

Hi ha diferents nivells de seguretat segons les dades que es guarden a l'ordinador, per exemple el sistema informàtic d'una entitat bancària, un ajuntament o de la Seguretat Social estan obligats a protegir les dades personals amb les quals treballen amb la instal·lació de rigoroses mides de seguretat.

### QUÈ ÉS?

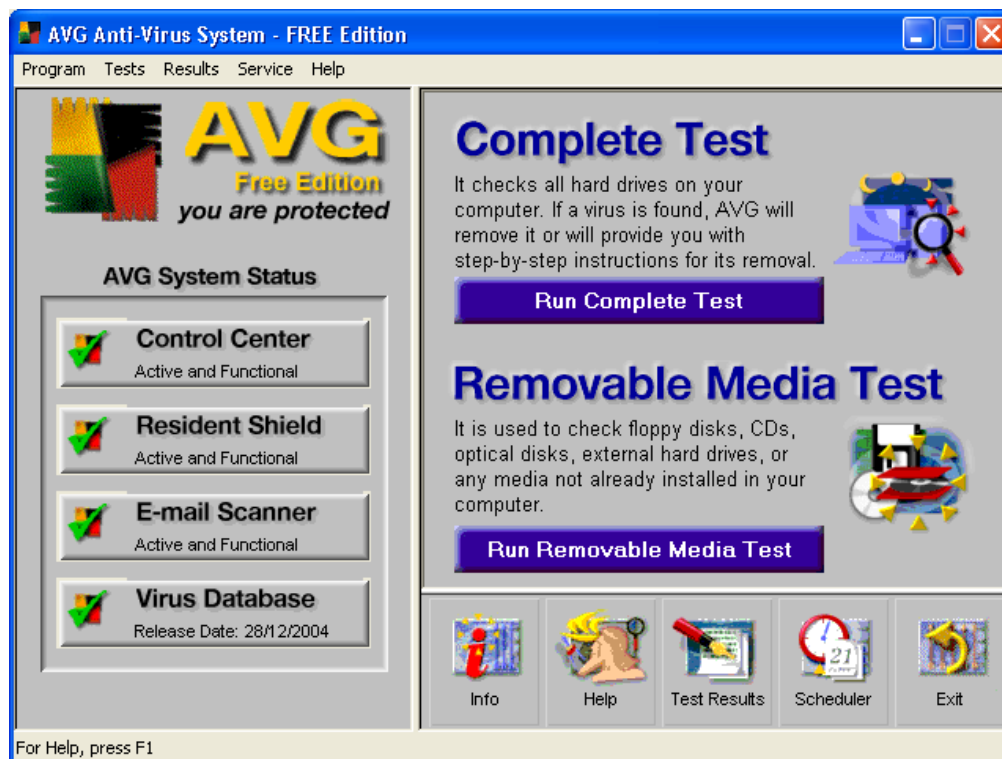
Programari que permet identificar els virus i, en alguns casos, eliminar arxius infectats de virus.

### COM ACTUA?

Revisa tota la informació existent a l'ordinador per trobar la presència o l'acció d'un virus informàtic.

Un antivirus pot donar també la funció d'eliminar virus informàtic.

### COM ES VISUALITZA?



**Pràctica 14:** *Instal·lar un programa antivirus i visualitzar-ne el funcionament (n'hi ha de gratuïts a Internet).*

## 4.3 VIRUS INFORMÀTIC

### QUÈ ÉS?

Els virus són **programes informàtics** que s'introdueixen als ordinadors de manera molt diversa, amb la finalitat de produir efectes no desitjats i nocius. Cada vegada que un virus entra al PC direm que s'ha produït una infecció.

El "virus ideal" (des del punt de vista dels autors de virus) seria aquell que es propaga de manera sigilosa, sense que ningú no ho adverteixi, i inicia la seva activitat destructiva una vegada que els ordinadors es troben ja infectats.

### COM ACTUA?

Produir **infeccions** en arxius i altres elements.

Fan **accions destructives** addicionals, que poden deixar l'ordinador fora de servei. Fan que no s'engegui o no arrenqui, esborren el contingut de la memòria, accedeixen a la informació confidencial de l'usuari que el fa servir, descobreixen les contrasenyes secretes, esborren arxius, fan que els nostres programes no funcionin o que no ho facin d'una manera correcta, etc.

### CONSELLS PER MINIMITZAR ELS RISCOS?

- ⇒ Feu servir un bon antivirus i actualitzeu-lo freqüentment.
- ⇒ Comproveu que el vostre antivirus inclou suport tècnic, resolució urgent de nous virus i serveis d'alerta.
- ⇒ Assegureu-vos que el vostre antivirus està sempre actiu.
- ⇒ Verifiqueu, abans d'obrir, cada nou missatge de correu electrònic rebut.
- ⇒ Eviteu la descàrrega de programes de llocs no segurs en Internet.
- ⇒ No agafeu arxius que no hagueu sol·licitat quan estigueu en xats o grups de notícies.
- ⇒ Analitzeu sempre amb un bon antivirus els disquets que feu servir l'ordinador.
- ⇒ Retireu els disquets de les disqueteres abans d'apagar o reiniciar l'ordinador.
- ⇒ Analitzeu el contingut dels arxius comprimits.
- ⇒ Pareu atenció davant accions sospitoses de possibles virus.
- ⇒ Feu periòdicament còpies de seguretat.
- ⇒ Estigueu informats.
- ⇒ Feu servir sempre programari legal.

## 5. ENLLAÇOS RECOMANATS

<b>PARES I EDUCADORS</b>	<a href="http://www.diba.es/chilias/info/navegueu.asp">www.diba.es/chilias/info/navegueu.asp</a>	Pàgina del Servei de Biblioteques de la Diputació de Barcelona amb informació i recomanacions sobre els beneficis i riscos d'Internet en els menors.
	<a href="http://www.navegacion-segura.red.es">www.navegacion-segura.red.es</a>	Destinada a pares i educadors amb consells per tutelar els menors en la navegació per Internet.
	<a href="http://www.protegeles.com">www.protegeles.com</a>	Pàgina que permet fer denúncies sobre llocs web relacionats amb pornografia infantil.
	<a href="http://www.aui.es/padres/progra.htm">www.aui.es/padres/progra.htm</a>	Llista completa de programes que limiten l'accés a certes pàgines de contingut pornogràfic, xenòfob i violent. Inclou una breu valoració d'algunes d'aquestes aplicacions i es fa especial menció de les que estan traduïdes a l'espanyol.
	<a href="http://www.pandasoftware.es/about/resp_soci al/children_internet/">http://www.pandasoftware.es/about/resp_soci al/children_internet/</a>	Campanya "Nens i Internet" que Panda Software ha llençat per informar a pares i mares dels perills que amaga la xarxa i per prevenir l'ús que en fan els més petits.
	<a href="http://www.guiaeducativa.net">www.guiaeducativa.net</a>	Material escrit i altres recursos que poden ajudar o orientar el treball amb l'educació, concretament en l'àmbit de la telemàtica i les TIC aplicades a l'educació (notícies relacionades amb aquest àmbit, contactes, recursos, articles i molts enllaços)
<b>INFANTS I JOVES</b>	<a href="http://www.xtec.es">www.xtec.es</a>	Pàgina de la Xarxa Telemàtica Educativa de Catalunya, amb materials, activitats i enllaços
	<a href="http://www.edu365.com">www.edu365.com</a>	Portal segur que ens dona informació sobre la seguretat en Internet. Hi trobarem també activitats per a nens.
	<a href="http://www.lamalla.net/canal/infantil/">www.lamalla.net/canal/infantil/</a>	Espai de la Diputació de Barcelona amb activitats, articles, notícies i activitats varies per a infants.
	<a href="http://www.chaval.es">www.chaval.es</a>	Portal infantil amb ofertes d'oci educatiu que aporta molts enllaços per infants i pares.
	<a href="http://www.cavallfort.net">www.cavallfort.net</a>	Pàgina web de la revista catalana per a infants i joves amb diversos recursos per aquestes edats.
<a href="http://www.piscolabis.net">www.piscolabis.net</a>	Portal per a menors de 14 anys amb activitats lúdiques i d'aprenentatge, fet amb l'assessorament i supervisió de l'ONG proinfància ACPI.	

## Sabadell fes Clic

### RECOMANACIONS PER A UN ÚS RESPONSABLE D'INTERNET

- ⇒ **Instal·leu** l'ordinador en una sala comuna i no al dormitori dels nens.
- ⇒ **Acompanyeu** els menors quan estiguin connectats a Internet.
- ⇒ **Interesseu-vos** per saber què fan i manteniu una bona **comunicació** amb ells.
- ⇒ Pacteu amb els menors una sèrie de **conductes**:
  - ✓ Horari i temps de connexió.
  - ✓ Accedir a webs coneguts i de confiança (ús de l'Historial i els Favorits)
  - ✓ Si en algun moment se senten incòmodes, sortiu immediatament del lloc web i avisar els adults.
  - ✓ No donar mai dades personals ni de la seva família sense la supervisió d'un adult (ni contrasenyes, nom d'usuari).
  - ✓ Quan els menors utilitzen informació d'Internet per fer els seus treballs escolars, que indiquin sempre la font (la pàgina web) on l'han trobat.
  - ✓ Si es connecten en un lloc públic (espainetnet) que no s'oblidin de tancar la connexió, ja que una altra persona es podria fer passar per ells.
  - ✓ Ser respectuosos amb les altres persones i no fer res que pugui ferir o perjudicar ningú.
  - ✓ Evitar ser autor d'un delictes (amençar o assetjar algú, distribuir, copiar o publicar dibuixos, música o text amb *copyright* obtinguts de webs sense permís).
  - ✓ No fer compres sense la supervisió d'un adult.
  - ✓ Avisar sempre un adult (pare, mare o tutor) quan algú intenti fer una trobada amb ells.
  - ✓ No obrir missatges de desconeguts ni aquells dels quals no s'està segur de la veracitat del seu contingut.
- ⇒ Utilitzeu **Eines de Control**, programes informàtics que permeten:
  - ✓ Bloquejar l'accés a continguts no recomanats.
  - ✓ Controlar el temps de connexió.
  - ✓ Programa antivirus actualitzat.