MANUAL DE MANTENIMENT DE SISTEMES INFORMÀTICS

Autor: David Rodriguez, Esteban Ruggero, Paloma Gomez, Cesar Gonzalez, Xavier Moya, Xavier Baró, Eduard Martinez, Gabriel Gonzalez, Carles Sant Emeterio

ÍNDEX CONTINGUTS MANTENIMENT DE SISTEMES

Normativa d'ús dels equips:

Recull de normes bàsiques

Aquí us recomanem un seguit de normes que hem recollit d'alguns punts Òmnia. No tots els punts Òmnia tenen la mateixa utilització per això és possible que algunes de les normes que hi ha en aquest recull no les puguis fer servir en el teu punt (vegeu normes amb *).

	Normes bàsiques dels punts
	No pots instal·lar (ni des de Internet ni des de qualsevol altre suport) cap programa ni pots canviar cap configuració sense demanar permís al responsable de l'aula.
	No pot haver-hi usuari si no hi ha un responsable a l'aula.
	No pots menjar ni beure a l'aula. Tampoc pots fumar!
	No cal fer soroll. Prova de mantenir un bon ambient de treball.
	Durant els espais d'ús comunitari tenen prioritat en l'ús dels ordinadors els que estudiïn o treballin.
	Porta els teus disquets i utilitza'ls, però abans avisa el responsable de l'aula perquè els hi apliqui l'antivirus.
	Quan hagis d'imprimir, avisa el responsable de l'aula. Les impressores només les pot tocar ell!
*	Únicament es podrà imprimir X fulls per usuari
	No et canviïs d'ordinador t'has de quedar al que t'han donat a recepció.
	Respecteu els horaris i els torns.
*	Tots els usuaris poden tenir una carpeta per poder desar els seus treballs encara que has de saber que el responsable de l'aula periòdicament buida el contingut d'aquestes carpetes
	No apagueu els ordinadors sense avisar al responsable de l'aula.
	Les pàgines i correus amb continguts que puguin ser ofensius amb els altres poden ser motiu d'expulsió de l'aula.
	Els usuaris no podem treballar amb el servidor
	Qualsevol dubte pregunta al responsable de l'aula.
	En cas de pluja apagueu tot el material informàtic perquè la garantia no cobreix els desperfectes produïts per efectes naturals ni manipulació.
*	En els cursos de formació es obligatòria l'assistència en cas de no poder assistir s'oferirà el curs a la pròxima persona de la llista d'espera.

Programes del bàsics del Punt Òmnia

Recorda que depenent de l'antiguitat dins del teu punt dins del programa Òmnia podràs tenir variacions en el software que has rebut aquí tens una llista amb els programes bàsics que almenys hauries de tenir.

Office diferents versions

Conjunt de programes pensats per poder gestionar una petita o mitjana empresa.
Aquest conjunt de programes esta format per:
Word: És un processador de textos que et permetrà crear, llegir, desar i imprimir documents de text de tot tipus des de cartes fins a taules d'horari.
Excel: És un full de Càlcul, els fulls de càlcul serveixen per portar la comptabilitat, fer gràfics i automatitzar processos en els quals s'hagin de fer moltes operacions.
Acces: És un programa per crear i gestionar una base de dades. Les bases de dades serveixen per poden administrar tot tipus de informació. Pots fer consultes a la informació afegir més informació, esborrar, imprimir.
Power Point: És un programa que et permet fer presentacions on es podem combinar textos, imatges, sons, pel·lícules.

Programes de retoc fotogràfic

Paint Shop Pro i **Corel Draw**: Són dos programes per realitzar tasques de tractament d'imatges, pots afegir efectes a les imatges, retallar-les, imprimir-les, i amb la combinació de l'escaner es poden escanejar imatges. Paint Shop Pro és més senzill que el Corel Draw que et permet treballar a un nivell molt professional.

Creació de pàgines Web

Dreamweaver: és un programa que et permet crear pàgines Web. Amb aquest programa pots inserir fàcilment en una pàgina web de text imatges, taules per presentar la informació, sons i fins i tot animacions fetes amb flash.

Mecanografia

Flying Fingers i **accutype:** són programes per aprendre mecanografia depenent de l'antiguitat del punt tindràs un o l'altre. Fent exercicis l'usuari pot aprendre a fer servir el teclat més eficientment.

Creació de CD's

Easy CD creator és un programa que acompanya a la gravadora, serveix per fer CD de dades, documents, imatges i CD's de música inserint arxius de Àudio en format wav o mp3 (depenent de la versió)

Anti virus
Panda Antivirus: Programa que has de tenir instal·lat en totes les màquines per protegir-te dels atacs produïts per virus informàtics. Vigila amb els documents adjunts que rebeu pel correu, les pàgines web que visiteu que a vegades estan infectades, i els arxius que els usuaris descarregant des de Internet o a vegades porten en disquets o CD's.

Eines de compressió
Winzip: És un programa que serveix per comprimir i descomprimir arxius. És molt útil perquè la majoria d'arxius que es descarreguen d'Internet estan comprimits en aquest format per ocupar menys espai i baixar-se d'Internet més de pressa. Si no el tens no podràs veure aquests arxius.

Descàrregues de fitxers: música, executables.

La descarrega de fitxers de música esta prohibida dins d'un punt Òmnia degut a que aquests **programes que s'utilitzen per baixar música** fan servir unes estratègies de connexió que **absorbeixen tot l'ample de connexió i limiten la utilització d'Internet a la resta d'usuaris**.

També **esta prohibida l'execució d'arxius .exe** .com .pif .bat .dll .cpl aquests arxius **podem canviar la configuració de les màquines**, poden **instal·lar software** que ens facin automatismes que fan que les màquines vagin més lentes, poden **instal·lar programes del tipus dialer** que es fan servir per connectar-se a pàgines trucant a un número de telèfon que no és el de la tarifa plana creant una despesa extra a la entitat. Moltes vegades **aquest arxius poden ser virus** o actuar com a tal.

La millor manera de saber si un usuari no ha fet cas de les normes i ha instal·lat algun programa per descarrega música és veure en el funcionament de la Xarxa quan tots els usuaris estan connectats a Internet, si algú baixa música la Xarxa anirà tan lenta que alguns usuaris ni tan sols podran obrir el correu. També podeu fer recerques al disc dur d'arxius mp3. Si trobeu que la majoria de arxius estan en una mateixa carpeta és molt possible que aquesta sigui la carpeta que faci servir el programa per descarrega música vigileu la persona que sempre es vulgui posar en aquell ordinador i ja heu enganxat al vostre usuari que baixa música.

Per evitar l'altre problema, el dels arxius perillosos, s'han de vigilar bé els usuaris i sobretot tenir ben actualitzat l'antivirus.

Correus usuaris: webmail. Configuració Outlook correus de sortida

Ara que parlarem del tema del correu et recomanen que sempre que enviïs correu **afegeixis l'assumpte**. L'assumpte és un quadre de text que normalment esta sota del quadres de text de **para**: **con copia**: **con copia oculta**. L'assumpte és com el titular de l'e-mail. Fent aquesta recomanació perquè últimament el correu esta massa atacat per virus amb aquesta petita estratègia pots assegurar a la persona que rebrà el correu que ets tu qui li ha enviat i que no esta infectat perquè normalment els virus també posem assumpte els e-mail infectats però solen ser frases vulgars en Angles o Castella.

També **et recomanen que facis contes de correu via web a tots els usuaris que vulguin fer servir correu electrònic**. És un correu personal, que els usuaris podran fer servir des de qualsevol màquina que tingui connexió a Internet. **No et recomanem que facis servir l'Outlook com a gestor de correu per els usuaris** per que si ve podran enviar correu el problema serà si l'usuari a de rebre resposta.

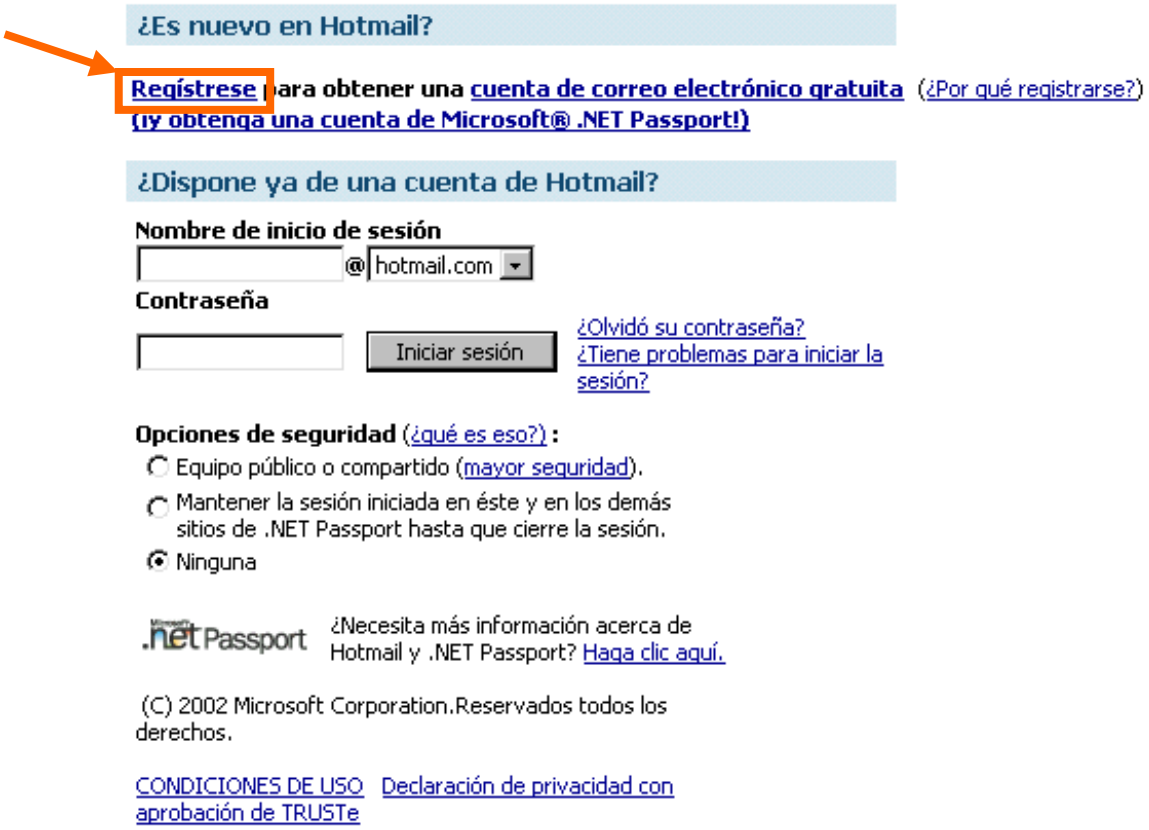
1. Si configures l'Outlook com a només correu de sortida podràs enviar correu però no podràs rebre correu,
2. si configures un compte de correu per a totes les màquines el primer que es connecti descarregarà el correu i
3. si configures un compte de correu per a cada màquina obligues a que la persona que ha fet servir una màquina per enviar correu més endavant voldrà connectar-se a la mateixa màquina per comprovar si ha rebut correu la qual cosa pot originar un caos entre l'ocupació dels usuaris.

Aquest dos últims casos fan que el correu tingui greus problemes de privacitat per aquests motius et recomanen que no facis ser l'Outlook com a gestor de correu. Un altre problema que té l'Outlook es el forats per entrar virus on l'antivirus no pot fer res.

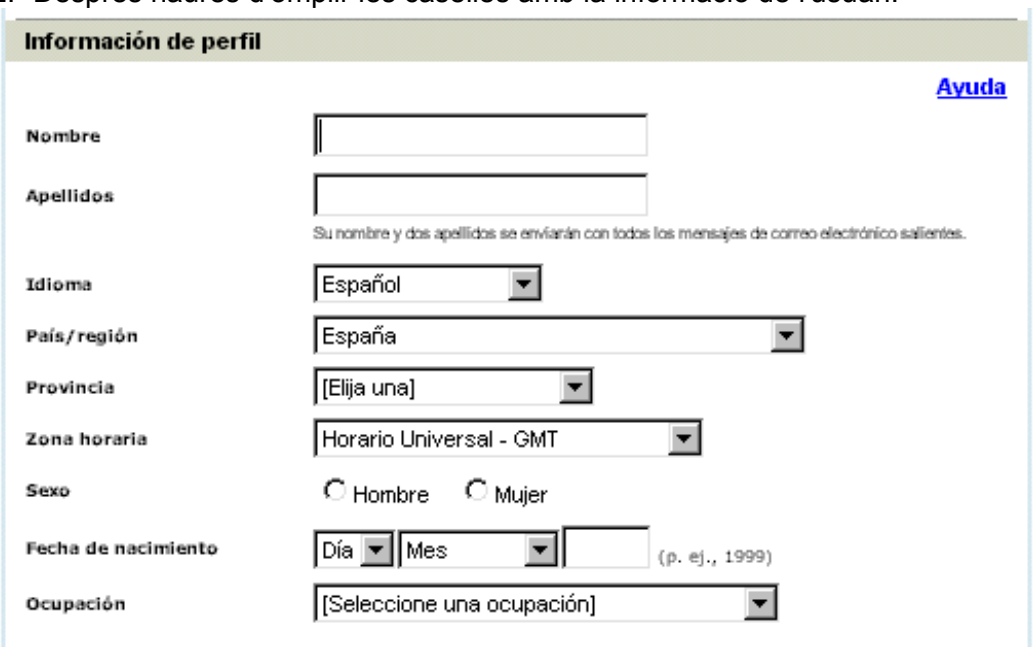
El problema que tenen les contes de correu via web és el següent, si els usuaris estan visitant una pàgina és possible que aquesta tingui una secció per enviar un correu. Normalment el que s'encarrega de fer la pàgina posa una instrucció mailto. Aquesta instrucció s'encarrega d'obrir automàticament l'Outlook per enviar un correu nou amb una adreça determinada. Com que vosaltres no tindreu el Outlook configurat això no serveix de res. La solució es copiar l'adreça que aparegui en la secció para del nou correu que s'ha obert a l'outlok i enviar un correu normal des de l'adreça de correu via web de l'usuari a l'adreça de correu que heu copiat.

A continuació t'expliquem com pots crear un compte de correu web des de l'adreça web www.Hotmail.com aquest correu també els usuaris el podran fer servir per connectar-se al Messenger.
També us donem altres adreces en les que també us podeu crear comptes de correu via web.
www.yahoo.es
www.iespana.es
www.3xl.net

1.- Una vegada has entrat en la pàgina fes clic a l'opció. Regístrese.



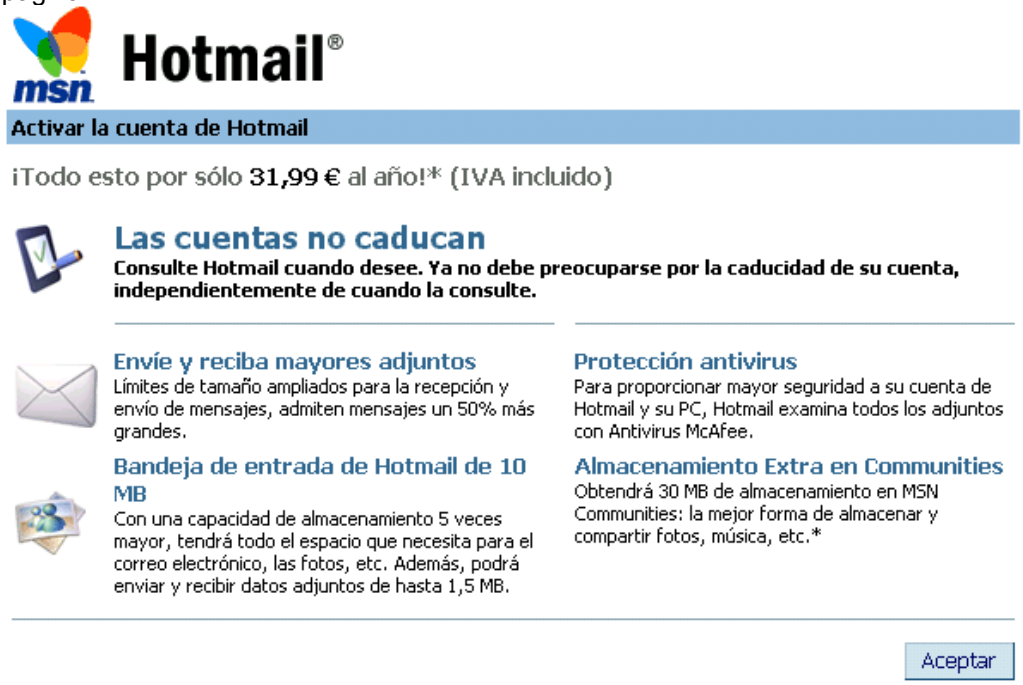
2.- Després haures d'omplir les caselles amb la informacio de l'usuari.



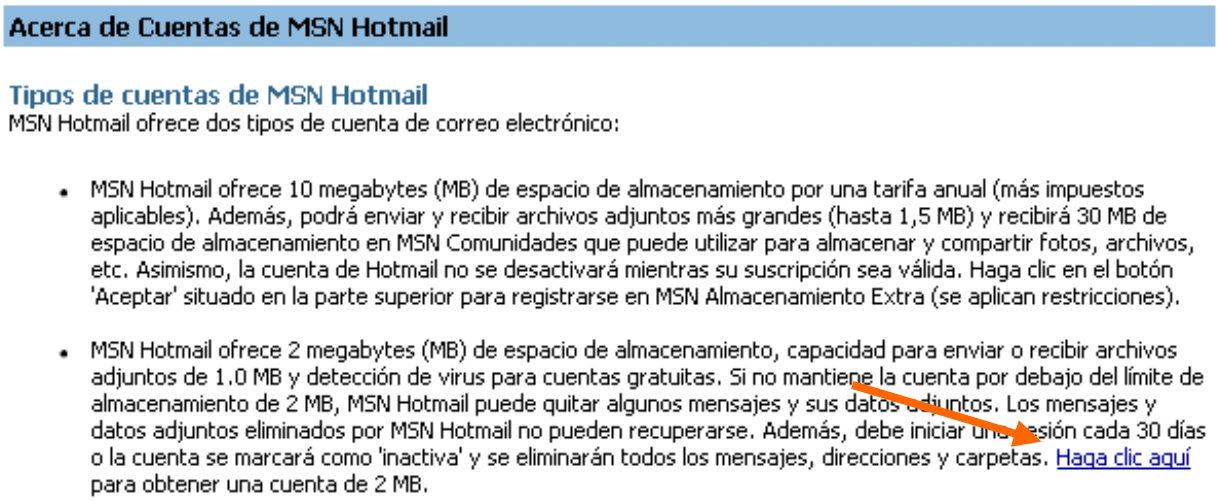
3.- Les dades de la compta són oblidades normalment per l'usuari així que hauries de recordar-li que es molt important que recordi l'adreça i la contrasenya. Al final hi ha dues caselles: Directorio de Usuarios de Hotmail i pàgines blanques de Internet. Tots dues serveixen per compartir les teves dades amb Internet. La primera és només per donar a conèixer les teves dades entre els usuaris de Hotmail i la segona vol ser com unes pagines grogues però d'Internet.

4.- Després fes clic al botó acceptar si has tingut alguna errada el procés tancarà amb lletres de color vermell quina casella no has omplert correctament. Normalment els usuaris volen adreces que ja existeixen i han de canviar-la.

5.- Finalment després de passar per dos pàgines d'enquestes per rebre publicitat arribes a aquesta pàgina de la qual no facis molt cas i mou el bloc de desplaçament fins que puguis veure el final de la pàgina.



6.- El final de la pàgina es així llavors només has de fer clic a l'opció Haga clic aquí per poder fer servir el compte de correu



Acerca de Cuentas de MSN Hotmail

Tipos de cuentas de MSN Hotmail

MSN Hotmail ofrece dos tipos de cuenta de correo electrónico:

- MSN Hotmail ofrece 10 megabytes (MB) de espacio de almacenamiento por una tarifa anual (más impuestos aplicables). Además, podrá enviar y recibir archivos adjuntos más grandes (hasta 1,5 MB) y recibirá 30 MB de espacio de almacenamiento en MSN Comunidades que puede utilizar para almacenar y compartir fotos, archivos, etc. Asimismo, la cuenta de Hotmail no se desactivará mientras su suscripción sea válida. Haga clic en el botón 'Aceptar' situado en la parte superior para registrarse en MSN Almacenamiento Extra (se aplican restricciones).
- MSN Hotmail ofrece 2 megabytes (MB) de espacio de almacenamiento, capacidad para enviar o recibir archivos adjuntos de 1.0 MB y detección de virus para cuentas gratuitas. Si no mantiene la cuenta por debajo del límite de almacenamiento de 2 MB, MSN Hotmail puede quitar algunos mensajes y sus datos adjuntos. Los mensajes y datos adjuntos eliminados por MSN Hotmail no pueden recuperarse. Además, debe iniciar una sesión cada 30 días o la cuenta se marcará como 'inactiva' y se eliminarán todos los mensajes, direcciones y carpetas. Haga clic aquí para obtener una cuenta de 2 MB.

Actuació en cas d'incidències

En cas d'**incidència del maquinari (hardware)**, heu d'enviar un correu directament al Xavi Pastor de la Direcció General de Serveis Comunitaris xavipastor@ctv.es indicant:

- Núm. de sèrie del maquinari per reparar
- Descripció de la incidència
- Persona de contacte
- Horari de contacte
- Telèfon de contacte
- E-mail de contacte
- Adreça del Punt

En cas d'**Incidències de Programari (Software):** Heu de posar-vos en contacte amb:

- Associació per a joves TEB tel. 93.442.58.67 Carles o Vladi teb@xarxa-omnia.org
- La Fundació coordinadora corresponent.

Després de tramitar la incidència si passen 3 dies, sense resposta torneu a reclamar.
Una vegada solucionada la incidència, cal notificar al Xavier Pastor la reparació de l'avaria. Si feu alguna reparació pel vostre compte la garantia no la cobrirà. Recordeu sempre que la garantia no cobreix danys per fenòmens naturals com pluja ni per manipulació del Hardware.

Organització d'equips

Organització d'equips

Gestió de la informació

1. Polítiques de la gestió de la informació
    1.1. Organitzar l'espai d'emmagatzematge
    1.2. Còpia de seguretat dels continguts dels usuaris
    1.3. Evitar la pèrdua accidental dels fitxers del sistema

2. Manteniment del sistema
    2.1. Neteja de fitxers temporals
    2.2. Scandisk
    2.3. Compactador de discs
    2.4. Instal·lació de programari
    2.5. Desinstal·lació de programari
    2.6. Neteja del registre
    2.7. Assistent de manteniment

Gestió de la Informació

1. Polítiques de la gestió de la informació

1.1. Organitzar l'espai d'emmagatzematge per a usuaris

Els ordinadors de cada punt han d'emmagatzemar diferents tipus d'informació dels usuaris:

- Documents, imatges, fulls de càlcul, etc.
- Descàrregues d' Internet
- Favorits d' Internet

Amb la finalitat que aquestes informacions no es desin sense ordre ni control en les diferents màquines, és necessari crear un espai d'emmagatzematge centralitzat i controlat. Cada nou usuari haurà de ser informat sobre aquest espai / carpeta, i també de la seva utilització.

Tenim dues possibilitats a l'hora de treballar amb aquesta carpeta:

1. creació d'una sola carpeta compartida en el servidor de manera que inclogui a la seva vegada diferents carpetes amb el nom i els cognoms dels diferents usuaris que venen a la sala, i a on ells mateixos poden anar ficant els seus materials de feina.

   Avantatges de la utilització d'aquesta carpeta compartida:

   - major accessibilitat i control tant per l'usuari com per l'administrador de la sala.
   - Evitem ocupar els discs durs amb continguts de particulars i així resta espai disponible per instal·lar nou programari.

2. Creació d'una carpeta d'ús compartit en cada màquina a on a la seva vegada es generaran tantes sub-carpetes com usuaris n'hi hagi. Aquestes carpetes hauran de ser accessibles no tan sols des de la pròpia màquina sinó també des de qualsevol altra que es trobi dins de l'aula a través de l'entorn de xarxa, evitant d'aquesta forma que un determinat usuari hagi sempre de fer servir la mateixa màquina per a accedir als seus arxius.

   Avantatges d'aquest sistema:

   - No es sobrecarrega el trànsit d'informació a través de la xarxa cap a una determinada màquina.
   - No depenem del bon funcionament d'una màquina central per a l'accés a la informació.

- Es reparteix l'ús de l'espai en el disc entre les diferents màquines de la sala.

Deixem al criteri de cada dinamitzador la utilització d'un o un altre sistema, segons les característiques de la seva sala i usuaris.

Procediment per compartir una carpeta

1. Cliquem amb el botó dret del ratolí sobre la carpeta que volem compartir i seleccionem la opció *compartiment* del menú emergent.
2. Seleccionem l'opció *compartit amb el nom* i escrivim el nom que tindrà la carpeta.
3. Marquem la opció *ple* dins del tipus d'accés.
4. Cliquem el botó *aplicar*.
5. Observem que la icona que representa la carpeta compartida ha canviat i apareix una mà que la sosté per la base.

Un procediment important per limitar la accés a la informació és també la possibilitat que ens dóna el sistema d'*amagar* carpetes. Abans de tot hem de comprovar que tenim activada l'opció "*No mostrar arxius ocults o del sistema*" a dins del menú *Veure*, *Opcions de carpeta i Veure*.

Per amagar una carpeta ho farem amb el següent procediment:

1. Seleccionem amb el botó dret del ratolí la carpeta que volem amagar.
2. Del menú emergent que surt hem d'anar a la darrera opció "*Propietats*"
3. A dins de propietats hem de seleccionar la opció que apareix a la part d'*Atributs* corresponent a "*Ocult*".

Si més endavant volem que aquesta carpeta sigui visible de nou haurem de seguir el procés anterior i treure la marca que hem fet a la casella corresponent.

1.2. Còpia de seguretat dels continguts dels usuaris.

Amb la finalitat de d'evitar la pèrdua accidental de la informació de qualsevol dels discs de les màquines és convenient planificar una còpia diària o setmanal dels continguts treballats per cada usuari, a ser possible de forma automatitzada i programada, mitjançant l'ús d'una aplicació dedicada a aquesta tasca com poden ser *Second Copy* o *Filebackup* (a www.softonic.com podeu trobar-ne moltes).

És important de qualsevol forma, educar l'usuari en la necessitat que s'acostumi a fer còpies de seguretat dels seus materials en disquets ja que els discos de la sala són "netejats" amb certa regularitat per evitar la manca d'espai.

1.3. Evitar la pèrdua accidental de fitxers del sistema.

Amb aquesta finalitat és convenient activar la opció "*No mostrar arxius ocults o del sistema*". Per això, i des de qualsevol finestra seguirem el següent procediment:

1. Opció *veure*, i dintre d'aquest menú *opcions de carpeta*.
2. En la finestra que s'obrirà marquem la pestanya *veure*.
3. Marquem l'opció *No mostrar arxius ocults o del sistema,* pitgem el botó *com la carpeta actual* que es troba en la part superior i finalment *Aplicar,* a la part de sota a la dreta.

2. Manteniment del sistema

2.1 Neteja de fitxers temporals

És convenient automatitzar l'eliminació d'una sèrie de fitxers temporals que es generen en la feina diària amb el sistema Windows. Trobem diferents tipus d'arxius:

1. Fitxers amb extensió *tmp* que s'emmagatzemen en la carpeta *C:\WINDOWS\TEMP*, i que son generats pel software amb el qual treballem com a arxius temporals que després no són eliminats.
2. Fitxers amb extensió *chk* que s'emmagatzemen a l'arrel del disc dur C:\ i que es generen quan s'executa un test del disc amb la utilitat *SCANDISK* per donar forma a fragments perduts d'arxiu.
3. *Cookies* d'Internet. Fitxers de text que contenen informació sobre el visitant i el moment en el qual visita una determinada pàgina web. Aquesta informació és utilitzada per les pàgines per personalitzar el tractament que ens donen quan tornem a aquestes webs.
4. Fitxers amb extensió *old i bak* que s'emmagatzemen en diferents zones del disc, fonamentalment en *C:\WINDOWS* i que són versions antigues de fitxers amb el mateix nom, normalment fitxers de registre de successos.
5. Fitxers temporals d'Internet. Arxius gràfics, de flash i de hipertext de les pàgines visitades més freqüentment que s'emmagatzemen localment per disminuir el temps de càrrega d'aquestes pàgines.
6. Fitxers amb configuracions personalitzades d'accessos telefònics a xarxes, els anomenats *dialers* que acostumen a "facilitar" l'accés a pàgines poc recomanables.

Per eliminar els del tipus 1, 2 i 3 en cada arrencada del sistema i evitar així que ocupin espai innecessari podem generar un fitxer de procés per lots al qual anomenaren per exemple *NETEJA.BAT* i que tindrà la següent estructura:

```
@echo off
deltree /y c:\Windows\temp\
deltree /y c:\*.chk
deltree /y c:\Windows\cookies\
```

i que editarem amb el bloc de notes mateix, desant-lo finalment en la carpeta d'inici del menú programes de Windows. D'aquesta forma en cada inici del sistema s'executarà i eliminarà aquests fitxers.

Com que aquest fitxer que acabem de crear és un fitxer que s'executa en MS-DOS és interessant modificar una opció per tal que es tanqui la finestra fosca que s'obre quan finalitza la seva feina. Veiem com:

1. cliquem amb el botó dret a sobre de la icona NETEJA.BAT i seleccionem *propietats* del menú emergent.
2. en la finestra *propietats,* marquem en la pestanya *programa* i a dins de les opcions que ens presenta marquem l'opció de *tancar al sortir* i finalment pitgem el botó *Aplicar*.

Per eliminar el 3er tipus de fitxers, és a dir, amb extensió OLD i BAK, farem servir la recerca del menú inici assenyalant *.old i *.bak com a nom de l'arxiu a buscar en la unitat C i marcant la opció *incloure sub-carpetes* si no estigués marcada ja. Cliquem el botó *Buscar ara* i en el quadre inferior apareixeran els fitxers que acompleixen el criteri de recerca. Podem senyalar-los tots i eliminar-los.

Per evitar que es vagin acumulant el fitxers temporals d'Internet abans mencionats seguirem el procediment següent:

1. obrirem Internet Explorer
2. Marcarem *opcions d'Internet* dins del menú *Eines*
3. Ens anem a la pestanya *Opcions avançades* i dins d'aquesta a l'apartat de *seguretat* que es troba més avall.
4. Finalment marcarem l'opció *Buidar la carpeta arxius temporals d'Internet* quan es tanca l'explorador.

Per esborrar el darrer tipus de fitxers, els anomenats *dialers* no hi ha cap procés automàtic. Cal vigilar com a responsables de l'aula els discs dels ordinadors i tenir cura del seu contingut, vigilant la presència d'aquest tipus de programes que s'instal·len a la màquina pel desconeixement o la manca de prudència de l'usuari.

2.2. Scandisk

Serveix per verificar l'existència d'errors en les unitats de disc del sistema i fer una reparació sempre que és possible.
Malgrat que *Scandisk* s'executa automàticament en iniciar l'ordinador si Windows ha tancat incorrectament, és convenient fer-lo de forma manual cada mes aproximadament per solucionar problemes amb els discs.

Existeixen dues modalitats:

1. *Estàndard*: és l'opció més ràpida i tan sols verifica la taula de localització d'arxius *(FAT)*. Acostuma a ser suficient en la majoria de casos.
2. *Exhaustiva*: es verifica la integritat física del disc ja que es repassa tota la superfície enregistrada del disc. No és precís modificar les opcions de configuració d'aquesta modalitat. Aquest segon tipus és convenient fer-lo servir quan sospitem que poden haver-hi errors físics en la superfície del disc dur degut a talls de llum inesperats i similars que poden perjudicar seriosament les zones on s'emmagatzemen les dades.

En ambdós casos és convenient tenir marcada l'opció de *reparar els errors automàticament* per què no s'interrompi el procés amb preguntes a l'usuari.

Scandisk, de la mateixa forma que la utilitat de defragmentació que veurem a continuació, es troba al menú *eines del sistema*, del menú *accessoris*, del menú *programes* del botó *inici.*

Ambdues utilitats fan un ús intensiu del disc i per tant seran interrompudes per qualsevol programa que estigui fent servir el mateix evitant així que acabi la seva acció. Per evitar això, lo millor és iniciar el Windows en *Mode a prova d'errors*, i executar-los en aquesta modalitat. Per fer això, només encendre l'ordinador, pitjarem la tecla F8 abans que aparegui la pantalla amb el logotips de Windows i així accedir al menú de modalitats d'arrencada i aquí seleccionar el *mode a prova d'errors*. També és important no tenir el salvapantalles activat.

2.3. Compactador de discos

En instal·lar, desinstal·lar, gravar o esborrar informació del disc dur, es produeix un repartiment desordenat de l'espai de disc utilitzat. D'aquesta manera el nostre ordinador pot arribar a alentir molt el seu rendiment.
El compactador de discs ens endreça tota la informació optimitzant el rendiment del nostre PC, és com tenir l'habitació endreçada o no, cada cosa al seu lloc ☺. El que fa realment és disposar de forma contigua en el disc dur els fragments que conformen un fitxer de programa o dades, ordenant segons carpetes, millorant i accelerant així la seva lectura / escriptura.

És molt important no tenir cap programa en marxa i no tenir un salvapantalles activat. Cada cop que un programa escriu informació al disc, el compactador s'ha de reiniciar.
Cal compactar el disc amb una periodicitat mensual aproximadament. Per a un correcte funcionament del compactador, és molt millor fer-lo amb Windows a *mode de prova d'errades.*

Un cop el compactador és a punt d'iniciar ens demana quina unitat volem compactar i quina configuració volem fer servir. Les opcions per defecte d'aquesta configuració ja ens van bé.

2.4. Instal·lació de programes

Sempre que ens disposem a instal·lar un programa és recomanable tancar totes les aplicacions que tinguem obertes, ja que n'hi ha moltes que reinicien l'ordinador automàticament i podríem perdre la feina que estiguéssim fent en aquells moments.

A l'hora d'instal·lar un programa cal diferenciar entre els que ens baixem de la xarxa en forma de:

- *.exe
- *.zip , *.rar, *.ace (tots arxius comprimits)

o els que instal·lem directament d'un CD o disquet.

La instal·lació des del CD s'inicia automàticament quan l'introduïm al lector (sempre i quan tinguem activada la *notificació d'autoinserció del CD-ROM).*
(Cal recordar que podem interrompre la lectura automàtica d'un CD si mantenim pitjada la tecla majúscula en introduir el CD a l'ordinador.)

Per continuar amb la instal·lació "Siguiente" // "Next"

La gran majoria de programes tenen la seva llicència que s'ha d'acceptar per a poder ser instal·lats.

Un cop s'ha acceptat la llicència hem d'introduir les nostres dades per a un posterior registre. Per continuar amb la instal·lació "Siguiente" // "Next"

Cal introduir el número de sèrie del producte, normalment és a la caixa o a la coberta del CD. Per continuar amb la instal·lació "Siguiente" // "Next"

Hi ha instal·ladors que ens permeten triar diferents opcions d'instal·lació; les típiques finestres on ens permeten triar entre Típica -- Compacta -- Personalitzada, si no dominem el software que estem instal·lant, la millor opció és Típica // Estàndard.

Arriba el moment de triar el directori a on instal·larem el programa, és molt recomanable deixar que el programa s'instal·li al que té per defecte.

Un cop hem triat totes les opcions, arriba el moment de començar la instal·lació, fins ara no hem "escrit" informació al nostre disc dur i podem cancel·lar el procés sense cap problema. Pitgem instal·lar i comença el procés.

Un cop acabat el procés l'instal·lador ens avisa.

En determinats casos ens demanarà reiniciar l'ordinador, si ho féssim tenint alguna aplicació oberta podríem perdre allò que estàvem fent, cal que tanquem abans, per tant, qualsevol document obert o programa.

Encara podríem recuperar les tasques que estiguéssim fent abans de reiniciar l'ordinador triant l'opció "No" o fent ús de la combinació de tecles Alt + Tab (Tabulador) per triar la tasca que volem finalitzar abans de reiniciar, o la tecla Windows + D per anar a l'escriptori i un cop allà guardar el treball que tenim.

Per instal·lar els programes que ens baixem de la xarxa o que estan continguts en un disquet o CD amb aplicacions tipus "Sinera", hem de buscar sempre els anomenats *SETUP o INSTALL*, en cas de no ser-hi triarem els *.exe amb el nom del programa que volem instal·lar.

Un cop iniciada la instal·lació es repetirà el procés vist anteriorment; acceptar la llicència, nom de l'usuari, número de sèrie, directori d'instal·lació, etc.

En el cas que el programa que volem instal·lar estigui en format comprimit (extensió *zip, rar, ace*, etc.) , primer l'haurem de descomprimir en una carpeta i després agafar i executar el programa d'instal·lació corresponent (setup.exe, instalar.exe, install.exe, etc.) tal i com hem comentat abans.

2.5. Desinstal·lació de programes

És molt important tenir clar que per desinstal·lar un programa correctament no tenim prou amb agafar la carpeta en el qual es troba i posar-la a la paperera del sistema. D'aquesta forma no eliminen fitxers compartits, de configuració i entrades de registre que el programa introdueix al Windows en ser instal·lat, i fem que el sistema es vagi embrutant de forma innecessària.

Hi ha molts programes que tenen el seu propi desinstal·lador de programes. Per instal·lar buscarem "*install*" i per desinstal·lar "*uninstall*".

Si el programa que volem no té desinstal·lador cal anar al *tauler de control* que és a dins del *menú inici // configuració // tauler de control* i cercar el programa que ens permet desinstal·lar... fem doble clic per obrir l'aplicació, aquesta mostra un llistat de programes, la majoria son instal·lats, però pot ser que ens mostri programes que hem desinstal·lat malament o que hem esborrat accidentalment, (més endavant veurem com solucionar aquest entrebanc).

Per desinstal·lar els programes els seleccionem de la llista i premem el botó *Afegeix / suprimeix.* El desinstal·lador s'executa i normalment ens demana reiniciar l'ordinador després de fer-ho.
Tal i com hem comentat al principi d'aquest apartat hem d'evitar sempre esborrar aplicacions (arxius amb extensió .exe) i/o carpetes que continguin aquests programes ja que la majoria d'aplicacions en instal·lar-se copien arxius vinculats en carpetes del sistema, aquests arxius no seran esborrats si no es fa una correcta desinstal·lació. L'altre problema que podem tenir és amb l'arxiu del registre que emmagatzema tota la informació referent a versió del programa, nom de qui el registra, caducitat (en cas de tenir-la), etc.

2.6. Neteja del registre

El registre del sistema és una part vital de Windows, i està format per un parell de fitxers *system.dat* i *user.dat*, tots dos situats a la carpeta Windows, i en ells es recull la informació del propi sistema i dels programes que fem servir. El correcte funcionament d'ells depèn del bon estat del mateix. A mesura que anem instal·lant programari, noves claus s'afegeixen als fitxers que conformen el registre fent que vagi augmentant la seva mida. Malauradament en fer la desinstal·lació, no tots el programes eliminen la informació que van introduir prèviament. Per evitar que la mida del registre sigui massa gran i per tant la feina amb el mateix pugui fer anar més lent l'ordinador hem de realitzar una neteja periòdica del mateix amb la utilitat *REGCLEANER.*

Aquest programa fet per un jove adolescent finlandès ens permet fer un gran nombre de tasques afegides a la neteja del registre.

- Desinstal·lar programes (oculs o no).
- Cercar i netejar arxius duplicats.
- Modificar la llista dels programes que s'inicien en arrencar el sistema.
- I força opcions per a usuaris avançats.

De totes les tasques que fem ens crea una copia de seguretat per a poder-les restaurar en cas de cometre un error.

- Neteja del registre amb Regcleaner.

Hem d'executar el menú d'opcions...
...a dins de Neteja...// Mètode // seleccionem automàtic.
Continuant dins el menú d'opcions // Neteja...// Còpia... // Crear una copia.

Un cop triades les opcions de neteja anem al menú eines // Netejar...// Neteja automàtica...

El programa analitza la memòria, elimina els registres erronis i crea una copia de la tasca que hem fet per si cal restaurar-la.

- Desinstal·lar amb Regcleaner

Seleccionem la pestanya de "Menú de desinstal·lar", triem el programa desitjat i cliquem al botó desinstal·lar de la part de baix.

És molt important utilitzar amb precaució aquesta utilitat ja que qualsevol error es podria traduir en un funcionament incorrecte de Windows o qualsevol altre programa que tinguem instal·lat en ell, o fins i tot, podria no iniciar-se correctament el sistema.

2.7. Assistent de manteniment

Malgrat que en apartats anteriors hem donat mètodes de solució per automatitzar tasques com la neteja de fitxers temporals (veure apartat Neteja de fitxers temporals), aquesta utilitat que ens ofereix Windows és prou útil i interessant per tenir-la en compte de cara a fer-la servir en aquesta mateixa tasca o en d'altres que pot idear l'usuari. Veurem un exemple de la seva utilització.

Automatització de neteja d'arxius temporals *.tmp

Podem estalviar feina de manteniment creant una tasca que el sistema efectuï de forma automàtica en arrencar. Cal obrir l'administrador de tasques programades que és a dins de *El Meu Ordinador // Mi PC,* triar l'opció *agregar tasca programada.*

S'inicia un assistent que ens mostra la majoria de programes executables, però l'aplicació que farem servir funciona sota MS-DOS i hem de buscar-la fent clic a examinar i triant l'arxiu *deltree.exe* que és a *c:\Windows\command*

Després hem de donar un nom a la tasca i triar la freqüència amb la que volem que el programa s'executi, cada cop que el PC s'arrenqui.

Abans de donar per finalitzada la tasca hem de triar l'opció de *propietats avançades*
...quan cliquem al final se'ns obrirà una finestra a on hem d'acabar de depurar la tasca. El deltree.exe és una aplicació que esborra el contingut de carpetes senceres i la carpeta que volem esborrar és la dels fitxers temporals **.tmp* que com sabem és a *c:\Windows\Temp.*
Cal escriure una sèrie d'instruccions pròpies de la sintaxi de MSDOS respectant els espais i les comes

Command\deltree.exe /y c:\Windows\temp.* ,exit*

i finalment clicar *Acceptar.*

Tal i com hem comentat aquest *Assistent de Manteniment* té moltes més utilitats i es pot servir també, per exemple, per planificar *Scandisk i Defragmentacions* del disc dur de forma periòdica.

Configuració i manteniment dels equips

Un ordinador, com qualsevol màquina necessita un manteniment per aconseguir un rendiment màxim durant el seu funcionament. Aquest manteniment no es limita a la neteja externa del equip sinó a una sèrie d'activitats i procediments que s'has de fer per que els nostres ordinadors ens durin més temps y fallin el menys possible.

Una cosa a tenir en compte en quant al rendiment de l'ordinador es que, per mes que el Windows sigui un sistema "multitarea" i que els processadors actuals seguin ràpids, hi ha uns factors com la memòria, els discs influeixen directament en la velocitat i el rendiment.

Comencem amb la memòria RAM: Es una part de l'ordinador on s'almacenen els programes que estem executant tal com el Word, el mateix Windows i un munt de programes "residents". Aquesta memòria es molt limitada en capacitat i es, en comparació capacitat-preu amb altres sistemes d'emmagatzematge, molt cara i vulnerable.

Sempre que un programa es posi en marxa, aquest es carrega en la RAM però no es l'únic programa que s'està executant, llavors el Windows te un recurs anomenat Memòria Virtual, que és un arxiu ficat al disc dur que fa les vegades de memòria i, aquí es quan comencen els problemes de rendiment.

El Windows per si mateix consumeix molt memòria i si, a més a més tenim programets com el Messenger, Tweakers i txorradetes d'aquestes, no ens quedarà prou memòria per fer anar el nostre programa. Llavors el Windows comença a utilitzar el disc dur com Memòria i, si no tenim ben "net i organitzat" el nostre disc, la velocitat de funcionament de l'ordinador pot caure de una forma considerable.

Ara us donarem uns consells per mantenir el vostre ordinador i com treure'l el millor rendiment.

Primer de tot es crear un **"disc d'arrancada"**. Aquest disc ens pot servir per arreglar el sistema en algun moment. Té una pega i es que treballa en "MODO TEXTO"; antic MS-DOS. Es una interfície de text on les ordres les hem d'escriure. Aquest disc el crea el mateix Windows. Hem d'anar al: PANEL DE **CONTROL -> ADICIÓ DE PROGRAMES**. Seleccionar la pestanya on posa "disc d'Arrencada" i fer clic al botó Crear Disc. Hem de tenir a mà el disc del Windows.

El Windows quan arranca carrega una sèrie de controladors i programes pel seu funcionament. Alguns d'aquests els podem controlar nosaltres.

Per controlar quins programes poden arrencar de forma automàtica i quins no hi ha una aplicació anomenada "MSCONFIG". La posarem en marxa des del comandament INICI -> EXECUTAR

Des d'aquest programa controlem el contingut de l'AUTOEXEC.BAT, del CONFIG.SYS i el que ens interessa, els programes que s'executen a l'**Iniciació** del Windows.

Aquí surt una llista dels programes d'iniciació del Windows. Si als programes li traiem la marca de l'esquerra el programa no s'executarà a la propera iniciació.

Hi ha alguns programes com l'EscanDisc o el Compactador de Windows (Defrag) que per culpa de alguns programes "residents" en memòria com els antivirus, Salvapantalles, etc... produeixen que no completin mai la seva feina per escriptures continuades als discs.
Per evitar això, quan hàgim programat el manteniment dels equips els arrencarem en el **Mode A prova d'errades.**
Aquest mode de funcionament del Windows el que fa es posar en marxa el sistema amb uns controladors bàsics i estàndards. Solament funciona el monitor en 16 colors, ratolí teclat i discos, no funcionen els lectors de CD, ni targetes de Xarxa ni de So. Tampoc carrega CAP programa dels d'iniciació de manera que podrem fer la neteja del sistema sense problemes.

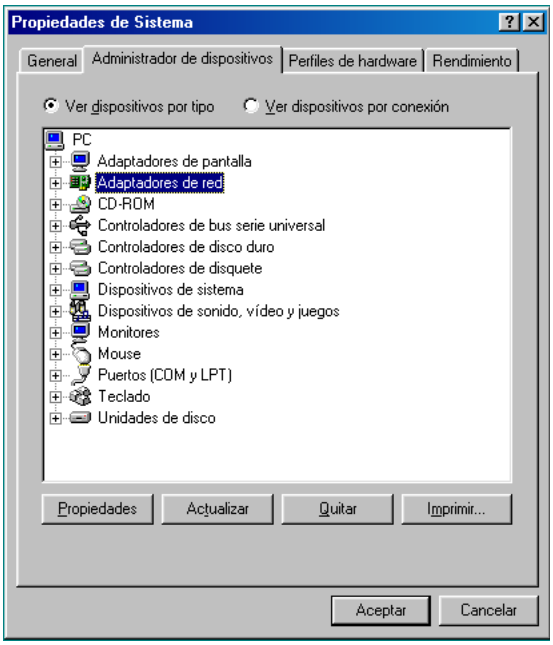
Per arrancar en Mode A prova d'errades hem de reiniciar l'ordinador i just (o una mica abans) quan apareix **INICIANT EL WINDOWS 98** polsem la tecla **F8**.

Ens sortirà un menú d'arrancada. Amb les fletxes seleccionem el **Mode A prova d'errades** i polsem l'INTRO.

Aquest mode es més lent que el mode normal.

Netegem, arreglem i reiniciem l'ordinador.

La majoria dels dispositius que tenim als ordinadors son **Plug & Play** i compatibles amb el Windows, el que vol dir que el mateix Windows els reconeix, instal·la els drivers i posa en marxa el dispositiu.



en el cas que un dispositiu no funcioni be, el Windows ens ho fa saber. Obrint el diàleg de les Propietats del sistema (PANEL DE CONTROL -> SISTEMA) tenim l'administrador de dispositius. Aquest administrador, si hi ha algun dispositiu que no funciona el marca o amb una creu vermella o amb un signe d'admiració groc. Ens els dos casos el dispositiu no funciona però un cas es pitjor que l'altre.

També pot passar que el Windows no reconegui el dispositiu, en aquest cas, si es PnP (plug & play) apareixerà en un apartat anomenat dispositiu desconegut. No tenim més opció que instal·lar els controladors del dispositiu des d'un disquet o d'un CD que normalment porta el mateix dispositiu, sempre que sigui original.

El mètode d'instal·lació acostuma a estar dins el disquet o el CD en un fitxer de text (TXT) anomenat README.TXT

En quant als programes del mateix Windows o d'altres, amb el temps arriben noves versions o actualitzacions.

El Windows 98 Primera Edició, que es la que tenim als Omnies, te l'Internet Explorer 4 i molts programes obsolets de versió a mes de tenir molts forats de sistema i de seguretat.

A l'Internet Explorer es molt recomanable que l'actualitzeu a l'ultima versió, la 6.0, ja que porta millores considerables, sobretot en la seguretat i xifrat de pàgines. Un altre programa recomanable d'actualitzar es el Windows Media Player, pels vídeos i ràdios d'Internet .

Aquests programes els podreu trobar o al CD que és va donar al curs o a la web de Microsoft. ***http://www.microsoft.es*** a l'apartat "**AREA DE DESCARGA**". No trobareu actualitzacions en català així doncs cal que seguiu alguns consells.

En quant als programes con Internet Explorer, Windows media, netmeeting... us ho podreu baixar en castellà i no hi hauran problemes.

Quan vulgueu actualitzar controladors com els DirectX, o actualitzacions de seguretat haureu de baixar les versions en anglès a l'adreça:
http://www.microsoft.com/Windows98/downloads/corporate.asp

La opció de Windows Update no funciona amb la primera versió del Windows.

Creació d'imatges i restauració del sistema (GHOST)

- **Introducció**

El programa Ghost serveix per crear imatges del disc dur, que més tard podrem restaurar i deixar l'ordinador configurat com abans de realitzar la imatge del disc.

- **Restauració del sistema a partir d'una imatge Ghost**

1. CD Autoarrencada

Si tenim un CD d'autoarrencada amb una imatge del disc en format Ghost, per restaurar-la haurem de seguir els passos següents:

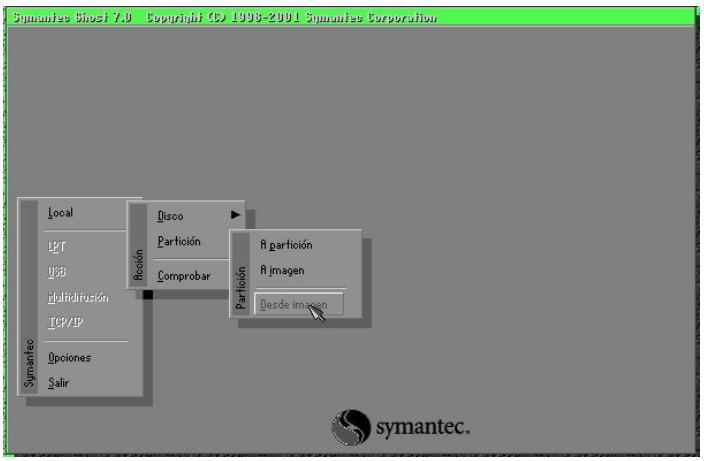
a) Arranquem l'ordinador i entrem a la "bios" (polseu "Supr" o "F2", segons l'ordinador)
   a. Busquem secció "**Boot**" i activem com a primer dispositiu d'arrencada el cd-rom, és a dir, "**Atapi cd-rom**", amb les tecles + o – posarem aquesta opció com a número 1. Amb el Cd a la unitat de Cd-rom sortim de la "bios", "**Exit**", i gravem els canvis (passeu al punt c).
   b. En ordenadors Siemens, amb F2, buscarem a "**Main**" l'opció "**Boot Options**", seguidament "**Boot Sequence**" i amb les tecles + o – posarem com a primera seqüència d'arrencada "**Cd-Rom Drive**".

b) Si la "bios" no reconeix aquesta opció, s'haurà de crear un disc d'arrencada de Windows 98. Obrirem el "Panel de Control", obrirem "Agregar treure programes", polsarem sobre "Disc d' Inici", "Crear disc" i seguirem el procés.

Arrancarem l' ordinador i entrarem a la "bios" (polseu "Supr" o "F2", segons ordinador). Buscarem secció "**Boot**" i activarem com a primer dispositiu d'arrencada la unitat de 3½", "**Removable Device**". Amb el disquet a la unitat, sortirem de la "bios", "**Exit**", i gravarem els canvis. Quan l'ordinador arranqui triarem l'opció de "**compatibilitat amb cd-rom**".

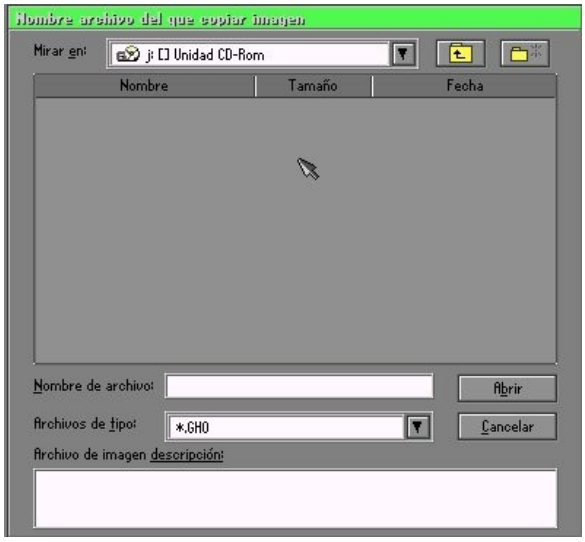
c) Arrancarem l' ordinador des del cd-rom o des del disquet i el Ghost s' activarà (si no s'activés des del símbol de sistema teclejarem: **GHOST**).
En aquesta operació el ratolí no és operatiu, (treballem sota DOS). Avançarem pels camps amb la tecla de TABULADOR, seleccionarem amb les FLETXES del teclat i executarem amb l'INTRO
Cal tenir present que al fer un "ghost" ESBORRAREM tot el disc dur, per tant cal salvar abans tot allò que no vulguem perdre.
Elegirem:

Local -> Partición[1] (o Disco) -> Desde Imagen

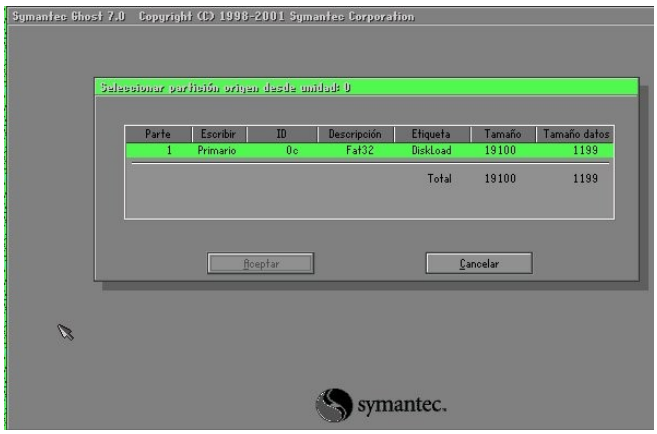


Buscarem unitat de Cd-rom i arxiu d'imatge a:

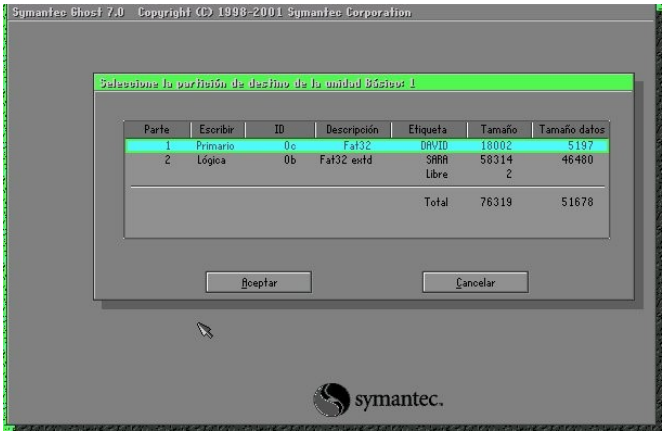
[1] Els discos d'Òmnia estan configurats amb dues particions, per tant l'opció correcta és "Partición".



Seleccionarem, a continuació la partició d'origen, lògicament la primària.



Seleccionarem, després, la unitat de destí, lògicament la primera, i a continuació la partició de destí, lògicament la primària.



Començarà a copiar la imatge, si necessita més d'un cd el programa els anirà demanant. Finalitzada la còpia, retirarem el cd i polsarem sobre "Reiniciar Pc". Nota: s'ha de tenir en compte que el sistema operatiu es troba en la situació en la qual es va realitzar la imatge. És a dir, si la imatge ve d'un altre ordinador s'hauran de tornar a configurar drivers (targeta de so, vídeo, targeta de xarxa, impressores, protocols de xarxa (TCP/IP), etc.) Veurem més endavant aquests apartats.

- **Creació d'una imatge del disc**

Una imatge no és més que una còpia exacta del disc dur d'un ordinador en un moment donat. Aquesta imatge recull tots els programes instal·lats, totes les configuracions i també tots els defectes que l'ordinador tingui. L'objectiu és disposar d'una imatge actualitzada i neta de fitxers inútils. Fer la nostra imatge vol dir estalviar-se feina en els futurs clonatges. Per exemple la instal·lació dels controladors de la tarja de so i la dels ports d'impressió no caldrà tornar-la a fer en el futur. Un cop ens assegurem que tenim l'ordinador imatge tal com volem estem en disposició de començar a fer la imatge:

a. Arranquem l'ordinador des de MS-DOS, amb el disquet d'arrencada o amb el Cd-rom.

Consideracions prèvies: Si des del símbol de sistema escrivim -> **ghost –h** ens mostra totes les opcions disponibles. Les que utilitzarem seran les següents:

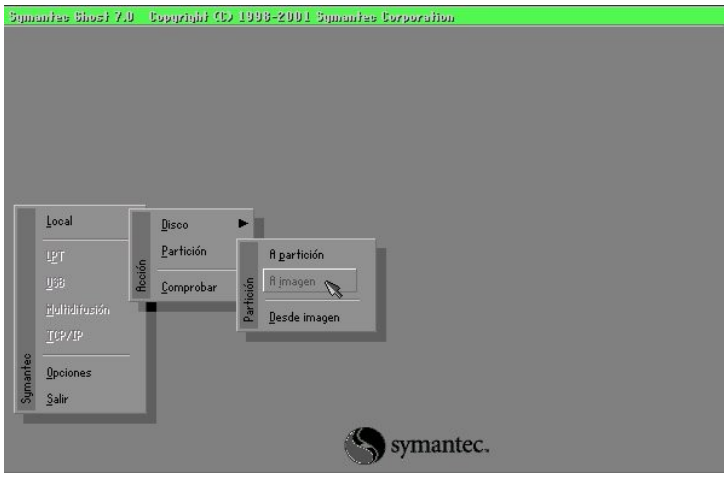
-auto -> no sol·licita nom d' arxius dividits, utilitza nom predeterminat
-span -> activa la divisió en diversos volums
-split=n -> divideix l'arxiu imatge en parts petites de [n] Mb en crear imatges (això ens servirà per passar la imatge a cd-roms)

b. Des del símbol de sistema arranquem el Ghost amb :

Ghost –auto –span –split=650[2]

c. Elegirem l'opció:

Local -> Particion[3] (o disco) -> A imagen



[2] Capacitat del cd-rom. Per poder gravar la imatge més endavant.
[3] Els discos d'Òmnia estan configurats amb dues particions, per tant l'opció correcta és "Partició".

Seleccionem la unitat origen de la clonació (la primera), després la partició de la clonació (sempre la primària). Tot seguit indiquem el destí de la clonació[4] i el nom del fitxer a crear. Finalment el nivell de compressió de les dades. Una vegada acabada la imatge, retirem el cd o el disquet i reiniciem el pc.

Tindrem un fitxer amb extensió ghost “gho” i més fitxes amb extensió “ghs”, els quals es podran copiar a cd-roms (un fitxer a cada cd), des d’on podrem realitzar més endavant la restauració de la còpia en el cas de desconfiguració; problemes amb el sistema operatiu; virus, afegir un nou ordinador a la xarxa; etc.

[4] En el cas de traballar amb un disc dur amb dues particions, clonem la partició d’arrencada a la partició de dades. Si tenim un disc amb una sola partició necessitarem un segon disc on realitzar la imatge del disc.

Configuració i manteniment d'impressores

Instal·lar una impressora no es una feina complicada ja que les d'última generació son Plug&Play i això simplifica molt les coses. A més a més, les impressores HP porten un CD d'autoinstal·lació amb el qual solament li hem de dir "endavant" a totes les pantalletes de l'assistent d'instal·lació.

Hi ha dos tipus d'impressores: Les USB i les de Port Paral·lel.

Per instal·lar una impressora USB, lo primer que hem de fer es instal·lar el programa de la impressora (o els drivers). Una vegada instal·lats hem de reiniciar l'ordinador i, una vegada ja s'ha engegat el Windows, endollem la impressora i llestos.

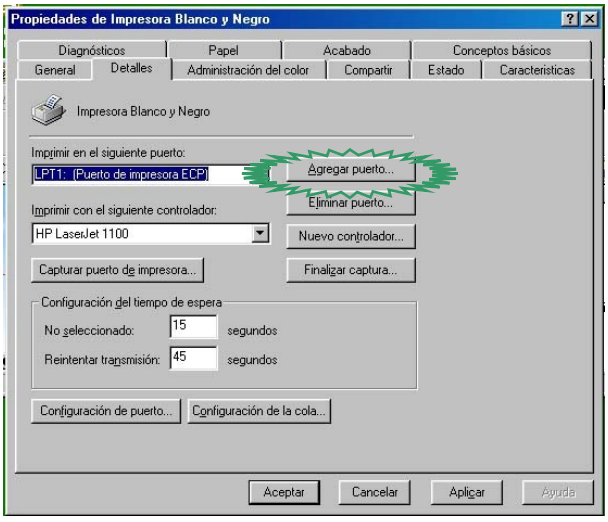
Quan es tracta d'una impressora per Port Paral·lel hem d'actuar de la mateixa manera, primer instal·lar els programes, endollar la impressora i a imprimir.

Els problemes comencen quan tenim un port JetDirect per gestionar les impressores.

Be, no son realment problemes sinó que la instal·lació te un quants passos més.

La explicació que faré ara està feta amb una unitat JetDirect 500X de 3 ports i es de àmbit explicatiu. El mètode amb un altre JetDirect no canvia gaire.

Els passos a seguir son:



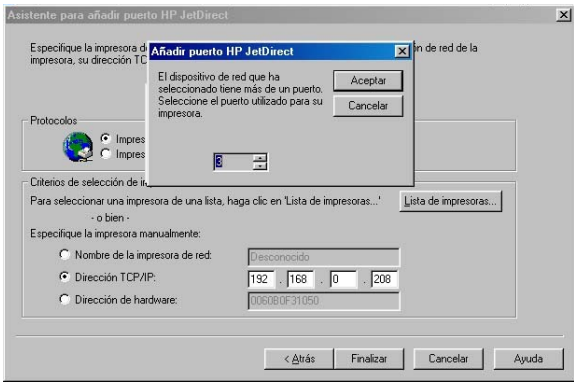
1. Instal·lem la impressora seguint els passos normals i quan ens demana el port d'impressió li donem el normal l'***LPT1:*** tal i com ho tenim a la foto.

2. Una vegada fet això fem clic al botó Afegir un Port (Agregar Puerto). Quan s'obre el quadre de diàleg hem de fer clic a l'opció **Altres** i seleccionar on posa **HP JetDirect Port**.

3. En aquest moment s'obre el programa per afegir ports de JetDirect.

En la primera pantalla que surt ens demana una instal·lació avançada o fàcil, nosaltres seleccionem la fàcil i fem clic al botó Següent.

A la següent pantalla ens demana el tipus de xarxa que tenim, com la nostra en TCP/IP seleccionem aquesta opció i fem clic al botó “Listado Impresoras”.



En aquest moment el programa es posarà en contacte amb el dispositiu JetDirect per veure la quantitat de ports que té disponibles. Si es la primera vegada que afegim ports ens sortiran 3 ports, si no, ens llistarà els ports que estiguin disponibles. Seleccionem el port on es troba endollada la impressora i li donem a D’Acord.

Al cap d’una estoneta ens sortirà una pantalla com la que veiem. Aquesta finestreta petita ens demana que confirmem a quin port del JetDirect volem que es connecti el programa. Seleccionem el port 1, 2 o el 3 segons correspongui i fem clic a D’acord.

Ens confirmarà que s’ha creat el port al JetDirect i quan tornem a la pantalla de **Detalls** de la Impressora veurem com on abans teniem **LPT1: (port d’impressora ECP),** ara ens posa:

192.168.0.208_P1 (HP JetDirect Port)

En principi no te que haver cap problema. Podem imprimir una pàgina de prova per veure si tot va be.

Organització de les impressores

Per una bona gestió i un bon control de les impressores es recomanable que les dues impressores estiguin controlades per un son ordinador i, a ser possible, pel Servidor. D'aquesta manera podrem controlar quan es pot imprimir i quan no.

Per fer això hem d'instal·lar les impressores a un ordinador com a impressores locals i després "compartir-les" a la xarxa.

1. Per poder compartir les impressores hem de tenir activat el protocol de **Compartiment d'impressores i arxius.** Per veure si està instal·lat hem d'anar a la configuració de la xarxa.

2. Una vegada hem confirmat que està tot preparat per compartir recursos anem a la carpeta d'impressores seleccionem una impressora i entrem a les propietats.

3. Seleccionem la pestanya de **Compartir.** Li donem un nom que identifiqui la impressora a la xarxa i llestos La impressora ja està disponible a la xarxa.

Ara, a la resta de terminals hem de configurar, les impressores per que utilitzin aquest recurs.

4. Situats en un terminal anem a la carpeta d'impressores que, en teoria estarà buida. Fem doble clic a la opció **Addició una Impressora**.

5. Fem clic a Següent

6. Després ens pregunta si instal·larem una impressora local o de xarxa, seleccionem "de xarxa" i fem clic a Següent.

7. Ara ens demana el camí a la xarxa fina a la impressora. El més senzill es fer clic a **Navega**. Els ordinadors que ens sortiran a la llista son els que tenen impressores compartides a la xarxa. Obrim l'ordinador fent clic al signe +, seleccionem una impressora i fem clic a següent.

La primera impressora que instal·lem l'ordinador la posarà com **Predeterminada**. A mesura que anem instal·lant impressores ens anirà demanant si volem que la nova impressora sigui la predeterminada. Vosaltres mateixos.

Per ficar un altre impressora hem de seguir els passos del 4 al 7.

¿Per què es interessant centralitzar les impressores? Perquè d'aquesta manera la cua d'impressió la gestiona un ordinador de manera que, si hi ha 20 documents per imprimir i nosaltres volem un document que resulta que es l'últim, l'únic que hem de fer es moure el nostre document de la última posició a la primera.

Problemes amb les impressores.

Problemes tindrem sempre i de diversa manera. Aquí posarem uns quants de més comuns i com solucionar-los.

Problema:

Les impressores no funcionen.

Causes:

Comprova que estiguin endollades i les llumetes del davant enceses.

Comprova que els cables de comunicació de la impressora cap a l'ordinador o al

Jetdirect estan ben connectats.

En cas d'utilitzar JetDirect:

Comprova que el JetDirect estigui ben endollat.

- està endollat al corrent elèctric.
- està endollat a la Xarxa.

Comprova que el HUB funciona correctament.

Problema:

La impressora no imprimeix:

Causes:

Comprova que la impressora te paper a la safata.

Comprova que la impressora no te un paper encallat.

Comprova el nivell de tinta/tonner de la impressora.

Problema:

Tinc la impressora ben instal·lada però quan li fico el port del JetDirect no funciona.

Causes:

La configuració de la xarxa no es correcta.

Comprova amb el JetAdmin si gestiona be els ports de la impressora.

Problema:

No puc trobar les impressores a la Xarxa.

Causes:

L'ordinador que gestiona les impressores està apagat.

L'ordinador que gestiona les impressores no te les impressores compartides.

Hi ha problemes amb el HUB.

Configuració manteniment de xarxes

Introducció a les Xarxes

Una de les millors definicions d'una xarxa es d'identificar-la com un sistema de comunicacions entre ordinadors. Com tal, està formada d'un suport físic que, avarca el cablejat , plaques addicionals als ordinadors i un conjunt de programes que formen el sistema operatiu de xarxa.

Tipus de xarxa:

Per la relació que hi ha entre els membres de la xarxa, aquestes es subdivideixen en dos grans grups: xarxes amb servidor i xarxes entre iguals.
En una xarxa **basada en un servidor**, els recursos a compartir es centralitzen en una màquina denominada SERVIDOR (server). Les altres es denominen **estacions de treball** (workstation) o clients. Aquests només poden utilitzar recursos propis o del servidor.

En una xarxa **entre iguals** qualsevol estació pot oferir recursos per compartir.
Les avantatges de treballar amb una xarxa son moltes:

- Mantenir bases de dades actualitzades al instant i des de qualsevol lloc.
- Facilitar la transferència d'arxius entre ordinadors.
- Facilitar la còpia de seguretat dels sistemes.
- Comunicar-se amb altres xarxes (Internet).
- Etc...

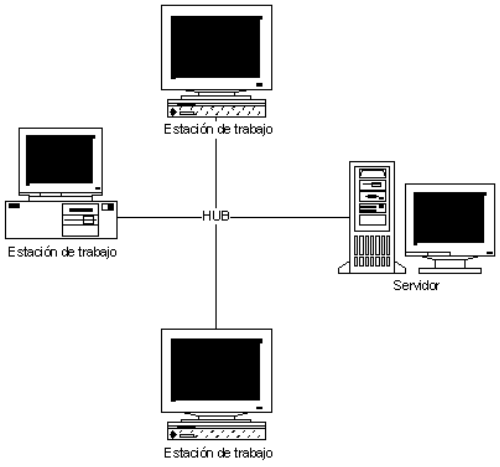
A més a més, si les estacions no disposen de disquetera o la tenen bloquejada:

- Evitem l'ús il·legal de software.
- Evitem la entrada de virus.

Topologia de la LAN de l'Òmnia

La topologia de la LAN (Local Area Network – Xarxa d'Àrea Local) la defineix el harward que la compon.

A l'Òmnia tenim la topologia denominada Estrella (Star). Es diu així perquè hi ha un punt central denominat HUB en el qual convergeixen totes les línies de comunicació. Cada màquina te un enllaç amb el HUB. Aquest HUB no es més que un repetidor de senyal. Quan rep un senyal de una màquina, el repeteix a totes les altres.



Hi ha dos tipus mes de topologies de xarxes:

Bus: En aquesta hi ha un cable que recorre totes les màquines sense formar camins tancats. Totes les màquines es connecten al bus en paral·lel a aquest cable.

Anell: En aquest cas, les línies de comunicació formen un camí tancat. La informació recorre l'anell en un sentit, es el mes lent.

Recordeu te tenir ben localitzat el CD-ROM o la carpeta on es troba el Windows 98 ja que durant el procés de configuració el pot demanar.

Configuració de la Xarxa:

NOTA: Abans de tocar res de la configuració hem d'apuntar sense equivocar-nos ens numerets del DNS i de la Pasarel·la ja que si posem malament aquests números l'ordinador no es podrà connectar a internet.

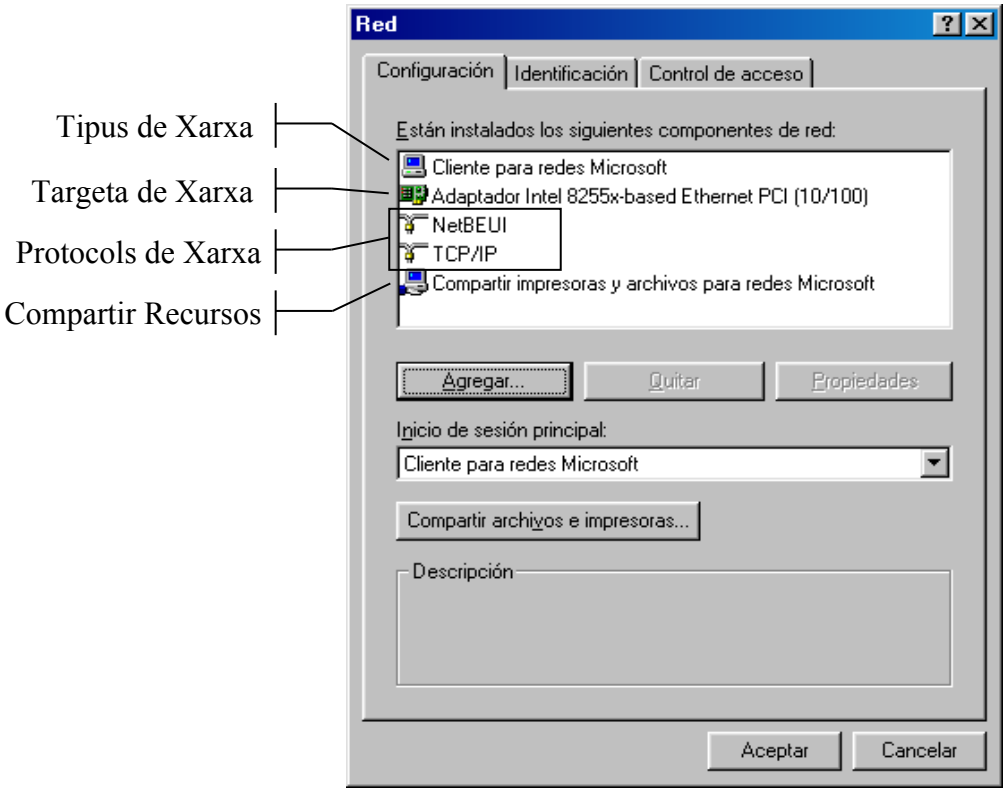
Per localitzar aquests números podeu utilitzar el programa WINIPCFG que s'explica més endavant.

Per configurar o canviar algun paràmetre de la xarxa, es necessari entrar al Panel de Control de Xarxa.

El podem trobar de dues maneres:

1. Entrant al Panel de Control INICI -> CONFIGURACIÓ -> PANEL DE CONTROL i fent doble clic sobre la icona Xarxa.
2. Fent clic amb el botó secundari sobre la icona de Veïnatge de la Xarxa a l'escriptori y fent clic a propietats.

Quan s'obre la configuració de Xarxa el primer que ens surt es la part de configuració dels dispositius i dels protocols.



En aquesta primera pantalla es on nosaltres configurarem els PROTOCOLS de comunicació y de compartiment de recursos.

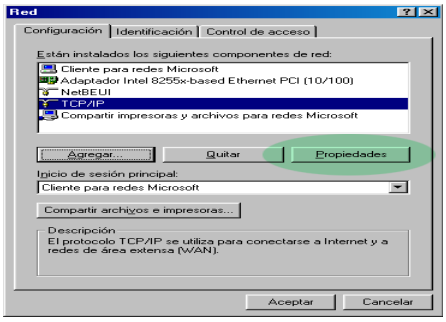
Un protocol de xarxa es un llenguatge que utilitzen els ordinadors per comunicar-se i poder enviar-se informació entre ells.

Un ordinador pot tenir més d'un protocol instal·lat. Això s'utilitza quan tenim una xarxa amb diferents sistemes operatius o com a mesura de seguretat en el cas que caigui un protocol, tenim l'altre com recolzament.

El fet de tenir més d'un protocol al nostre sistema no afecta gaire al rendiment de la xarxa. El sistema operatiu quan detecta més d'un protocol ens demana quin d'ells serà el predeterminat i es el que utilitzarà sempre. Si aquest no rep resposta al enviar alguna senyal per la xarxa, utilitzarà el següent.

Cada protocol te una raó de ser. Llavors quin es el millor protocol per la meva xarxa? Depèn de les necessitats de la meva xarxa. En el nostre cas el que millor s'adapta a les necessitats de l'Òmnia es el TCP/IP ja que ens permet compartir recursos a la xarxa i connectar-nos a Internet.

Anem a veure com s'ha de configurar la xarxa per que funcioni correctament.

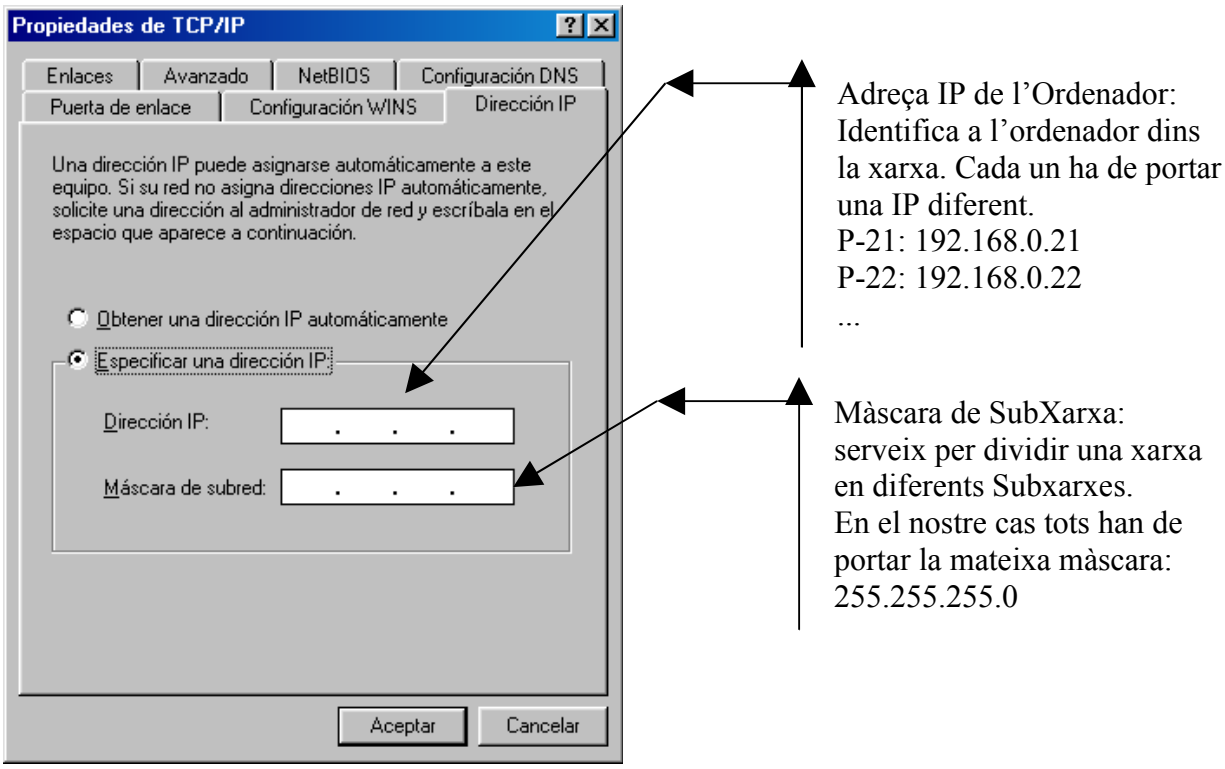


Configuració del TCP/IP

Una vegada tenim obert el diàleg de configuració de la Xarxa, fem clic sobre TCP/IP i seguidament sobre el botó propietats.

En aquesta primera pantalla anomenada Adreça IP es on posarem l'adreça de l'ordinador amb la qual s'identificarà dins la xarxa.

CADA ORDINADOR HA DE TENIR LA SEVA PROPIA ADREÇA. SI PER ERROR POSEM LA MATEIXA ADREÇA A DOS ORDINADORS AQUESTS NO FUNCIONARÀN EN XARXA I DONARÀN ERRORS.



Anem a comentar una mica aquesta pantalla:

Adreça IP: Es un número composat per quatre series que van des del 000 (00h) fins al 255 (FFh) i separats per un punt. Aquests números juntament amb uns altres que porten les targetes de xarxa formen l'adreça que identificarà l'ordinador dins la xarxa.
Com nosaltres estem configurant una xarxa interna o LAN tenim una sèrie d'adreces que podem utilitzar. Aquesta sèrie va des del 192.168.0.0 fins al 192.168.255.255
Si feu uns petits càlculs veureu que es poden connectar uns quants milers d'ordinador a la xarxa.
Cada ordinador ha de tenir la seva pròpia IP i ha de ser diferent dels altres ordinadors.

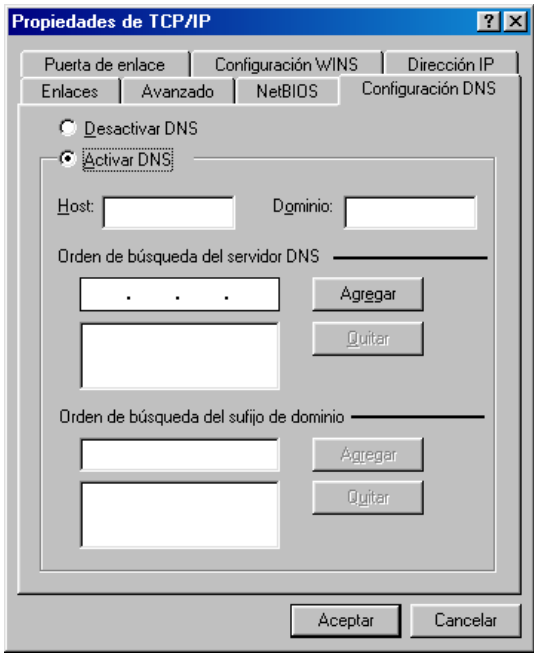
Per exemple:
Ordinador 1: 192.168.0.21
Ordinador 2: 192.168.0.22
.
.
.
Ordinador 9: 192.168.0.29

Màscara de SubXarxa: Aquesta màscara el que fa es separar una xarxa en diferents subxarxes. Per fer això es fa una multiplicació lògica entre la adreça IP i la màscara de subxarxa. D'aquesta manera un ordinador amb la màscara 255.255.255.0 no podria trobar a un altre amb la màscara 255.255.0.0

En el nostre cas utilitzarem en TOTS els ordinadors la màscara 255.255.255.0

i volem que els ordinadors es connectin a Internet hem de configurar també els DNS.
Aquests números DNS son les adreces IP del nostre servidor d'Internet, per tant si no les posem be l'ordinador no es connectarà a Internet.
Llavors fem clic, sense tancar res, sobre la etiqueta Configuració DNS.

NOTA: No tots els punts tenen les mateixes adreces DNS, per tant abans de fer res apúntate-les en un lloc segur o pregunta al TEB quines son les teves DNS's.
L'ordre de les DNS també es important. Si poseu la segona DNS en lloc de la primera tampoc funcionarà el tema.



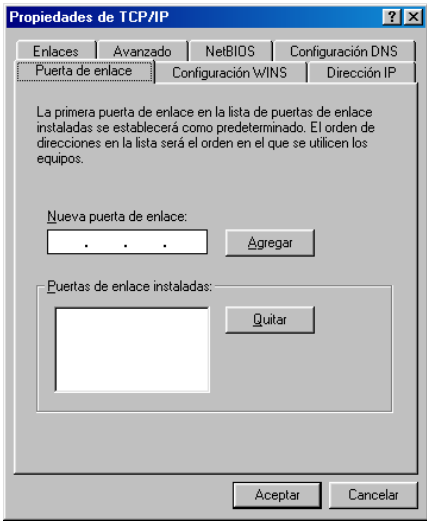
En aquesta pantalleta el més important son les adreces DNS. Las hem de col·locar en el mateix ordre que ens les van donar allà on posa "ordre de cerca del servidor DNS". Quan posem la primera hem de fer clic sobre el botó Afegir. Seguidament posem la segona i tornem a fer clic sobre Afegir (agregar). Les adreces han d'aparèixer en un llistat a sota d'on posem les adreces. Si ens equivoquem en alguna adreça o la hem de canviar per algun motiu, la seleccionem de la llista i fem clic sobre esborrar (quitar).

En quant on posa HOST i DOMINI, hem d'omplir-los amb alguna cosa ja que si no posem res no ens deixarà sortir.

Podeu posar:
HOST: P-21
DOMINI: xtec.es
O poseu el que vulgueu.

A més a més de les DNS, un altre dada important a configurar es la Passarel·la (GateWay).
Les passarel·les son programes o dispositius que connecten dues xarxes diferents, fa una funció de "pont" entre les xarxes.

Nosaltres l'utilitzem per connectar-nos a Internet, i la nostra passarel·la es el ROUTER



ADSL. Per accedir a la passarel·la hem de fer clic sobre la pestanya que te aquest nom i ficar el número que correspongui.

NOTA: No tots els punts tenen la mateixa Passarel·la, per tant abans de fer res apúntate-la en un lloc segur.

Heu de posar el 4 números de la passarel·la i fer clic al botó Afegir.

Un cop fet tot això li doneu al botó d'acord i tornarem al diàleg de configuració de la xarxa.

Ara ens queda configurar el **nom** de l'ordinador i el **grup de treball**.

El **nom** de l'ordinador serveix per identificar de una forma més entenedora per nosaltres a l'ordinador dins la Xarxa. Es més fàcil identificar un ordinador per MANTENIMENT-1 que no per 192.168.23.45, per exemple. Aquest nom ha de ser únic en TOTA la xarxa, ja que com les IP's, no pot poden existir dos ordinadors diferents amb el mateix nom.

El grup de treball serveix per identificar un grup determinat d'ordinadors dins la mateixa xarxa de una forma més ràpida.

Per exemple: Si tinguéssim 20 ordinador dels quals 4 son base de dades, 4 s'utilitzen per disseny gràfic i 2 per fer pàgines WEB, el més coherent seria agrupar el 4 ordinador de base de dades en un grup anomenat **DADES**, els altres 4 en un altre anomenat **DISSENY-GRAF** i els que queden en **WEB.** D'aquesta manera, al obrir el Veïnatge de la Xarxa el primer que veuríem serien els ordinadors del nostre mateix Grup de Treball. Si volguéssim trobar un ordinador d'un altre grup, obriríem, l'element TOTA LA XARXA i ens sortirien tots els altres grups de treball.

Per configurar això obrirem el diàleg de configuració de Xarxa i seleccionarem l'element **Identificació.**

Dins aquest element ens trobem amb 3 quadres a omplir. Els 2 primers son obligatoris, el tercer es opcional.

El primer serveix per posar el Nom de l'ordinador (P-21, P-22... P-29) Recordeu que han de ser diferents.

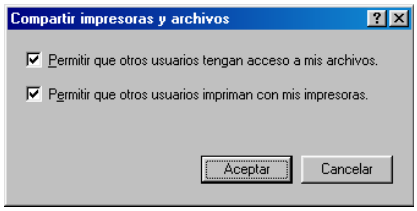
On posa Grup de Treball, el més còmode es posar tots els ordinadors en el mateix grup de treball així quan obrim el Veïnatge de la xarxa ens sortiran tots els ordinador a l'hora.

Posarem el que ens doni la gana, però ha de ser el mateix a tots els ordinadors.

I en la descripció podem posar la funció que farà l'ordinador, que l'utilitza normalment... no influeix en el funcionament de la xarxa.

Si volguéssim que a l'ordinador es puguin intercanviar arxius o que es pugui imprimir a les seves impressores hem d'activar el protocol de **Compartir arxius i Impressores.**

Per fer això obrim el diàleg de configuració de xarxa i, a la secció de configuració, hi ha un botó que posa **Compartir arxius i Impressores.** El polsem i activem TOTES les caselles que ens surtin. Donem a D'Acord a totes les finestres, el sistema es reinicia i l'ordinador ja està preparat per compartir recursos.



Si hem fet tot be, al reiniciar les màquines, al obrir el Veïnatge s'haurien de veure TOTS els ordinadors.

Si no es veuen tots, ens esperem uns segons i actualitzem la pantalla. A vegades triga una mica que un ordinador reconegui a tots els altres. Por passar que en un ordinador es vegin a tots i en un altre es vegin la meitat.

Si passat un temps no es veu l'ordinador es que alguna cosa no hem fet be o que no funciona.

Solucionar problemes amb la Xarxa

Aquí es proposaran solucions de les més fàcils a les més complicades.

1. intentar entrar des d'un altre ordinador l'ordinador que no es veu. Això es fa des de El Meu Ordinador (o des del Veïnatge de la xarxa). Hem de cridar a l'ordinador pel seu nom de la següent manera:
   a la barra d'adreces hem de posar ***NomDeL'ordinador***
   Per Nom de l'ordinador s'entén P-21 o be P-22 etc.

Si tot va be ens haurà de sortir en nom de l'ordinador a la barra d'adreces i els elements que tingui compartits (si els te).

I... ¿per què no ens surt al Veïnatge de la xarxa? Segurament es per que ens hem equivocar al posar el Grup de Treball. Verifiquem que estigui be.

Si la cosa no funciona surt un missatge dient que l'ordinador no es troba a la Xarxa.

2. Verifiquem que hàgim posat be les IP a l'ordinador. Per això utilitzarem un programa anomenat **WINIPCFG.**

Aquest programa ens diu com està configurat les dades IP de l'ordinador. Per posar-lo en marxa hem d'anar a **INICI -> Executar**, escrivim **WINIPCFG** i fem clic a d'acord.

En aquest programa veurem 3 dades importants de l'ordinador:
L'adreça IP de la màquina, la Màscara de SubXarxa i la Passarel·la. Verifiquem que estiguin les dades be.

3. Verifiquem que tinguem instal·lat el protocol de compartir impressores i arxius ja que si no el tenim activat l'ordinador no es reconegut en la xarxa. Però pot utilitzar recursos de la xarxa.

Si encara l'ordinador no funciona en xarxa el problema es físic.

Per aquesta part de solució de problemes es important saber quin cable pertany a quin ordinador y a quin port del HUB es connecta cada ordinador.

Aquest HUB te uns indicadors a la part del davant que, amb llums verdes o taronges, indica quin port se està utilitzant.
Recomano que, si no ho teniu ja, l'ordre dels ports i dels ordinadors siguin els mateixos. El P-21 al port 1, el P-22 al port 2... el P-29 al port 9. i la resta de dispositius com el JetDirect i el ROUTER els poseu a qualsevol dels altres però sabent en quin port els poseu.

4. mirem a l'ordinador per darrere i localitzem el cable de xarxa. Normalment la targeta de Xarxa te 2 llums fixos i un que pampalluega. Si alguna cosa no funciona be ha de tenir com a mínim una llumeta encesa.

Llavors:

- Si no tenim NINGUNA llum encesa es la targeta de Xarxa que no funciona.
- Si tenim només una llum encesa provem primer de canviar de port del HUB. Normalment, si la xarxa no funciona per un problema físic, el port que correspon a l'ordinador que falla està apagat o pampalluega.
  A vegades canviant el cable de port es soluciona el problema.

Si no funciona connectem l'ordinador amb el cable d'un altre.

- Si les llumetes del darrere s'encenen i el port del hub també, el problema es el cable de xarxa que haurem de canviar.

Connectivitat i Internet

Tipologia de connexió ADSL.

ADSL ***(Asimètric Digital Suscriber Line) És un mètode de transmissió de dades a través dels fils telefònics. Utilitza la línia telefònica bàsica però permet que les dades es transmetin de forma asimètrica amb la qual cosa s'aprofita millor l'ample de banda disponible. Quan estem connectats a Internet la major part de les dades viatgen en sentit Internet - Usuari, mentre que algunes dades viatgen en sentit Usuari - Internet. És a dir, quan fem una petició per a veure una pàgina enviem poques dades, només l'adreça de la pàgina, mentre que al rebre aquesta pàgina rebem moltes més dades com: imatges, text, etc. Un avantatge d'aquesta tecnologia és que la connexió és permanent, 24 h. al dia, no necessitem marcar cada vegada el nombre de telèfon per a connectar-nos. A més a més podem parlar per telèfon i estar connectats a Internet alhora. Amb aquest tipus de connexió s'aconsegueixen velocitats des de 256 Kbps fins a 2 Mbps en sentit Internet-Usuari, segons la modalitat que es contracti.***

ISP.

En anglès significa Internet Service Provider (Proveïdor d'Accés a Internet). Un ISP és una empresa que disposa d'una xarxa, la qual està connectada a Internet mitjançant línies dedicades d'alta velocitat. Aquestes empreses ofereixen el servei d'accés a Internet a altres empreses o individus, qui per un càrrec (mensual, anual, semestral) es troben habilitats per a connectar-se a Internet via mòdem i amb això tenir accés a una sèrie d'aplicacions com: World Wide Web, correu electrònic per a enviar i rebre e-mails, mantenir un lloc web, xat, newsgroups, etc.

Configuració de la xarxa

NOTA: Abans de tocar res de la configuració hem d'apuntar sense equivocar-nos ens numerets del DNS i de la Pasarel·la ja que si posem malament aquests números l'ordinador no es podrà connectar a internet.

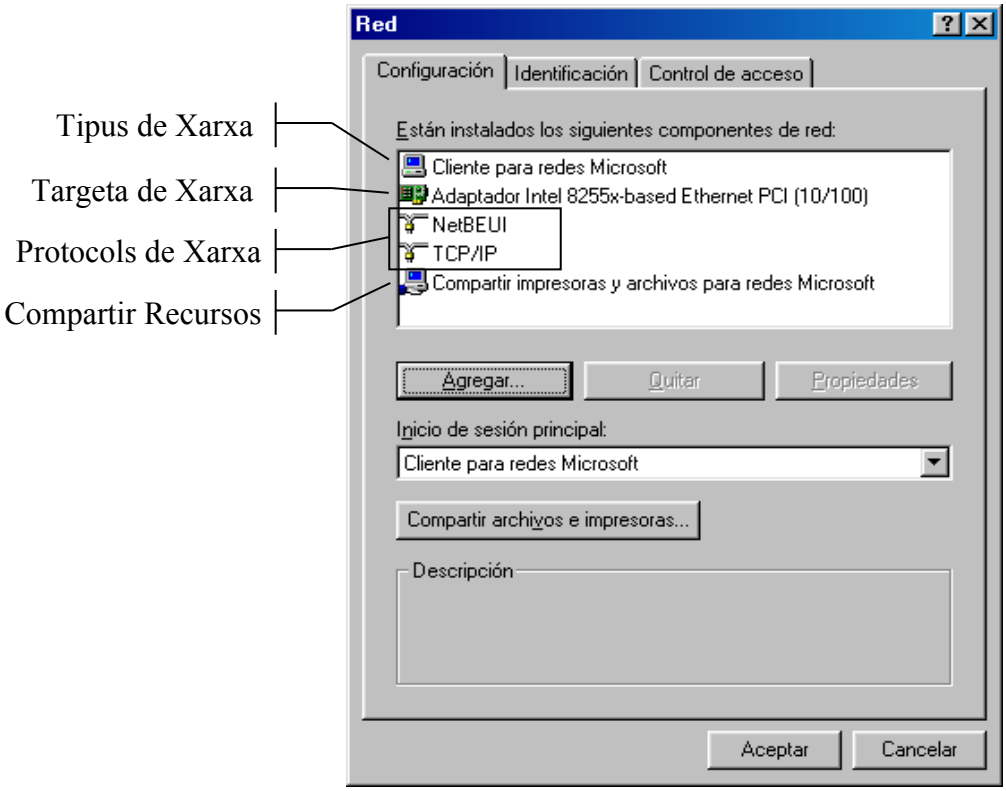
Per localitzar aquests números podeu utilitzar el programa WINIPCFG que s'explica més endavant.

Per configurar o canviar algun paràmetre de la xarxa, es necessari entrar al Panel de Control de Xarxa.

El podem trobar de dues maneres:

3. Entrant al Panel de Control INICI -> CONFIGURACIÓ -> PANEL DE CONTROL i fent doble clic sobre la icona Xarxa.
4. Fent clic amb el botó secundari sobre la icona de Veïnatge de la Xarxa a l'escriptori y fent clic a propietats.

Quan s'obre la configuració de Xarxa el primer que ens surt es la part de configuració dels dispositius i dels protocols.



En aquesta primera pantalla es on nosaltres configurarem els PROTOCOLS de comunicació y de compartiment de recursos.

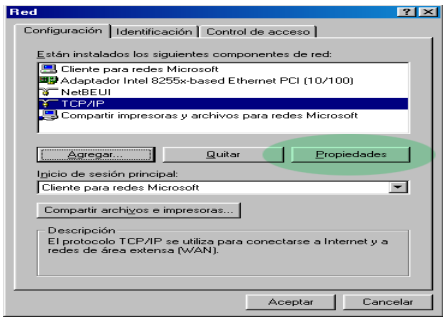
Un protocol de xarxa es un llenguatge que utilitzen els ordinadors per comunicar-se i poder enviar-se informació entre ells.

Un ordinador pot tenir més d'un protocol instal·lat. Això s'utilitza quan tenim una xarxa amb diferents sistemes operatius o com a mesura de seguretat en el cas que caigui un protocol, tenim l'altre com recolzament.

El fet de tenir més d'un protocol al nostre sistema no afecta gaire al rendiment de la xarxa. El sistema operatiu quan detecta més d'un protocol ens demana quin d'ells serà el predeterminat i es el que utilitzarà sempre. Si aquest no rep resposta al enviar alguna senyal per la xarxa, utilitzarà el següent.

Cada protocol te una raó de ser. Llavors quin es el millor protocol per la meva xarxa? Depèn de les necessitats de la meva xarxa. En el nostre cas el que millor s'adapta a les necessitats de l'Òmnia es el TCP/IP ja que ens permet compartir recursos a la xarxa i connectar-nos a Internet.

Anem a veure com s'ha de configurar la xarxa per que funcioni correctament.

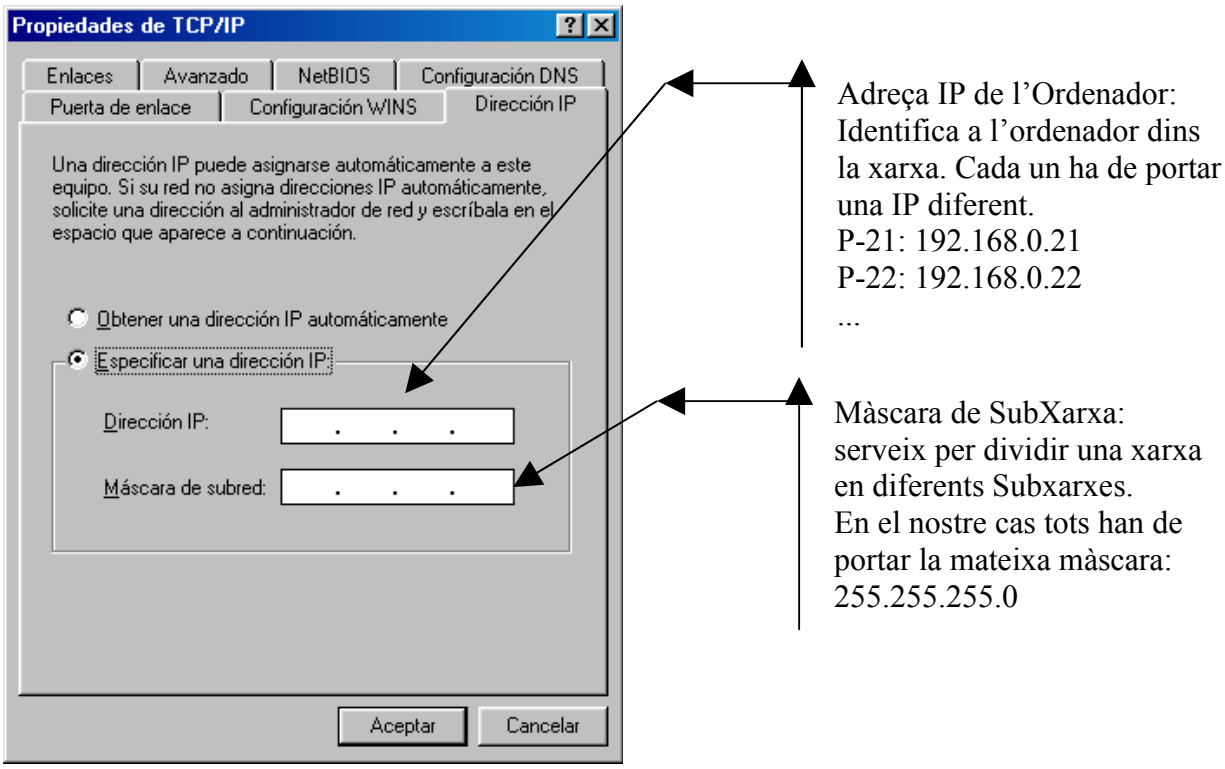


Configuració del TCP/IP

Una vegada tenim obert el diàleg de configuració de la Xarxa, fem clic sobre TCP/IP i seguidament sobre el botó propietats.

En aquesta primera pantalla anomenada Adreça IP es on posarem l'adreça de l'ordinador amb la qual s'identificarà dins la xarxa.

CADA ORDINADOR HA DE TENIR LA SEVA PROPIA ADREÇA. SI PER ERROR POSEM LA MATEIXA ADREÇA A DOS ORDINADORS AQUESTS NO FUNCIONARÀN EN XARXA I DONARÀN ERRORS.



Anem a comentar una mica aquesta pantalla:

Adreça IP: Es un número composat per quatre series que van des del 000 (00h) fins al 255 (FFh) i separats per un punt. Aquests números juntament amb uns altres que porten les targetes de xarxa formen l'adreça que identificarà l'ordinador dins la xarxa.
Com nosaltres estem configurant una xarxa interna o LAN tenim una sèrie d'adreces que podem utilitzar. Aquesta sèrie va des del 192.168.0.0 fins al 192.168.255.255
Si feu uns petits càlculs veureu que es poden connectar uns quants milers d'ordinador a la xarxa.
Cada ordinador ha de tenir la seva pròpia IP i ha de ser diferent dels altres ordinadors.

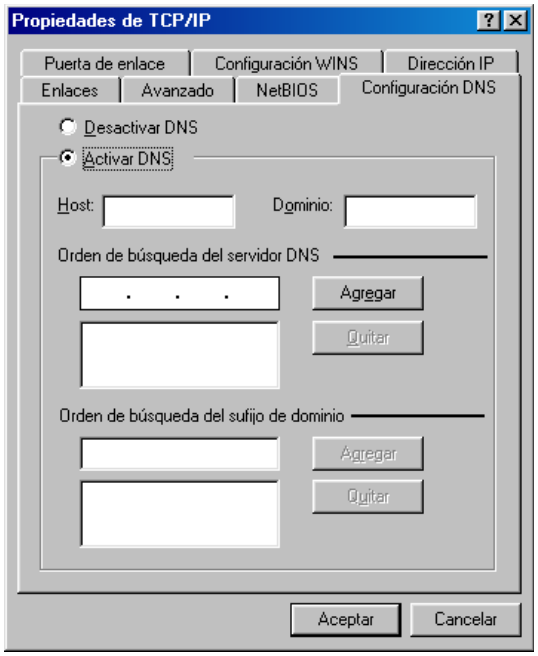
Per exemple:
Ordinador 1: 192.168.0.21
Ordinador 2: 192.168.0.22
.
.
.
Ordinador 9: 192.168.0.29

Màscara de SubXarxa: Aquesta màscara el que fa es separar una xarxa en diferents subxarxes. Per fer això es fa una multiplicació lògica entre la adreça IP i la màscara de subxarxa. D'aquesta manera un ordinador amb la màscara 255.255.255.0 no podria trobar a un altre amb la màscara 255.255.0.0

En el nostre cas utilitzarem en TOTS els ordinadors la màscara 255.255.255.0

Si volem que els ordinadors es connectin a Internet hem de configurar també els DNS. Aquests números DNS son les adreces IP del nostre servidor d'Internet, per tant si no les posem be l'ordinador no es connectarà a Internet.
Llavors fem clic, sense tancar res, sobre la etiqueta Configuració DNS.

NOTA: No tots els punts tenen les mateixes adreces DNS, per tant abans de fer res apunta-les en un lloc segur o pregunta al TEB quines son les teves DNS's.
L'ordre de les DNS també es important. Si poseu la segona DNS en lloc de la primera tampoc funcionarà el tema.

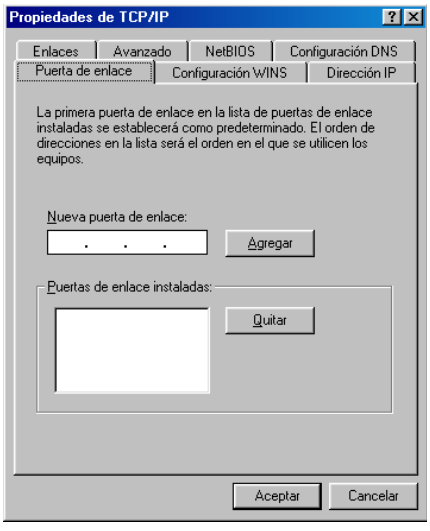


En aquesta pantalleta el més important son les adreces DNS. Las hem de col·locar en el mateix ordre que ens les van donar allà on posa "ordre de cerca del servidor DNS". Quan posem la primera hem de fer clic sobre el botó Afegir. Seguidament posem la segona i tornem a fer clic sobre Afegir (agregar). Les adreces han d'aparèixer en un llistat a sota d'on posem les adreces. Si ens equivoquem en alguna adreça o la hem de canviar per algun motiu, la seleccionem de la llista i fem clic sobre esborrar (quitar).

En quant on posa HOST i DOMINI, hem d'omplir-los amb alguna cosa ja que si no posem res no ens deixarà sortir.

Podeu posar:
HOST: P-21
DOMINI: xtec.es
O poseu el que vulgueu.
A més a més de les DNS, un altre dada important a configurar es la Passarel·la (GateWay).
Les passarel·les son programes o dispositius que connecten dues xarxes diferents, fa una funció de "pont" entre les xarxes.
Nosaltres l'utilitzem per connectar-nos a Internet, i la nostra passarel·la es el ROUTER ADSL. Per accedir a la passarel·la hem de fer clic sobre la pestanya que te aquest nom i ficar el número que correspongui.

Heu de posar el 4 números de la passarel·la i fer clic al botó Afegir.



NOTA: No tots els punts tenen la mateixa Passarel·la, per tant abans de fer res apúntate-la en un lloc segur.

Un cop fet tot això li doneu al botó d'acord i tornarem al diàleg de configuració de la xarxa.

Ara ens queda configurar el **nom** de l'ordinador i el **grup de treball**.

El **nom** de l'ordinador serveix per identificar de una forma més entenedora per nosaltres a l'ordinador dins la Xarxa. Es més fàcil identificar un ordinador per MANTENIMENT-1 que no per 192.168.23.45, per exemple. Aquest nom ha de ser únic en TOTA la xarxa, ja que com les IP's, no pot poden existir dos ordinadors diferents amb el mateix nom.

El grup de treball serveix per identificar un grup determinat d'ordinadors dins la mateixa xarxa de una forma més ràpida.

Per exemple: Si tinguéssim 20 ordinador dels quals 4 son base de dades, 4 s'utilitzen per disseny gràfic i 2 per fer pàgines WEB, el més coherent seria agrupar el 4 ordinador de base de dades en un grup anomenat **DADES**, els altres 4 en un altre anomenat **DISSENY-GRAF** i els que queden en **WEB.** D'aquesta manera, al obrir el Veïnatge de la Xarxa el primer que veuríem serien els ordinadors del nostre mateix Grup de Treball. Si volguéssim trobar un ordinador d'un altre grup, obriríem, l'element TOTA LA XARXA i ens sortirien tots els altres grups de treball.

Per configurar això obrirem el diàleg de configuració de Xarxa i seleccionarem l'element **Identificació.**

Dins aquest element ens trobem amb 3 quadres a omplir. Els 2 primers son obligatoris, el tercer es opcional.

El primer serveix per posar el Nom de l'ordinador (P-21, P-22... P-29) Recordeu que han de ser diferents.

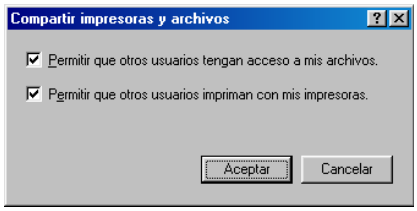
On posa Grup de Treball, el més còmode es posar tots els ordinadors en el mateix grup de treball així quan obrim el Veïnatge de la xarxa ens sortiran tots els ordinador a l'hora.

Posarem el que ens doni la gana, però ha de ser el mateix a tots els ordinadors.

I en la descripció podem posar la funció que farà l'ordinador, que l'utilitza normalment... no influeix en el funcionament de la xarxa.

Si volguéssim que a l'ordinador es puguin intercanviar arxius o que es pugui imprimir a les seves impressores hem d'activar el protocol de **Compartir arxius i Impressores.**

Per fer això obrim el diàleg de configuració de xarxa a la secció de configuració, hi ha un botó que posa **Compartir arxius i Impressores.** El polsem i activem TOTES les caselles que ens surtin. Donem a D'Acord a totes les finestres, el sistema es reinicia i l'ordinador ja està preparat per compartir recursos.



i,

Si hem fet tot be, al reiniciar les màquines, al obrir el Veïnatge s'haurien de veure TOTS els ordinadors.

Si no es veuen tots, ens esperem uns segons i actualitzem la pantalla. A vegades triga una mica que un ordinador reconegui a tots els altres. Por passar que en un ordinador es vegin a tots i en un altre es vegin la meitat.

Si passat un temps no es veu l'ordinador es que alguna cosa no hem fet be o que no funciona.

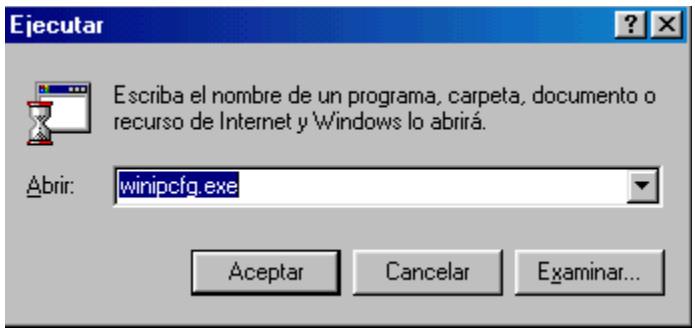
Què és el Winipcfg?

Aquest programa et servirà per saber la configuració de la teva xarxa interna, com per exemple saber la ip del ordinador, la màscara de xarxa, la porta d'enllaç...

Execució del Winipcfg.

1. Anem fins el botó d'**Inici** de Windows .S'obrirà la finestra del menú de Windows i cliquem a sobre d'Executar,

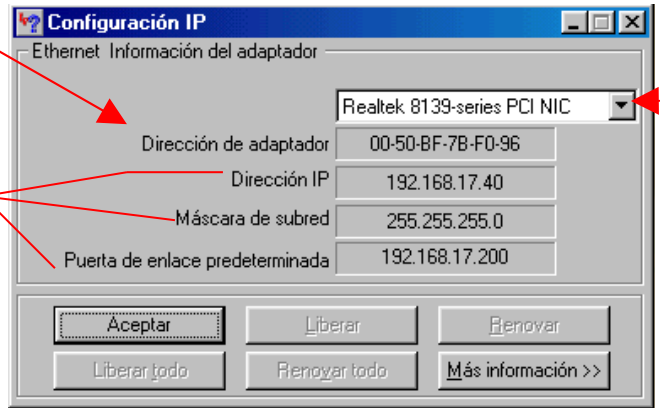
2. S'obrirà una nova finestra on haureu de posar el nom del programa amb l'extensió exe. (winipcfg.exe)



3. El Winipcfg és el programa que ens mostra l'estat de configuració del protocol tcp/ip. Amb la següent finestra ja en tindrem prou per saber la configuració de l'ordinador.

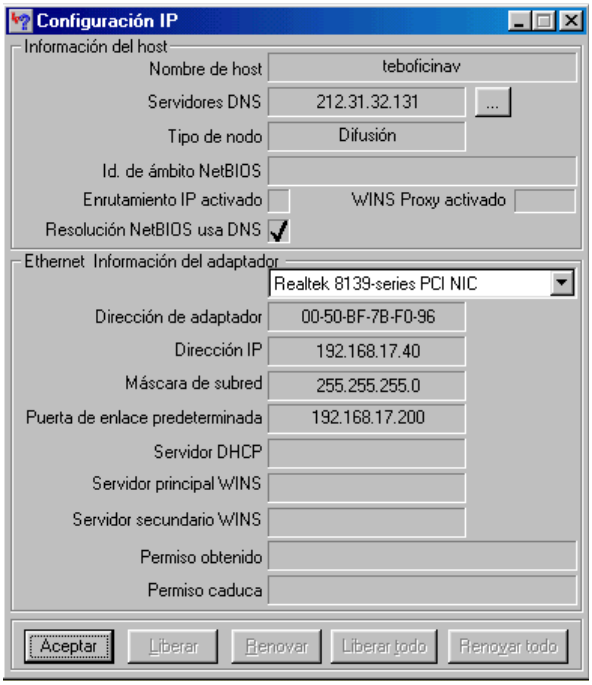
Direcció MAC de la Tarja de Xarxa (Vindria a ser com el Nº de sèrie de la tarja)

Aquests 3 apartats mostren la configuració que té en aquests moments la tarja de xarxa.



Model de Tarja de xarxa

4. Si fem clic al botó "Més informació" anirem a la següent finestra, amb més informació sobre el TCP/IP.



Taxonomia d'errors i possibles solucions

Com és el Router ADSL?

Aquests són els Router ADSL que normalment trobem als nostres centres Òmnia. A continuació citarem alguns del possibles errors que et pots trobar.

1. **No tens connexió a Internet?**
   Comprova que tinguis el Router encès.
   Comprova que el LED DSL es troba de color verd. Si en cas contrari fa pampallugues i canvia de color verd a vermell això vol dir que no troba la connexió a Internet.
   Si no troba la connexió a Internet pot ser per diverses raons.
   1.1- El cable del telèfon està ben connectat del router a la línia telefònica?.

1.2- El cable Rj-45 (cable de xarxa) està ben connectat del router al hub o al ordinador?

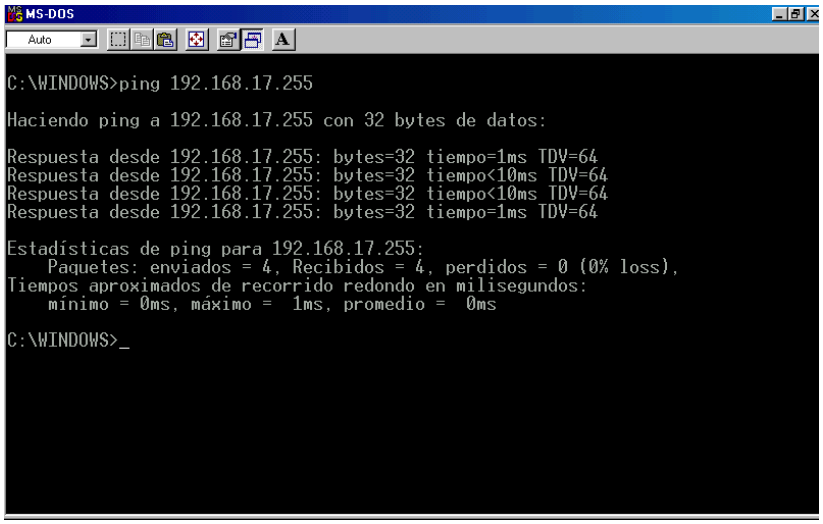
1.3- Si els 4 LEDS es troben en color verd però sense fer cap moviment desconnecta el router de la llum i torna a connectar-lo i espera fins que el led vermell es posi de color verd.

2. Si després de totes aquestes comprovacions continua sense funcionar Internet i has comprovat que no funciona Internet a cap dels ordinadors de tota la sala Òmnia i que tampoc té connexió el servidor posa't en contacte amb el tècnic.

Si tens connexió a Internet a tots els ordinadors excepte a un ordinador aleshores és un problema de la xarxa d'Internet. Fes les següents comprovacions.

Per saber si l'ordinador té connexió a la xarxa fes el següents passos:

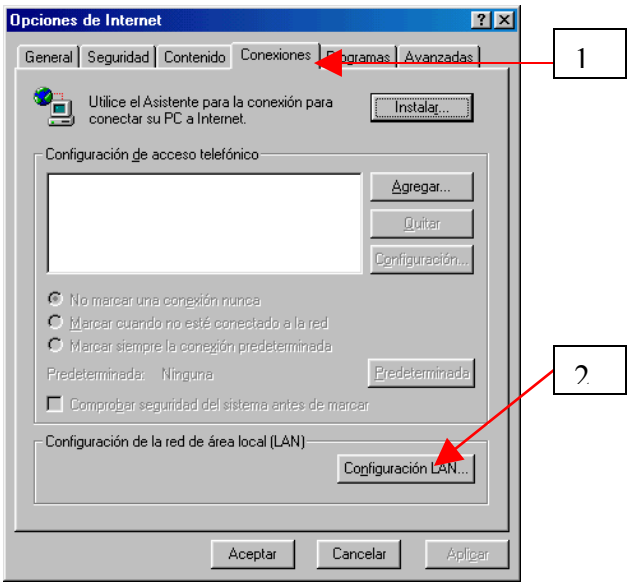
3.1- Ves a Inici-> Programes ->
3.2- Fes: ping [nom-servidor]
"Nom-servidor" és el nom del servidor de la sala Òmnia que heu escollit per a que us respongui. Si l'ordinador té ben configurada la tarja de xarxa hauria d'aparèixer el següent missatge., "Respuesta desde [nom-servidor] bytes 32 tiempo=X TDV = X"



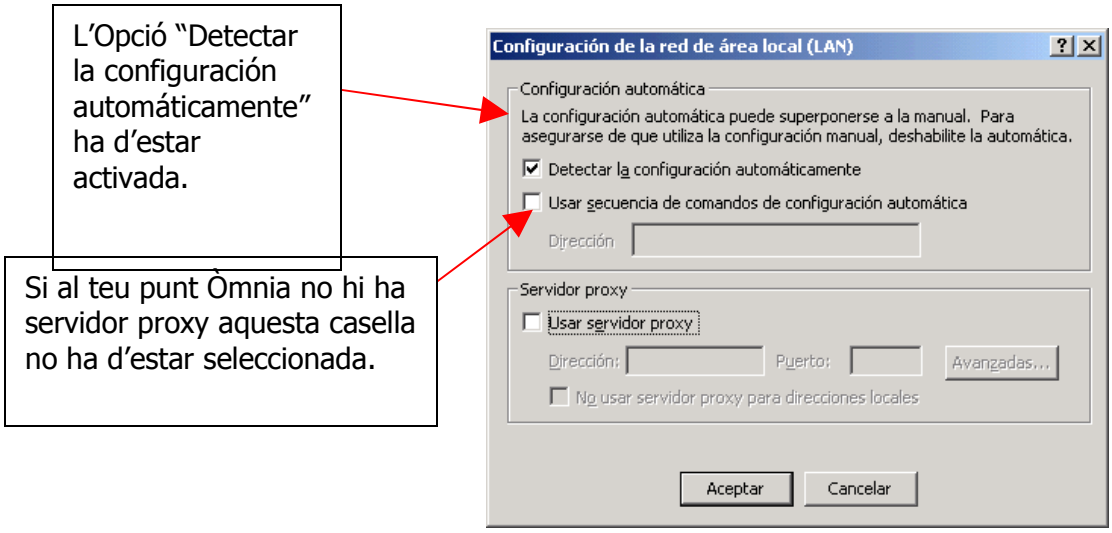
3.3- Si la connexió d'Internet encara no funciona però tens accés a la xarxa Internet aleshores haurem de mirar la configuració del Internet Explorer.

3.3.1- Obrim L'Internet Explorer.
3.3.2- Anem a l'opció "Herramientas" i després a "Opciones de Internet".

3.3.3- S'obrirà la finestra d'opcions del Internet Explorer. Hem d'anar a la pestanya "Conexiones" i després farem clic a "Configuración LAN..."



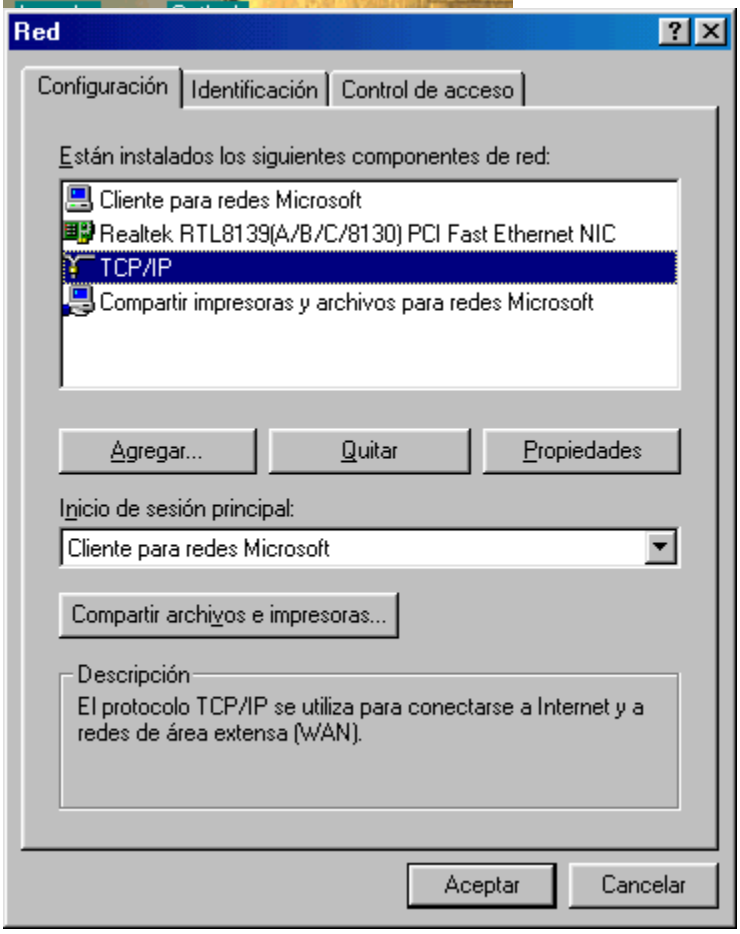
3.3.4- Si en el teu punt Òmnia, no feu servir un Ordinador com a proxy per a la connexió a Internet t'haurà de sortir una finestra com la següent.

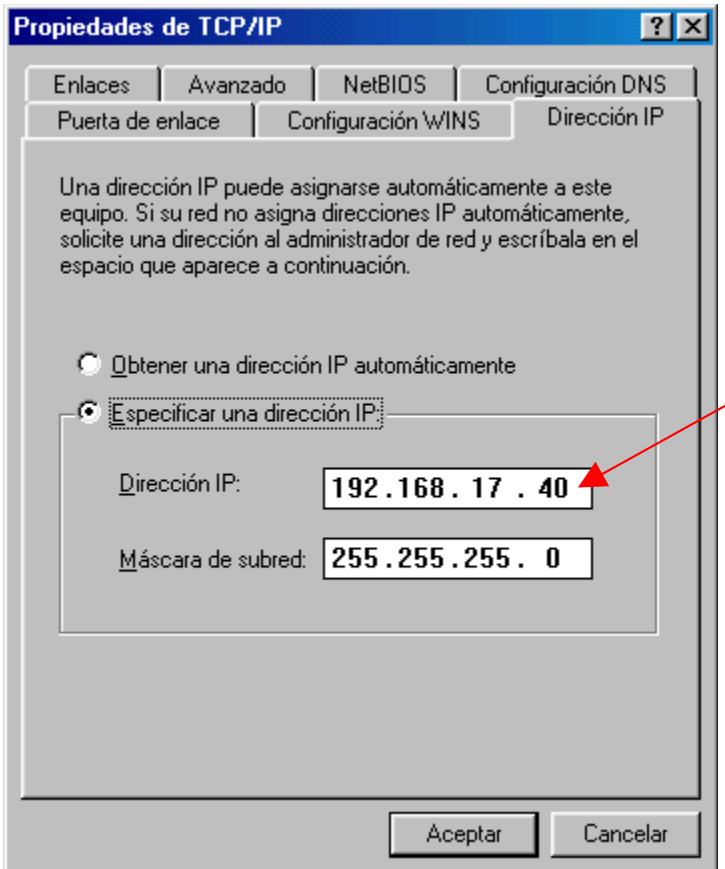


3.4- Quan fem la comanda PING a la finestra MS-Dos i surt el següent missatge d'error "Esgotat el temps per a la petició", en aquest cas el PC no té ben configurada la connexió TCP/IP.

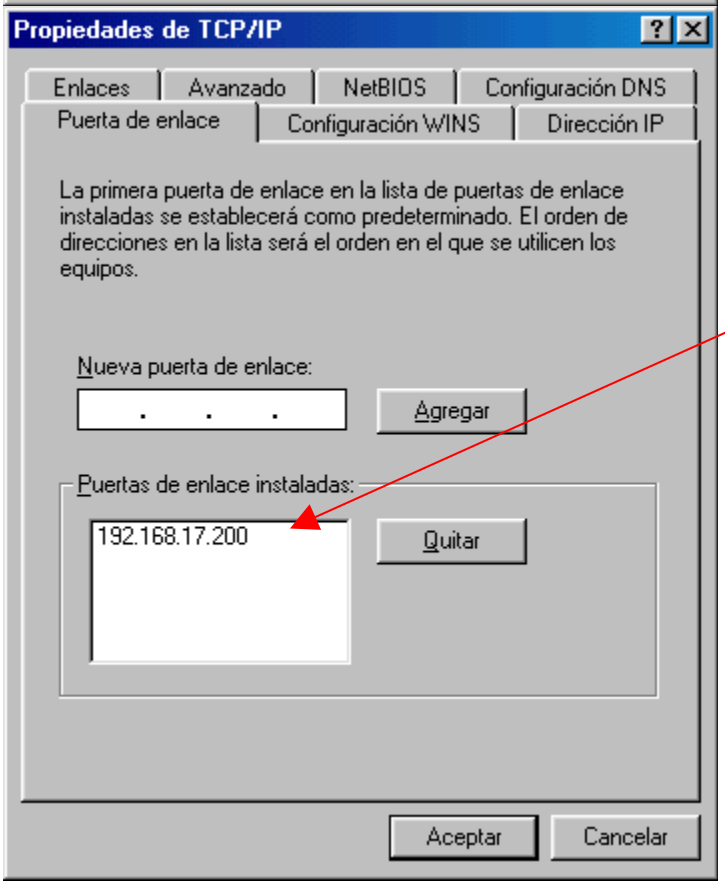
3.4.1- Configuració del protocol TCP/IP. Per poder configurar el protocol tcp/ip s'han de seguir els següents passos.

Cliquem aquí.

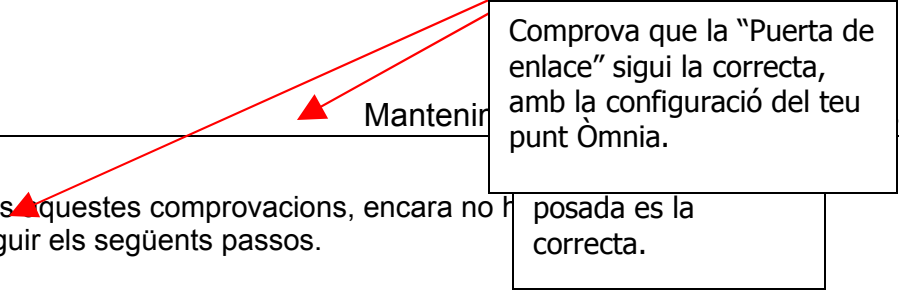




Aquí tindràs que posar la teva configuració del teu punt Òmnia, O mirar si la que hi ha posada es la correcta.



Comprova que la "Puerta de enlace" sigui la correcta, amb la configuració del teu punt Òmnia.



Si després de fer totes aquestes comprovacions, encara no h
problema. Has de seguir els següents passos.

Incidència a nivell de hardware:

Contactar amb en Xavier Pastor i passar còpia al coordinador o coordinadora (per a portar a terme el seguiment de la incidència):

Direcció General de Serveis Comunitaris (DGSC)tel. 93.228.71.00 607074008

Xavier Pastor (xavipastor@ctv.es)

* La manera més senzilla és enviar-li un mail.

Dades que es requereixen per passar incidència:

- Nº de sèrie de la màquina que requereix la reparació.
- descripció de la incidència.
- Persona de contacte.
- Horari de contacte.
- Telèfon de contacte.
- Adreça del Punt

Important:

- Després de tramitar la incidència si passen 3 dies, sense resposta torneu a reclamar.

Una vegada solucionada la incidència, cal notificar al Xavier Pastor la reparació de l'avaria

Incidència connexió a Internet:
Si el router no es pot connectar a Internet has de trucar a Telefònica i alhora enviar la incidència a Xavier Pastor.

Telèfon de Telefònica: 902 357 000 ADSL
Assistència tècnica de telefònica ADSL: 900 502 010
Assistència tècnica RDSI : 900 111 002

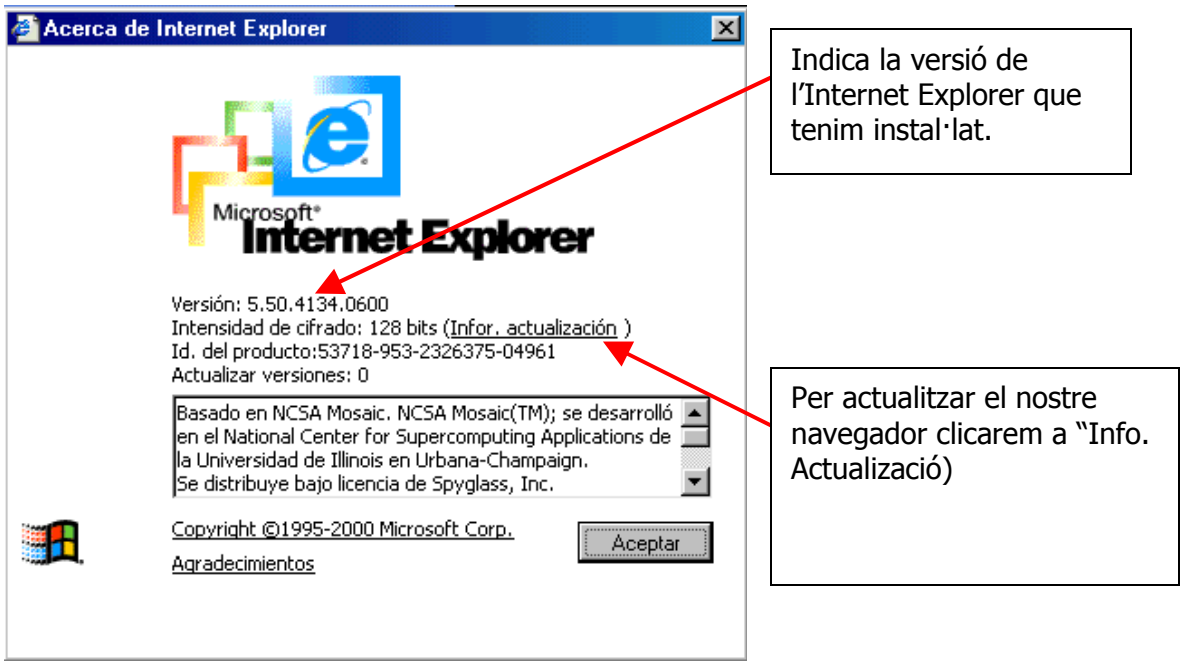
Recorda que quan truquis has de tenir a mà el telèfon de la teva ADSL.

Actualització Navegador

Per saber quina versió del explorador tenim instal·lat al nostre ordinador farem els següents passos:

1. Obrim l'Internet Explorer.
2. Cliquem sobre la finestra d'Ajuda.

3. Anem fins a l'opció " Acerca de Internet Explorer", i cliquem.
4. Des d'aquesta mateixa secció podrem actualitzar el nostre navegador.

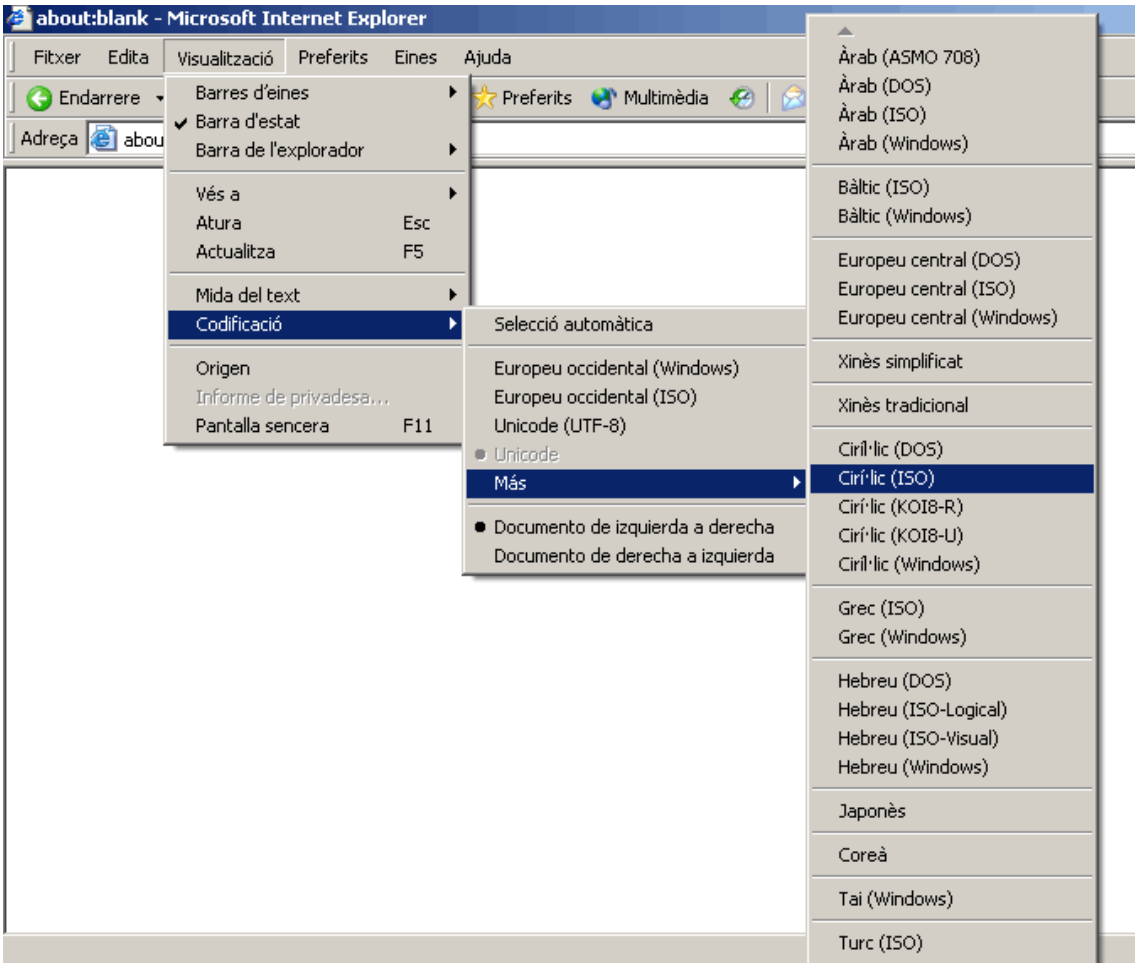


5. S'obrirà una nova plana on podràs escollir l'actualització que prefereixis.

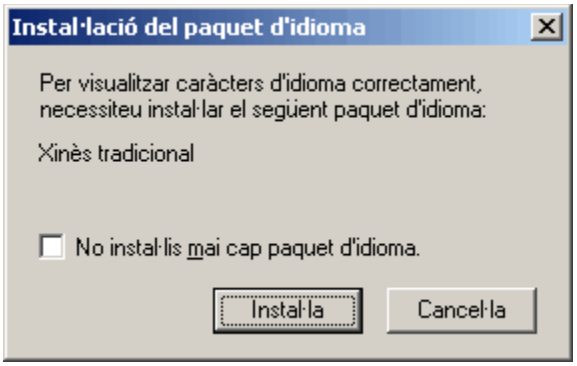
Intèrpret de multillenguatge.

En aquest apartat explicarem com canviar l'idioma del navegador.
Això ens serà útil quan algun usuari o nosaltres mateixos vulguem veure pàgines en un altra idioma (xinès, àrab...)

1.



Quan visitem una pàgina en un altre idioma, pot ser que ens surti la següent finestra.



Quan fem una instal·lació d'un idioma és possible que ens demani el CD del Windows o bé que ens indiqui que està buscant a la carpeta : **c:\Windows\precopy**

Protocols Http, ftp, Gestors ftp.

HTTP (Protocol de transferència d'hipertext)
El mètode mitjançant el qual els documents es transfereixen de l'ordinador del sistema principal o del servidor als exploradors i usuaris individuals.

FTP

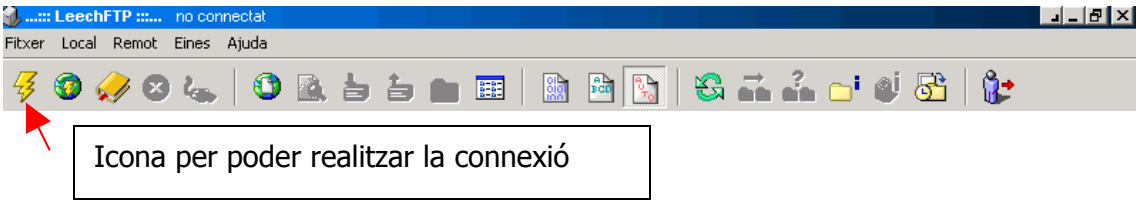
Acrònim de "File Transfer Protocol" (Protocol de transferència d'arxius), un mètode molt usat per a transferir arxius d'un ordinador a un altre remot a través d'Internet. FTP és un mode especial d'entrar en un altre servidor de web a Internet, per enviar o transferir arxius. Mitjançant FTP es poden obtenir no només arxius, sinó també moltes aplicacions, entrant als servidors en què aquestes es troben disponibles, usant el nom de compte anònim (ing.: anonymous). Aquests servidors s'anomenen "servidors FTP anònims". FYI Veure "For Your Information".

Gestors ftp

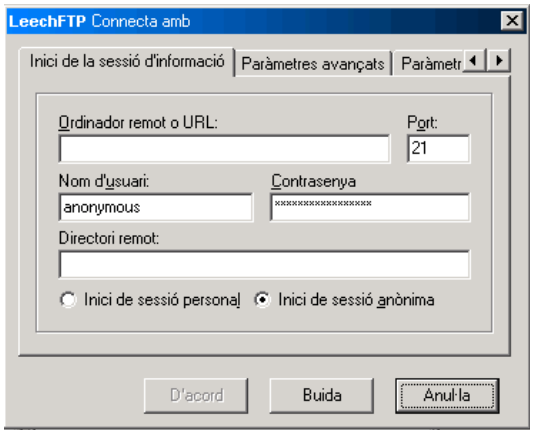
És el programa utilitzat per la transferència de fitxers amb el protocol de transferència d'arxius ftp.

Un bon gestor ftp és el "Leech ftp". Gràcies aquest programa podrem accedir al servidor ftp.

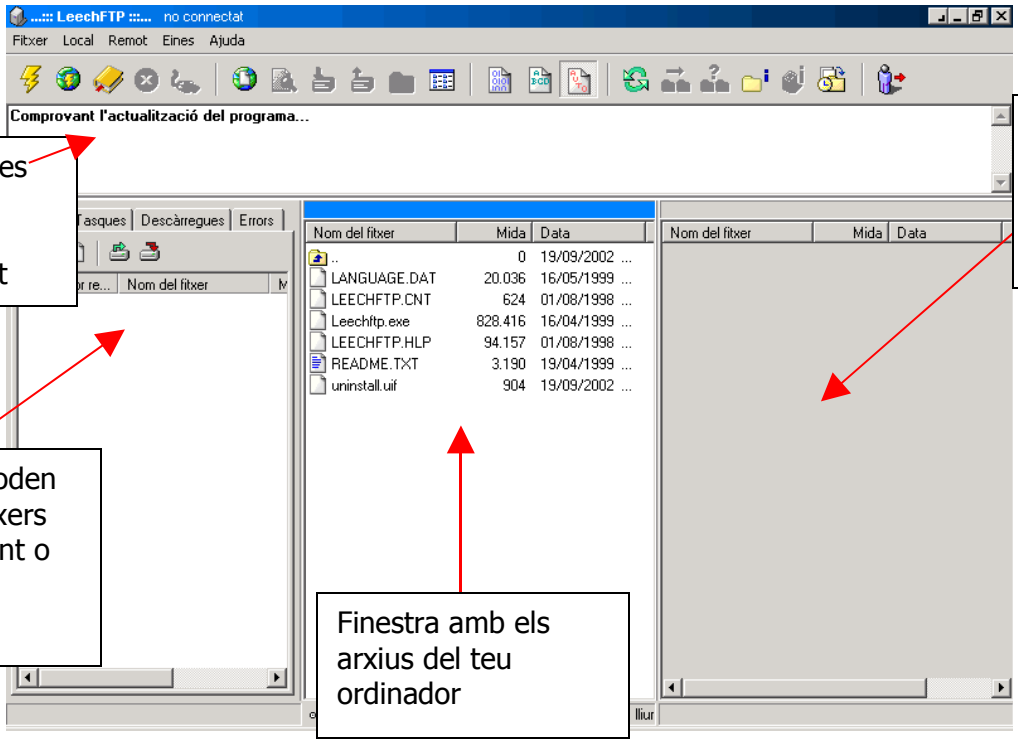
1. ***Per realitzar la connexió amb l'ordinador remot feu clic a la primera icona***



2. ***Omplir el camps requerits.***



3. **Explicació de les finestres del LeechFTP**



Visualització de les comandes de conexió amb l'ordinador remot

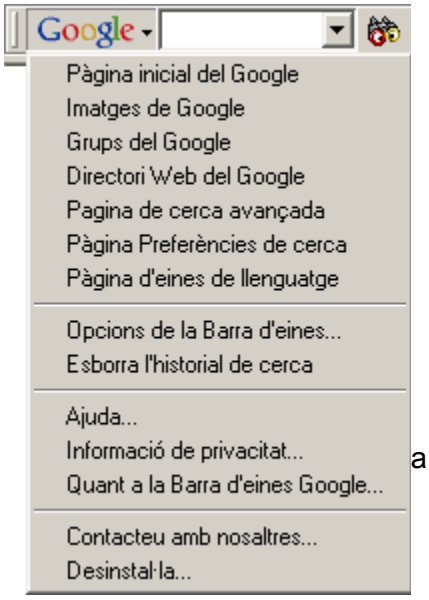
Finestra dels arxius de l' ordinador remot.

Finestra on es poden visualitzar els fitxers que s'estan rebent o enviant.

Finestra amb els arxius del teu ordinador

Integració de buscadors al navegador

La nova Barra d'Eines de Google incrementa les possibilitats de trobar informació des d'arreu d'Internet i només triga uns segons en instal·lar-se. Quan la Barra d'Eines de Google s'ha instal·lat, automàticament apareix amb les barres d'eines d'Internet Explorer. Això vol dir que fàcil i ràpidament pots utilitzar Google per buscar, des de qualsevol pàgina que estiguis visitant, sense tornar a la plana de Google per començar una altra cerca.



La Barra d'Eines de Google està disponible gratuïtament i inclou aquestes característiques:

- **Cerca amb Google:** Accedeix a la tecnologia de recerca de Google des de qualsevol pàgina.
- **Busca dins el lloc:** Cerca només les pàgines dins del lloc que estàs visitant.
- **PageRank:** Mira el lloc de la pàgina en el rànquing de Google.
- **Informació de la pàgina:** Accedeix a més informació sobre la pàgina incloent-hi pàgines similars, pàgines que hi enllacen i captures de pantalla emmagatzemades.
- **Destacament:** Destaca els termes de recerca que has introduït quan apareixen en aquesta pàgina, cada paraula en un color.
- **Recerca de mots:** Troba els termes de recerca que has introduït dins d'aquesta pàgina.

Pots usar la pàgina d'opcions de la Barra d'eines Google per personalitzar-ne el format, per incloure funcions com per exemple el botó "Avui tinc sort!", així com els botons de cerca de Grups Google i els d'Imatges.

Però pots trobar diferents “Toolbars” d’altres buscadors com per exemple:

- Terra. (http://barradenavegacion.terra.es/)
- Eresmas (http://www.eresmas.com/minieresmas/)
- Yahoo (http://es.companion.yahoo.com/)
- Google (http://toolbar.google.com/intl/ca/install)

Messenger.

Com ja molts de vosaltres sabeu el Messenger és una utilitat que ofereix MSN, al crear-se un compte de Hotmail o un Passport.

El Messenger com tants altres programes no està lliure de la possibilitat de que t'entrin virus. Una de les entrades més habituals és mitjançant la recepció de fitxers. Sempre que ens enviïn un fitxer, hem de estar ben segurs de que no és un virus.

Com es pot saber que és un virus o que conté virus.

1.- Quan t'enviïn un fitxer .exe, .zip . rar .ace, l'acceptes però abans d'executar-lo, passa'l per l'antivirus.

2.- Quan t'enviïn un fitxer .pif . bat .cpl no l'acceptis, el 90% de les vegades és un virus.

3.- Quan t'envien un fitxer amb doble extensió "p.ejem: foto.pif.jpg." això vol dir que es un virus, només veure aquest tipus de ruta no accepteu l'arxiu.

Correu electrònic

Gràcies al correu electrònic, podem comunicar-nos amb una altra persona a qualsevol part del món en uns minuts. Fins i tot podem enviar-li fotos, so i fitxers amb una gran quantitat de dades, tot això d'una forma fàcil i ràpida. Per la seva eficàcia, el correu electrònic o e-mail és el servei més utilitzat d'Internet juntament amb la Web.
Hi ha diversos tipus de comptes POP3 i SMTP, les POP3 són les més usats. El correu per Internet, igual que el correu normal, ha de ser privat, per això tots els programes per a llegir el correu disposen de protecció mitjançant una contrasenya. Tot i que això no assegura que algú pugui interceptar el correu mentre viatja a través de la xarxa.

El correu electrònic o e-mail és una forma d'enviar missatges entre ordinadors connectats a través d'Internet. Com la majoria dels serveis d'Internet el correu es basa en l'arquitectura client/servidor. Els clients són els ordinadors de la sala Òmnia que utilitzen el correu i el servidor és l'ordinador que gestiona el correu, el servidor pertany a l'entitat proveïdora del correu. Quan algú envia un correu, primer arriba al servidor de correu i aquest ho envia al servidor del destinatari. Quan el destinatari es connecti la servidor, aquest li enviarà tots els seus missatges pendents. Per això, no és necessari que el destinatari estigui connectat a Internet en el moment en què se li envia un missatge.

Podem configurar el nostre correu perquè cada vegada que s'arrenqui llegeixi els missatges pendents o bé que només els llegeixi quan premem el botó "Rebre". Cada vegada que es llegeix un missatge, s'esborra de la bústia del servidor i passa a l'ordinador del client. La bústia té una grandària fixa, per tant si s'acumulen molts missatges en el servidor i el client no els llegeix, la seva bústia pot bloquejar-se. Tot i que abans el servidor acostuma a enviar un missatge d'avís per tal que la buidem. Quan ens diuen que un compte de correu és de, per exemple, 2 Mb. es refereixen a l'espai de què disposem a la bústia del servidor.
Els clients disposen d'un programa – client de correu, per exemple, l'Outlook Express o bé tenen l'opció de poder visitar el correu via web.

El servidor és un ordinador que té un programa servidor de correu que pot atendre milers de comptes de correu. Normalment el servidor de correu resideix en una màquina diferent al servidor de pàgines web, per això pot ser que en un moment donat no funcioni el servidor web però sí el servidor de correu o viceversa.
Un correu consta de diversos elements: l'adreça de correu del destinatari, el text del missatge i potser algunes coses més com fitxers adjunts, etc.
Una adreça de correu té una estructura fixa: nom_compte@nom_servidor, per exemple: pepito_grillo69@xarxa-omnia.org

Cada adreça de correu és única per tot el món, no poden existir dues adreces de correu iguals.
Podem crear comptes a llocs web que els ofereixen gratuïtament com Hotmail, hispavista, yahoo, ravalnet.org, cataloniamail.com, etc. Hi ha tres formes bàsiques d'utilitzar el correu, a través d'un programa de correu, mitjançant webmail i la missatgeria instantània.

- Programes de correu.

Per exemple, l'Outlook Express de Microsoft, el Messenger de Netscape o Eudora són programes específics per a treballar amb el correu i que hem d'instal·lar al nostre Pc. La primera vegada que s'utilitzen cal configurar-los amb les dades del compte i

servidor de correu. Per tant només és pràctic utilitzar-los a l'ordinador de casa i del treball.

Explicació protocols.

SMTP:

El significat de les sigles de SMTP, és Protocol Simple de Transmissió de Correu (Simple Mail Transfer Protocol). Aquest protocol és l'estàndard d'Internet per a l'intercanvi de correu electrònic. SMTP necessita que el sistema de transmissió posi a la seva disposició un canal de comunicació fiable i amb lliurament ordenat de paquets, amb la qual cosa l'ús del protocol TCP en la capa de transport, és l'adequat. Perquè dos sistemes intercanviïn correu mitjançant el protocol SMTP, no és necessari que existeixi una connexió interactiva, ja que aquest protocol usa mètodes d'emmagatzematge i reenviament de missatges.

POP:

El significat de les sigles POP és Protocol d'Oficina de Correus (Post Office Protocol). El protocol SMTP, va aparèixer quan la xarxa Internet no estava en auge. El protocol SMTP va sorgir quan els usuaris tenien comptes a ordinadors que estaven contínuament connectats a Internet, de tal forma que quan un usuari volia llegir el seu correu, entrava en una sessió de terminal i sol·licitava al servidor el missatge que tenia emmagatzemat per a ell. Aquesta situació ha canviat considerablement, avui en dia, els usuaris es connecten a la màquina servidora de correu per un període de temps molt breu, el necessari per a sol·licitar l'enviament del correu mitjançant un programa client. Per tant, el servidor de correu electrònic ha de mantenir emmagatzemat el correu en les seves caselles i enviar-lo als clients quan es connectin i ho sol·licitin. Aquest és l'objectiu pel qual es va crear el protocol POP.

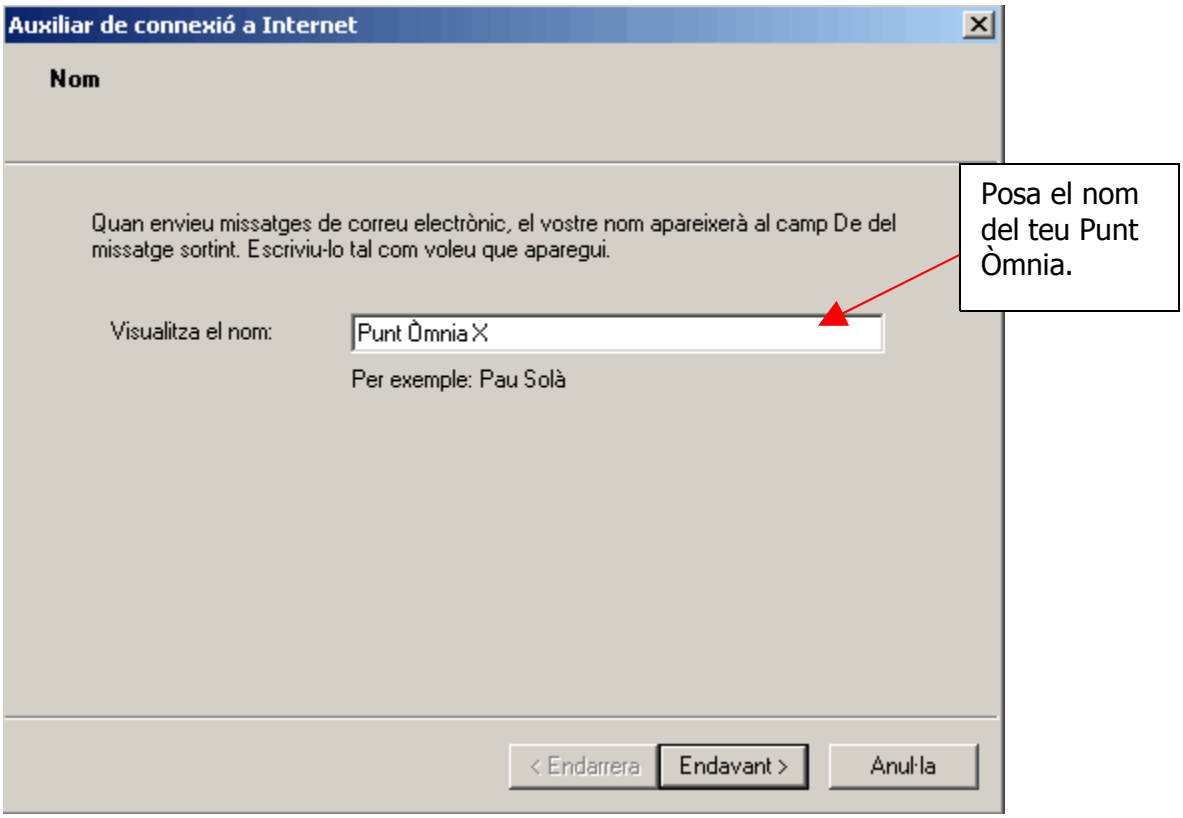
Actualment, s'utilitza el protocol SMTP per a l'enviament de correu i per a la recepció de correu s'utilitza el protocol POP, el qual, ja està en la seva tercera versió des de la seva aparició (POP3), la qual no posseeix grans novetats respecte a l'original, ja que bàsicament, segueix permetent la descàrrega dels missatges arribats a la casella de l'usuari.

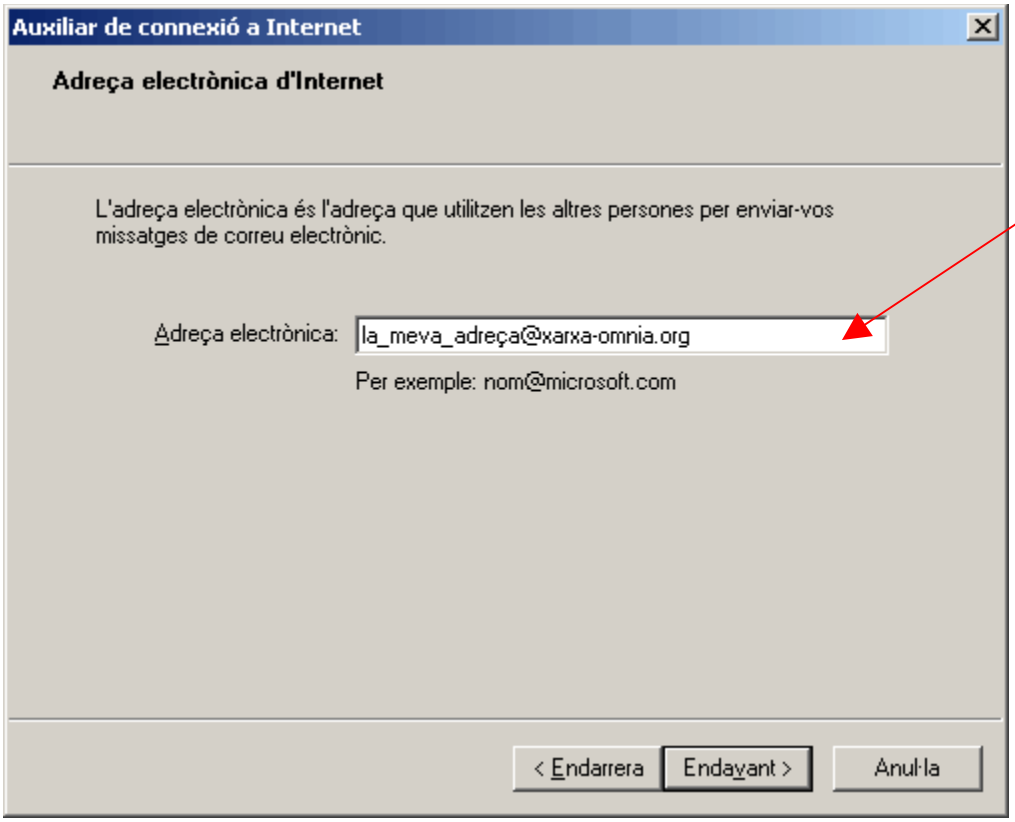
Configuració del Outlook Express.

Per defecte, als ordinadors d'Òmnia no hi ha cap compte configurat a l'Outlook.
Els següents passos són per configurar un nou compte a l'Outlook utilitzant la configuració del servidor de correu d'Òmnia.

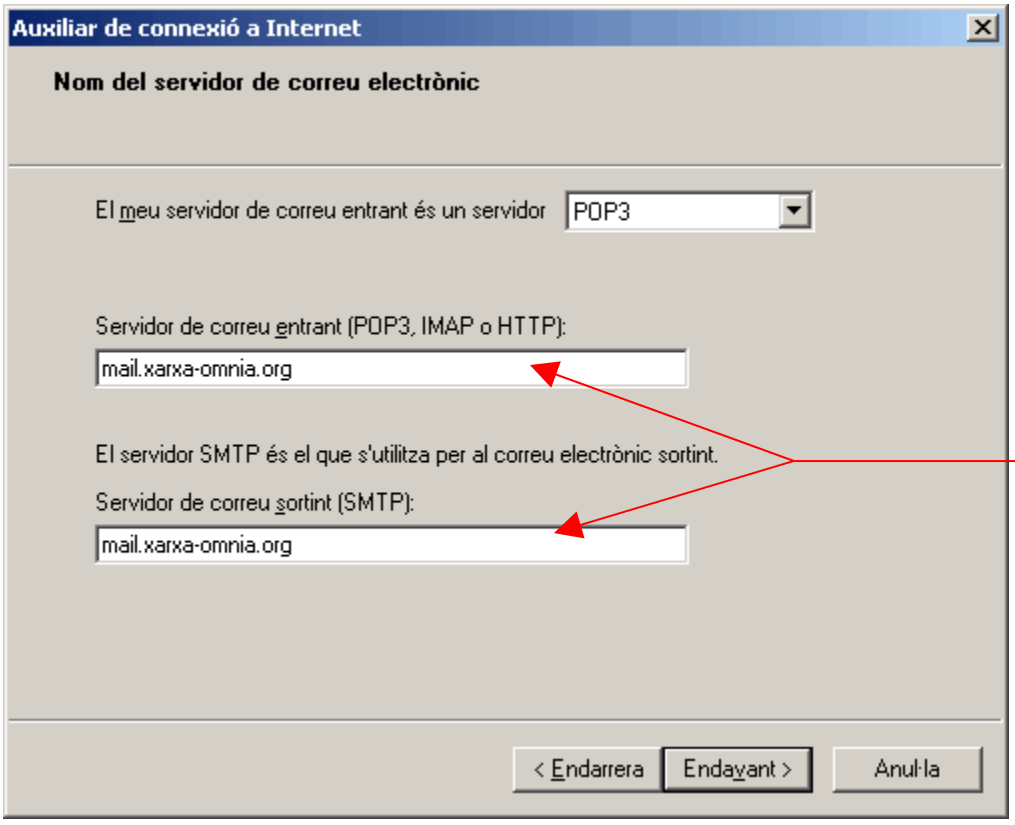
Quan obrim l'Outlook per primera vegada ens avisarà que no hi ha cap usuari configurat al programa, et demanarà si vols utilitzar l'assistent de configuració de l'Outlook. Li direm que SÍ.

Aleshores s'executarà l'Auxiliar de connexió a Internet. Haureu d'anar omplint les dades que us demani.

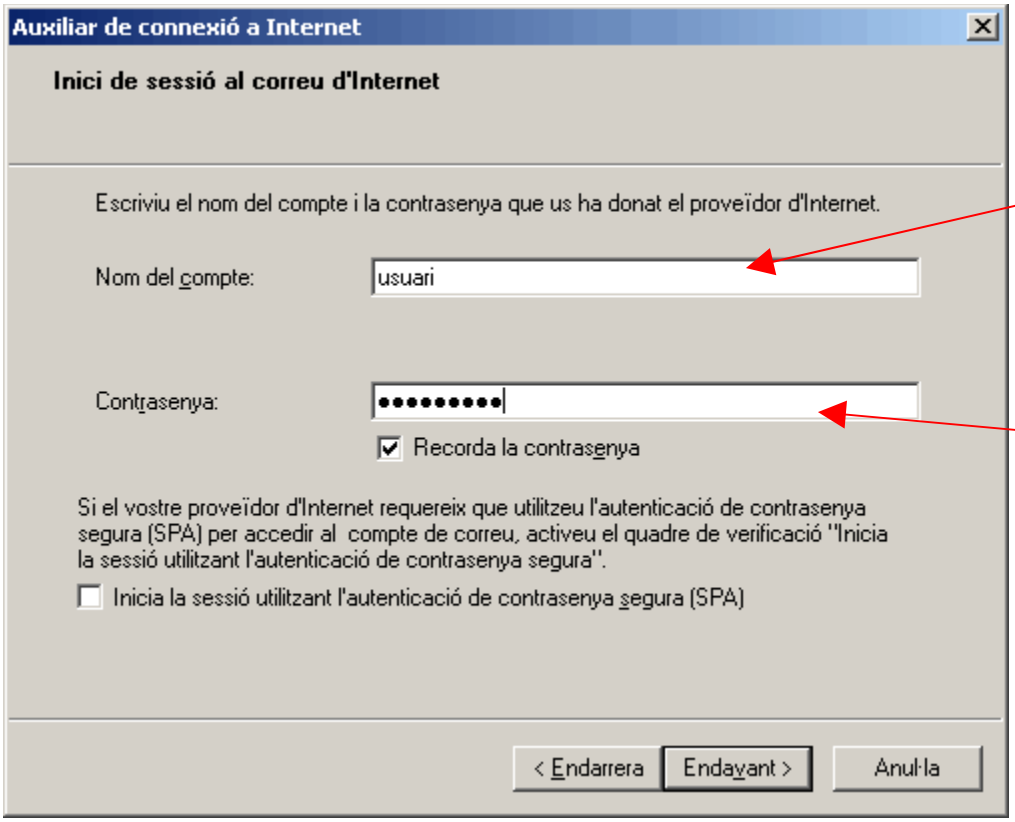




Posa l'adreça electrònica.



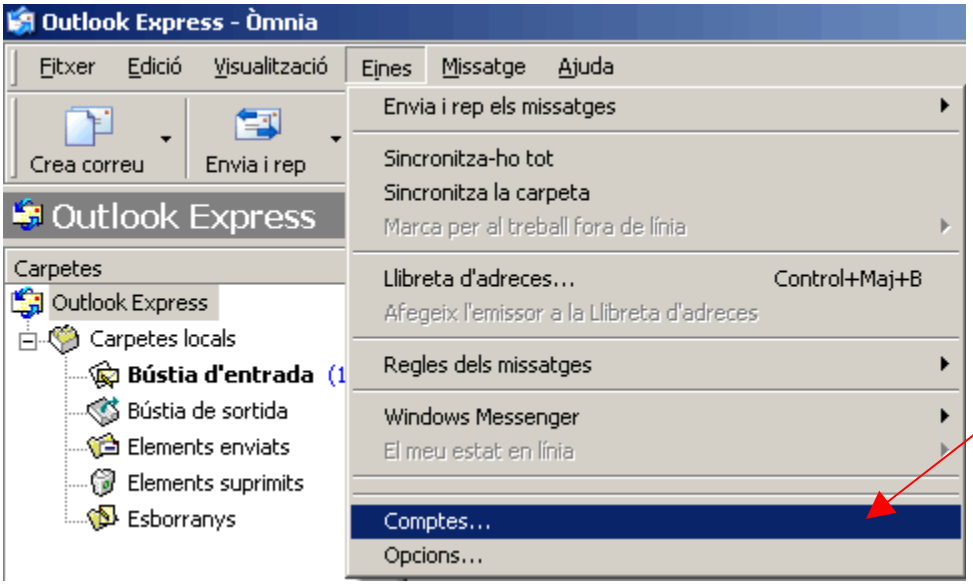
Posa el servidor entrant i sortint del correu.



Posa el teu nom d'usuari.

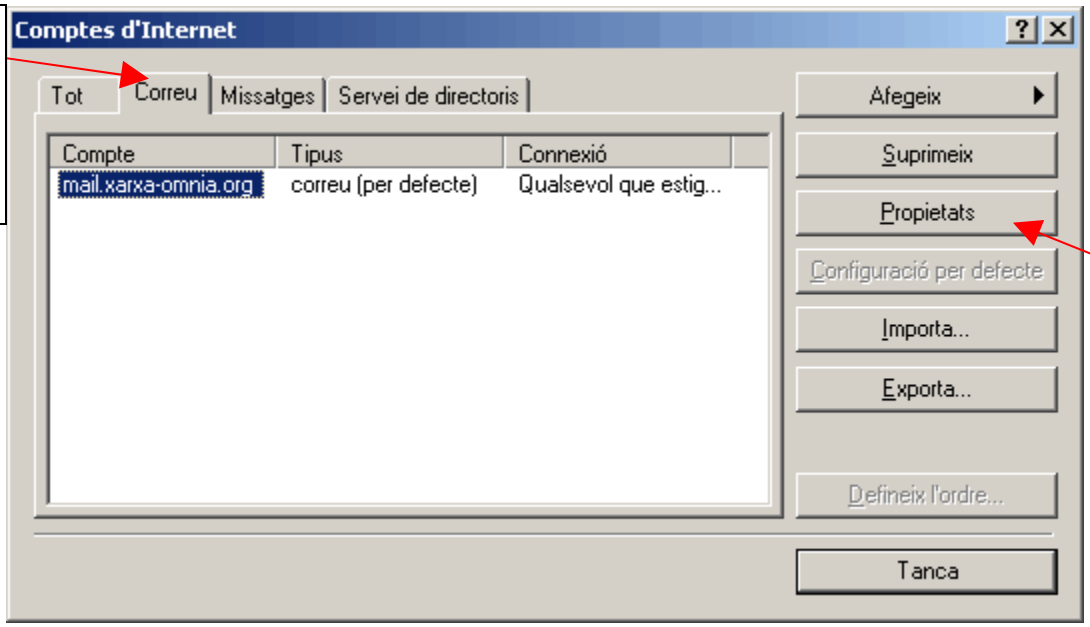
Posa la teva contrasenya

Després d'omplir totes les dades clica a "finalitzar".
Una vegada emplenada tota aquesta informació per tenir a punt el compte de correu del servidor de xarxa-òmnia, s'han de fer uns últims passos.

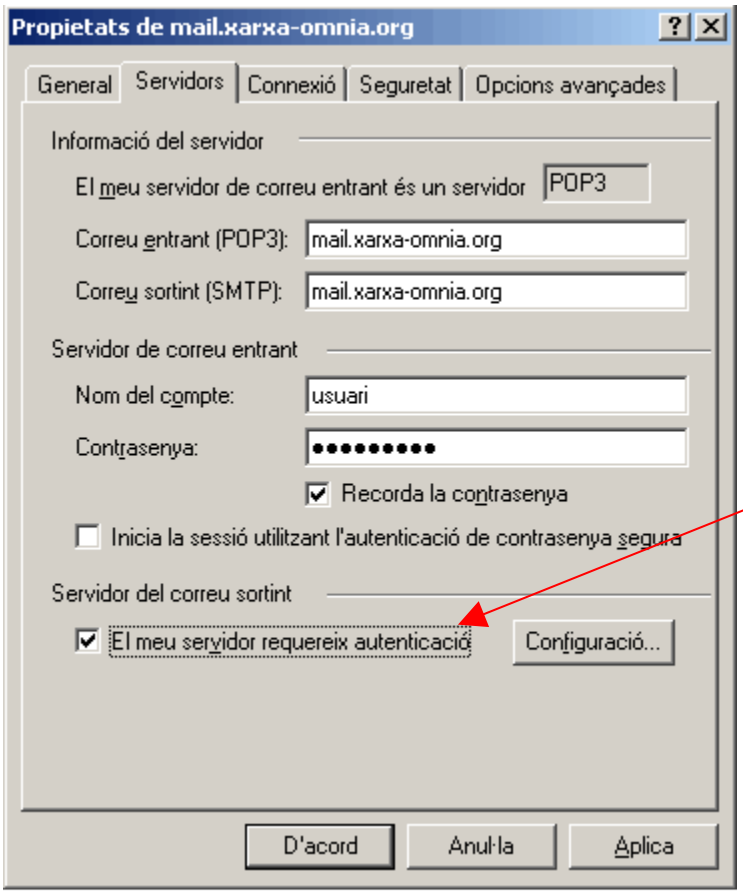


Fem clic aquí.

Fem clic a la pestanya de "Correu"



Després cliquem a propietats.



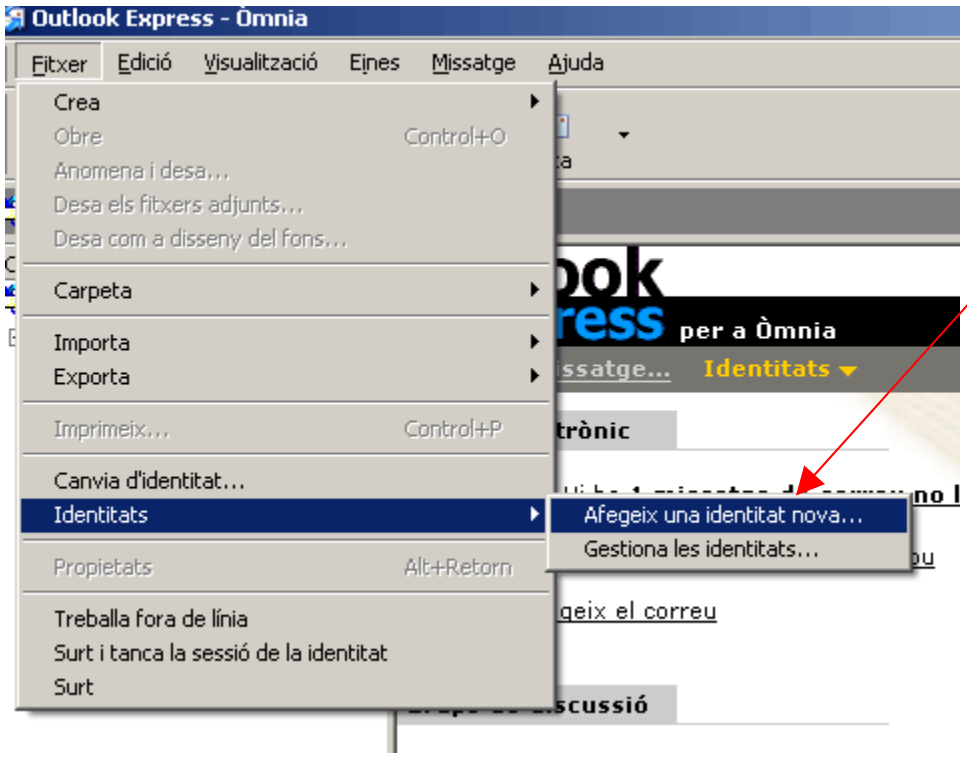
Per poder enviar o rebre correus electrònics aquesta opció ha d'estar habilitada.

Ara ja està tot configurat per poder enviar i rebre correus.

Crear una nova identitat d'usuari.

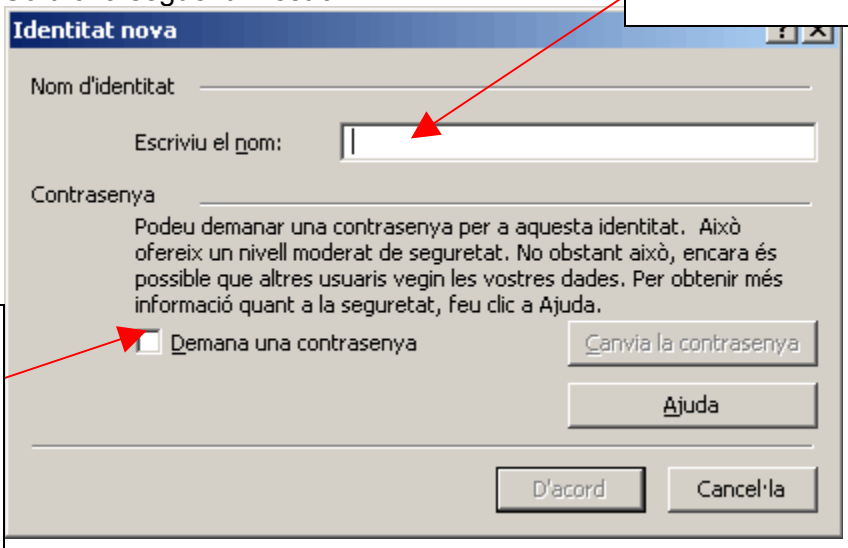
Per poder tenir més comptes d'Outlook de diferents persones hem de fer els següents passos.

1.



Cliquem aquí per afegir una nova entitat.

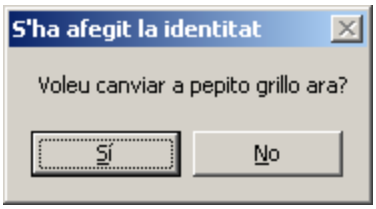
2. Sortirà la següent finestra.



Aquí es posa el nom que es vol que tingui aquesta nova entitat.

Aquesta opció és molt important si vols que la gent no utilitzi ni visualitzi el teu compte.

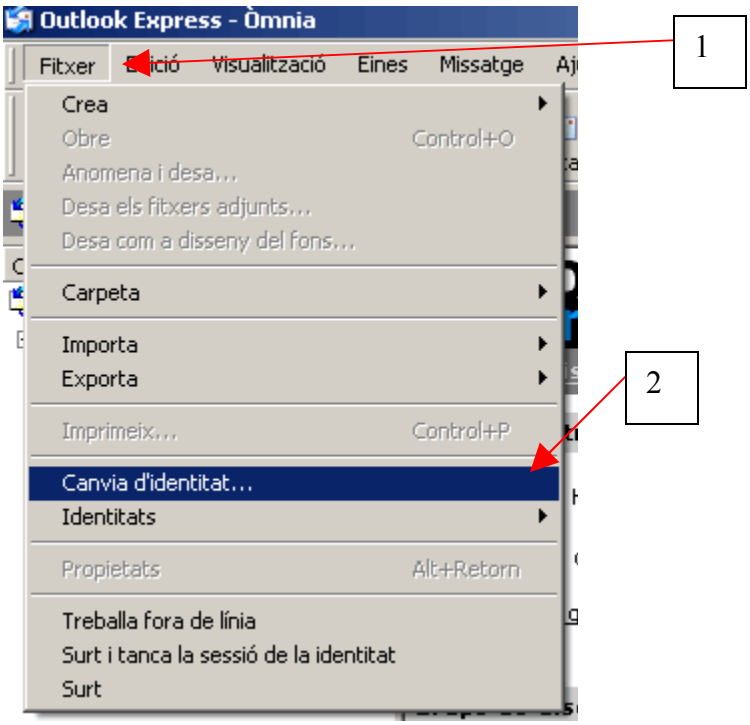
4. Una vegada emplenades totes les dades requerides, et demanarà si vols canviar el nou usuari i un cop el canviïs et demanarà si vols utilitzar l'assistent de l'Outlook.



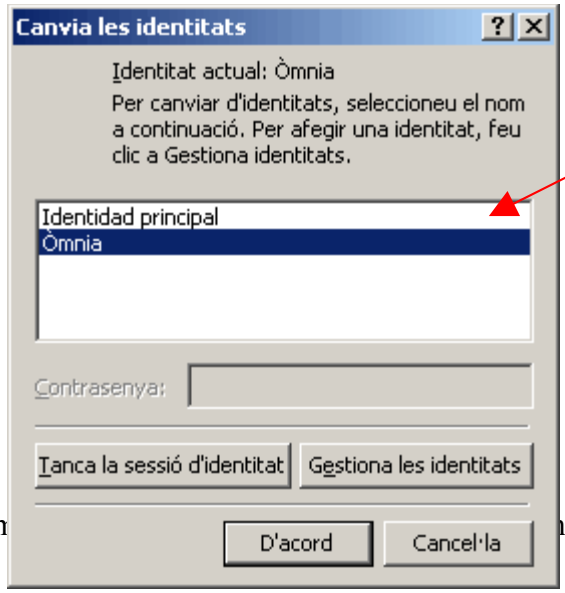
Com canviar d'usuari a l'Outlook.

Per poder canviar d'usuari hem d'anar a :

1.



2.



Aquí has d'escollir el compte d'usuari per poder iniciar la nova sessió.

Infecció i desinfecció de sistemes: Virus i antivirus

1. **Virus i Antivirus.**
2. **Troians**
3. **Firewalls**
4. **Altres arxius perillosos**
5. **Normes i consells per evitar infeccions**
6. **Potser no hi ha per tant**
7. **Adreces interessants**

1-Virus i antivirus

Definició:
Potser primer de tot hem de donar una definició el més exacta possible de què és un virus i que pot fer dins el nostre sistema. Un virus és un programa, un codi que s'introdueix en el nostre sistema per distintes vies, causant al seu torn múltiples efectes , la major part d'ells, nocius i sense donar pistes sobre si mateix, per a poder actuar amb el major sigil i ocupant el mínim espai en el disc (la seva grandària és vital per a passar desapercebut). Normalment el primer que farà el virus és autoreplicar-se/, reproduir-se amb la finalitat d'infectar el major nombre possible de sistemes, i romandre en ells fins ser activat.

Efectes que pot produir un virus en el teu sistema.
Depenent del tipus de virus que es tracti, aquest pot afectar el teu ordinador d'un o més de les següents maneres:

- Reproduir-se i actualitzar-se per si mateix.
- Omplir el disc duro copiant-se a si mateix o a altres porcions de text.
- Esborrar o modificar arxius imprescindibles per al funcionament del sistema.
- Esborrar o modificar el sector d'arrencada, amb el que no és possible tornar a arrencar l'ordinador.
- Esborrar o modificar la informació continguda en les carpetes.
- Saltar d'ordinador en ordinador en una xarxa.
- Influir/ en la impressora, activant o desactivant.
- Ralentir tot el sistema.
- Bloquejar o anul·lar els programes antivirus.
- Impedir l'execució de programes.
- Formatar el disc dur.
- Eliminar la taula de partició .
- I per a quan acabi d'escriure això, segurament s'hauran detectat ja mitja dotzena més d'efectes nocius.

Símptomes d'infecció.
¿Com saber si estem infectats? Sembla una "perogrullada", ja que el més lògic seria tenir en funcionament un bon antivirus, perfectament actualitzat i NO infectar-nos, però anem a suposar que així i tot tenim possibilitat, al cap i a la fí apareixen nous virus gairebé diàriament.

La presència d'un d'aquests símptomes pot indicar que tenim un virus:

1. La velocitat de procés del sistema es ralenteix (si, encara més..)
2. Tenim problemes a l'hora d'executar alguns programes. Fins i tot impossibilitat d'accedir a ells.
3. No podem arrencar.
4. Falla el disc dur.
5. Funcionen programes com la suite Office, però les plantilles i documents estan danyats.
6. L'ordinador es reinicia una vegada i una altra espontàniament.
7. En la pantalla apareixen símbols estranys, caràcters ASCII o les lletres dels textos que veiem en pantalla sembla que cauen o desplacen.
8. Detectem activitat en el disc dur o disquets quan no se suposa que n'ha d'haver.
9. La memòria RAM disponible disminueix alarmantment.
10. Desapareixen arxius o canvien la seva ubicació.
11. I altres símptomes que van apareixent diàriament.

Tipus de virus.

La distinció de tipus de virus sol fer-se d'acord amb el mitjà a través del com infecten el sistema i/o les tècniques utilitzades per a la infecció. Veurem per exemple

- Els virus de boot o arrencada, aquest tipus de virus no sol afectar als arxius i carpetes continguts en l'ordinador, sinó a l'arrencada del mateix (disquet o disc dur)
- Els virus de programa infecten programes o arxius executables.
- Els virus de macro que realitzen infeccions sobre els arxius creats amb determinats programes.
- Virus de sistema afecten bàsicament als arxius fonamentals del sistema operatiu DOS
- Virus polimòrfics que combinen diverses estratègies per a atacar el sistema.

Cucs no són exactament virus...o si ho són, però no intenten infectar més fitxers, el seu únic interès és reproduir-se. El seu objectiu és la infecció en massa.

Mitjans de contagi.

1. El primer i potser més antic :els disquets i qualsevol altre mitjà d'emmagatzematge, Zips, cdroms, etc. En el cas dels disquets és recomanable protegir-los sempre contra escriptura.
2. Xarxes d'ordinadors: ja que aquests es troben connectats entre si físicament
3. Internet: en les seves distintes aplicacions.
4. Correu electrònic: executant arxius adjunts, potser actualment el mitjà més difós.
5. Pàgines Web: mitjançant controls ActiveX/ , que executats, propaguen la infecció.
6. Descàrrega d'arxius, per la possibilitat de traspassar arxius d'un ordinador a altre.
7. IRC (xats) , és un mitjà molt emprat per a autoreplicar-se.
8. News, permeten rebre correus, publicar notícies, etc.

En qualsevol cas, hi ha diverses pàgines d'interès amb informació exhaustiva sobre el tema, una de les millors és la següent:
www.pandasoftware.es/enciclopedia/IntroVir.htm
On trobarem resposta a qualsevol dubte que es presenti sobre el tema virus.

2-Troians i antitroians.

Els Troians, o Cavalls de Troia no poden considerar-se virus. El seu nom indica el seu funcionament, igual que el cavall de fusta utilitzat a Troia per a entrar en la fortalesa i una vegada dintre, descarregar tot el contingent militar que amagava. Un Cavall de Troia es camufla com un programa inofensiu , a vegades acudits, brometes o qualsevol altra cosa que ens inciti a executar-lo. És en aquest moment quan s'activa el “altre” programa. Encara que pot tenir efectes similars als dels virus , esborrat d'arxius,etc. Normalment la seva funció és la d'obrir “portes del darrere” que permetin l'accés al nostre ordinador de forma remota. Una vegada obertes aquestes portes i amb lliure accés des de l'exterior, qualsevol pot obtenir informació del nostre sistema: contrasenyes, claus de targetes de crèdit, adreces de correu, etc/. O fins i tot realitzar operacions sense el nostre consentiment. És a dir , permeten un maneig pràcticament total d'un PC, que físicament no es troba a l'abast de les nostres mans, per mitjà d'una connexió directa des d'altre PC. El programa d'accés remot deu estar instal·lat en ambdós ordinadors i la seva comunicació es produeix generalment via Internet o via xarxa. L'altra diferència bàsica amb un virus és que no són autoreplicants. A part d'aquestes característiques, té unes altres que li confereixen un caràcter maliciós:

- S'aprofita de bugs i fallades de seguretat de programes i sistemes.
- L'usuari que el seu ordinador és controlat, no té consciència d'això, ni tan sols sap que té instal·lat un troià.

Mitjans de contagi

En principi el mateix que els virus: disquets, e-mail, descàrregues de ftp, programes de missatgeria instantània, IRC/ , etc/. però en tot cas és necessària l'actuació de l'usuari que va a ser controlat, per tant cal passar desapercebut per mitjà, per exemple, del sistema de doble extensió, mitjançant enviament de fotos, música, etc/. O camuflat en altre arxiu al que va "enganxat".

Detecció

En el cas dels troians, aquest és un aspecte més problemàtic que en els virus, ja que els antivirus inclouen detectors dels troians més comuns, però si apareixen virus sovint, l'aparició de troians és encara més nombrosa amb la qual cosa és molt difícil l'actualització dels antivirus. Cal desconfiar dels arxius que presentin doble extensió, per a veure-les, deurem activar l'opció "veure totes les carpetes" del menú veure de l'explorador de Windows. També desconfiarem d'arxius la grandària dels quals no es correspongui amb el contingut, per exemple una foto jpg de 850 K.
Normalment són més efectius els programes que es troben en Internet com per exemple The Cleaner , però atenció, tingueu molta cura amb alguns d'aquests "programets", que sota l'aparença de antitroians s'allotgen còmodament en el teu sistema, jo he ensopegat ja amb un parell d'ells (un d'ells és el famós Anti-Trojan). Afegeixo aquí les adreces d'algun d'aquests programes útils:

The Cleaner http://www.moosoft.com/download.php
TSD Trojan Suite Defender http://www.heinekenteam.com.ar/kids/TSD.zip

Evidentment i com en el cas dels virus, la instal·lació d'un firewall impedirà o almenys posarà traves a la instal·lació d'un troià. I sobretot , mantenir una vigilància sobre els ports que romanen oberts. Veure adreces de scan de ports, encara que aquí t'afegeixo una : http://seguridad.internautas.org/scanonline.php

Recorda, si alguna finestreta no està en verd i no posa O.k, compte!....és gairebé tan dolent tenir un port obert com tenir-lo tancat però visible. L'ideal és que ni tan sols es detecti la seva existència

3-Firewalls/ o tallafocs.

El principi del firewall és senzill, funciona com les portes tallafocs en cas d'incendi: El programa s'interposa entre l'ordinador i Internet i controla tot l'intercanvi d'informació. Res no surt de l'ordinador ni entra a ell si no es compleixen unes determinades normes que nosaltres mateixos haurem configurat En principi el firewall monitoritza totes les connexions (ports) , si una aplicació autoritzada envia dades a la xarxa, passaran, si no està autoritzada se'ns informarà si escau d'aquest fet. El mateix succeeix al revés. Si arriben dades autoritzades, passessin, si no és així, es bloquejarà la seva entrada i se'ns notificarà. Això val tant per a Internet com per a intercanvi d'informació entre xarxes locals. Existeixen tants firewalls com empreses d'antivirus, però si estem cercant una triple B (bó, bonic i barat) no tenim més remei que fer referència al conegut Zone Alarm , de Zone Labs, en les seves dues opcions normal, i Pro , aquest últim per a empreses. Tens un fantàstic manual d'utilització del Zone Alarm/ en la següent adreça:
http://seguridad.internautas.org/prc1zone.php

Un altre, el qual hem inclòs en el temari per la seva reduïda grandària i que pots descarregar en format Word, es troba aquí:
http://webs.ono.com/usr040/Agika3/5Tutorial/Zone/tutorialZone.htm

I un altre, també molt bo en aquesta altre:
http://www.almendron.com/librillo.htm

I per últim, aquest...també molt complet:
http://software.ethek.com/Software/contenido.asp?IDContenido=313

Hem de tenir en compte que en un firewall el més important és la correcta configuració. Si per error donem la nostra autorització a una aplicació, el programa no ens advertirà si és o no convenient fer-ho. Simplement obeirà les nostres ordres. Per tant, devem deixar ben clares les regles de restricció. Com hem dit abans, inserim aquí un petit tutorial de maneig i configuració del Zone Alarm.

Tutorial ZONE ALARM.

Un dels tallafocs o firewall amb major difusió. La política de Zonelabs de gratuïtat per a l'usuari particular i la seva eficàcia, fan d'ell una de les proteccions preferides per molts internautes.
Característiques generals: Tallafocs amb capacitat de control del tràfic entrant i sortint, fàcilment configurable mitjançant el seu sistema de selecció de nivells de seguretat per a xarxa local i Internet. Possibilitat de control dels programes als quals vam permetre l'accés a Internet, bé configurant-los permanentment, bé mitjançant petició d'autorització cada vegada que un programa vagi a connectar-se. Això és certament interessant, ja que sempre estarem informats de les connexions que estableixen els programes, cosa molt útil contra Troians, Spywares i alguns virus amb component troià.
Instal.lació: Podem descarregar l'última versió del tallafocs gratuïta de la seva pàgina oficial: http://www.zonelabs.com/ Una vegada descarregat l'arxiu executable, començarem la instal·lació elegint el directori desitjat.

El panell principal

Des d'aquest panell realitzarem la configuració del firewall d'una manera molt senzilla. El panell principal compta amb els següents elements:

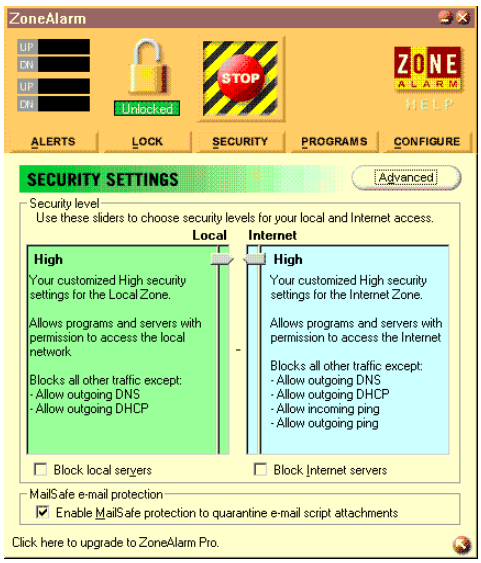
Monitor de tràfic.
Ens indica gràficament el tràfic d'entrada i sortida, mitjançant unes barres dinàmiques , verd per a la recepció, vermell per a la transmissió. Aquesta informació també es reprodueix en la zona d'inici de barra de tasques.
Cadenat de bloqueig.
La icona del cadenat permet bloquejar o desbloquejar l'accés dels programes a la xarxa, segons premem sobre ell adquirirà la condició d'obert o tancat.
Botó de Stop. Permet tallar instantàniament tot el tràfic amb Internet. És una mesura extra de seguretat.
Zona de representació de programes connectats.
Aquí es representen mitjançant la seva icona corresponent els programes connectats a la xarxa.
Accés directe d'ajuda.
Ens direcciona a la pàgina d'ajuda de Zone Alarm en anglès.
Botons de funcions:

ALERTS, LOCK, SECURITY, PROGRAMS y CONFIGURE

Ara vegem les seves possibilitats de configuració.
Security. La primera configuració que realitzarem serà seleccionar el nivell de seguretat del firewall. Tenim possibilitat d'assignar un nivell de seguretat diferent a cadascuna de les zones que incorpora el firewall: La zona d'Internet i la zona de xarxa d'àrea local (LAN) Els nivells que vénen predeterminats són nivell "Medium" en la zona local i nivell "High" en la Zona d'Internet. Aquests valors, que serien adequats en la majoria dels casos, no són els que anem a escollir. S'ha donat el cas, en algunes versions del tallafocs, que el programa en certs casos molt concrets reconeix com locals algunes connexions des d'Internet, pel que els aplica menor grau de seguretat. veure

http://www.securityfocus.com/archive/1/225205

ENLLAÇOS DE SEGURETAT recomana mantenir el nivell de les dues zones en High (Alt). Usuaris connectats mitjançant LAN (Cable mòdem) deuen tenir especial interès a incrementar el nivell de la zona local a High. En la zona d'Internet el nivell el mantindrem sempre en High.

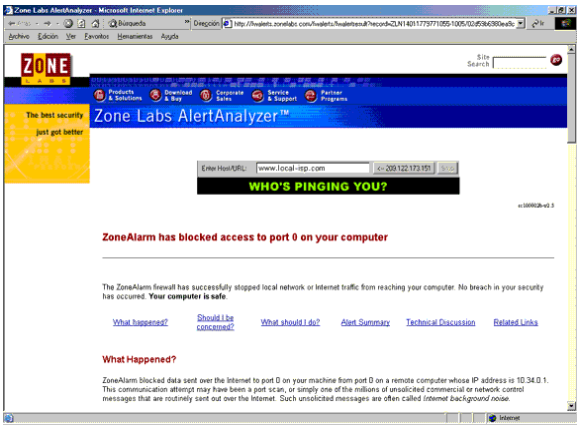


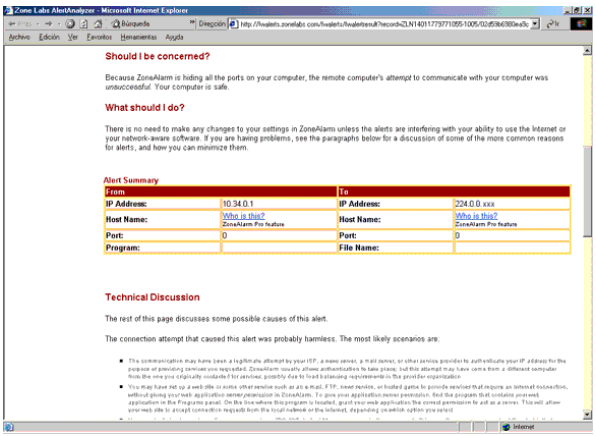
Descripció dels nivells de seguretat.
Aquestes característiques són aplicables a les dues zones:
Alt. Serveis de Windows bloquejats (Netbios), igual que arxius i impressora. En aquest nivell., el tallafocs obre automàticament els ports si el programa sol·licitant està prèviament autoritzat. L'ordinador està en manera steath (Sigil) en el qual els ports que no estiguin en utilització per programes autoritzats es troben bloquejats i no són detectables en la zona d'Internet. Nivell altament recomanat.
Mitjà. Ordinador visible a la zona d'Internet. Serveis de Windows bloquejats. Realització de la funció de bloqueig automàtic. Nivell no recomanat.
Baix. Ordinador en manera visible, NetBios no bloquejat... perquè seguir, aquest nivell es desaconsella enèrgicament.
Les opcions avançades permeten mantenir el nivell de seguretat en la zona local en "Alt", permetent agregar altres ordinadors i elevar l'abast de la zona local. És molt convenient per als usuaris de cable mòdem deixar els subnets del cable deshabilitats. L'activació de la casella "block localInternet servers" situada sota cada zona impedeix l'actuació dels programes com servidors per a les zones respectives, impedint a les aplicacions escoltar els ports. Tindrem això en compte, ja que si volem executar un servidor per a Internet aquesta casella deurà estar desactivada. Els programes com ICQ/ o Netmeeting requereixen aquesta desactivació.
"Mailsafe E-mail Protection" AL seleccionar aquesta casella activarem la capacitat del tallafocs d'interceptar scripts de Visual Basic, potencialment perillosos, en els correus rebuts, aïllant-los abans de la seva execució.
Aquesta funció s'aplica a gestors de correu que utilitzin protocol POP3 i IMAP.
Alerts -Internets alerts (Alarmes) Al expandir aquesta finestra obtenim informació sobre les amatents que ha reflectit el firewall, així com del tràfic d'Internet en el nostre ordinador. Això últim es reflecteix en la casella "Today´s summary".

En la casella "Current Alerts" (Alertes actuals) visualitzem l'última alarma, prement en la fletxa corresponent veiem l'anterior i així successivament. Aquestes alertes ens informen d'un intent de connexió per part d'un programa allotjat en el nostre ordinador o d'un intent de connexió exterior. La informació que reflecteix l'alerta és la següent: Data i hora.
Adreça IP de la font i port d'accés.
Adreça IP de la destinació i port d'accés.

Indicació del tipus de transport TCP, UDP, ICMP, o IGMP
L'opció "More Info" (Més informació) possibilita ampliar la informació sobre les causes de l'alarma i els seus riscos, direccionant-nos a una pàgina específica per a això de zoneLabs, (en anglès) on fins i tot podem efectuar un seguiment mitjançant Whois o traceroute de l'adreça IP entrant bloquejada .

.





La pàgina inclou una sèrie d'explicacions de les alarmes més freqüents i les seves possibles causes, indicant-nos si el nostre sistema roman segur o per contra existeix alguna acció contra la nostra vulnerabilitat.

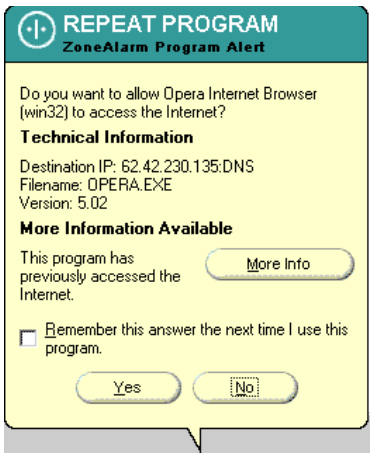
"Alert settings"

En aquesta casella podem seleccionar un parell de funcions relatives als avisos d'alarma que ens dóna el firewall.
Una opció que pot resultar interessant és la possibilitat de guardar en un fitxer de text la relació de les alarmes succeïdes, el que possibilita la seva consulta i comparança posterior.

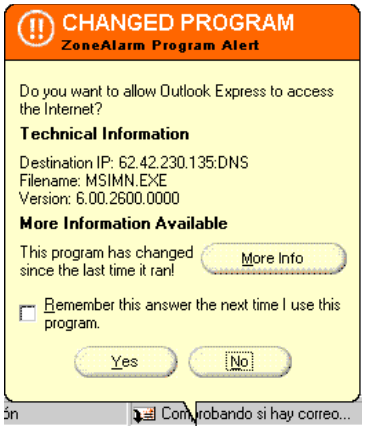
Per això activarem la casella "Log alerts to a text file ".

Perquè les alarmes siguin mostrades en una finestra independent en el moment que es produeixin, activarem la casella "Show the alert popup window".
Aquest seria l'avís d'un bloqueig entrant:

Recordem que no tots els bloquejos entrants corresponen a atacs maliciosos, això s'escolta amb freqüència en fòrums i consultes, ja que és possible tenir diverses alertes de bloquejos entrants el mateix dia. Moltes vegades les mateixes empreses subministradores de la connexió efectuen comprovacions mitjançant l'ocupació de "Pings" els quals no afecten a la integritat del nostre sistema. Aquesta circumstància és de fàcil comprovació mitjançant l'ocupació de l'opció "More Info" de la mateixa finestra d'avís, des de la qual accedirem a la pàgina de Whois de Zone Labs, com hem vist anteriorment. Si els avisos suposessin un emprenyament, és possible impedir l'avís marcant la casella "Don´t show this dialog again" o deshabilitar l'aparició de les finestres emergents des de la finestra "Alerts" desmarcant la casella "Sohw the alert in popup window".
Aquesta és la finestra que sol·licita el permís de connexió d'un programa a la xarxa. Si volem permetre l'accés del programa habitualment, cas per exemple dels navegadors, podem autoritzar l'accés evitant ser consultats, per a això marcarem la casella "Remember This answer the next.....". Això també podem fer-lo des de la finestra "programs", com més endavant veurem. D'aquesta manera, és senzill configurar el tallafocs seleccionant gairebé per si només els programes que tindran lliure accés o per contra necessitaran de la nostra autorització per a connectar-se, o inclòs els que estaran bloquejats .



En aquesta finestra en canvi, Zone Alarm ens dóna l'avís d'un programa en el qual ha detectat un canvi des de l'última vegada que es va executar, el qual intenta connectar-se a Internet. Si el programa no ha estat actualitzat per nosaltres significa que aquest canvi pogués ser d'origen maliciós. Això és de gran utilitat en la detecció de virus i troians.



LOCK (Bloqueig)

Aquest apartat s'ocupa de configurar les possibilitats de bloqueig del tallafocs.

"Lock status"

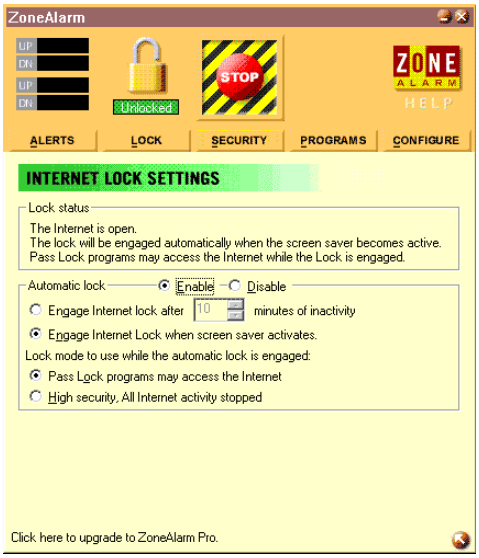
Aquesta casella reflecteix les condicions de bloqueig de connexió en que es troba el tallafocs. La seva condició d'obert o tancat varia segons accionem la icona del cadenat, obrint-lo o tancant-lo.

"Automatic lock" (Bloqueig automàtic)
Seleccionant "enable" possibilitarem que el firewall bloquegi la connexió quan s'activi el protector de pantalla o després de cert temps d'inactivitat. Per a seleccionar qualsevol d'aquestes dues opcions, o ambdues, activarem les caselles: "*ngage Internet lock after (aquí introduirem els minuts d'inactivitat requerits per a activar el bloqueig) minutes of inactivity"

"Engage Internet lock when screen saver activateds" per el protector de pantalla.

També podem autoritzar a un programa a accedir a la connexió passant el bloqueig. Això és útil per a aplicacions que necessiten connectar amb periodicitat o permanentment, com els gestors de correu. Per a això seleccionarem l'opció "Pass lock programs may access to Internet".

Seleccionant, per contra, "Hig security, all Internet activity stopped" detindrem tota l'activitat en Internet a tots els programes quan el bloqueig automàtic s'activi.



Programs.

Quan un programa es connecta a Internet per primera vegada , estant activat el tallafocs, serà afegit en la relació d'aquesta finestra, des d'on podrem elegir el seu nivell d'autorització d'accés. Per defecte, tots els programes sol·liciten autorització per a connectar-se. Marcant l'opció " Remember the answer each I use this program" podem autoritzar a aquest programa en concret que accedeixi directament sense prèvia consulta. Això pot resultar pràctic amb alguns programes de freqüent utilització. Sempre tindrem la possibilitat de variar això últim en la finestra "Programs".

V - La marca de comprovació verd permet a un programa connectar sempre.

X- El X vermell denega l'accés a Internet fins que sigui assignada la marca de comprovació o el signe d'interrogació

?- El signe d'interrogació. Configuració per defecte. Alerta i sol·licita autorització quan un programa intenta accedir a Internet.

Els programes no poden tenir majors drets d'accés a la zona Internet que a la zona local. Per a llevar un programa de la llista, anirem a l'entrada del programa i seleccionarem l'opció d'eliminar. Això no impedeix que el tallafocs vigili l'aplicació, que serà detectada la següent vegada que intenti accedir a la xarxa.
També podem canviar els drets d'accés a Internet d'un programa usant el menú del botó dret del ratolí.

"Allow conecct"

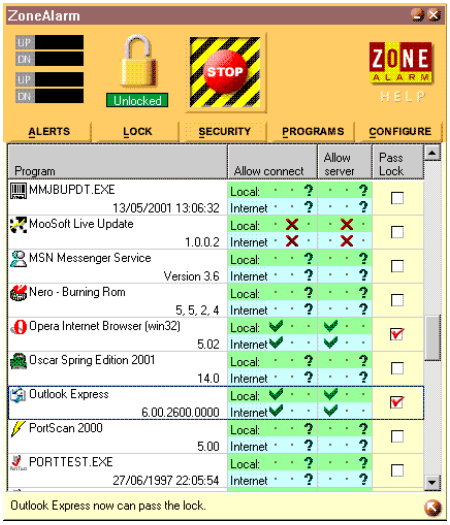
En aquesta columna podem veure l'estat d'autorització de cada programa, en ambdues zones

"Allow server"

Aquí podem seleccionar si autoritzem o no que un programa servidor d'Internet pugui admetre peticions de l'exterior. Si no marquem res tampoc tindrà accés. Seleccionant els programes que puguin efectuar aquest tipus de comunicació donem un pas important en la nostra seguretat. Els programes troians són aplicacions que responen a peticions remotes, qualsevol intent de resposta no autoritzada provocarà el consegüent avís d'alerta.

"Pass Lock"

Marcant aquesta casella autoritzem al programa a connectar-se encara que hàgim activat la funció Lock (Veure apartat amb el mateix nom).



"Configure".

Casella "Configuració". Aquí podem seleccionar que el tallafocs ens informi de qualsevol activitat del nostre ordinador en Internet, mitjançant els corresponents missatges d'alerta. Per a això marcarem " on top during Internet activity ".
La opció "Load ZoneAlarm at startup", la qual ve seleccionada per defecte, provoca que el tallafocs s'inicií a l'arrencar el sistema, la qual cosa es recomana.
AL desactivar-la, hauríem d'executar ZoneAlarm manualment cada vegada que necessitem les seves funcions. Les opcions "updates" i"notificació pop-up" permeten rebre automàticament informació sobre noves versions i productes de Zone Labs Inc. i no és necessària la seva activació per al funcionament eficaç del programa.

Conclusió:

Zone Alarm és un bon tallafocs, d'eficàcia provada i garantida, maneig senzill i un nivell de possibilitats de configuració correcte. a més, és gratuït. En definitiva, un company de navegació molt aconsellable.

4-Altres arxius .

❖ Spyware

Com hem comentat abans, a part dels virus, i troians, hi ha uns "visitants" que també molesten força en el nostre ordinador, que, sense causar-nos un mal immediat o visible, estan violant la nostra intimitat. Ens referim al spyware. ¿Qui no s'ha ensopegat amb un bonic programa d'animació de cursors en el seu ordinador? Ens referim evidentment al "famós" Comet Cursor. I ¿qui no ha intentat eliminar-lo del seu ordinador veient que és molt,molt difícil?. I el que és més, una vegada eliminats, les aplicacions que els van introduir en el sistema deixaven de funcionar.

Com aquest, tenim dotzenes de programets espies similars : Aureate/Radiate, Cydoor, Webhancer, Gator, etc.
Podem trobar-los còmodament instal.lats dins aplicacions tan típiques i habituals com AudioGalaxy, Babylon, FlashGet, iMesh, JPEG Optimizer, NeoPlanet, Opera Freeware, Real Audioplayer, GetRight o Go!zilla.
Realment té una lògica...tot aquest programari...¡gratuït?. Sembla ser que un dels sistemes de finançar-se és la venda d'adreces, hàbits de consum i perfils d'usuari per a enviaments publicitaris. A vegades, per desgràcia es comercialitza fins i tot amb temes més personals, s'enregistra cada formulari que s'emplena, cada nombre de compte que s'introdueix, cada contrasenya que s'escriu. I el més curiós és que ,en molts casos, donem el nostre consentiment al "Acceptar" el contracte del programari sense haver llegit la lletra petita. Vegi's l'exemple de KazAa, en les primeres línies deixa bé clar que es va a procedir a la instal·lació d'aplicacions Cydoor i Brilliant, sengles programes espia.
Existeix una base de dades Spychecker, on podem veure si un programari concret amaga o no programes espies.
A part, existeix una aplicació: Ad-Aware, de Lavasoft. Es pot descarregar sense cap problema de diverses adreces fiables de programari, com per exemple www.softonic.com.

Aquesta aplicació realitza un escaneig i posterior eliminació de tots els programes espies assentats en el nostre sistema.

❖ Spam

L'Spam (castellà, correo-basura) només serveix per a fer-nos sortir de polleguera i , en el cas de pagar per temps de connexió (o sigui, la majoria) incrementar la nostra despesa telefònica. Se'l defineix també com correu comercial no sol·licitat o indesitjable, per a diferenciar-lo del correu físic, que no té cost per a qui ho rep. Tenim pocs sistemes realment vàlids per a lliurar-nos d'aquesta molèstia. Evidentment un d'ells és utilitzar els filtres antispam del nostre compte de correu. El que sí puc donar-vos són un parell de cosetes per a evitar que el teu compte de correu sofreixi un allau:

- La primera és molt simple. La major part d'enviaments d'spam inclouen al final una casella de verificació perquè indiquis si vols o no seguir rebent publicitat. Molt bé, marcant que si, o que no, és el mateix, l'única cosa que aconsegueixes és que , des d'aquest moment el que t'envia correu sàpiga que la teva és una adreça de correu vàlida. Ignora'ls, esborra aquests missatges directament i punt.
- Utilitza un dels "programets" antispam que corren per allí, alguns són realment efectius, com el Bounce Spam. Aquí t'afegeixo unes adreces d'on baixar-los.

AntiSpam 1.0 http://www.xde.net/antispam

Bounce Spam Mail 1.8 http://ay.home.ml.org/bsm

E-Mail Remover 2.4 http://home.pacific.net.sg/~thantom/eremove.htm

♦ Hoax (boles, mentides)

Què són hoax?

Llegiu això, pot ser que a algú li soni, va ser molt famós fa un any o any i escaig:

"Subject: alerta virus!!

Disculpen si ya recibieron el mensaje, si no vale igual.

Un amigo nos advirtió del VIRUS y lo teníamos en la compu.
Revisen en su PC, al menos por previsión.
Busca el archivo: sulfnbk.exe (lo eliminamos por lo que no lo enviamos nuevamente).
ir a menu iniciar, localizar (o find) y localizar este archivo y borrarlo (se aloja en C:/Windows/command)
borrarlo también de la papelera de reciclaje.
Se trata de un virus que viene a través de e-mails sin que
te des cuenta y va a destruir tu computador el 01 (se activa el primero de cada mes)
Este alerta fue pasado por el sector de computación de la FEG/UNESP."

¿us sona? És un Hoax, un hoax dels més típics. A l'usuari confiat l' incita a comprovar l'existència d'aquest arxiu en el seu ordinador, i quan descobreix que evidentment si existeix, li aconsella esborrar-lo, amb la qual cosa ha convertit en "virus" al propi usuari. Aquest és només un exemple, hi ha milers més....totes aquestes cadenes que ens prometen l'or i el "moro" si reexpedim qualsevol estupidesa a 15 persones, o aquesta quantitat de nens malalts de terribles patiments i que només milloraran si reexpedim

aquesta carta a 25 amics abans de dues hores....o les empreses comercials que ens regalaran un telèfon mòbil si enviem la publicitat a 20 coneguts, i posteriorment aquestes 20 adreces a un e-mail de la companyia.

Alguns estan preparats només per fer mal, com el que acusa al grup vasc La Oreja de Van Gogh de col.laborar amb el 50% dels seus guanys al sosteniment de ETA, o els milers que volten per la xarxa anunciant de manera apocalíptica que tanquen msn, o eliminen usuaris de Hotmail.

¿Com actuar?

La millor actuació davant un hoax és la no-actuació. En el mateix moment que rebis una ximpleria d'aquest tipus, esborra'l i oblida'l. Sobretot NO ho reenviis, amb cada reexpedició només estàs alimentant les llistes de distribució de vés a saber qui. I el que és pitjor, ens comportem com a virus....reproduïm al hoax /.
MAI esborris un arxiu del teu ordinador només perquè t'ho digui algú per e-mail, per molt de confiança que sigui el "algú".
Pots trobar una llista de hoax en aquesta adreça:
www.vsantivirus.com/hoaxes.htm
o en aquesta altra que, a mi particularment, em sembla una pàgina genial sobre el tema...no te'ls perdis.
www.rompecadenas.com.ar

És més, vaig a afegir-te un altre exemple del que és filar encara més prim:

Asunto: Alerta!! Hotmail se cierra....
Si usas Hotmail manda este mensaje a todos los que sepas que lo usan, de lo contrario el dueño de Hotmail (Jon Henerd) borrará tu mail de aquí.
Hotmail se esta sobrecargando y necesitamos librarnos de gente y queremos saber cuales son los actuales usuarios que estan usando sus cuentas de Hotmail.
Así que si tu eres un usuario, por favor manda este e-mail a todos los que puedas, pero si no lo pasas a nadie se borrará tu cuenta de Hotmail.
Gracias por tu cooperación
Mr.
Ja veieu exactament de què es tracta....una pèrdua de temps, de diners en les connexions de RTB , d'espai en els nostres comptes de correu i una manera d'augmentar la col·lecció d'adreces vàlides de correu amb fins comercials (espero...)

4- Protecció de menors a la xarxa.

Aquest és un capítol al qual hem de prestar especial atenció vist el tipus d'usuaris del Projecte Òmnia. Són molts els continguts inadequats que, expressament o per error, poden ser visitats pels petits, són també moltes les maneres en que gent sense cap escrúpols poden dirigir-se a ells amb llenguatges ofensius i fins i tot incitar-los a trobades físiques a través del xat. No cal caure en la paranoia que Internet és perillós i no es deu deixar accedir als menors, però si és cert que amb bastant facilitat poden caure en pàgines amb continguts xenòfobs, violents, o de pornografia, a vegades fins i tot mentre es realitzen recerques de caràcter general. La ingenuïtat dels petits els converteix massa sovint en víctimes d'assetjaments via correu, fins i tot interrogatoris sobre informació personal i familiar. Els principals navegadors Internet Explorer i Netscape inclouen la possibilitat de filtrar la informació que es rep. En el cas del IE5, en les Opcions de Configuració trobem el denominat "Assessor de Contingut " que ens permet especificar llocs permesos i llocs prohibits. En el cas d'un aula d'informàtica, el més senzill és introduir la llista de llocs permesos, que seran aquells que prèviament haurem determinat

d'acord amb les classes que s'imparteixin.

5-Normes i consells p ns.

Els primers consells que us s'han difós des de l'Associació d'Internautes, des de la II Ca a Xarxa, en col·laboració amb Panda Software i altres emp

Recomanacions

1. Tingues sempre en la ment el tema de la seguretat, fins que sigui alguna cosa innata en la teva conducta al connectar-te a Internet. No ho abandonis per desídia. És la major font de problemes.
2. Comprova periòdicament el nivell de seguretat amb el qual estàs connectat (scan de ports, antivirus, firewall, dades sensibles en la configuració de comptes...)
3. Realitza periòdicament còpies de seguretat de les teves dades.
4. Si utilitzes connexions amb Tarifa Plana (ADSL/ i CABLE, ja que encara no tenim TARIFA PLANA per RTB) apaga l'ordinador quan no usis la connexió. A més estalviaràs energia :-)
5. Si utilitzes RTB revisa de tant en tant l'Accés Telefònic a Xarxes per a veure la connexió i vés amb compte amb algunes pàgines, sobretot de sexe, que creen per si mateixes, o et demanen que instal·lis, un nou Accés Telefònic a Xarxes (dialers)amb un núm. de telèfon de PAGAMENT (tipus 906)
6. Tingues especialment cura quan descarreguis programari de llocs dubtosos.
7. Si uses programes Servidors per a Internet, estigues atent a les actualitzacions dels programes perquè segurament arreglessin forats de seguretat.
8. Instal·la i tingues sempre actiu un Antivirus i, per descomptat, actualitza'l periòdicament.
9. Instal·la un firewall i estigues atent a les actualitzacions.
10. Configura en principi qualsevol programa, i especialment el navegador d'Internet, en el nivell més alt de seguretat que et permeti. Davant la necessitat, sempre pots baixar el nivell de seguretat i tornar-lo al seu nivell màxim quan deixis de necessitar-lo.
11. No et fiïs dels enllaços (links) de les pàgines. Comprova que et condueixen a la pàgina veritable on vols anar.
12. En les pàgines web on hagis d'introduir informació sensible (per exemple el nombre de la targeta de crèdit), procura que siguin sempre segures (comencen per https:
13. Configura el teu client de correu per a rebre i enviar correu en manera text. A més que no aporta gairebé mai gens l'html, és font de problemes de seguretat i de privacitat.
14. MAI executis un adjunt d'un correu amb doble clic, encara que t'ho hagi enviat el teu millor amic/@. Sempre és millor guardar l'adjunt, i executar primer el programa que hauria d'obrir obrir aquest adjunt i des d'aquest programa obrir el fitxer.
15. No propaguis els HOAX. SI, atreveix-te a trencar les cadenes de missatges. Actuant com un VIRUS ja que tu mateix ets el propagador.
16. Si no vols rebre SPAM, quan envies un missatge a les NEWS, posa tant en l'adreça de correu de la capçalera del missatge com en la signatura algun identificador que faci impossible que pugui ser recollit de forma automàtica per programes informàtics.

Per exemple nom@QUITAESTOdominio.com, nom@dominioESTONOVALE.com. Fes-lo SEMPRE a la dreta de l'arrova i MAI en el nom.

17. Encripta els teus missatges i fitxers més sensibles.
18. No acceptis mai arxius que no hagis sol·licitat quan estiguis en el xat (IRC) o grups de notícies (NEWS).
19. Davant el dubte, "abstenir-se"
20. Ajuda als altres. Dóna a conèixer aquestes normes de seguretat.

A aquests consells facilitats per l'Associació d'Internautes afegirem uns altres igualment importants i imprescindibles.

1) La millor eina per a protegir-se dels virus, a més d'un bon antivirus és el sentit comú. La gran majoria dels mals produïts per virus es deuen al comportament del propi usuari.
2) Cada vegada que siguis tu qui enviï un arxiu, posa en l'assumpte una frase del tipus "Pepe, t'envio tal arxiu sobre tal tema", perquè el destinatari sàpiga que ho envies tu i que no és un virus.
3) Evidentment assegura't de no enviar cap virus en els teus arxius.
4) Per descomptat, passa per l'antivirus qualsevol disquet que caigui en les teves mans. Últimament només ens recordem de les epidèmies per Internet, però és enorme encara el nombre de disquets infectats que "pululan" per tot arreu, de mà en mà.
5) Respecte a això, procura retirar els disquets de les disqueteres a l'apagar o reiniciar el teu ordinador.
6) Tingues un disquet d'arrencada net i a mà. Mai se sap.
7) Compte amb els documents de Office que duen macros.
8) Procura estar informat en la mesura del possible dels nous virus.
9) Deshabilita la vista prèvia de l'Outlook Express (alguns virus no necessiten que executem cap arxiu, s'activen només amb la vista prèvia del missatge)
10) Independentment de l'Antivirus que usis, no està de més passar altre del tipus online, són ràpids, eficaços, gratuïts i com se sol dir, veuen més quatre ulls que dos.
11) Utilitza sempre programari legal, compte amb les pàgines de Abandonware, malware, Hackez, Warez, etc. Són com caramels.
12) No diguis la teva contrasenya a NINGÚ. Sembla una estupidesa, i segurament ho és, però succeeix amb massa freqüència. Per la mateixa raó evita contrasenyes com "Josep210874", sobretot si et dius Josep i vas néixer el 21 d'agost de 1974.
13) Quan Windows et faci la famosa pregunta de si "desitja que Windows recordi aquesta contrasenya per a la pròxima vegada" evidentment digues-li que no. No volem que arxivi massa coses en l'ordinador, sobretot coses que puguin ser vistes, usades i robades per uns altres.
14) Compte, sempre molt de compte amb els xats, IRC/, programes de missatgeria instantània i de P2P.
15) I finalment, no caiguis en la paranoia. I amb motiu d'això.....

6-Potser no n'hi ha per tant...

- Només necessites usar el teu sentit comú, no cal caure en les paranoies.
- Com s'ha dit en el capítol corresponent, no tots els avisos del zone Alarm (ni de bon tros) indiquen que mig món estigui intentant entrar en el teu ordinador.
- No caiguis en la temptació d'instal·lar tots els "antitroians molt efectius" que es troben per la xarxa. La majoria escanejen el teu sistema buscant fallades de seguretat, te'ls notifiquen perquè vegis que bé funcionen, i de passada s'assentaran còmodament en

la teva màquina a passar la tarda. Els que cauen en la paranoia (m'incloc) som les seves víctimes més fàcils.

- Intenta "educar" als teus coneguts, tingues en compte que si ells t'envien Hoax o inclòs virus, en el 90% dels casos no tenen ni idea del que acaben de fer. Per principi tots som bona gent, i quan ens diuen que enviant això a 15 amics, fulanito de tal, aconseguirà complir el seu somni de col·leccionista abans de morir, evidentment ho enviem.
- Important: El maquinari NO es pot danyar. Escoltem veritables "fetes" per part dels virus, però sempre, sempre és el programari el que acaba danyat. Com a molt, algun virus que ataca en aquesta adreça afecta la Bios, però mai el maquinari. Això que expliquen dels monitors és fals...si, això altre també.
- Si tens el teu antivirus actualitzat, i et comencen a fallar coses, pensa que poden ser també altres les causes. Molt sovint nosaltres mateixos.

7-Adreces interessants.

http://webs.ono.com/usr016/Agika/botiquin.htm

- Links relacionats amb la seguretat, scan de ports, antivirus, etc.

http://security2.norton.com/ssc/vc_scan.asp?langid=mx&venid=sym&plfid=20&pkj=RDGIJPUVGCWETOMGMCY

- Es una anàlisi online de Norton-Symantec, molt efectiu. Només s'ha d'activar i acceptar cada cop que ens demana si volem descarregar un instal.lador. En 20 minutos està fet, però a diferència del Panda Active Scan NO es pot continuar treballant mentre fà l'anàlisi.

http://security1.norton.com/ssc/sc_ipcheck.asp?ax=1&langid=mx&venid=sym&plfid=20&pkj=RHHDPJUIYCZRWEJGSSK

- Aquesta també és de Symantec, però no és un antivirus, sinó que examina les vulnerabilitats del nostre sistema. Per anar bé, quan analitza els ports, tots han de sortir en silenci. Si surt que tots són “silenciosos”, hem de revisar el nostre sistema de seguretat.

http://www.pandasoftware.es

- Un altre scan antivirus online, ràpid i eficaç. Permet minimitzar la finestra i continuar treballant mentre neteja.
- Només cal polsar les icones de Active Scan i seguir les instruccions.

http://www.trendmicro.com/free_tools/

- Una altra anàlisi online de Trend Micro, els fabricants del conegut PC-Cillin, només cal adreçar-nos a l'enllaç “HouseCall” i acceptar les baixades dels instal.ladors.

https://grc.com/x/ne.dll?bh0bkyd2

- Aquesta pàgina és cosa de Steve Gibson, polsant "Probe my Ports" escaneja immediatament els ports lliures pels quals podrien colar-se visites indesitjables.
- Per anar bé. Tots els ports haurien de sortir en estat "Stealth" ,és a dir, que ni tan sols es detecta la seva existència.

www.seguridad.internautas.org

- Qualsevol dubte sobre seguretat, viurs, troians, firewalls, xarxes, el que vulguis.....molt probablement hi trobaràs la resposta.

Mètode desinfecció de virus.

El primer es que tinguem una sospita de que som portadors de virus, com ho podem saber?.
Per què el ordinador fa coses estranyes, tanca programes, es col·lapsa, surten pantalles blaves etc etc etc...., això també ho fa Windows sense virus potser ell es un virus.
No ara en serio amb la ultima fornada de cucs, lo mes probable es que quelcom os digui per mail **"**que es aquest arxiu que m'has enviat i tu penses jo no he enviat res**"**, això es una evidencia de que estàs infectat per algun virus.

La prioritat quant un virus entra en la xarxa es que no es contagi a d'altres ordinador, el Klez per exemple si el ordinador entra en carpetes compartides fica fitxers amb extensió .rar .scr .exe .bat si algú del altre ordinador executa aquests arxius, esta infectat. La solució desconectar lo de la xarxa lo mes aviat possible per tenir-lo en quarantena.
Evidentment si el teniu infectat, el antivirus o esta caducat o el virus ha acabat amb ell, amb lo que tindríem que passar un antivirus.

Ara ens toca la tasca mes difícil i alhora mes didàctica identificar el virus, ho podem fer connectant en exclusiva aquest ordinador a Internet i analitzant amb un scaner online antivíric. Un altre opció es fer uns disquets de desinfecció, els farem des de un ordinador que tinguem la seguretat que no esta infectat o quant instal·lem el antivirus en un ordinador nou i un cop actualitzat.

Els que teniu panda platinium ho teniu com una opció en el menú "herramientas" , en canvi els que tingueu titanium tindreu que anar a al directori del programa generalment a c:\archivos de programa\Panda Software\Panda Titanium\ i buscar un executable que es diu **sdisk32.exe**, aquest programa crea els disquets de desinfecció.
Si els disquets han tingut resultat tindrem un sistema desinfectat, i al arrencar veurem tot lo que hem perdut per causa del virus.

Però si no hem pogut desinfectar al 100% i sabem amb certesa el virus que ataca la nostra maquina, podem trobar un programa específic que el desinfecti, tipus eines de bitdefender o pandaquickremove.

Un cop tinguem el ordinador net, instal·larem de nou el antivirus i l'actualitzarem tot seguit.

Es molt important tenir el antivirus actualitzat al dia, abans potser l'actualització podia ser més de tant en tant però ara val a dir que període de latència del antivirus es de una setmana o menys, si el nostre antivirus passa aquest període lo mes possible es que ens puguem infectar.

Tot i això també cal actualitzar Explorer i Outlook unes de les entrades de virus mes important per culpa dels bugs i la mala programació de Microsoft.

Una de les preguntes freqüents es quin antivirus es el millor, i jo crec que la resposta seria el que estigui mes actualitzat.

Els últims virus lo primer que fan es donar de baixa tots els antivirus.

Per això si rebeu un cpl pel Messenger o un missatge estrany o un document que no sabeu que es comte al obrir quelcom que no ha passat per l'antivirus. Comte amb pagines web si el nostre Internet Explorer 5.0 5.5 o 6.0 no esta actualitzat.

Problemes amb el apvx.vxd

Per la quantitat de consultes sobre aquest tema posem aquest afegit.
Començant pel principi que es el apvx.vxd, es una llibreria dinàmica reminiscències de win3.11 i win95, resumin no es res mes que un programa que la seva funció es analitzar tots els programes que s'executen en el nostre ordinador.

Perquè es fica com ha vxd i no com ha dll llibreria dinàmica de win32, pues ho fa per prioritats les vxd el sistema les carrega abans que les dll amb lo que Windows te un control relatiu i actuen per sobre de ell.

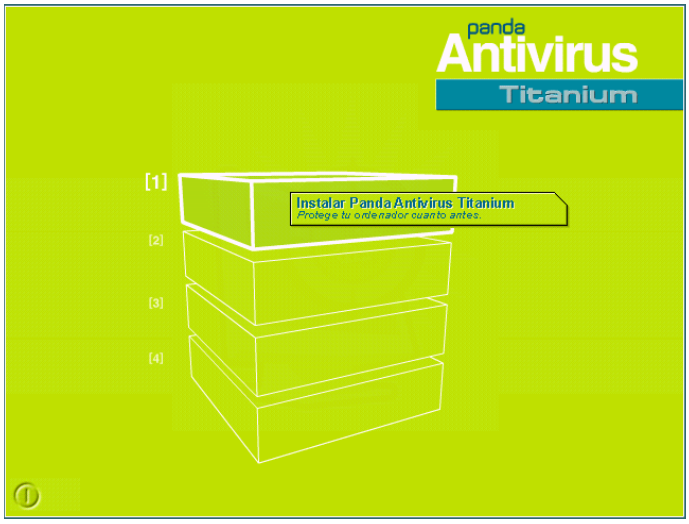
Aquestes llibreries es carreguen generalment des del system.ini o el win.ini i no des del kernel de win32. al ser carregades abans que el sistema , si no es troben o tenen un error on surt el típic missatger a la pantalla fosca de no ha trobat o ha tingut un error miri el system.ini o win.ini per solucionar el problema, i ens donem un gran ensurt.

Lo mes greu es que si aquest missatge ens surt al principi vol dir que del antivirus actiu l'únic que tenim es la icona del osset, amb lo que els virus poden infectar la maquina.
Estudiant el tema la solució que hem trobat han sigut dues o be fer una actualització manual, o sigui obrir el antivirus i dir li que s'actualitzi, o desinstal.lar, tornar a reinstal.lar i actualitzar tot seguit.

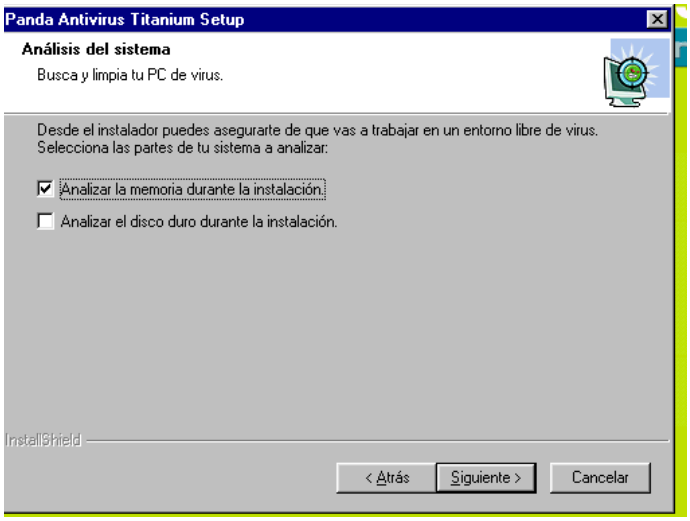
Les causes no les hem pogut esbrinar, lo que si que tenim certesa es de que va ser tot en un moment molt precís i que tothom va tenir mes o menys el mateix problema.

Instal·lació de l'antivirus (Panda).

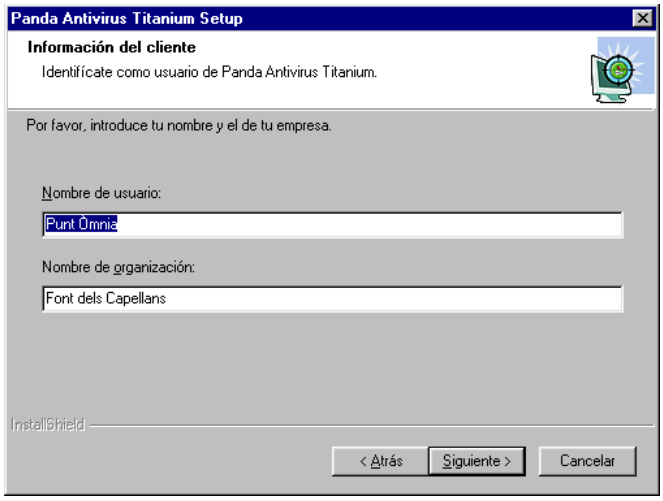
Després d'introduir el Cd amb l'antivirus s'arrenca una aplicació típica d'instal·lació de software, si no tenim el cd i utilizem un executable passem a triar directament el idioma. En un primer pas hem de triar l'idioma i procedir en el primer bloc dels quatre a la instal·lació de l'antivirus.



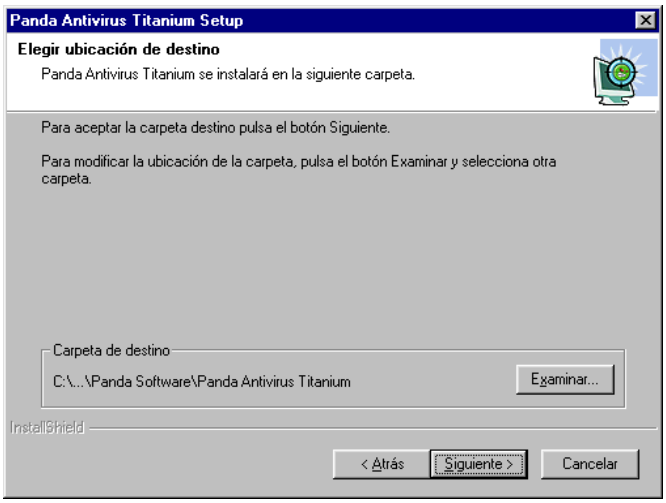
Un cop triada l'opció del menú que desitgem (Instal·lar), se'ns demana si volem analitzar la memòria o el disc dur a la cerca de virus mentre fem la instal·lació, l'única diferència en aquest procés resideix en la durada de la instal·lació, molt més llarga si triem alguna de les dues opcions. Un cop hem triat o no l'anàlisi de la memòria o disc dur seguim endavant.



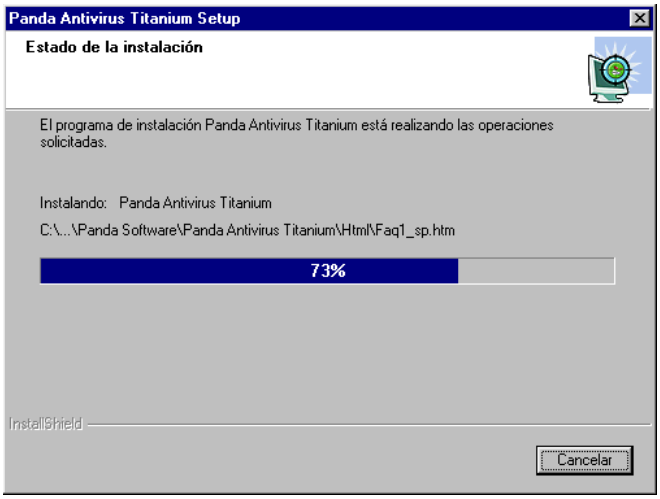
El següent pas és efectuar el Registre del Soft // Antivirus.



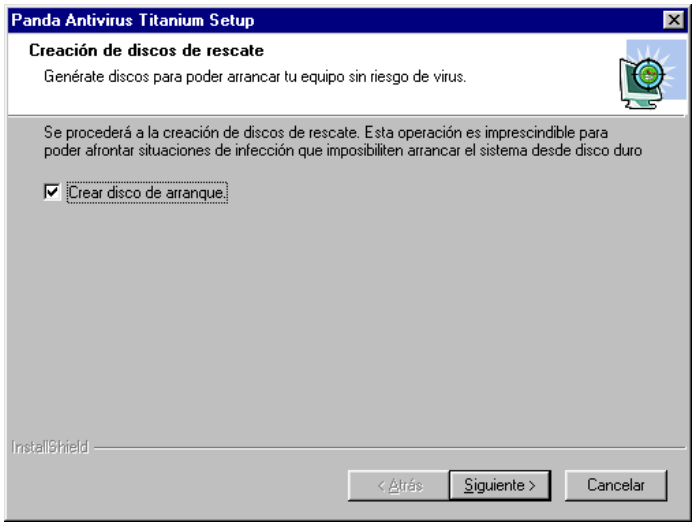
El proper pas és escollir la ubicació // carpeta a on instal·lar el soft. No modifiquem res i continuem endavant.



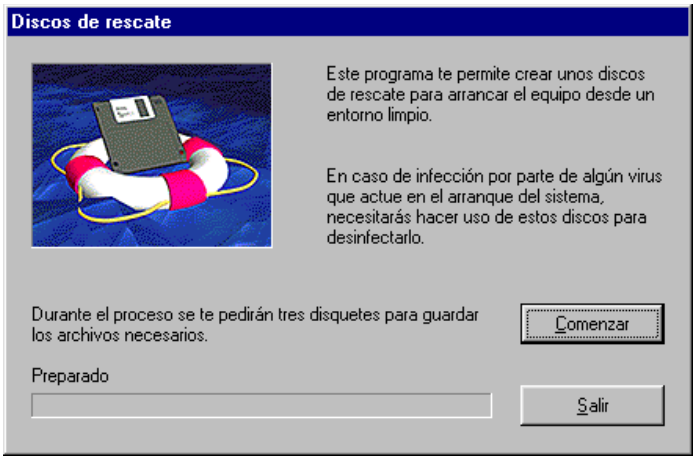
La instal·lació segueix el seu procés...



...i un cop finalitzada ens trobem en el moment de crear els útils discos d'inici**. És molt necessari** crear aquests discos per a poder restaurar el nostre sistema en cas que per qualsevol descuit se'ns infecti l'ordinador amb un virus. Els discos d'inici ens permetran arrencar el sistema sense virus i executar l'antivirus per poder netejar la memòria.

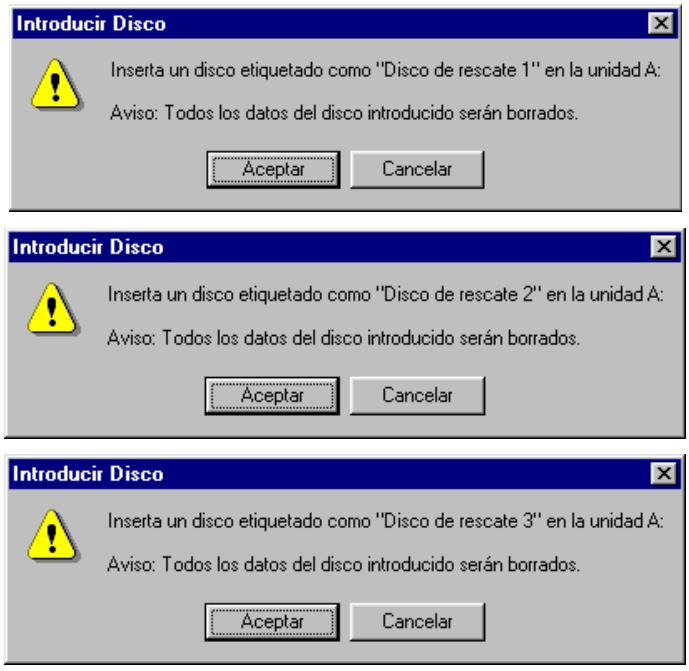


Continuem endavant i abans de començar se'ns informa que ens caldran tres disquets. Fem clic a "començar".

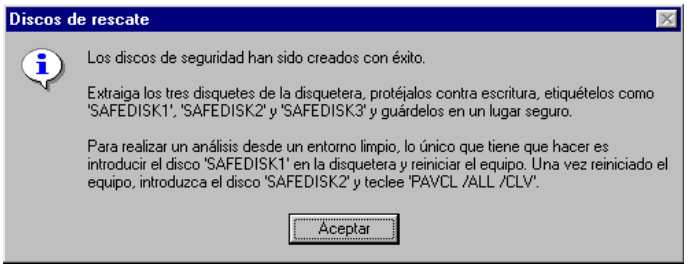


Durant el procés ens va demanant els disquets. És molt recomanable etiquetar-los correctament i desar-los en un lloc segur.

Val a dir que potser es millor fer els disquets un cop actualitzat el antivirus. Anar a c:\archivos de programa\panda software\panda titanium i buscar el arxiu sdisk32.exe que arrenca la mateixa aplicació de la que estem parlant i continuant fent els disquets.

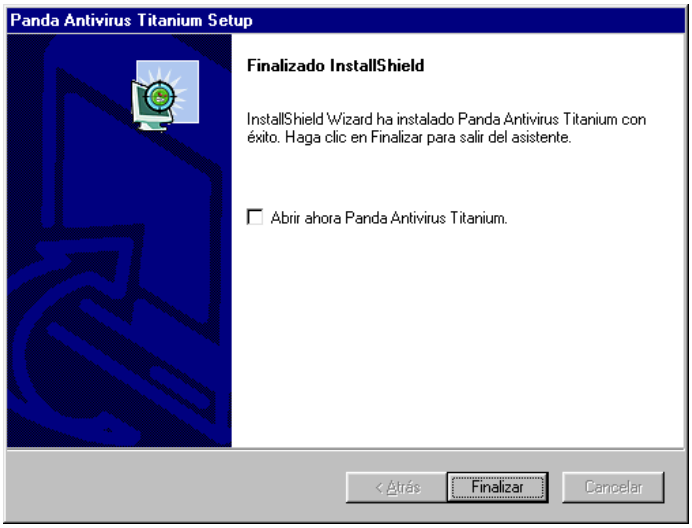


Quan acabem el procés ens informa de com realitzar correctament l'anàlisi arrencant el Pc amb els tres disquets.



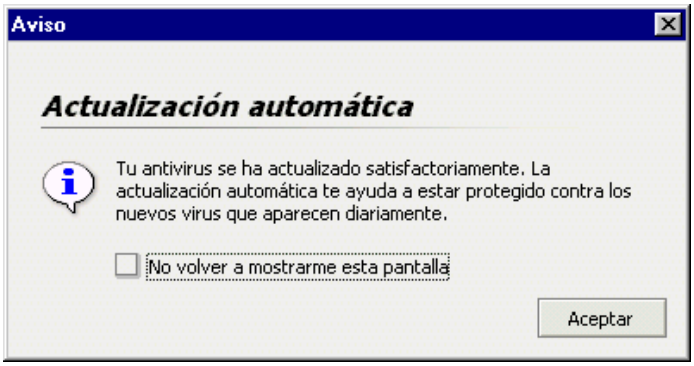
Si ens sembla necessari, podem anotar les instruccions en el primer disquet per a seguir correctament el procés.

En el proper pas, si ho desitgem, podrem efectuar el registre On-line o deixar-ho per més endavant, però sense un registre de l'antivirus no podrem actualitzar-lo, amb la qual cosa la seva efectivitat minvarà degut a la proliferació de virus a través de la xarxa.



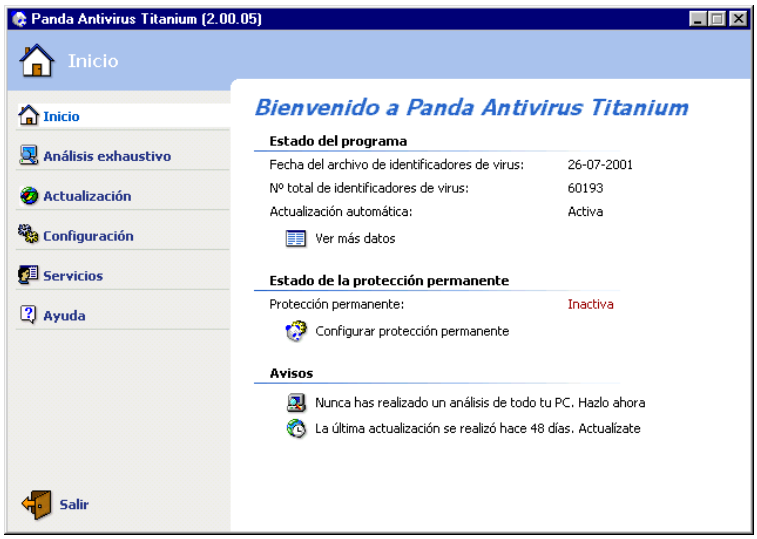
Un cop finalitzat el procés d'instal·lació podem obrir l'antivirus per a fer una primera anàlisi.

En cas de tenir l'antivirus registrat, i sempre que estiguem connectats a la xarxa, el Panda s'actualitzarà automàticament. Això ens permetrà tenir una correcta protecció.

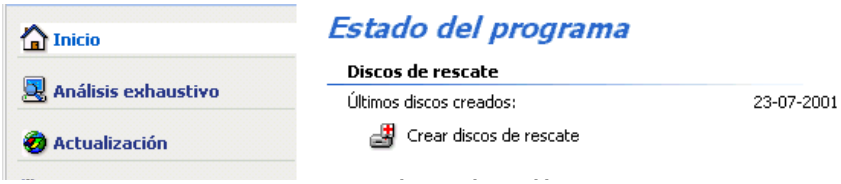


L'antivirus de Panda té una interfície molt intuïtiva que ens permet fàcilment analitzar el fitxer, carpeta, o unitat de memòria que desitgem; configurar la protecció permanent, que analitza tots els fitxers que obrim mentre treballem amb el nostre Pc; actualitzar la darrera versió, tot i que el programa ho fa de manera automàtica i d'altres útils com crear disquets de rescat nous, etc.

A la pantalla d'inici ens informa de la darrera actualització, de l'estat de la protecció permanent, activa o inactiva, i de si ens cal fer alguna tasca concreta, com per exemple una anàlisi de tot el PC.



Si cliquem a ***Ver más datos*** tenim un menú on poder crear els disquets de rescat, i on ens indica la data de la darrera vegada que ho vam fer. És recomanable actualitzar els disquets de rescat per a tenir major protecció en cas de quedar infectats.



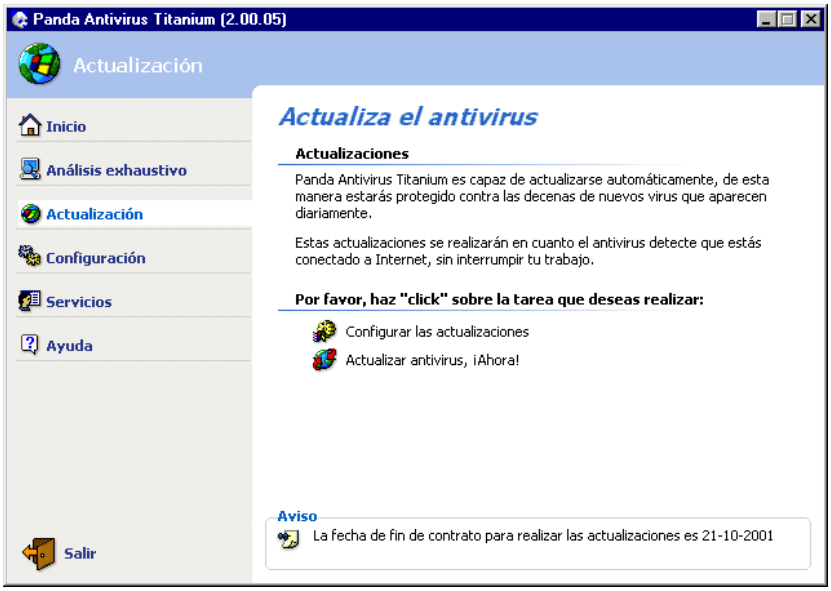
Dins el menú ***Análisis exhaustivo*** tenim diverses opcions d'anàlisi i una sèrie d'informes amb el resultat de les darreres vegades que hem fet servir l'antivirus.

Les opcions son del tot intuïtives. En triar l'opció desitjada s'inicia l'anàlisi de la mateixa i en acabar ens mostra un informe dels fitxers analitzats, infectats, etc.

2. Actualització de l'antivirus.

Dins el menú ***actualización*** podem configurar l'actualització automàtica i la notificació d'aquesta.

L'altra opció és l'actualització intel·ligent, però cal estar registrats ja que ens demana un nom d'usuari i un password.



Al menú ***configuración*** tant sols cal destacar una característica de la majoria d'antivirus. Normalment quan troben un fitxer infectat, en cas que no el puguin recuperar, el renombren com a fitxer infectat; extensions del tipus *.vir.

Al menú de ***servicios*** hi tenim les FAQ's (Frequently asked questions || Preguntes més freqüents), el suport via e-mail, bústia de suggeriments, enviament d'arxius sospitosos, etc. i dins el menú ***ayuda***, en l'apartat descripción del programa, hi tenim una breu explicació de cada un dels menús, i al link de *más información* una descripció exhaustiva del funcionament del programa amb un botó que ho imprimeix. De ben segur que serà de gran utilitat si tenim cap dubte respecte al funcionament del Panda.

Glossari de termes relacionats amb la seguretat

Certificat:
Document digital emès per una entitat independent que garanteix la identitat dels sistemes i de les persones a Internet. La seguretat del certificat està protegida per tècniques criptogràfiques.

Xifratge:
Codificació de dades mitjançant diverses tècniques matemàtiques que en garanteixen la confidencialitat en la transmissió.

Codi maliciós:
Qualsevol programa amb una intenció molesta, malèvola o il·legal. Generalment estan dissenyats perquè s'executin sense la intervenció de l'usuari.

Galeta o *cookie*:
Informació que, enviada per un servidor d'Internet al navegador, es torna posteriorment en cada nova connexió. Es poden utilitzar amb intencions legítimes, com la identificació d'usuaris, o malèvoles, com l'emmagatzematge no consentit de pautes de navegació.

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.

Correus encadenats
Són missatges de correu electrònic on es demana que el missatge s'enviï a més gent per tal que aquestes persones també els reenviïn. És una de les possibles fonts de problemes amb el correu electrònic, ja que de vegades porten notícies falses, poden ser portadors de virus, etc.

Criptografia:
Disciplina que s'ocupa de la seguretat de la transmissió i l'emmagatzematge de la informació.

Denegació de servei:
Atac informàtic que, sense que afecti la informació que conté un sistema, el deixa incapacitat per prestar cap servei. La denegació es pot aconseguir mitjançant la saturació o el bloqueig de les màquines.

Filtratge de continguts:
Conjunt de tecnologies que permeten un control de la informació transmesa per serveis d'Internet. El filtratge de continguts s'utilitza per bloquejar virus enviats per correu electrònic, per controlar l'accés a Internet de menors, etc.

Tallafoc o *firewall*:
Sistema informàtic que controla a quines màquines i a quins serveis es pot accedir dins d'una xarxa. Pot ser un sistema especialitzat o un programa instal.lat (firewall personal). Quan aquest control es realitza sobre la informació transmesa i no simplement sobre la connexió, el sistema emprat és un *Proxy*.

Tallafoc 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.

Signatura electrònica:
Informació digital associada a una operació en particular duta a terme a Internet que, juntament amb els certificats, permet garantir la identitat dels participants en una transacció.

Cuc:
Tipus de codi maliciós la característica principal del qual és que es copia d'uns sistemes a uns altres a través d'Internet.

Enginyeria social:
Tècniques que intenten atacar la seguretat dels sistemes informàtics enganyant-ne els usuaris i els administradors. La major part de les tècniques d'enginyeria social són semblants a les estafes.

Intrusió:
Atac informàtic en què l'atacant aconsegueix obtenir un control complet sobre la màquina. Durant una intrusió, l'atacant pot obtenir i alterar totes les dades de la màquina, modificar-ne el funcionament i fins i tot atacar noves màquines.

Servidor intermediari o *proxy*:
Sistema informàtic la missió del qual és fer d'intermediari entre un sistema i un altre a través d'Internet. Entre les missions d'un *proxy* hi ha el fet d'accelerar l'accés a Internet, filtrar els continguts als quals s'ha accedit i protegir els sistemes evitant-ne la comunicació directa.

Inundació o *spam*:
Correu comercial no demanat enviat a través d'Internet. El volum i el contingut de l'*spam* pot dificultar notablement l'ús de serveis del correu electrònic.

Troià:
Codi maliciós camuflat dins d'un altre programa aparentment útil i inofensiu. Els troians poden anar inclosos dins de programes coneguts, de manera que cal controlar la font d'on s'obté el *software*.

Virus:
És el tipus més conegut de codi maliciós. És un programa que es copia dins d'altres programes i s'intenta reproduir el major nombre de vegades possible. Tot i que no sempre és així, la major part de les vegades el virus, a més de copiar-se, altera o destrueix la informació dels sistemes en els quals s'executa.