Iniciación a
La Seguridad Personal

¿Quién soy?

¿Dónde estoy?

Definición de “seguridad personal”

¿Con quién me junto?

¿Qué acostumbro a hacer?

El hecho de poseer o poder manejar un ordenador hace que, aunque sea mínimamente, dentro de él almacenemos datos.

Por muy insignificantes que a veces nos parezcan, estos datos hablan de nosotr@s o bien de otras personas.

La seguridad personal sería el método por el que protegeríamos nuestros datos de miradas indiscretas, o accesos no permitidos a nuestro ordenador.

Lo que a nosotr@s puede no parecernos importante, a otr@s sí puede parecérselo.

¿En qué estoy?

¿Qué me gusta?

Información sensible

Información propia: (datos personales, trabajo, apuntes, …)

la creo,
la ofrezco o
la recojo

Información de otros:

Hay leyes que protegen los datos de carácter personal. Si alguien se hace con los datos de otros que están bajo nuestra custodia puede acarrearnos problemas legales.

¿Quién soy?

¿Qué me gusta?

¿Dónde estoy?

¿En qué estoy?

¿Qué acostumbro a hacer?

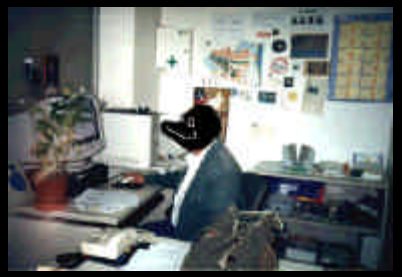
¿Con quién me junto?

La seguridad de los sistemas

Todos los S.O. son vulnerables.

El acceso local es la situación más vulnerable en todos los S.O.

Intruso conocido mundialmente debido a que cada vez que toca un ordenador, éste deja de funcionar



Formas de identificación

Iris

• *Se utiliza como sistema de control de acceso.* **Una cámara digital situada a unos centímetros de la persona lee los detalles del iris,** *que es la zona coloreada que hay alrededor de la pupila de los ojos, y la compara con su base de datos*

Rostro

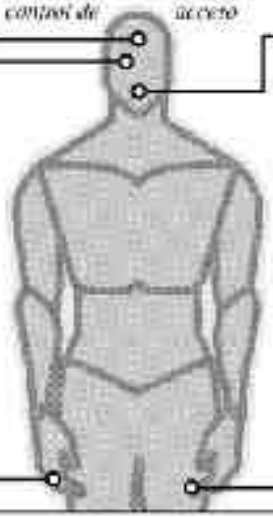
• *En el caso de sistema de vigilancia, las cámaras graban al público y los* **sistemas de rostros identifican y comparan todos los rostros con una base de datos** *en el que figuran las ya conocidas buscadas. También puede utilizarse como sistema de control de acceso*

Voz

• *Una palabra y el registro biométrico de las cuerdas vocales de la voz del usuario* **crean un modelo irrepetible que un dispositivo informático almacena.** *A partir de ahí, esa palabra y esa voz son la llave exacta e irrepetible para acceder a un determinado*

Firma

• *El usuario firma sobre un dispositivo especial, una especie de alfombrilla conectada al ordenador.* **El sistema informático compara el nombre, los rasgos, la rúbrica y la presión** *que ejerce al escribir con su base de datos*



Huella

• *La identificación mediante las huellas se utiliza desde muchos años por la policía.* **Los nuevos dispositivos biométricos permiten la informatización total del proceso** *incluso para utilizar como contraseña*

Contraseña de BIOS virtudes y defectos

No me permite arrancar el sistema.

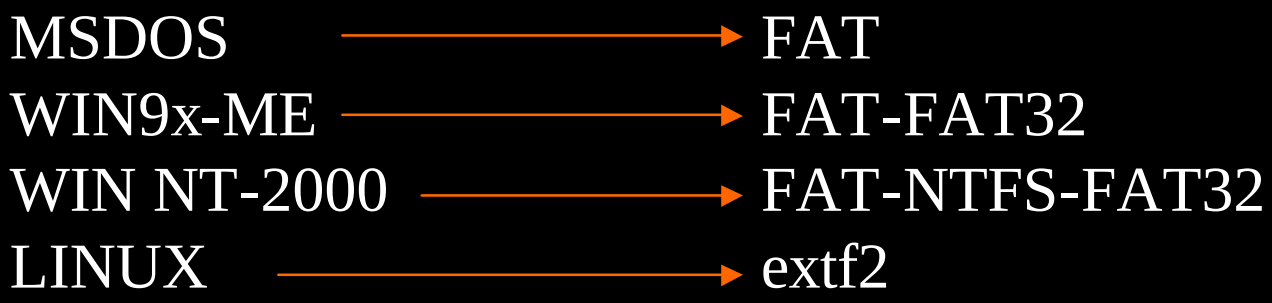
Por desgracia tiene llave maestra.

Sistemas operativos

El sistema operativo elegido como referencia es Windows 9x. (**por ser el más extendido y cuenta con un índice de usuarios más inexpertos**)
Sin embargo es importante saber que existen otros sistemas operativos, alguno de ellos incluso gratuito (conocidos como software libre).

MSDOS (corazón de los W95-98-ME)
MAC-OS
Windows 95-98-ME
Windows NT-2000
UNIX
NOVELL
LINUX

La seguridad de un sistema operativo empieza en su sistema de ficheros



Son más seguros aquellos que permiten establecer políticas de acceso a los datos.

¿Va a usar alguien más mi PC?

¿Tengo datos que no quiero que vean?

Uso de la contraseña

Contraseña pobre:
Uno de los errores más comunes a la hora de crear una contraseña es la de “hacerla facilita que tengo mala memória”

- 26 posibilidades en letras mayúsculas.
- 26 posibilidades en letras minúsculas.
- 10 posibilidades en números.

(contraseña: 7491) 10 x 10 x 10 x 10 = 10.000 posibilidades
(contraseña: mama) 26 x 26 x 26 x 26 = 456.976 posibilidades

Una contraseña un poco más útil:

Una contraseña medianamente segura, constará de no menos de 8 caracteres, entre los que se intercalarán mayúsculas, minúsculas, números y signos o espacios, vendría a ser:

- 26 posibilidades en letras mayúsculas.
- 26 posibilidades en letras minúsculas.
- 10 posibilidades en números.
- de 15 a 36 posibilidades en símbolos (depende de la aplicación)

&¡'º<_-)(

26 + 26 + 10 + 15 (x ej.) nos da un alfabeto de 77 caracteres.

Con una contraseña de 8 caracteres tenemos 77^8 posibles contraseñas o lo que es lo mismo 1,235736291548e+15 (más de un trillón de posibilidades).

Paquetes Básicos

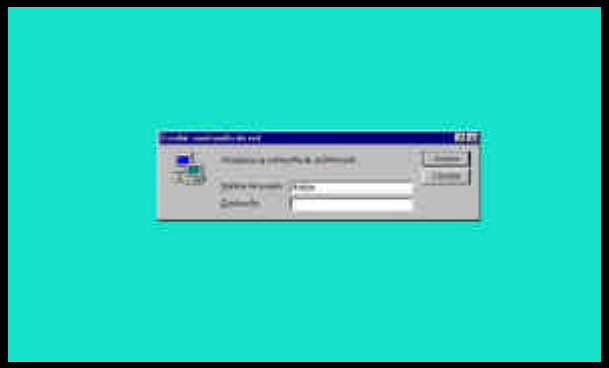
Qué nos viene normalmente con el sistema:

- Contraseña de inicio o de red
- Editor de usuarios
- Poledit

O programas de uso habitual:

- MSOffice...

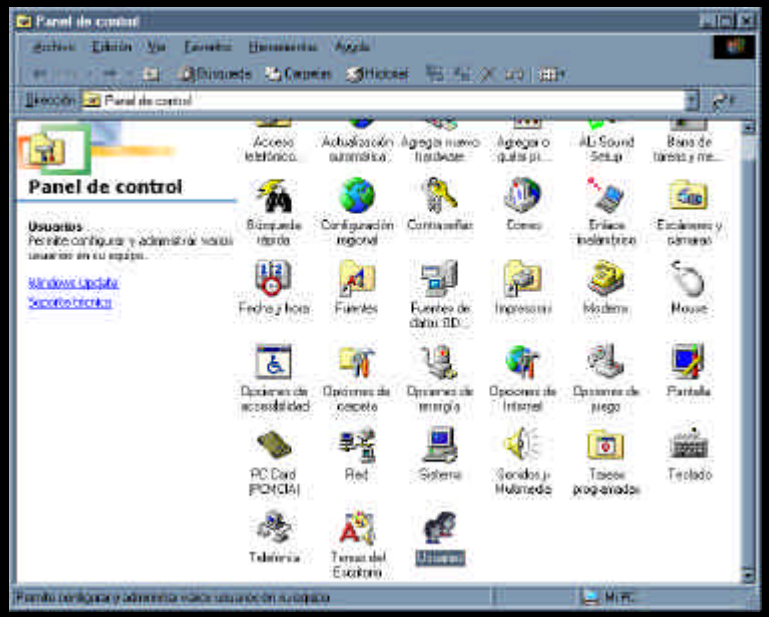
Contraseña de inicio de Windows 9x

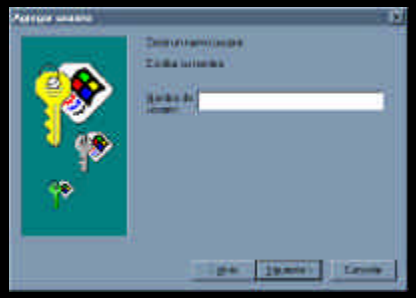


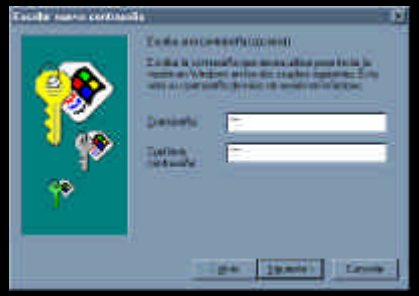
Sirve más para ordenar el trabajo por usuarios que para permitir o denegar el acceso a los datos.
Antes de llegar aquí ya se pasó por MSDOS.

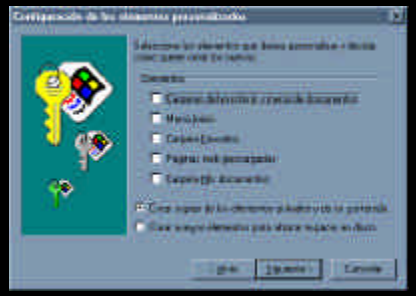
C:\WINDOWS>

Usuarios





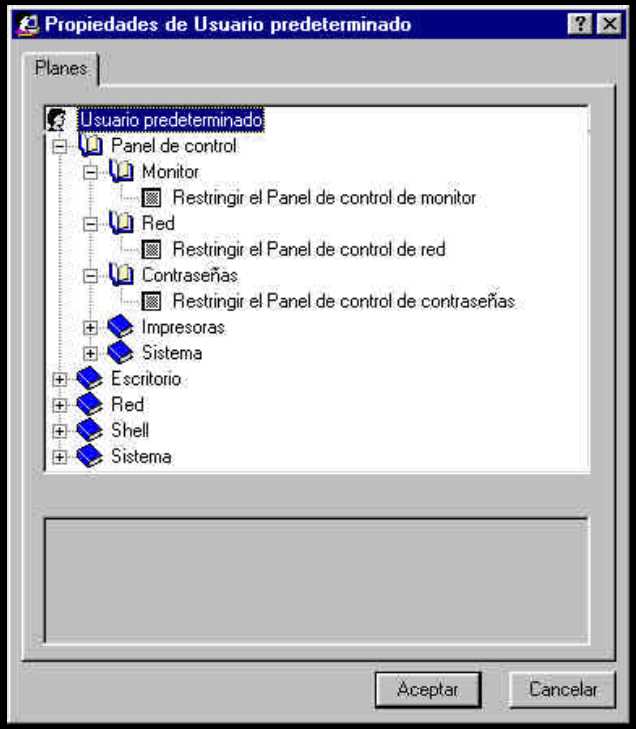




En el panel de control encontraremos una aplicación para crear usuarios. Pudiendo crear unas políticas básicas de orden y control del sistema.

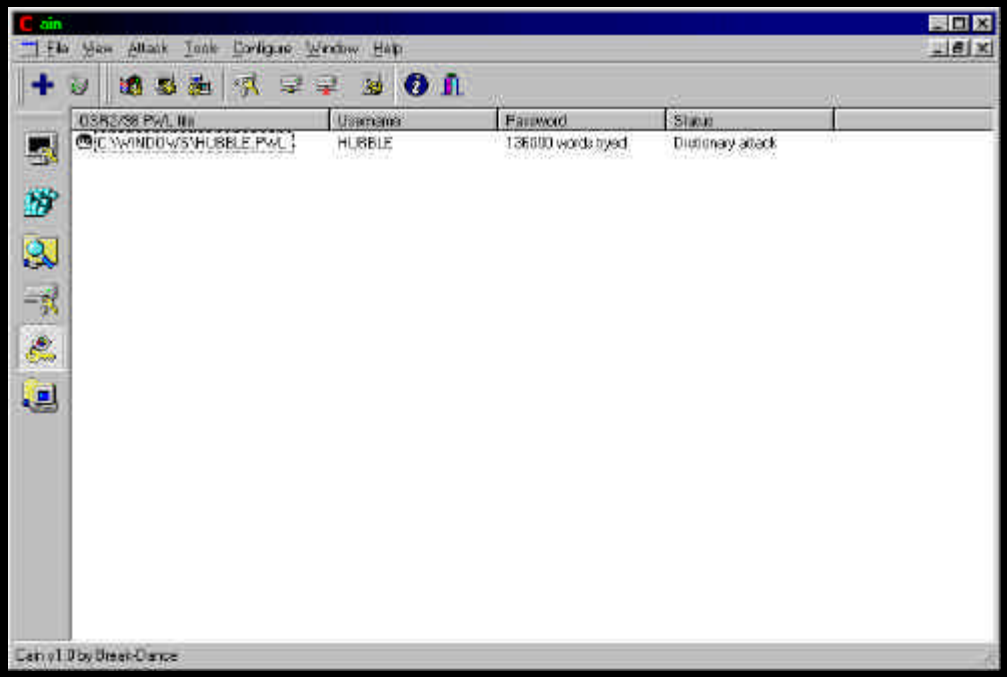
Poledit.exe

Se encuentra en el CD de instalación de Windows.



Podemos establecer políticas de usuarios y conceder según qué permisos. Sería indicado crear un usuario por defecto, que tenga restringida la mayoría de acciones, así cuando alguien acceda sin poner bien la contraseña tendrá ese perfil.

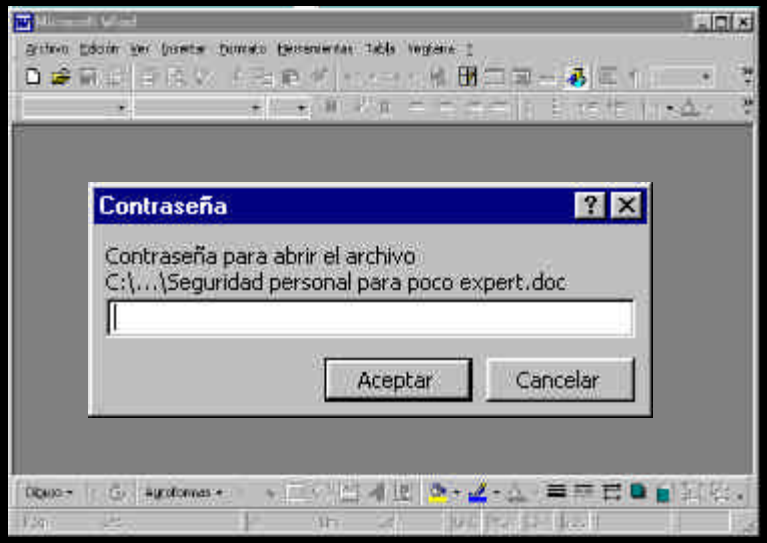
Contraseña de inicio de Windows 9x

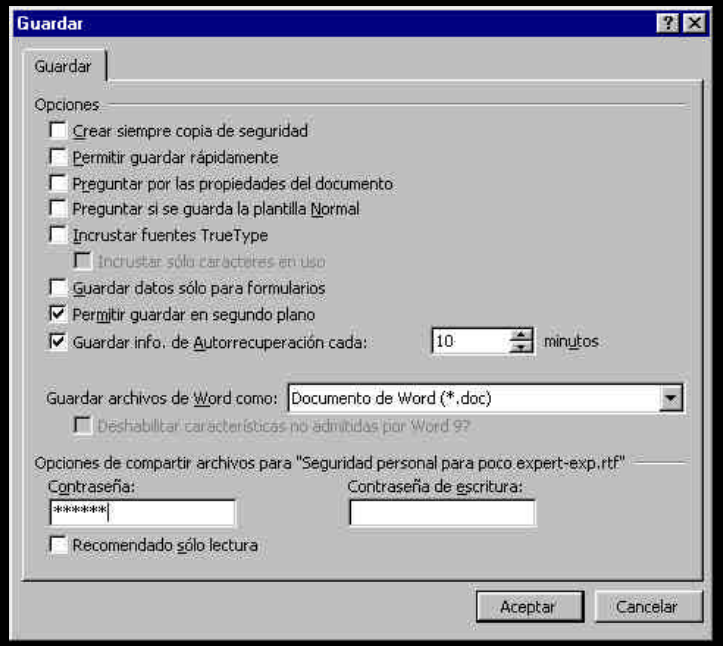


Hay multitud de programas especializados en “descubrir” contraseñas. Por ejemplo, en el gráfico el programa Cain con un buen surtido de utilidades, se usa normalmente para comprobar contraseñas, etc.

Office contraseñas de documentos

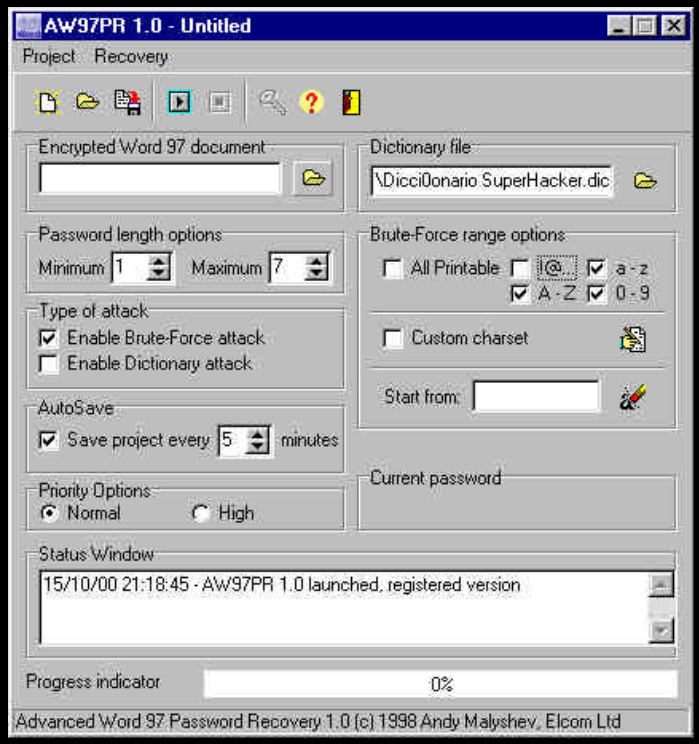
La mayoría de los programas del Office nos permite poner una contraseña al documento.





Office contraseñas de documentos

El problema está en que, aparte de utilizar un sistema propietario de encriptación, existen muchos programas para crackear las contraseñas de Office.



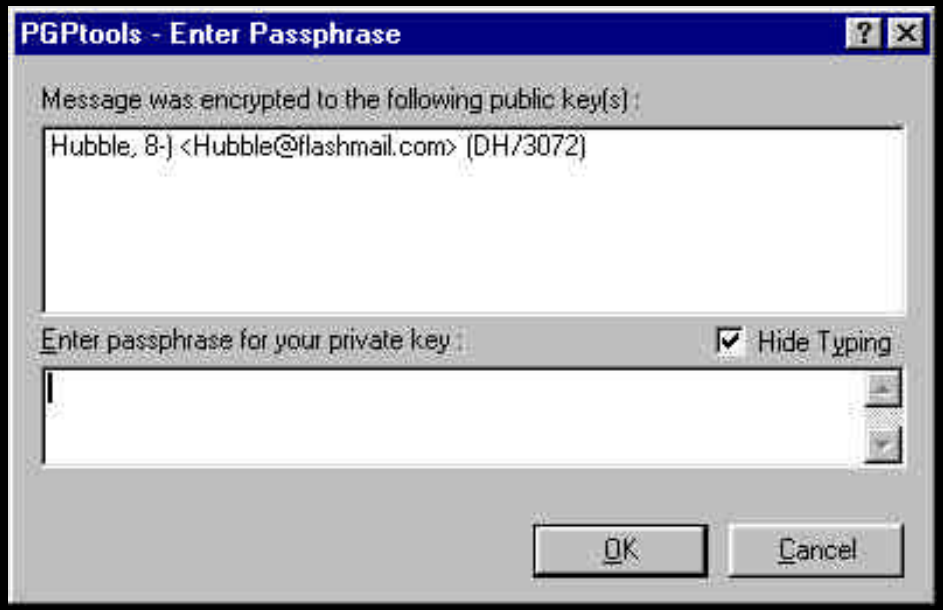
Encriptación

-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>
Comment: ***Las Claves en idap://certserver.pgp.com

hQEMAwAzyqlQ+OuLAQf7Bxj6HpFppqid4DRSVq1oeunH2gyJosY5h2aFRcbQM/fy
xcHYj4eNzFqkmhapnYuHcO3VaccgE6xNB7lA7uPsqH07BtK9IdM2hg3j3eAd44q1
ax6MJtM9eRjU33tw04PxEggmVAiEvqhKCtfcxCrFgJ4d0RTfHQtRPwpihtJ2d/U2
3nDyRnmCk++PQVAZ1MxU9ZLpi3WhRBimoB8sEqne2y6fS/p2E/aSQm/+zzP8PI47
7zjA/slrqRw1whThpmfH/yoPE+JlZLLb6OPSkGM7wXeQg/pER19yF/ergKsA13cm
WHyaQUG855K1IGYGjocwYmJOCnlnbbRuxyq6xciJBKSpGbLA6S6zY0fry9Spcail
tMTuVKalr1zmjw57ATEjRD7rspgYMH5REU4wXF5JNlURBDw/gI0eAGoB3wKQ7YoX
TIIzANU+YJeorhWPbrOo0zQrvRno16O3Ajwys5HrbDTv/dZsTEV1gN6PhOEoUKLF
leRWF3Mn8QeZ5/fq07HFt38BEoWirPasaDuT2qsl+aolWOwIOCJge0O16BugcUcB
NDwo4zbHOUxbeA==
=SoPE
-----END PGP MESSAGE-----

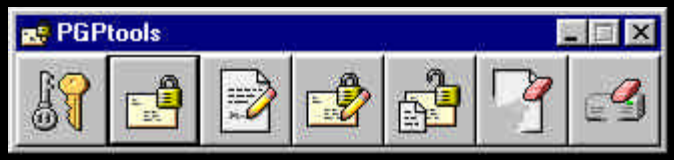
Encriptación

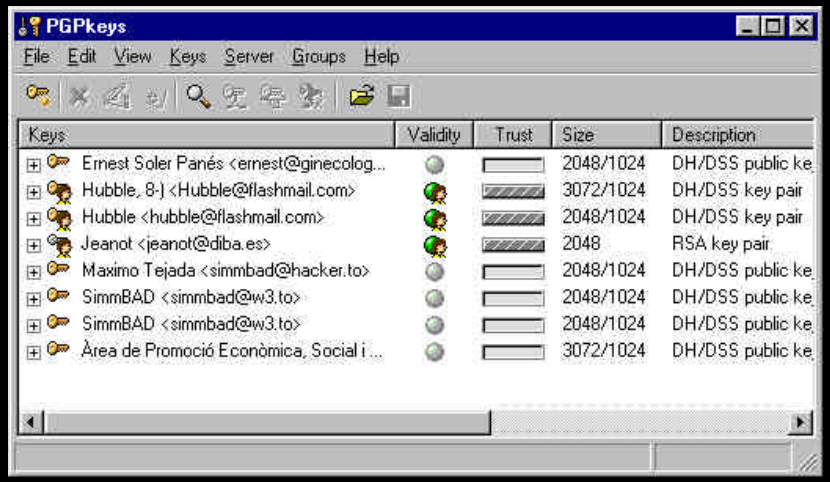
A veces el sólo hecho de encriptar un mensaje nos hace sospechosos delante de los organismos de control social, por que **¿para qué se necesita encriptar una información si no es que se está haciendo algo malo?**

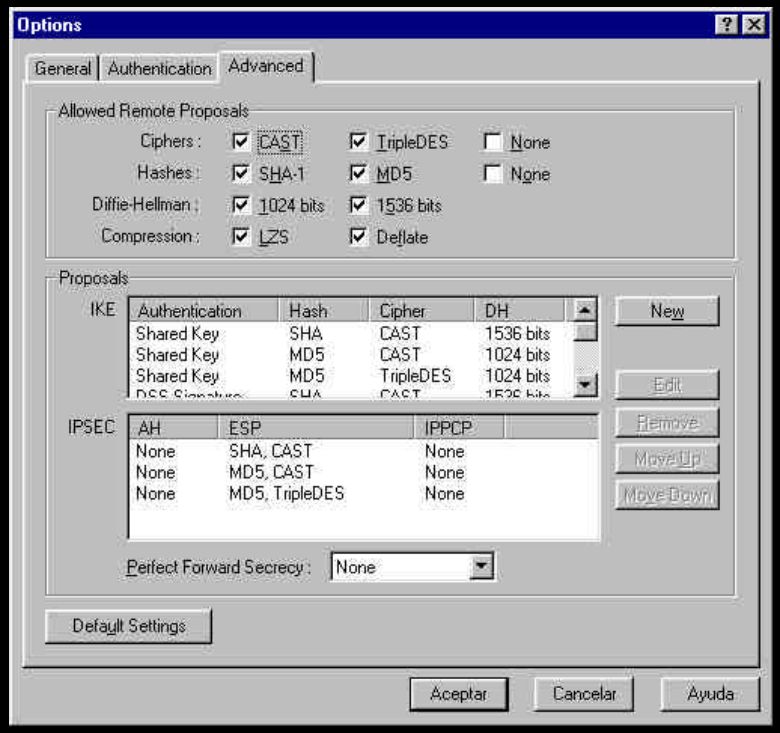


PGP
clave pública
clave privada
contraseña
vulnerabilidades

Encriptación







PGP es un software gratuito (para uso no comercial), viene con bastantes herramientas que nos facilitan su uso.

Sólo necesitamos la llave pública del destinatario para enviarle un mensaje encriptado.

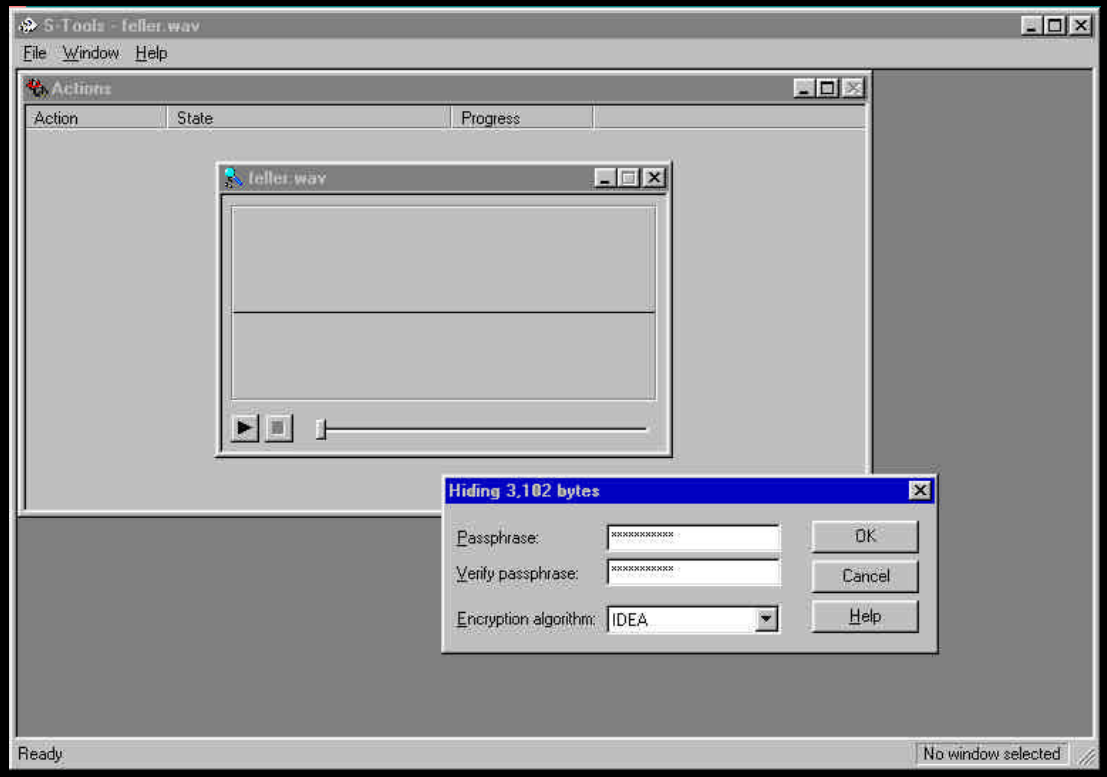
Sin embargo todas esas funcionalidades están haciendo que se vuelva vulnerable.

Existe encriptación para diferentes S.O., entre ellos para LINUX.

GNU-PG hace lo mismo y es software libre.

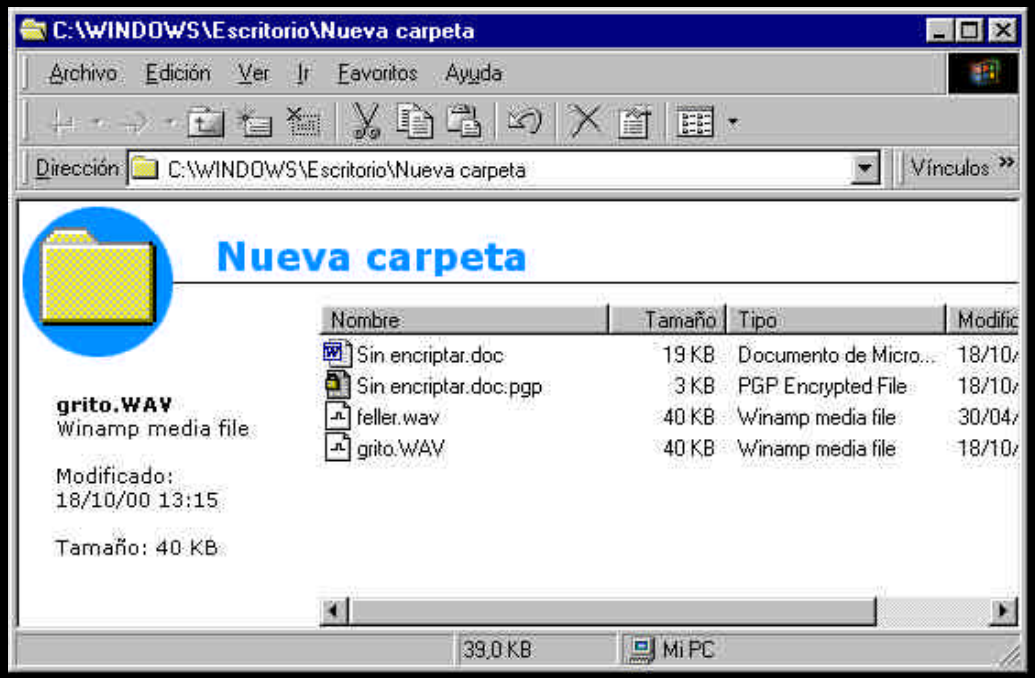
Esteganografía

En resumen, se trata de mezclar un fichero (en el que tenemos los datos sensibles) dentro de otro fichero, bien sea de imagen BMP o de sonido WAV, de apariencia totalmente inocente.



Esteganografía

El fichero creado seguirá teniendo las funciones que antes tenía, es decir el de sonido seguirá sonando y el de imagen seguirá presentando la misma imagen.



Si encripto un fichero y luego lo esteganografío en un WAV (x ej.) puede llegar a ser casi imposible descubrir mis datos sensibles

Virus:

Los **virus** son **programas**, y como tales no funcionan hasta que los **ejecutas**.

No todos los virus producen daño en el ordenador, muchos de los llamados virus simplemente son una broma.

Tener un **programa antivirus actualizado** es fundamental.
Hacer **copias de seguridad** de nuestros datos nos evitará muchos problemas.

No ejecutes nada nuevo sin antivirus. Vigila los documentos de Office de los demás (**macros**)

SEGURIDAD INFORMATICA PERSONAL II.

REDES

USO de ordenador en red e Internet

WEB

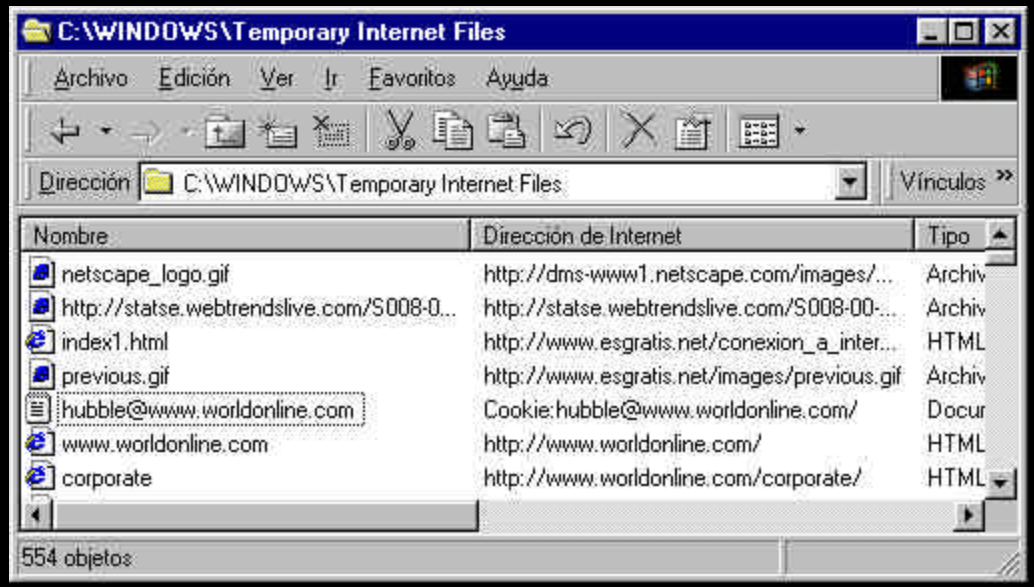
Cuando navegamos por la WWW, conforme avanzamos, siempre vamos dejando un rastro sobre nosotros, que nos puede parecer más o menos importante, pero que las empresas (entre otr@s) están dispuest@s a recopilar.

¿No os resulta extraño que si hace poco visitasteis una página de música, al visitar otras páginas os aparezca un baner en donde precisamente os anuncian algo relacionado con la música?
Double-click es una empresa que se dedica expresamente a eso.

El presidente de Sun Microsystems vino a decir en una ocasión: "La privacidad no es un problema. Olvídese de él. La privacidad ya no existe".

Cookies

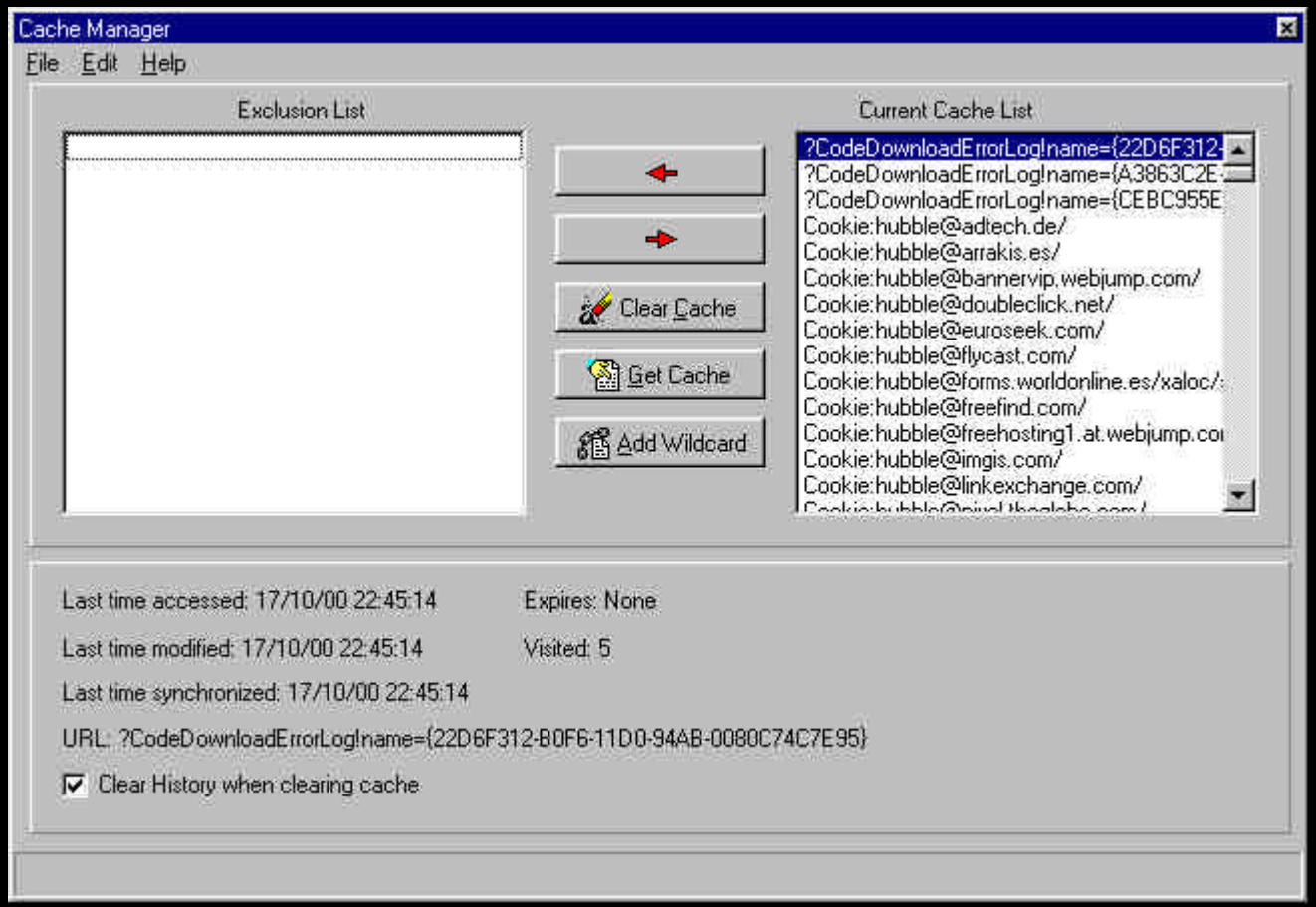
Las cookies son pequeños ficheros de texto, que algunos (hoy día la mayoría) de los servidores nos colocan en el ordenador.
Teóricamente son para hacernos más agradable la navegación por esa web (va guardando datos de cómo nos gusta la página, nuestra configuración, etc.).
El problema es que esa información la pueden recoger para ellos o para otros, y para esos fines o para otros menos “éticos”.



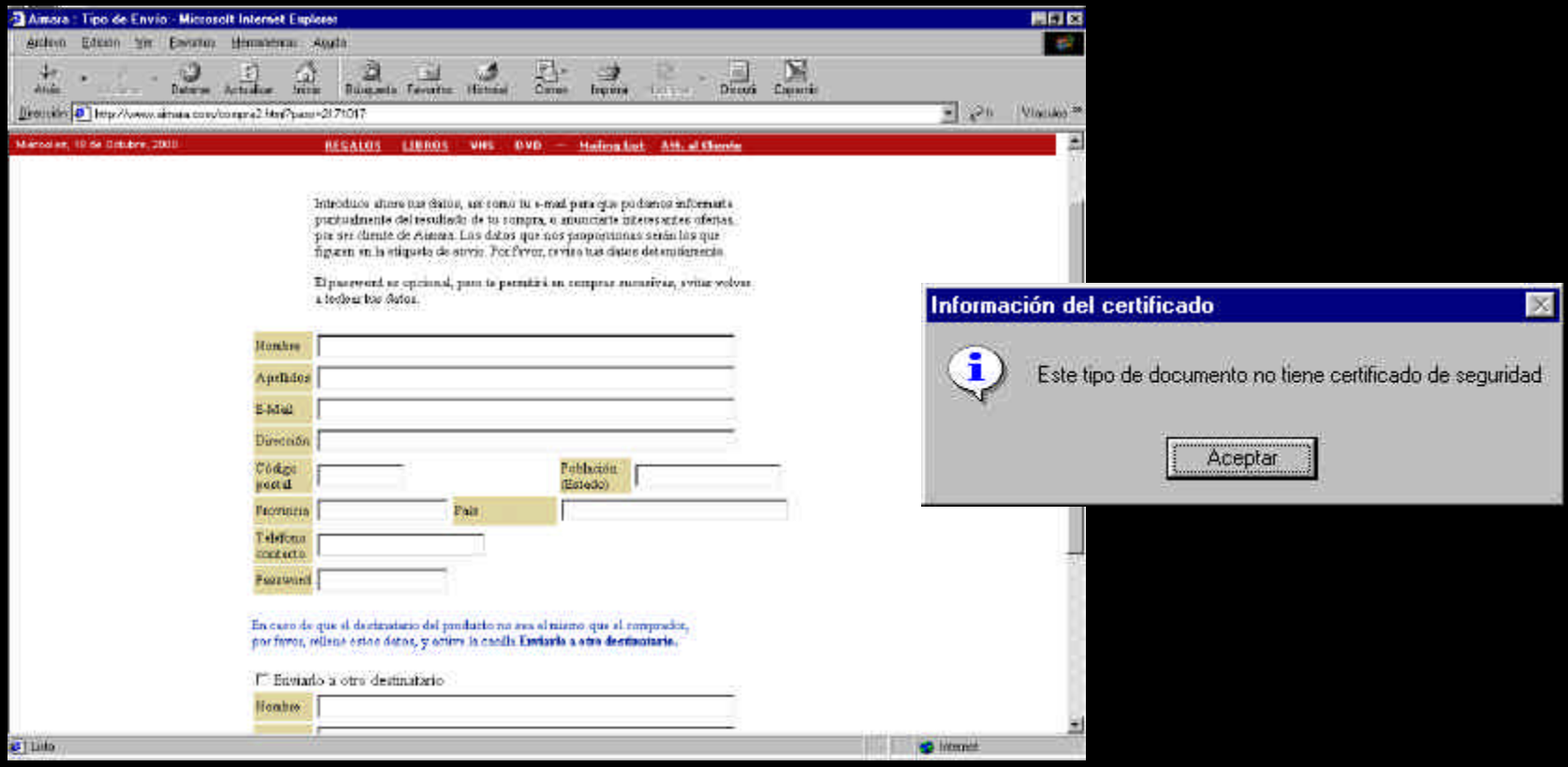
Limpiadores de caché y cookies

Hay programas por la red, algunos gratuitos, que nos limpian las cookies que hayamos recogido durante nuestra navegación, pudiendo borrar también el historial, ganando en intimidad y espacio.

Este se llama IETool, gratuito, y nos limpia las cookies y la cache siempre que queramos.



Formularios



En los formularios que nos encontramos vamos dejando datos a la ligera que otros pueden recopilar o espiar (visa, etc.).
En este ejemplo, aunque dicen que la transacción es segura, se puede comprobar que no lo es por la dirección y ausencia de candado.

Formularios

Es más, algún “desaprensivo” podría copiar una web de transacción, hacernos creer que estamos en el lugar al que queríamos ir y apoderarse de nuestros datos personales, etc.

Los datos que dejamos no desaparecen, normalmente alguien los guarda y puede mercadear con ellos, es cuestión de ir identificándote poco a poco, para poder obtener un perfil de ti mism@ que ni tan solo tú conoces o te podría dejar sorprendid@..

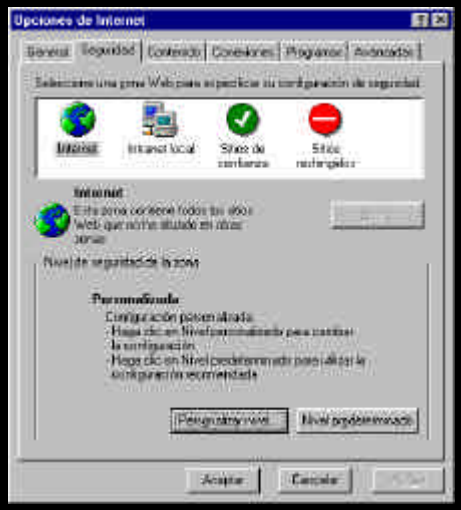
Java

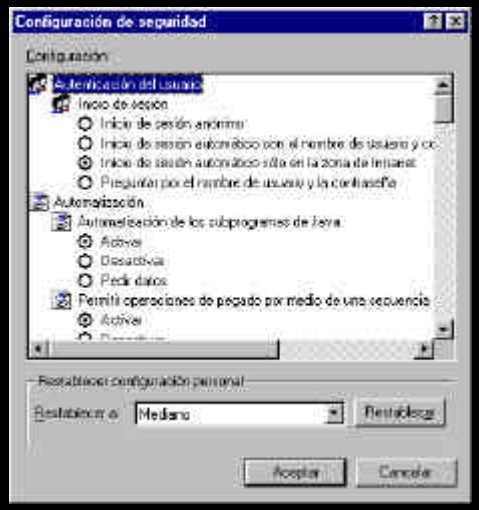
El java es un lenguaje de programación, y en Internet se usa sobre todo para enviar pequeños programas desde el servidor hasta nuestro PC, donde se ejecutará.
No es necesario decir lo peligroso que puede ser esto, sin embargo, su imposición en la web va cada día en aumento.

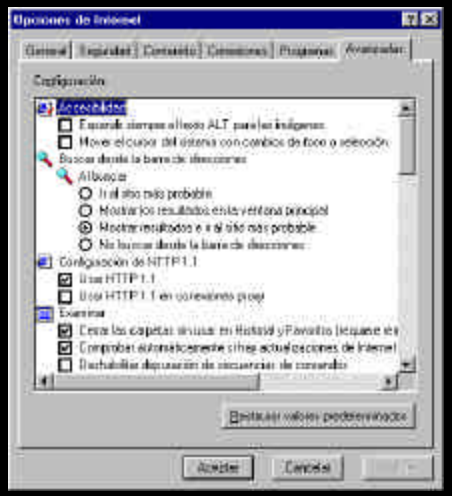
Controles Activex

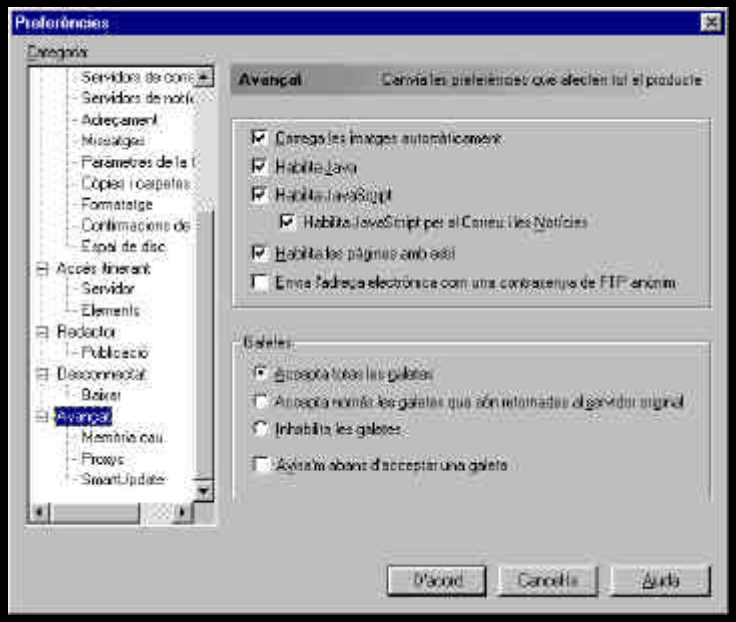
Son programitas como en el caso de java, pero en otro lenguaje. El peligro que entrañan es el mismo, aunque quizá mayor ya que es de Microsoft y con ellos ya se sabe...

Seguridad de los Navegadores









Tanto Netscape como Iexplorer nos permiten habilitar y desabilitar cookies, controles activex, java, etc. Sin embargo ello puede hacer que algunas páginas web no se vean como debieran e incluso que se nos deniegue el acceso a la página.

Seguridad de los Navegadores

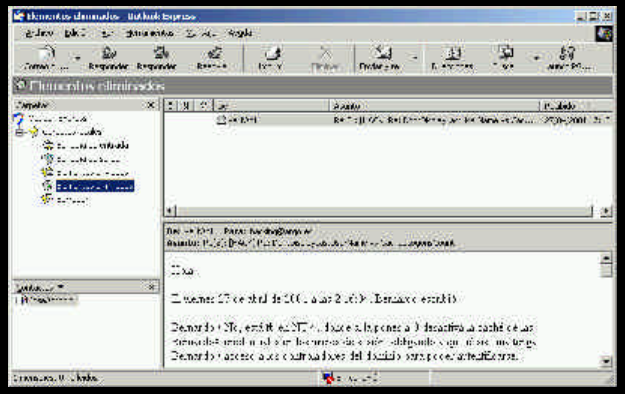
A pesar de la constante actualización de las versiones de los navegadores, se ha de tener en cuenta que a los pocos días (o antes) de sacar una nueva versión, ya se descubren nuevos agujeros de seguridad en ellos.

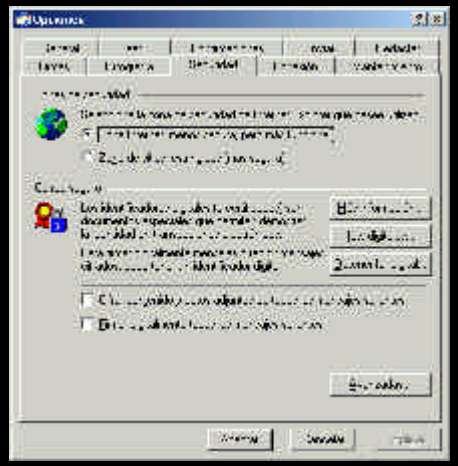
Hay quien se pregunta si todos esos agujeros (que a veces se niegan en reparar) no los dejarán a propósito.

Los navegadores acostumbran a tener alguna opción de actualización, (en IE Herramientas/windows update) que nos llevará a una página oficial del navegador, en donde nos testearán y nos aconsejarán sobre las últimas actualizaciones para hacer más ¿seguro? el navegador.

Correo electrónico

Quizá el mejor sistema de comunicación en la distancia.
Escribimos un mensaje y a los 10 segundos el destinatario ya puede leerlo.
Sin embargo es una de las puertas de entrada a nuestra intimidad más utilizada en la era internet.
Spam (correo no deseado), virus, troyanos, e incluso “amenazas anónimas” son cosas con las que diariamente nos podemos encontrar a la hora de abrir nuestro correo.





Spam

Resulta curioso, el hecho de visitar una web sobre cocina, y al día siguiente empezar a recibir un alud de correos que nos ofrecen desde ollas a presión hasta ajos de Calasparra.

Nosotros no pedimos ese correo, pero sin embargo hemos de pagar el gasto telefónico de bajarlo a nuestro PC e incluso que nos llegue a saturar nuestro buzón de correo impidiendo recibir aquellos mensajes que sí queremos.

No es aconsejable clicar en la dirección en donde dicen que no nos enviarán más correo, ya que con ello se aseguran que nuestra dirección de correo sí existe, el hecho que ya nos hayan enviado un correo no deseado nos demuestra que su ética deja mucho que desear.

Correo WEB

Son correos en los que para enviar o leer debes de conectarte a través de un web. algunos son Hotmail, terra, flashmail, etc.
Uno de los mayores problemas es el de la seguridad de la base de datos de los usuarios, y la facilidad de saltarse muchas contraseñas. Otras veces el programa que gestiona la web tiene agujeros de programación

Virus

Los **virus** son **programas**, y como tales no funcionan hasta que los **ejecutas**.

No todos los virus producen daño en el ordenador, muchos de los llamados virus simplemente son una broma.

Tener un **programa antivirus actualizado** es fundamental.

La mayoría de antivirus actuales tienen alguna implementación que les permite monitorizar constantemente la entrada de correo y avisarnos si llega algún virus (conocido por él).

Hacer **copias de seguridad** de nuestros datos nos evitará muchos problemas.

No ejecutes nada nuevo sin antivirus. Vigila los documentos de Office de los demás (**macros**).

Troyanos

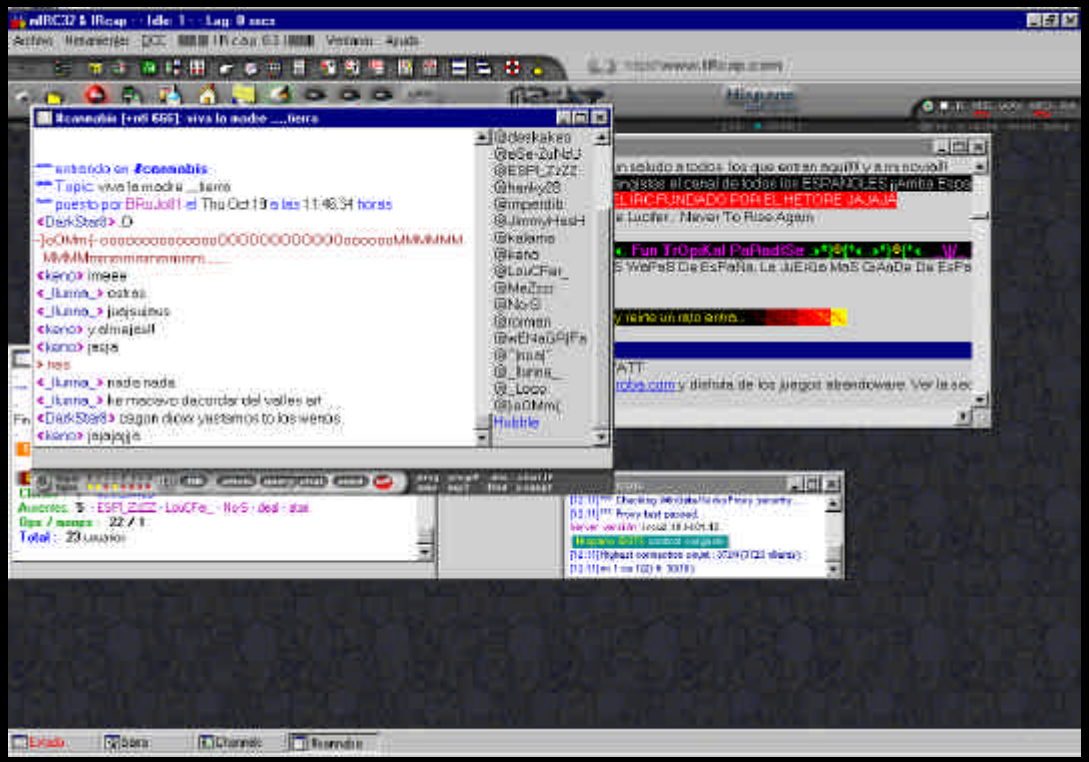
Se les llama así haciendo honor al caballo de Troya de la mitología griega. En definitiva es instalar un programilla en tu ordenador, sin que te des cuenta y por eso se usa muchas veces el correo.
Su misión es, en el momento que estás en la red o Internet, avisar a su propietario bien con un correo o bien a través de un canal de IRC, a donde le envía tu IP, sabiendo esto, y gracias al programa, el “desaprensivo?” puede tomar el mando de tu ordenador y trabajar en el como si estuviera físicamente delante del teclado.
La mayoría de troyanos tienen usos muy normales, como el de mantener ordenador a distancia.
Los programas antivirus suelen detectarlos.

IRC

Es el Internet Relay Chat, fueron los primeros chats que se crearon y se siguen usando.

Hay multitud de canales y servidores.

Sus problemas vienen a ser los de que te baneen (te saquen del canal), te envíen un virus o un troyano o te produzcan una denegación de servicio, o te nukeen (IRC-war).



Comunicadores instantáneos

Sirve para comunicar a la red que estás en linea. Existen diversos programas, AOL, ICQ, MSN, etc.

Además puedes enviar correo, hacer chat personalizado o no, hablar o usar webcams.

Siempre han sido vulnerables en muchos aspectos, desde el servidor de las empresas, hasta el propio programa cliente.

Firewalls

Son sistemas diseñados para prevenir el acceso no autorizado, tanto de usuarios como de aplicaciones a o desde una red privada, en general para intrusos desde Internet.
Se pueden utilizar por hardware (un ordenador u máquina especializada) y también por software, algunos de ellos gratuitos

Firewalls

Algunos, como el Esafe, disponen de antivirus y controlan los ficheros de Word, escaneándolos ántes de abrirlos.

Anonimizadores

Atendiendo a la falta de intimidad personal que existe en Internet, se han creado una serie de servicios para poder tanto navegar como enviar correo electrónico, sin dejar rastro de nosotros.
Para páginas web se puede visitar http://www.anonymizer.com/

Anonimizadores

También existen remailers anónimos, tu les envías un correo con un cliente de correo, la información se encripta, va a la máquina que está en Internet, le borra la cabecera con tus datos, le agrega un número de identificación (por si te contestan) y lo envía a su destinatario o bien a otro remailer.

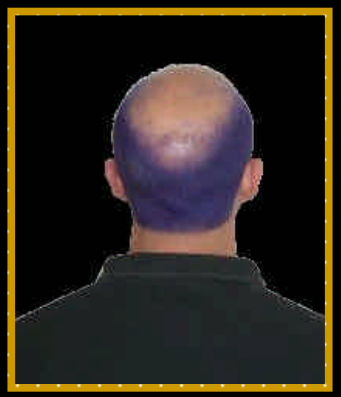
Hay servicios de anonimato gratuitos y otros de pago, más información en http://www.kriptopolis.com

Esto sólo ha sido una pequeña introducción a la seguridad personal, sin embargo no está de más que intentes descubrir por ti mism@ las dudas que puedas tener en este campo de la informática.

Un página para empezar puede ser la española:

http://www.kriptopolis.com

Agradezco a toda la red mundial y en especial a las denominadas zonas oscuras, la información que con el tiempo me han podido transmitir y me ha ayudado a poder transmitiros estos pocos conocimientos.
Las ideas deben de ser libres y por lo tanto la información también. Sin información no puedes llegar a hacerte la idea.



Hubble@flashmail.com