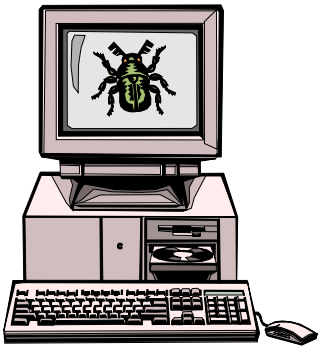
# CAPÍTULO 14:

# Otros temas



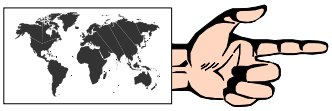
## Virus en Internet

Los virus de computadora son pequeños programas que han sido desarrollados para alterar el normal funcionamiento de las computadoras, sin la autorización o sin el conocimiento del usuario. Para obtener la categoría de virus, se deben cumplir dos condiciones: 1) que se ejecuten a sí mismos, y 2) que se repliquen.

Hasta hace unos pocos años la forma más común de que una computadora se contagiara de un virus era a través de disquetes que pasaban de mano en mano. Desde el primitivo "**virus de la pelotita**" (Ping–Pong), pasando por el renombradísimo ***Michelángelo***, hasta los muy peligrosos ***macrovirus*** y ***gusanos***, los usuarios de computadoras han debido recurrir sistemáticamente a las vacunas y antivirus para evitar males mayores.

Hoy en día, el empleo de Internet por parte de millones de usuarios en todo el mundo, es una plataforma continua de lanzamiento de nuevos y más peligrosos virus. En la actualidad hay unos 57000 virus en Internet, y se estiman en 750 los virus nuevos que aparecen cada mes.

Esto hace que las versiones de antivirus queden rápidamente desactualizadas y siempre por detrás de la realidad. Algunos de los más reconocidos antivirus, con sus versiones de prueba gratuitas, pueden descargarse en:



**Norton Antivirus Symantec**
**http://www.symantec.com/region/mx/**

**Kaspersky AVP**
**http://www.avp-es.com/**

**McAfee**
**http://www.mcafee.com/**

**DrSolomon's**
**http://www.drsolomon.com/**

**Panda**
**http://www.pandasoftware.es/es/**

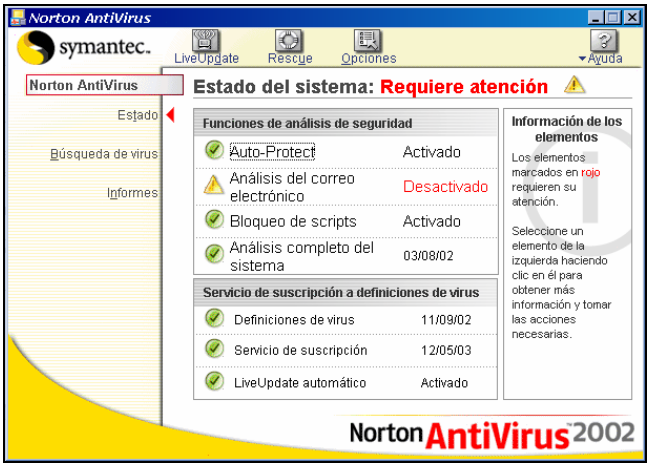


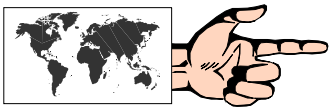

**Fig. 14.1:** Ventana principal de Norton Antivirus 2002 donde se detalla el estado del sistema.

Sin embargo, el “virus” más conocido de Internet, el **Good Times** (del cual se empezó a hablar en 1994) fue y es solamente un rumor que se hechó a correr, y como tal causó gran alarma entre los navegantes de la Red.

En efecto, se decía que si se recibía un mensaje por correo electrónico, cuyo subject (“Tema”) decía textualmente *“Good Times”* , y se lo abría, un virus formatearía el disco duro del usuario.

Miles de usuarios, que anteriormente habían recibido mensajes de advertencia en este sentido, se hicieron eco de los mismos y replicaron la cadena en forma exponencial.

Pueden consultarse las siguientes páginas en la Web con información acerca de los virus falsos y mitos sobre los mismos en:



**http://www.vmyths.com/**
**http://www.xtec.es/~vfeliu/falvir.htm**

Sin embargo, es bueno dejar en claro que, por lo menos en la actualidad, no existe ningún virus que pueda afectar una computadora por el solo hecho de leer un mensaje de correo electrónico, ya que se trata de una información textual que no puede ser ejecutada, y que por lo tanto, no puede activar ningún programa.

Distinto es el caso de aquellos mensajes que vienen con un “attach”, es decir, con un archivo insertado, el cual sí puede ser un virus que al ser ejecutado contagie la computadora.

En estos casos, obviamente, conviene -antes de abrirlos- escanear dichos archivos con un buen antivirus.

En este sentido, también deben tomarse precauciones al bajar un archivo desde la Web vía FTP, sea éste comprimido o no. Y al decir “archivos” también se hace extensivo a applets de Java, controles ActiveX o cualquier otro plug-in.

Otro tipo de virus que se ha extendido en Internet, y que es distinto a los virus tradicionales, son los denominados **“virus de macro”**, o **macrovirus**, que no dependen del sistema operativo y que además infectan documentos (en especial los de Word 6 y posteriores) en lugar de programas.

Para este caso también valen las precauciones citadas anteriormente: escanear antes de abrir un documento .doc. Es de destacar que estos “virus de macro” también se han extendido a otras aplicaciones Office tales como Excel y Access.

Finalmente, los **virus de gusano (worm)** son programas que crean réplicas de sí mismos sin necesidad de un archivo anfitrión. Son altamente autoreproductivos ya que se autoenvía a todas las direcciones de correo electrónico que encuentra en el programa cliente de correo (por ejemplo Outlook Express) del usuario infectado, difundiéndose de una manera exponencial a través de toda la red.

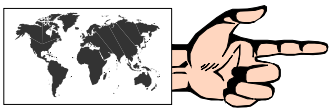
Un párrafo aparte merecen los denominados **caballos de Troya**, ya que no son virus (porque no crean réplicas de sí mismos) sino “impostores”, archivos que parecen tener una función deseable pero que en realidad son malignos.

## Traductores

Tal como se vio en el Capítulo 1, el inglés es el idioma predominante en la Web. Por dicho motivo, y ante la escasez de contenidos en español en algunos temas, es muy frecuente que se tenga que recurrir a páginas que se encuentren en la lengua de

Shakespeare y eventualmente en otro idioma. Para salvar este inconveniente, existen en la Web algunos servicios de traducción automática *online*, que si bien se limitan a traducir prácticamente "palabra por palabra" sin tener en cuenta la estructura gramátical, pueden ser de mucha utilidad a la hora de extraer algunas ideas base.

Los sitios más reconocidos en este sentido son Altavisa Babelfish y Free Translation. En ambos la mecánica es muy similar, al igual que los resultados. Primero se deberá elegir el tipo de traducción entre idiomas (por ejemplo Inglés a Español); luego si sólo se desea una frase se podrá tipear en el lugar asignado a tal fin y pulsar "Translate". En caso de querer traducir toda una página, se deberá indicar la dirección http, y pulsar "Translate."



**Free Translation**

**http://www.freetranslation.com/**

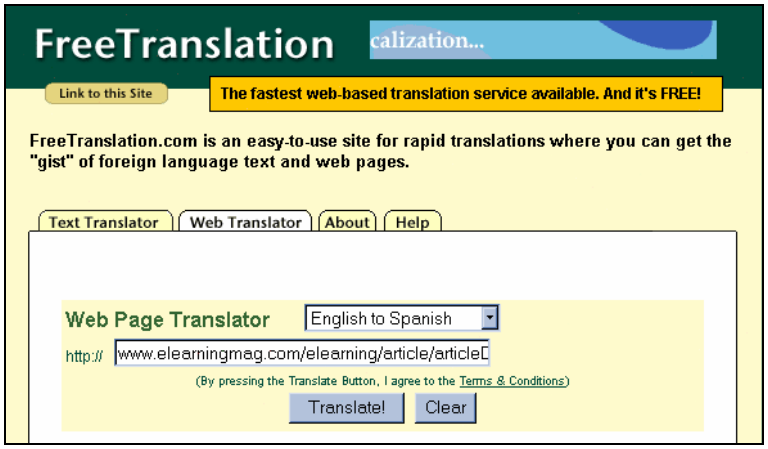
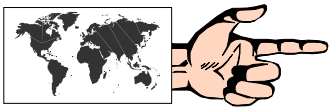



**Fig. 14.2**: Ventana para introducir el link a traducir en Free Translation.



**Altavista**

**http://babelfish.altavista.com/**

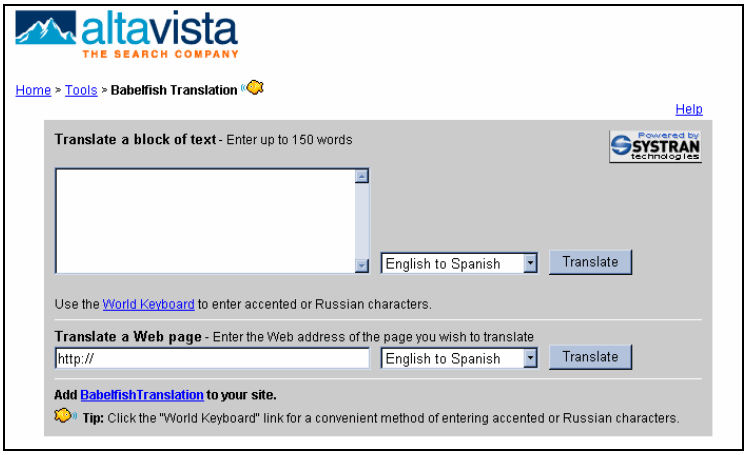
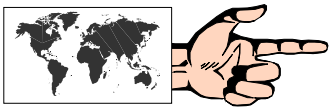



**Fig. 14.3:** Ventana para introducir texto o link a traducir en Altavista.



Otra opción, también muy usual, es emplear programas de traducción que previamente deben ser instalados. El más empleado por los usuarios de Internet es, sin lugar a dudas, **Babylon Translator**.

**http://www.babylon.com**

Este utilísimo programa permite conocer, en forma instantánea, el significado de un término, y eventualmente las acepciones de la palabra en el idioma de origen. Babylon se carga cada vez que se enciende la computadora, y queda en forma residente sin ocupar demasiados recursos. También dispone de la posibilidad de guardar el diccionario completo en el disco duro, con lo cual no se necesitará estar conectado a Internet para conocer la traducción de una palabra. La forma de operar es muy simple: se sitúa el cursor sobre la palabra a traducir y se pulsa la combinación de teclas que se haya elegido en la configuración inicial (por ejemplo: CTRL + botón derecho del mouse), e inmediatamente se obtendrán los resultados.


**Fig. 14.4:** Ventana principal de Babylon. Puede observarse la traducción según el Diccionario Inglés-Español, y la posibilidad de acceder a distintas acepciones de la palabra "Learning".

Finalmente, Babylon también dispone de un convertidor de medidas y monedas, el cual puede ser extremadamente útil teniendo en cuenta que brinda una información sumamente actualizada.


**Fig. 14.6:** Proceso de conversión automática de monedas en tiempo real mediante Babylon.

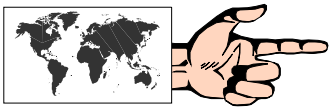
## Weblogs

Los weblogs, blogs, o simplemente bitácoras (en español) son un nuevo e interesante fenómeno que ha inundado Internet en los últimos meses. Básicamente, un weblog es una herramienta que permite a una persona, un grupo de personas, una empresa, o cualquier tipo de organización, expresar sus ideas en forma inmediata y cronológica, a través de posteos que van quedando registrados en una página web ad-hoc. La diferencia, con respecto a los tradicionales foros de discusión (Ver Cap. 6) se basa en el armado de todo un entorno (artículos base para la discusión, links a otros sitios, referencias cruzadas, etc.) que hace mucho más dinámico este espacio. La riqueza de los weblogs estriba en la continua actualización de contenidos que van incorporando el autor y los visitantes del sitio.

Las funciones que puede cumplir un weblog son variadas: ser una herramienta de intercambio de información y de comunicación para gente relacionada a un tema específico, o simplemente un espacio de difusión y entretenimiento de su autor. En la actualidad hay weblogs para todos los gustos y en todos los idiomas, desde los más triviales a los más académicos y formales. Se calcula que al día de hoy hay más de medio millón de weblogs en actividad.


**Fig. 14.7:** Un modelo de Weblog.

Para la creación de los weblogs se requiere de programas que cumplan con esta función. Los más conocidos y utilizados son:

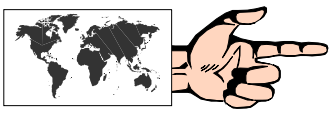


**Blogger**
**http://www.blogger.com**

**Movable Type**
**http://www.movabletype.org**

**Greymatter**
**http://www.noahgrey.com/greysoft**

Un muy completo directorio de weblogs en español puede encontrarse en:



**http://www.blogdir.com/**

donde también hay tutoriales muy claros acerca de la instalación de los programas mencionados.

## Intranet

Una **intranet** es "*una red corporativa, privada, que utiliza las mismas tecnologías y servicios que Internet*".

Básicamente, las intranets son:

- redes privadas, o sea que no pueden ser accedidas por el público en general; y
- utilizan el protocolo de transmisión TCP/IP y los servicios propios de Internet.

De lo anterior se desprende que no es necesario tener conexión a Internet para implementar una intranet.

Las empresas, fundamentalmente, son quienes en los últimos años han comenzado a instrumentar este tipo de redes en función de:

- encontrar información rápidamente;
- publicar información con facilidad;
- colaborar con otros miembros de la intranet.

Por otro lado, la estructuración de la información interna a través de links hipertextuales aporta familiaridad a los usuarios que ya han hecho sus primeros pasos en Internet, con lo cual se evitan pérdidas de tiempo en capacitación.

Obviamente, uno de los temas más importantes de la implementación de una intranet, consiste en prever un eficiente sistema de protección y seguridad contra accesos no autorizados que podrían no sólo acceder a información reservada sino también poner en peligro el correcto funcionamiento de la propia red.

El tipo de **"barrera de protección"** que se establece entre Internet (red externa) y la intranet (red interna) se denomina genéricamente **"firewall"** (literalmente "*paredes de fuego")* y es el sistema que posibilita el nivel de seguridad requerido.

En las instituciones educativas el concepto de intranet está directamente relacionado con:

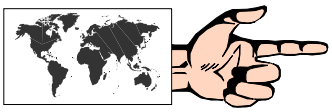
- La posibilidad de seleccionar los contenidos de las páginas web a visitar por los alumnos, evitando así los sitios pornográficos o agresivos.
- El costo relativamente bajo de su implementación.
- La facilidad de trabajar en un mismo entorno de trabajo que Internet, aprendiendo el manejo de programas y navegación sin el costo de conexión.
- La rapidez que significa la conexión "*off-line"*, evitando así la ansiedad propia de los niños y adolescentes en las lentas bajadas de páginas, típicas de las conexiones telefónicas a Internet.
- El acotamiento de los lugares a visitar, con lo cual se reduce el **"vagabundeo"** por sitios que sólo producen pérdida de tiempo, a la par de distracción en el objetivo final.

En contrapartida, una intranet de estas características en el ámbito educativo presenta la desventaja de tener la visión de aquel o aquellas personas que se dedican a **"filtrar"** los contenidos, así como también produce una sensación de aislamiento de la propia Internet.

## Firewalls personales

Con el advenimiento de la banda ancha, los usuarios “domésticos” se han visto amenazados por la posibilidad de que los “hackers” introduzcan programas dañinos en sus computadoras. Para prevenir este tipo de ataques han aparecido una nueva serie de firewalls, similares a los usados en las grandes empresas, que se colocan entre el sistema operativo de la computadora del usuario y su conexión a Internet, a fin de examinar en todo momento el tráfico y alertar ante posibles intrusiones.

Dos de los programas más empleados en este sentido, y que pueden descargarse de la web son:



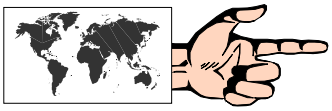
**Zone Alarm**
**http://www.zonelabs.com**

**Norton Personal Firewall**
**http://www.symantec.com**

## Pop up’s

Los **pop-up’s** son esas molestas ventanas que se abren automáticamente cuando se visitan ciertos sitios web, conteniendo en general avisos publicitarios. A fin de evitar este accionar existen programas que se encargan de eliminar estas ventanas, y que para cumplir con su cometido deben estar activos durante la navegación.

Si bien el programa que inició este género, denominado **Pop-up Killer**, fue discontinuado, en la actualidad existen otros que inclusive han superado las prestaciones originales. Los más recomendados son:



**Smasher**
**http://www.popupstop.com**

**Advertising Killer**
**http://www.buypin.com**

## Cookies

Los **cookies** son pequeñas cadenas de caracteres de texto que se envían al disco duro del usuario mientras éste visita una página web. De esta forma, los cookies permiten registrar el perfil de los usuarios.

Un cookie muy usual es aquel que solicita el nombre al usuario. La próxima vez que éste regrese a esa página, el servidor web de la misma “reconocerá” al usuario llamándolo por su nombre.

Sin embargo, detrás de esa apariencia trivial, los cookies pueden esconder ciertos riesgos: en primer lugar el hecho de colocar información en el disco duro del usuario es de por sí un elemento a tener en cuenta; y en segundo lugar, dado que los cookies recogen información de los hábitos del navegante, esto puede resultar nocivo en cuanto a privacidad se refiere.

Para salvar este inconveniente, algunos programas alertan al usuario sobre la actividad de un "cookie” y permiten que sea él quien determine si rechaza o no ese cookie.

**Cookie Crusher** y **Cookie Pal** son dos de los programas que ayudan al usuario a protegerse de los cookies.

En Microsoft Internet Explorer 6, dentro de Herramientas, Opciones de Internet, y eligiendo la solapa Privacidad (Opciones Avanzadas), se puede restringir o directamente eliminar el uso de cookies.