SEGURIDAD INFORMÁTICA

1 OBJETIVO

Comprender los principios fundamentales sobre la seguridad informática y porqué debemos proteger nuestros sistemas de intrusos y otras molestias. Para poder erradicar estos de una o varias PC's es necesario conocer cuales son los elementos que causan problemas, como actúan y como deshacerse de ellos. La diversidad de formas y mecanismos que afectan la seguridad de una PC hace que debamos conocer cómo funcionan y cuáles son sus métodos para penetrar en nuestras PC's.

2 INTRODUCCIÓN Y GENERALIDADES

La proliferación de los sistemas informáticos y las redes que interconectan a estos ha traído un avance en las comunicaciones con el consiguiente desarrollo de programas cada vez más especializados, complejos y de la más diversa índole que nos hacen la vida más fácil en el trabajo cotidiano, trajo aparejada también el surgimiento de otros programas y métodos para introducirse en nuestras computadoras, algunos con el solo objetivo de penetrar, pero otros con finalidades dañinas o de hurtar nuestra información. Para estudiar estos elementos deberemos clasificarlos por su metodología y forma de comportamiento. Esta clasificación es la siguiente:

- Virus Informáticos
- Gusanos
- Troyanos
- Software Intruso
- Programas que aprovechan fallas de seguridad: Scanners, Snifers, ETC.

Ahora nos adentraremos en el estudio de cada uno de estos artilugios, conociendo su principio de funcionamiento y sus formas básicas, para orientarnos en las soluciones que podríamos utilizar.

3 VIRUS INFORMÁTICOS

En la historia de la informática, ningún programa ha generado tantas historias extrañas, mitos y terror entre los usuarios de computadoras.

Muchas veces se realizan analogías del mundo de los virus informáticos con los del mundo biológico. Este es un error ya que, si bien el nombre de *virus* fue tomado de la biología, porque había un comportamiento similar al de los virus biológicos, ellos en realidad no responden a leyes naturales y por ende se comportan de una manera totalmente diferente.

Primero de todo, **los virus informáticos son creaciones humanas y se comportan de acuerdo a los patrones de comportamiento especificados por su creador**. Puede haber virus que invadan rutinas guardadas en partes específicas del disco rígido o disquetes, otros que infecten archivos ejecutables y algunos que hagan las dos cosas.

Los virus se transportan en programas comunes infectados, conocidos como **"portadores"**. **Como un programa infectado pasa totalmente desapercibido para el usuario, al usar dicho programa normalmente, el virus se activa e infecta a otras aplicaciones de la PC**.

Los virus pueden llegar a la computadora de varias maneras, a través de un disquete infectado, un CD ROM, un disco Zip, un archivo adosado a un correo electrónico, en un archivo bajado e Internet, por la red interna de una empresa, etc., etc.

La mejor prevención es **nunca ejecutar un programa cuyo origen no sea legítimo o muy bien conocido, pues puede ser portador de virus.** Además es recomendable hacer copias periódicas del disco rígido, y tener instalado un antivirus actualizado.

3.1 ¿QUÉ SON Y POR QUÉ SE LLAMAN "VIRUS INFORMATICOS"?

SON SIMPLEMENTE PROGRAMAS, AUNQUE MUY BIEN ESCRITOS Y DESARROLLADOS, EN LOS QUE UNA DE SUS CARACTERÍSTICAS, LA REPRODUCTIVA, LES OTORGA LA CLASIFICACIÓN DE "VIRUS".

Son programas que una vez instalados en la computadora **se auto copian (se reproducen) dentro de otros programas (infectándolos)** en todos los medios de almacenamiento disponibles (discos rígidos y disquetes).

Los **programas infectados** pueden ser **archivos ejecutables** (aquellos con extensión EXE, COM, OVL, etc.) o **programas instalados en las zonas de arranque** del sistema operativo, como **tabla de particiones** o **registro de arranque (boot record)**.

Debido a que el MS-DOS es el sistema operativo más difundido en el mundo, éste fue el más propicio "caldo de cultivo" para los virus. Aunque por supuesto los demás sistemas operativos, que manejan informaciones importantes, también fueron blanco, habiendo virus para todos ellos (Windows NT, UNIX, OS/2, etc.).

3.2 ¿CUÁLES SON SUS CARACTERÍSTICAS Y CÓMO OPERAN?

Un virus, por el solo hecho de residir en un disco o disquete, **no significa que esté activo**. Para ello debe obtener el control de la computadora. Los que se instalan dentro de un programa **ganan el control de la PC cuando dicho programa infectado se ejecuta**. Aquellos que se instalan en la Tabla de Particiones o en el Boot Record, **toman el control cuando arranca el sistema operativo desde dicho disco o disquete infectado**.

En el **Master Boot Record** de un disco rígido, aparte de tener grabados los datos de dónde empiezan las particiones, cuál es la partición activa, etc., **hay un programa que se carga en memoria y se ejecuta durante el procedimiento normal de Boot**. Un virus que se instale en el Master Boot Record, **infecta a dicho programa y gana control desde el momento del arranque del sistema operativo**.

Un disquete debidamente protegido contra escritura es inmune a los virus, ya que es imposible modificar su contenido mediante un software. El sistema de protección contra escritura en la disquetera es algo que se resuelve enteramente por hardware.

Del mismo modo, NO ES POSIBLE que un virus "se meta" en nuestra computadora cuando estamos conectados vía módem con otra, **si lo único que hacemos son consultas sobre una base de datos, utilizando programas locales.** Salvo que **copiemos un programa** infectado desde la base de datos y luego **lo ejecutemos en nuestra computadora**.

Por eso, un virus SIEMPRE se instala en archivos ejecutables, desde donde puede tomar el control.

Algunos archivos por su naturaleza pueden parecer archivos de datos únicamente, que no contienen programación alguna; y por lo tanto inmunes de infecciones. Sin embargo algunos de ellos son programables dentro de su entorno operativo. Tal es el caso de los documentos de Microsoft Word, Excel o similares.

Los programas como Microsoft Word o Microsoft Excel por ejemplo, **permiten incluir programas en sus documentos**. Estos son personalizaciones utilizando "**macros**" (conjunto de operaciones normales predefinidas y automatizadas) y/o programas escritos en **Word Basic** (lenguaje de programación incluido).

UN VIRUS PUEDE ALOJARSE ENTONCES DENTRO DE UN DOCUMENTO DE WORD O EXCEL, SIMULANDO SER UN PROGRAMA DE PERSONALIZACIÓN DEL DOCUMENTO.

*Esto fortalece el concepto de que **un virus siempre infecta programas**.*

Una vez que el virus toma el control de la computadora, se instala en la memoria como un programa residente, es decir que se mantiene activo en la memoria aunque el programa portador haya terminado, e intercepta las operaciones del sistema operativo con las unidades de almacenamiento magnético.

A partir de ese momento, **en medio de una operación normal de lectura o escritura** de cualquier programa (incluyendo al MS-DOS) el virus está en condiciones de infectar a otros programas o disquetes. Por ejemplo, **si un virus está activo en la computadora, el solo hecho de hacer un DIR sobre un disquete desprotegido, puede infectarlo**.

Generalmente los virus **luego de una etapa sólo reproductora**, **cuando satisfacen sus requerimientos o se dan ciertas condiciones**, **activarán su** "**bomba**" (objetivo final del virus), la cual **puede ser destructiva** (como el "Viernes 13" donde todos los programas usados ese día se borran) **o bien inofensiva** ("Bouncing Ball" que presenta una pequeña pelotilla que rebota en la pantalla, molestando al operador).

Los daños provocados por los virus pueden ir desde la molestia de un comportamiento anormal, a la destrucción (borrado) de programas y/o datos en el disco, la destrucción de las FAT's, Boot Record y/o Tabla de Particiones, hasta la corrupción (alteración de la integridad) de algunos archivos o del disco completo.

3.3 ¿CÓMO CLASIFICAR A LOS VIRUS?

Resumiendo las características de los virus estudiadas, podemos ya reunirlas en una clasificación según el tipo de programas (portadores) que infectan:

- **Virus ACSO**

Infectan a programas vitales para el arranque del sistema operativo. **Generalmente ubicados en la Tabla de Partición o en el Boot Record**. Estos ganan el control del sistema cuando se intenta iniciar la carga del sistema operativo desde un disquete o disco rígido infectado. Su nombre indica que logra activarse **A**ntes de la **C**arga del **S**istema **O**perativo.

- **EXEVIR**

Infecta a programas comunes, como los *.exe, *.com, *.ovl, etc. Para obtener el control del sistema **el usuario debe ejecutar un programa infectado** (obviamente sin saberlo) en su computadora.

- **Multipartitos**

Son virus que simultáneamente **utilizan dos portadores**: **las zonas de arranque** de los discos y disquetes, **y los programas comunes**. Esto les garantiza una propagación más eficaz, y una difícil remoción.

- **Virus de Macro**

Infectan documentos de Word, planillas de Excel, etc. Sólo "viven" dentro de ese entorno en particular, como por ejemplo Microsoft Word, Microsoft Excel, etc., aprovechando el hecho que un documento o una planilla al ser programables, transportan código (programa).

- **Hoax**

En realidad no son virus, se trata de mensajes que son enviados mediante el correo electrónico, alertando la existencia de falsos virus. La intención es de extenderlos mediante Internet creando cadenas de mensajes y alertas falsas. También tienen la forma de cadenas de mensajes de ayuda falsos. Y algunos tienen alertas de virus que *introducen* archivos en el directorio Windows y recomiendan borrarlos cuando en realidad lo que se está eliminando es un archivo de Windows (generalmente vital para el sistema operativo).

3.4 ¿POR QUÉ HACEN A LOS VIRUS?

Mucha gente se pregunta por qué alguien se toma la molestia de fabricar un virus. Muchos de los virus vistos hoy en día son hechos por una de dos razones:

a) Para probarle al mundo que el autor o grupo de autores son capaces de crear virus.
b) Para tomar venganza sobre alguien en particular.

Los autores se regocijan al saber de la notoriedad lograda por sus creaciones. Algunos inescrupulosos dotan a sus virus de gran poder destructivo, para lograr fama rápidamente, como es el caso del Michelangelo, que borra toda la información del disco rígido en forma irrecuperable el seis de marzo de todos los años.

Los que persiguen una venganza, sólo activan la bomba cuando logran llegar a la PC buscada (la de la víctima). Tal es el caso del virus PHX, quien busca una PC en particular, y si la encuentra, borra información específica de esa máquina.

3.5 ¿QUIÉNES HACEN A LOS VIRUS?

Los autores de virus son básicamente programadores avanzados que pertenecen al círculo "***underground***" de la computación. Caminan por una delgada línea que separa a los estudios avanzados en informática y la delincuencia y muchos de ellos lo hacen únicamente "*por diversión*". Se identifican entre ellos con un seudónimo y tienen una relación altamente competitiva entre sí.

3.6 SISTEMAS DETECTORES DE VIRUS, LIMPIADORES Y ANTIVIRUS

Los detectores de virus (scanners), **son programas que buscan dentro de la memoria y en los discos y disquetes, una serie de bytes** que corresponden a una parte del código (programa) del virus conocido**.** Por lo tanto estos scanners **pueden detectar solamente a los virus conocidos hasta el momento de su desarrollo y NO a los virus de posterior aparición**.

Por ello, es necesario actualizar permanentemente las versiones de estos programas antivirus.

Algunos detectores además de la búsqueda por comparación con cadenas de bytes conocidas, **analizan el comportamiento de los programas** y en el caso de que alguno de ellos se direcciones a lugares del sistema a los que normalmente un programa (que no sea el sistema operativo) no debe acceder, **informan sobre la existencia de un "posible" virus**, ya que sin tener la absoluta certeza de que lo sea, alarma por un comportamiento indebido o muy poco común. **Este sistema de análisis de programas se denomina heurístico.**

Conjuntamente con los detectores, los productos incluyen **programas de limpieza o "limpiadores" (cleaners)**, pudiendo estar éstos integrados a los detectores. Su función es la de remover a los virus del sistema.

LA REMOCIÓN DEL VIRUS DEL PORTADOR, DEJANDO AL PROGRAMA COMO ORIGINALMENTE ESTABA ANTES DE LA INFECCIÓN, ES UNA TAREA COMPLEJA Y NO IMPLEMENTADA PARA TODOS LOS VIRUS DETECTADOS.

En estos casos el limpiador nos indicará que para remover al virus **debe borrar al programa portador**. Luego de la "limpieza" **habrá que reinstalar los programas borrados**.

Los sistemas antivirus (vacunas) son programas residentes que **intentan evitar que un virus se instale en el disco, disquete o la memoria**. Estos programas detectan maniobras ilegales de escritura sobre los dispositivos magnéticos o maniobras no autorizadas de un programa para quedar residente en memoria.

Otros detectan la alteración de la longitud o el contenido de los programas en el disco, las fechas, y en otros casos controlan todas estas posibilidades juntas. Obviamente la utilización de estos programas preventivos no nos puede dar un 100 % de garantías y además restan velocidad operativa y capacidad de memoria RAM. De todas formas será una buena precaución en ambientes donde el origen de los programas utilizados puede no ser fiable.

De todos modos, las vacunas no son infalibles, ya que es posible, de algún modo, burlar las medidas de seguridad, porque en definitiva esta vacuna preventiva está hecha de software y un virus también es software, y podrá invadir y neutralizar la vacuna.

Como dijimos anteriormente los scanners basan su operación de rastreo de virus en la comparación de un conjunto de bytes que pertenece al programa del virus. **Si el virus modificara sus bytes de infección a infección, el scanner no podría identificarlo**.

Por este motivo algunos virus tienen **conductas mutantes** que les permiten **transformar partes de su programa para evitar ser reconocidos**, sin perder sus cualidades principales de reproducción y destrucción.

Algunos Motherboards traen un sistema antivirus en el BIOS, rechazando cualquier intento de escritura sobre la Tabla de Particiones (esto es debido a que estas zonas no se reescriben durante la operación normal), sin embargo, **un virus** que no utilice los servicios del BIOS, es decir **que utilice directamente el hardware**, estaría igualmente habilitado para **borrar o alterar dichas zonas**.

POR TODO ESTO, PODEMOS AFIRMAR QUE NO HAY NINGÚN SISTEMA INVIOLABLE O QUE BRINDE UNA SEGURIDAD TOTAL. SIN EMBARGO, TENER ALGO, SIEMPRE ES MEJOR QUE NADA.

3.7 PRECAUCIONES Y MEDIDAS DE SEGURIDAD A SER OBSERVADAS

El técnico de mantenimiento es muy propenso a recibir algún tipo de infección en sus disquetes de diagnósticos por el hecho de **portar dichos disquetes de una a otra máquina**. Luego, un disquete de diagnóstico infectado puede seguir infectando a otras máquinas de otros clientes **con las consecuencias imaginables y desastrosas**.

Es indispensable entonces, tener disquetes libres de virus y correctamente protegidos contra escritura para evitar infecciones.

Además, antes de incorporar al paquete de disquetes de diagnóstico un programa nuevo, se debe chequear exhaustivamente la “salud” del mismo con un scanner actualizado.

Antes de utilizar los disquetes de diagnóstico en una **máquina no conocida**, se deberá asegurar **que el sistema de detección del Write Protect de la disquetera funcione correctamente**. Esto lo podemos comprobar, intentando grabar algo sobre un disquete protegido, si da error de protección contra escritura, entonces está funcionando bien y podemos confiar en él, por otra parte si no funcionara debidamente podría ocurrir que al colocar un disquete protegido, el sistema pueda grabar igual sobre él y por lo tanto infectar nuestros disquetes.

3.8 PROGRAMAS COMERCIALES ANTIVIRUS, SCANNERS, ETC.

El **Norton Anti Virus (NAV)** es un programa que una vez instalado en la computadora, crea un archivo auxiliar de cada uno de los archivos “*.COM “ y “*.EXE” de todo el disco, en el cual deja grabados datos de su longitud, suma de chequeo (checksum) que le permite saber si su contenido a sido alterado, fecha, etc. La función de estos archivos de control es poder detectar si algún programa ha sido alterado (presumiblemente por un virus). Además provee servicios de Scanner y Cleaner

Otro programa fue el **Central Point Anti-Virus (CPAV)**, el cual fue incluido en el sistema operativo de Microsoft **MS-DOS Ver. 6. x bajo el nombre de MSAV**. Existen también los de uso libre o Shareware (software compartido) como ser **el F-PROT, el Dr. SOLOMON, etc. muy difundidos por Internet**.

Algunos programas antivirus están siendo incluidos con los nuevos motherboards, como el **PC CILLIN y el Norton Antivirus**.

También se pueden bajar de Internet y actualizar automáticamente desde la red.

Otros programas disponibles que cumplen estas funciones son **el SCAN xxx, CLEAN o CLEANDRV** de **MC Afee**, el **VIRUSCAN de IBM**, **Thunderbyte** y otros.

3.9 CONCLUSIONES

Cada tipo de virus requiere una forma de detección y limpieza diferente. Afortunadamente, ya casi todos los fabricantes de antivirus combinan diferentes métodos heurísticos con bases de datos de **características actualizadas permanentemente por Internet**, para ofrecer una protección muy efectiva.

En el campo de la protección informática los productos de seguridad no eliminan las amenazas, estas dependerán de las políticas de seguridad que uno implemente. Es un problema de asepsia en el manejo de la información, la frase "**Prevenir es mejor que curar**", tiene sentido en el cambio de hábitos y estrategias.

Finalmente, es indispensable determinar los procedimientos a seguir si todo lo anterior falla, es decir si un virus nos infecta, para tener la certeza de poseer una protección completa. Saber actuar con un antivirus, respetar la cuarentena del equipo infectado, revisar todos los disquetes que hayan pasado por ese equipo y **averiguar el origen del virus** (¿por qué se infectó la máquina?) **para evitar que vuelva a suceder**.

NOTA: Es importante que los programas ANTIVIRUS sean de últimas versiones disponibles, ya que si nuestro disco o disquete está infectado con un **virus no reconocible** por el scanner que estamos usando, éste **no reportará ningún virus**. Con los detectores de virus en tiempo real (vacunas) se puede tener un nivel de certeza un poco superior ya que además de buscar virus conocidos analizan el contenido de los programas buscando instrucciones que puedan conformar un comportamiento sospechoso o característico de un virus **(análisis heurístico)**. En este último caso un antivirus podría reportar **un posible virus sin certificarlo ni identificarlo** ya que, no sólo no está seguro que lo sea, sino que tampoco lo conoce, solo reporta un probable virus.

3.10 TÉRMNOS MÁS COMUNES REFERIDOS A LOS VIRUS

- **In the Wild**: Este término se refiere a una lista oficial de los virus que en ese momento están en su apogeo, y no significa que en esa fecha se activen. En esta lista se encuentran los virus que más ataques están teniendo en este periodo de tiempo. Esa lista se renueva todos los meses, entrando entonces nuevos virus y saliendo de ella los que ya han perdido *actualidad.* Esta lista se puede encontrar en http://www.wildlist.org .
- **Payload**: Este término se refiere al efecto que produce la actividad de un virus en nuestra computadora que va desde cambios en la configuración a la destrucción de la información.
- **Payload trigger**: Es el momento (fecha) o el modo (condición) por el que el virus ejecuta el "*payload*", dicho de otra manera, el tipo de activación del virus.
- **Malware**: Es el término que se utiliza generalmente para referirse a cualquier software que cuente con código malicioso como virus, troyanos, gusanos, ETC.
- **Nivel de distribución**: Se refiere a que grado de extensión puede tener un virus en cuanto a la rapidez de su propagación.
- **Síntoma de infección**: Son las acciones que toma un virus en propagación o los efectos que produce durante o posteriormente a su activación.

- **Infection Length**: es el tamaño del código que inserta el virus en un programa. Si se trata de un troyano es el tamaño completo del mismo.

4 VIRUS DE WINDOWS

Muchos de los virus diseñados para DOS, sencillamente no funcionan dentro del entorno Windows. Otros interfieren de tal modo al sistema operativo, que no permiten la operación normal de Windows.
Generalmente los virus residentes, como los del tipo **ACSO**, dentro del entorno Windows provocan que el sistema operativo funcione con los recursos "en modo compatibilidad con MS-DOS", perdiendo toda mejora en el rendimiento de acceso a disco. El mensaje mostrado en la **figura 23.1** hace referencia a este problema de rendimiento. Fue generado por la presencia del virus Michelangelo en el Master Boot Record (donde normalmente se instala).

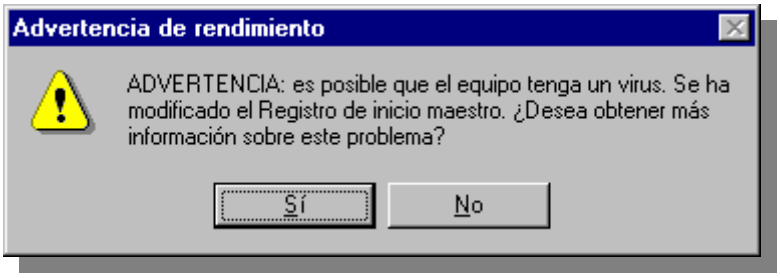

Figura 23.1: Advertencia de rendimiento de Windows frente a la interferencia de un virus ACSO.

El problema de rendimiento es notorio desde la ficha "**Rendimiento**" en **Propiedades del sistema**. Para acceder a estos informes de estado, podemos hacer clic con el botón derecho del Mouse sobre el icono Mi PC, y luego eligiendo "propiedades" dentro del menú emergente, o bien navegando desde el menú de inicio ⇒ configuración ⇒ Panel de Control ⇒ Sistema. Luego seleccionamos la ficha "**rendimiento**" dentro del panel que aparece (ver **figura 23.2 y 23.3**).

Cabe hacer la aclaración, que no es únicamente un virus lo que puede provocar una pérdida de rendimiento. Un driver mal configurado también puede provocar este desperfecto.

Los virus exitosos que primero aparecieron dentro del entorno Windows, son los ***virus de macro***, aquellos que funcionan dentro de un entorno como **Microsoft Office**.

El **Microsoft Word**, (y los otros integrantes del paquete **Office:** Excel y Access), sufren virus de macro, que infectan la plantilla general, llamada ***Normal.dot***.

Esta plantilla almacenará instrucciones que se ejecutarán cada vez que un documento se abra, infectándolo para poder diseminarse por otras computadoras.

Los documentos infectados, cuando se abran en otra PC, modificarán la plantilla general de esa máquina, y así sucesivamente. La **bomba** de estos virus puede ser corromper archivos o destruirlos.

Otro tipo de la misma familia son los virus ***class***, que si bien son similares a los ***macro,*** **se esconden en otros directorios y deshabilitan los mensajes de confirmación del Word cuando se guardan las modificaciones**. Además, son virus mutantes o polimórficos, que cambian su código cada vez que se reproducen. También se los conoce como virus fantasmas o ***stealth*** porque **no se los puede encontrar fácilmente**.

Figura 23.2: Presentación del informe con un rendimiento óptimo.

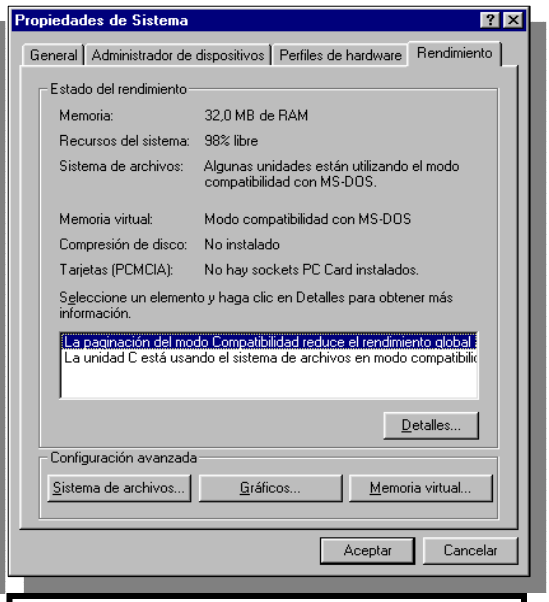

Figura 23.3: Presentación del informe con un rendimiento pobre, en modo compatibilidad.

El propio Word permite mostrar automáticamente una ventana de advertencia cuando un documento que va a abrirse contiene macros, e indica que **podrían ser un virus**, esto lo podemos apreciar en la figura 23.4.

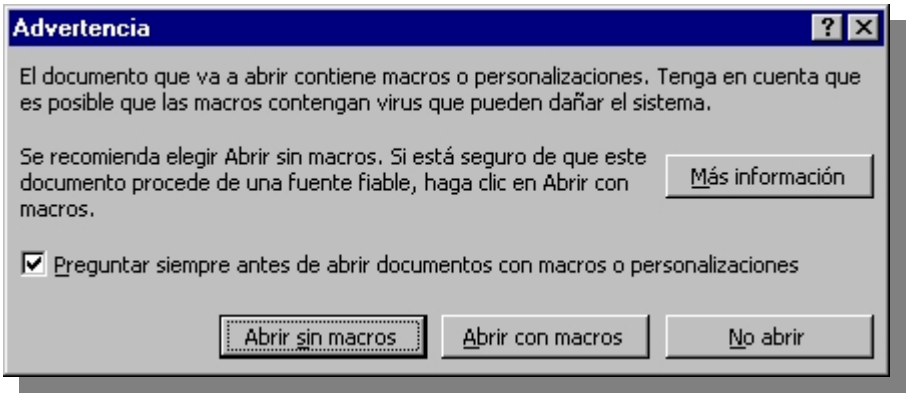

Figura 23.4: Advertencia de Microsoft Word ante la presencia de macros en un documento que se desea abrir.

Las macros o personalizaciones de los documentos, tienen su utilidad normal y ya que el **Word no es en realidad un programa antivirus,** sólo puede informar de la presencia de macros en los documentos. Podrían ser personalizaciones genuinas o virus, quedando a criterio del usuario si se procede a abrir el documento con o sin macros.

Si la procedencia del documento no es fiable, **siempre es recomendable abrir los documentos sin macros, pues siempre será posible ver el contenido sin riesgo a infectarnos, aunque no funcionen algunas automatizaciones genuinas.**

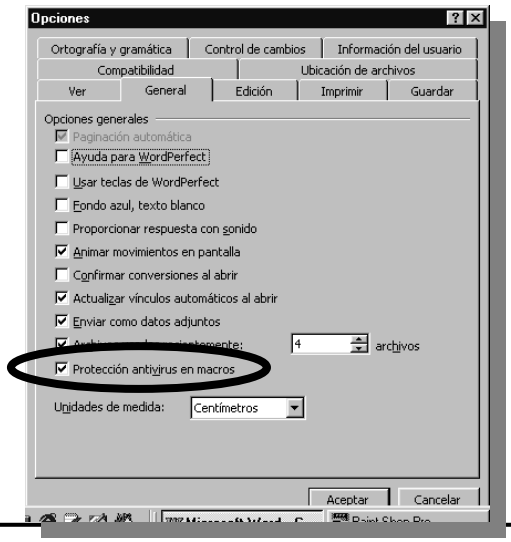

Figura 23.5: Opción de aviso de macros en el Word

Esta opción se habilita desde ***Herramientas/Opciones/ ficha General*** y activar la opción ***Protección de antivirus en macros*** (ver figura 23.5).

ADVERTENCIA

Recordemos que es imposible que un virus infecte un disquete adecuadamente protegido contra escritura. El sistema de protección contra escritura en la disquetera es algo que se resuelve enteramente por hardware por lo tanto es invariable por el software y como un virus es en definitiva software no podrá alterarlo. Por ejemplo, si un virus está activo en la computadora, el solo hecho de hacer un DIR sobre un disquete desprotegido, puede infectarlo.

Pero no podemos proteger al disco rígido contra escritura porque no existe mecanismo equivalente de hardware, por lo que está siempre disponible para ser infectado.

Los virus que aparecen por el correo electrónico pueden estar escondidos en archivos adosados (indicados con un "📎"). Una buena práctica es, además de conocer el origen de los mensajes, **no abrir los programas adosados si no hay garantía de su seguridad**. Solicitar que los mensajes traigan la información escrita directamente en el cuerpo del mensaje, o usar procesadores de texto como el Word Pad o el Write que no poseen macros para abrir los archivos "**.dot**".

5 GUSANO

Es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos, o parte de ellos.

Un incidente registrado a fines de 1988, marcó el comienzo de los programas definidos como "gusanos". Robert Morris (23), hijo de un experto en seguridad informática de la Agencia Nacional de Seguridad (USA) fue el autor y quien desató el programa en Arpanet (precursora de Internet).
Dicho programa se replicó usando algunos conocidos baches de seguridad en los sistemas de correo del momento. El programa se replicó tan rápido (más allá de las expectativas de Morris) que dejó sin recursos prácticamente a todas las computadoras de la red Arpanet.
Morris fue sentenciado a tres años en suspenso, 400 horas de servicios comunitarios y 10.500 dólares de multa.
Los gusanos infectan nuestra máquina de la manera que se describe más arriba solo que tienen metas diferentes. Algunos como *"los gusanos de script" IRC* (Internet Relay Chat) que infectan archivos de Windows que se utilizan para este servicio, como el Scripts.ini y Events.ini, y funcionan a través de programas como MIRC, etc.
Los gusanos de *Win32* basan su reproducción infectando APIs de Windows MAPIs (Message Application Program Interface) o clientes de correo como Outlook, estos gusanos tienen la habilidad de propagarse a través de la libreta de direcciones (enviándose a todas las direcciones que encuentre) o también puede enviarse como un archivo adjunto a toda dirección de correo que el usuario envíe un mensaje.

6 TROYANO

Un troyano es un programa que puede funcionar independientemente, no se pueden considerar virus ya que no se replican o no hacen copias de sí mismos, y necesita además que el operador lo ejecute voluntariamente para comenzar su tarea. Para motivar al operador para que lo ejecute, generalmente el archivo tiene un nombre atractivo, que sugiere ser algo totalmente distinto a lo que realmente es.

El termino **Troyano** tiene su origen en el "Caballo de Troya" de la Ilíada de Homero, donde cuenta que los griegos, en guerra con la inexpugnable ciudad fortificada de Troya, ofrecen un gran caballo de madera a modo de regalo. Cuando los Troyanos introducen a éste dentro de las murallas de su ciudad, unos griegos **escondidos dentro del caballo**, salen y abren las puertas de la muralla, permitiendo el ingreso de las tropas griegas y así conquistando Troya.
Entonces pueden llegar a nuestra máquina acompañado (dentro) de otro programa y tratar de permanecer oculto y sin dar muestras de su existencia (por lo menos por ese momento). Al activarse pueden abrir huecos en la seguridad del sistema y permitir que intrusos entren en nuestra PC y puedan robar información, como contraseñas, información personal (tarjetas de crédito, ETC.).

7 SOFTWARE INTRUSO

En la actualidad el auge de Internet trajo grandes adelantos, uno de ellos es poder *bajar* software y probarlo antes de decidirnos a comprarlo, a esto se le llama bajar un programa "Sha*reware"*, también hay programas de uso gratuito o sea "Free*ware"*, muchos de estos, en realidad la mayoría, no representan ningún peligro, pero hay otros que nos ***"Cambian"*** la cuali-

dad de ser gratis por introducirnos en nuestras computadoras software espía o que realizan funciones que no autorizamos en el momento de instalar el programa original. A este software Espía lo podemos catalogar en tres divisiones clasificadas por su comportamiento:

- **Adware**
- **Spyware**
- **Scumware**

7.1 Adware

El Adware es un software, que instalado muchas veces sin el consentimiento del usuario, permite visualizar *Banners (ventanas de publicidad dentro o fuera de una página Web)* de publicidad mientras estamos conectados a Internet, esta publicidad se muestra dentro de la interfaz del programa anfitrión. Muchos de estos programas son los que de una u otra manera subvenciona a los desarrolladores de software gratis.

7.2 Spyware

El "*Spyware*" es, como su nombre en ingles lo dice, un software espía, es decir un software que monitorea nuestros hábitos de navegación y después vende esta información a empresas dedicadas a esto. Para explicarlo de otro modo si nosotros visitamos páginas de autos después de un tiempo nos llegará correo ofreciéndonos distintos modelos de automóviles. Esto viola claramente la seguridad de nuestra PC puesto que envía nuestra información personal a terceros sin nuestro consentimiento (Correo electrónico como mínimo).

7.3 Scumware

Este software tiene como objetivo reemplazar los Banners del sitio que estamos visitando por otros que son de propiedad de los autores de este software, es decir si un sitio de Internet tiene un *banner* o un *link (acceso directo a otra página Web)* es sustituido por una dirección o publicidad que no son los originales y están dirigidos a otra página Web y que, obviamente, están patrocinados por otra empresa. Como ya lo imaginarán, es una clara violación a los derechos tanto del visitante de la página como para el diseñador de la misma, que se ve afectado por no poder patrocinar sus propias páginas de publicidad. Como lo muestra la figura 23.6

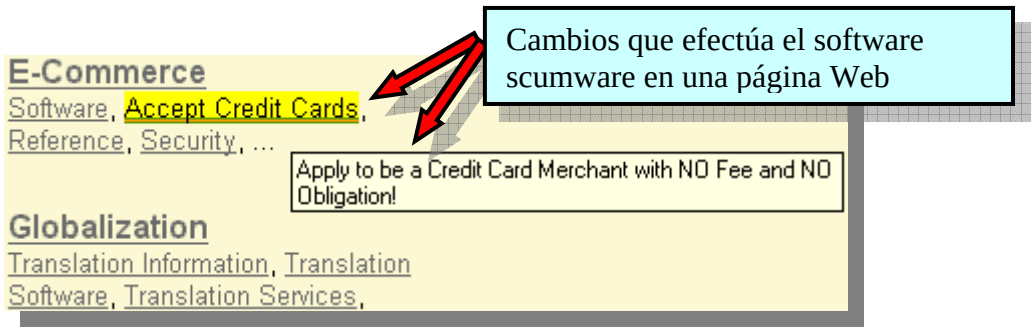

Figura 23.6: Acción del scumware

Como dijimos más arriba esta clase de programas invade nuestra PC y sin que se pueda tomar alguna decisión con respecto a su instalación lo tendremos en ella sin enterarnos de su existencia, pueden tomar las acciones que quieran, puesto que no hay control sobre ellos y estas acciones van desde la instalación de estos programas en nuestro disco, hasta estar residentes en memoria, O MODIFICAR NUESTRO REGISTRO DE WINDOWS, y lanzar otros programas asociados a él, que bajan actualizaciones del programa con nuevas características como es el caso de "***GATOR ",*** un programa que supuestamente nos guarda todas las contraseñas de las páginas que visitamos en la Web *"para hacernos la vida mas fácil"* pero que a escondidas actúa como un software *Spyware* y *Scumware* juntos. como primera medida tiene por objetivo espiar nuestros hábitos de navegación y después enviarnos vía correo electrónico propaganda relacionada con las páginas visitadas. Pero la tarea del *Lagarto (Gator)* no concluye aquí, también en las páginas visitadas reemplaza los banners y propaganda del sitio por propaganda propia y además reemplaza, como muestra la figura 23.6, Links a otras páginas por otros dirigidos a páginas de sus patrocinadores. Mencionamos a ***GATOR*** a modo de ejemplo, obviamente, porque como este programa hay cientos de ellos diseminados por cuanto programa shareware o freeware (ya aclaramos que no son todos) bajemos y/o instalemos en nuestras PCs. Sin ir más lejos, uno de los más populares programas para compartir archivos por Internet, el "*KAZAA"*, trae de regalo varios de estos programas intrusos. La manera más fácil de erradicar este software es con programas dedicados a esta tarea de limpiar nuestra PC (y obviamente, la de nuestros clientes). Uno de los más conocidos es AD-AWARE de la empresa "*lavasoft*" http://www.lavasoftusa.com un programa muy fácil de usar y su versión de prueba es totalmente funcional. Figura 23.7. Este programa "*escanea"* la memoria, el registro de Windows y todas las unidades de disco. Y sus resultados son muy precisos.

Figura 23.7: pantalla principal de AD-AWARE

NOTAS

CUESTIONARIO CAPITULO 23

ESTUDIO

1. **¿Cuál es la finalidad de los virus informáticos?**

2. **¿Dónde se ubican los virus tipo ACSO?**

3. **¿Qué hacen las “vacunas”?**

4. **¿Cómo se defiende un técnico de los virus?**

5. **¿Cómo puedo detectar la presencia de un virus?**

6. **¿Cuál es la finalidad de los gusanos informáticos?**

7. **¿Qué hacen los antivirus contra los virus polimórficos?**

8. **¿Que diferencia existe entre el intruso Adware y un Spyware?**