UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

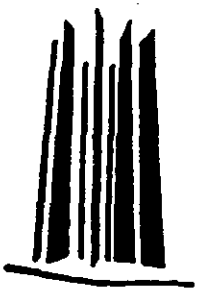
ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGON

# "ESTRUCTURA DE PROCEDIMIENTOS DE SOPORTE TECNICO PARA LA APLICACIÓN Y ERRADICACION DE VIRUS INFORMATICOS"

# T E S I S

QUE PARA OBTENER EL TITULO DE
**INGENIERO EN COMPUTACION**
P R E S E N T A :

ROGELIO ZARCO ROBLEDO



ASESOR: ING. JUAN GASTALDI PEREZ

**MÉXICO** **1999**

***Dedico este trabajo con mucho cariño y respeto****

*A mis padres:*

*C. Sr. Mariano Zarco Bernal*

*C. Sra. María Agustina Robledo de Zarco*

*Como un testimonio de eterno agradecimiento al apoyo, amor comprensión y abnegación, que siempre en forma incondicional me han brindado, y que ahora me permiten culminar una de mis grandes metas.*

***Dedicado también a mi esposa e hijos****:

*C. Sra. Sara Ma. Victoria Esquivel de Zarco*
*Ian Rogelio Zarco Esquivel*
*Karen Zarco Esquivel*

*A mi esposa, por su comprensión, ayuda, motivación y ánimos para salir adelante.*
*A mis hijos, como un ejemplo de superación a sus vidas.*

*Y a todas aquellas personas que de momento han escapado de mi mente, y que de una forma directa o indirecta contribuyeron para hacer realidad este trabajo.*

*Que Dios los bendiga a todos, por siempre.*

INDICE

PAGINA

## CAPITULO 3

## CAPITULO 9



## CAPITULO 10

# INTRODUCCION

Cuando un lector pretende conocer que es un virus informático y como trabaja, generalmente lo hace investigando a partir de la bibliografía disponible, encontrándose por un lado principalmente con libros que le explican los daños que causan a los sistemas, además de los recursos y beneficios que se pueden obtener al utilizar un Antivirus. Se menciona en estos libros que un virus es un enorme mal en las computadoras y que aparecen en todos los países y que millones de usuarios pueden tener o contaminar sus equipos de cómputo. Para lograr esto, las miles de redes que componen a los sistemas de cómputo hoy en día como Internet; los virus interactúan haciendo el uso de dos elementos primordiales. Uno de estos elementos es la infraestructura de comunicación establecida con base en ruteadores que hacen las veces de una interface física y que además permiten el enlace de todas las redes. El otro elemento es un conjunto de sistemas elaborados en lenguaje de alto nivel que permiten la propagación en los equipos y, en las redes que pueden comunicarse mediante un lenguaje común. Este conjunto de sistemas es identificado con el nombre de "Virus" o "Macrovirus" y tales libros explican su operación.

Por otro lado, cuando se revisa bibliografía referente a virus el lector se encuentra con libros que usan demasiado el vocabulario técnico y que presuponen un cierto conocimiento de soporte técnico en computadoras estándares. Es decir, están enfocados a un auditorio especializado como pueden ser los administradores, diseñadores y desarrolladores de sistemas de redes. Estos libros usualmente muestran como implementar una normatividad usando los Antivirus como protectores de la información.

Esta problemática motivó la realización del presente estudio, en el cuál se pretende hacer una aportación que auxilie al lector interesado en sistemas informáticos, para

dar a conocer cómo trabaja un Antivirus, y poder dar a conocer las aplicaciones, servicios y recursos que gozan millones de usuarios a través de todo el mundo.

El objetivo es ofrecer una información equilibrada que fusione tanto el aspecto teórico como técnico, y que ayude a tener una idea cierta de lo que es un virus y un Antivirus, y a partir de este conocimiento obtener los máximos beneficios para el usuario.

El presente trabajo está dividido en catorce capítulos con algunas ilustraciones que definen a un sistema de Antivirus, como una herramienta de la que es necesario explicar los conceptos relacionados con ella, tales como los diferentes tipos de sistemas que existen, los elementos que los componen, las diferentes topologías que utilizan, así como los servicios que ofrecen a los usuarios finales. Todos estos aspectos son explicados claramente; también tienen la finalidad de sentar bases para el comportamiento de conocimientos evolutivos.

El Capítulo I, describe la historia de los virus. Este capítulo se presenta con el fin de mostrar al lector que es un virus, cuales fueron los motivos que provocaron su surgimiento, y su gran desarrollo a través de sus casi tres décadas. Estos capítulos muestran con detalle, como los Antivirus son el producto de una serie de esfuerzos cooperativos de diferentes entidades; las cuales van desde instituciones militares, la comunidad científica y académica hasta llegar a las organizaciones comerciales. Se describen a los Antivirus, como los sistemas de prevención de su propio generador; que siempre está ingeniando nuevas ideas, experimentos, pruebas, etc. Culminando en una serie de servicios y productos, para satisfacer las necesidades de protección; que finalmente con el paso del tiempo, ha sido ofrecido al usuario final.

Así mismo, este capítulo nos muestra la evolución y robustecimiento de los Antivirus como un producto de la necesidad de soportar el crecimiento explosivo de

los virus que se han manifestado en las PC's, redes y su estratificación, así como un repaso a la tecnología.

Los Capítulo II y III constituyen la parte medular de este trabajo, los cuales presentan como están implementados los Antivirus, se muestra claramente como este importante conjunto de sistemas son los responsables de proteger las PC's y las redes de computadoras de diferentes tecnologías y plataformas que se pueden comunicar e infectar permitiendo la conectividad universal. Estos capítulos muestran con notoriedad la interacción de diversos virus, ya que para llevar a cabo las tareas de comunicación de la red, los sistemas complejos de comunicación requieren subdividir los problemas y delegárselos a un Antivirus en particular.

El *principal fin*, es tener una perspectiva más amplia y facilitar al lector el entretenimiento del papel del Antivirus dentro de la computación.

El Capítulo IV, trata en detalle los aspectos de ocultamiento y activación de infección con los dispositivos de *hardware*, tales como los ruteadores y las computadoras receptoras de la información, pero siempre vistos desde el enfoque de los medios encargados de llevar el contagio a esos equipos.

Los Capítulos V y VI, hacen mención de los principales servicios que ofrece un Antivirus implementado en un equipo de cómputo, haciendo especial énfasis que estos servicios están soportados también por usuarios avanzados en soporte técnico.

Existe una gran variedad de servicios de Antivirus disponibles para los usuarios de cómputo, y cada día surge una gran variedad de virus, lo cual deja de manifiesto el poder de la tecnología. En los demás capítulos, no se pretende describir todos los servicios que existen, ya que como se mencionó al inicio de esta introducción, existen varios libros dedicados exclusivamente para tal propósito, y éste no es el fin

del presente trabajo. Mas bien lo que se quiere mostrar en estos capítulos, son las aplicaciones o servicios típicos que un Antivirus ofrece a sus usuarios, describiendo la situación particular en la cual uno de ellos es utilizado, pero además de esto mostrar como funcionan internamente y que relación tienen con los demás Antivirus. De esta manera se describen los Antivirus; así mismo dentro del Capítulo XI, se mencionan a grandes rasgos, algunos servicios adicionales con el fin de mostrar herramientas que tiene a su disposición el usuario, para explorar y explotar un Antivirus en PC's personales y en redes.

Como cualquier área del saber humano que integra su propio lenguaje y terminología, un Antivirus posee una gran cantidad de términos, abreviaturas, siglas y acrónimos; que en ocasiones son difíciles de recordar, por ello es recomendable hacer apuntes o contar con un manual actualizado. Los virus informáticos se han convertido en una amenaza de grandes proporciones, debido a su capacidad de afectar el patrimonio más valioso de cualquier usuario de computadoras: su información.

En teoría, se tiene por hecho que un virus informático es un programa como cualquier otro, con una característica que lo distingue: es capaz de reproducirse introduciendo copias de él mismo dentro de los programas ejecutables. Un virus infecta una computadora de una manera muy discreta, en general no produce ningún síntoma que pueda delatar su presencia, esto le da la oportunidad de pasar desapercibido un largo tiempo, mientras tanto se reproduce el mayor número de veces, contaminando programas o discos; que luego infectarán a otras computadoras para continuar su diseminación. En la mayoría de los casos, después de un largo tiempo el virus decide activarse u ocasionar algún efecto, que puede ser inofensivo; como producir: variaciones en el funcionamiento del la PC, sonidos e imágenes, o algo quizás mayor, como formatear el disco duro. Todo esto lo hará sin el consentimiento del usuario, que de esta manera se convierte en su víctima.

# CAPITULO 1

## FUNCIONAMIENTO DE LOS SISTEMAS DE SOPORTE CONTRA "VIRUS"

### 1.1. ORIGENES DE LA INFORMATICA(*)

El nacimiento de la *informática* (computación), está relacionado con la necesidad que ha sentido siempre el hombre, de disponer de un sistema que le permita manejar gran cantidad de información con relativa rapidez así como de efectuar cálculos a gran velocidad y de un modo mecánico. Los primeros antecedentes de sistemas rudimentarios destinados a solventar estos problemas, son por ejemplo los ábacos, marcos dotados de guías metálicas por las que se mueven cuentas ensartadas en ellas cuyas posiciones permiten realizar operaciones aritméticas sencillas con rapidez. Estos dispositivos rudimentarios de cálculo todavía se emplean en la actualidad en algunos lugares del Asia. Sin embargo, los antecedentes de los ordenadores son sin duda, los mecanismos para la resolución de dichos problemas, creados en épocas posteriores; que en lo referente al cálculo, se deben a los trabajos de *Blaise Pascal* (1623-1662) y *Gottfried Leibniz* (1646-1716). El primero (*Pascal*), creó una máquina capaz de sumar y restar, mediante la combinación de una serie de ruedas dentadas; cada una de dichas ruedas tenía 10 dientes que corresponden a los números del 9 al 0, siendo el sistema de tal tipo. El paso de nueve a cero, da lugar a un salto de la rueda inmediatamente continúa por el lado izquierdo. El dispositivo, llamado *pascalina*, era semejante a los dispositivos mecánicos que se emplean en la actualidad en los velocímetros, que cuentan los kilómetros recorridos por los vehículos automóviles y motocicletas. *Pascal* llegó a introducir en versiones posteriores mejoradas, un elemento de memoria mecánico que permita acumular resultados parciales durante la realización de las operaciones. Por su parte,

(*) Revista de Computacion "Los Ordenadores Modernos"

*Goottfried Leibniz* desarrollo y mejoró el dispositivo creado por *B. Pascal*, logrando que la máquina fuese capaz de realizar las cuatro operaciones aritméticas básicas; la suma, la resta, la multiplicación y la división de forma mecánica. Sin embargo, en sentido estricto, cabe considerar que los auténticos inicios de la informática datan del siglo XIX. Mas concretamente de los trabajos realizados por *Hermann Hollerith* (1860-1929), miembro de la oficina del censo de los Estados Unidos de Norte América. La contribución de *Hollerith* consistió en emplear una cinta (que más tarde sustituyó por tarjetas), en la que se grababa la información mediante perforaciones en lugares determinados, siguiendo la idea de los telares automáticos desarrollados por el mecánico e inventor francés *J. Marie Jacquard* (1752-1834) en 1805 para la realización de ciertos prototipos de telas cuyas muestras eran de difícil reproducción. Gracias a dicho dispositivo creado en 1990, era posible realizar mecánicamente operaciones tales como la clasificación, duplicación y copia de fichas perforadas (y por lo tanto de los datos en ellas contenidos). Las máquinas desarrolladas por *Hollerith* permitieron realizar el censo de los EE.UU. (que por aquel entonces era de unos 60 millones de habitantes) en un tiempo de apenas dos años y medio. Los sistemas de este tipo que reciben el nombre de pre-ordenadores, se siguen empleando en la actualidad de un modo restringido. El siguiente paso en el camino del tratamiento automático en la información, se debió a los trabajos de *Howard H. Aiken* (1900-1973), quien desarrolló entre 1939 y 1944 y en el seno de la compañía IBM (creada en 1924 a partir de la *Tabulating Machine Company* fundada por *H. Hollerith* ) el ordenador conocido por ASCC (siglas de *Automatic Sequence Controlled Calculator*) o *Mark I*. Esta máquina se basa desde el punto de vista del sistema físico, en un dispositivo eléctrico simple, en *relé* y su programación se llevaba a cabo mediante una cinta perforada, es decir, seguía las ideas de la "máquina analítica", capaz de realizar cualquier operación matemática sin intervención humana, diseñada por *Charles Babbage* (1792-1891) pero lo que no pudo construirse ya que el nivel técnico de la época no lo permitía. El *ASCC* o *Mark I*, que puede considerarse el primer ordenador de la historia, se basaba como ya se

ha dicho en el empleo del *relee* (es decir, un dispositivo electrónico que permite abrir y cerrar un circuito) y disponía de una capacidad de memoria de 72 números de 23 cifras decimales. Sin embargo, era extraordinariamente lento ya que necesitaba unos 10 segundos para llevar a cabo la multiplicación de dos números de 10 cifras, su peso era de unas 5 toneladas, incorporaba unos 5,000 *relés* y ocupaba mucho espacio. Dicha instalación funcionó desde 1944 hasta 1959. En el campo teórico del investigador *John Von Neumann* (1903-1957) creó en la década de los años 50, el modelo teórico de la configuración de los ordenadores modernos, desarrollando las ideas de que el programa debe almacenarse en el sistema, del mismo modo que se hace con los datos que el sistema debe disponer de capacidad lógica y que el propio programa debe estar formado por un encadenamiento de sentencias lógicas.

### 1.1.1. LOS ORDENADORES MODERNOS

El siguiente paso se produjo gracias a la aplicación de la Electrónica y a la resolución de este tipo de problemas. En 1946, la escuela *Moore* de Ingeniería Electrónica situada en Filadelfia, EE.UU, construyó la primera máquina electrónica de calcular. Había sido diseñada en la *Universidad* de *Pennsylvania* entre 1943 y 1946, por *Mauchy, J.P. Eckert* y *H.H. Goldstine*. Se llamaba *ENIAC* (las siglas inglesas de *Electronic Numerical Integrator and Computer*), (calculador e integrador numérico electrónico). Fue el primer calculador digital carente de piezas móviles salvo los dispositivos de entrada y salida de la información. EL *ENIAC* estaba formado por 18,000 válvulas, pesaba unas 30 toneladas y consumía 150 KW. Sus dimensiones eran tales que se encontraba albergado en un edificio expresamente construido para tal fin. Su construcción costó aproximadamente 2'000,000.00 de dólares. Sin embargo, a pesar de sus dimensiones ciclópeas, un micro ordenador moderno compuesto por un único chip de 25 $mm^2$ de superficie es capaz de trabajar unas 100 veces más rápido que el *ENIAC* (ya que este necesitaba 0.003 segundos para resolver una multiplicación de dos números de 10 dígitos) con un consumo de tan sólo 1W. La programación del ENIAC se llevaba a cabo mediante el

establecimiento de conexiones entre cables eléctricos y el accionamiento de gran cantidad de interruptores. En las décadas siguientes, el progreso de este tipo de instalaciones fue cada vez más acelerado y siguió la serie de etapas que reciben el nombre de generaciones y que abarcan períodos determinados según se trate del sistema físico o lógico, si bien las generaciones están inter-relacionadas ya que uno y otro dependen entre sí.

La PRIMERA GENERACION, la constituyen los ordenadores que se construyeron entre los años 1950 y 1960, se trata de las primeras máquinas de este tipo que se fabricaron con fines comerciales, siendo el componente electrónico básico que hacía posible su funcionamiento la válvula de vacío (dispositivo electrónico formado por dos electrodos encerrados en una ampolla en la que se ha practicado el vacio). Estas máquinas se programaban directamente en lenguaje de máquina y eran capaces de realizar hasta 1000 instrucciones por segundo; disponían así mismo de una capacidad de memoria que podía llegar hasta las 20,000 posiciones.

La SEGUNDA GENERACION, es la que comprende los ordenadores construidos entre los años 1960 y 1965, dicha generación se caracteriza por el hecho de que el componente electrónico básico sobre el que descansa es el transistor (dispositivo electrónico que actúa como un interruptor ya que determina el paso o no de la corriente entre dos puntos en función de la tensión aplicada aun tercero). El empleo de este hace que dicha generación sobresalga por lograr una reducción del consumo de energía y del volumen ocupado por las máquinas, así como un enorme aumento de fiabilidad y de la velocidad del cálculo de las instalaciones (que llegaba hasta el millón de instrucciones por segundo). Los progresos del sistema lógico de los ordenadores dieron paso así mismo a la aparición de los sistemas operativos, el procedimiento en régimen de tiempo compartido y los lenguajes de alto nivel, etc.

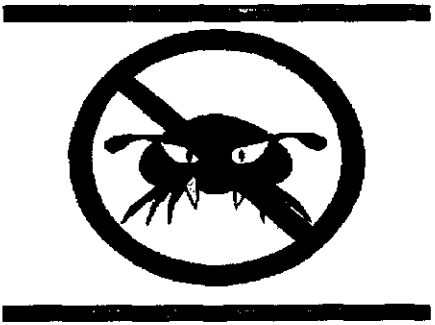
La TERCERA GENERACION, que abarca desde 1965 a 1975, se caracteriza fundamentalmente por la reducción de las dimensiones de las instalaciones ya que su construcción y funcionamiento se basa en el empleo de los circuitos integrados (Hacia 1974 se logró obtener gracias a las técnicas *VLSI Very Large Scale Integration*, integración a muy gran escala). Un circuito integrado que albergaba hasta 20,000 componentes en una superficie de 25 $mm^2$.

La CUARTA GENERACION, finalmente abarca desde 1975 hasta 1981, y se caracteriza fundamentalmente por la continuación del proceso de integración que culminó en 1975, con la consecución de una escala de integración que permite colocar 60,000 componentes en una superficie de 25 $mm^2$. A este respecto, la integración de los circuitos alcanza el nivel de *VSLI*, es decir, la de al menos 100,000 transistores en los mismos 25 $mm^2$. Así mismo está relacionada con la aparición del microprocesador (chip en el que se integran la unidad aritmética lógica, la unidad de control y los registros; como la obtención mediante circuitos integrados de una unidad central de proceso). La aparición del primer microordenador permitió que la informática se popularizase, llegando a todos los rincones del planeta y aplicándose a gran cantidad de actividades del ser humano, pasando a formar parte de su vida. Esta etapa caracteriza la especialización de aplicaciones de la informática. Entre ellas destacan las telecomunicaciones, el tratamiento electrónico de las imágenes. (gracias a ellas se pueden crear y manipularse por medio del ordenador), las bases de datos (colecciones de datos inter-relacionados y estructurados que se almacenan independientemente del programa utilizado y que permiten problemas tales como los de la reduplicación de la información contenida en los archivos, la inteligencia artificial (rama de la Informática, que superando el nivel del cálculo aritmético se especializa en el tratamiento lógico de la información), el desarrollo de sistemas expertos (que se aplican ya a la medicina y a la ingeniería, etc.), el desarrollo de los autómatas o robots capaces incluso de reconocer formas para interactuar con el medio en que

desarrollan su actividad y cuya creciente aplicación de los procesos industriales, ha generado la nueva rama de las técnicas llamada "Robótica".

Finalmente la llamada QUINTA GENERACION, puesta en marcha por las industrias japonesas del sector y mediante la cual a partir de 1981 se trabaja en el desarrollo de ordenadores inteligentes, desde el punto de vista físico trabajan sobre la base de simulación de los procesos que tienen lugar en el intelecto humano. Recibe el nombre de Quinta Generación, dado que se considera este nuevo concepto revolucionará los ordenadores tal y como sucedió con las válvulas de vacío y los circuitos integrados, etc. El concepto de las máquinas de la Quinta Generación se basa en dos elementos fundamentales: El Módulo de Resolución de Problemas y El Dispositivo de Gestión de las Bases de Conocimientos (es decir, aquella parte del sistema que alberga conocimientos de los especialistas, en la materia y, en la que la información está representada mediante reglas de producción o redes semánticas).

## 1.2. TEORIA DE LOS VIRUS[1]



Los virus que causan resfriados y enfermedades en seres humanos, suceden de forma natural y, son diferentes a los virus de computadora; donde cada sistema de virus es programado. Los motivos para crear virus informáticos son innumerables, pero **NO EXISTEN VIRUS BENEFICOS**, algunas veces son aparecen escritos, como un mensaje o una broma, quizá para irritar a la gente desplegando un mensaje

(1) PC Anti-Virus Book
Dr. Alan Solomon & Tin Kay

humorístico; en estos casos, el virus no es mas que una molestia. Pero cuando un virus es malicioso y causa daño real, ¿quién sabe realmente la causa? ¿Aburrimiento? ¿Coraje? ¿Reto intelectual?. Cualquiera que sea el motivo, el efecto puede ser devastador.

Prevención de la infección, afortunadamente proteger un sistema contra virus no es tan difícil, es posible protegerlo con un poco de conocimientos y algo de *software* de utilerías que se tengan a la mano; primero que se requiere conocer, es en que momento corre peligro de infección su sistema. Una vez que está dentro de la memoria de la computadora, el virus puede destruir programas y archivos de datos en su disco duro, la manera más común de pescar un virus de computadora es mediante el intercambio de programas o discos con otras personas. Aún programas comprados en paquetes sellados se han encontrado que algunos han tenido virus. La mejor precaución es tratar a todos los discos como portadores potenciales de infección, el verificar si hay virus, requiere de un *software* Antivirus, el cual explora los discos y programas en busca de virus conocidos y los erradica. Estos sistemas pueden ser fácilmente empleados una vez instalado en un sistema y activado; un buen programa Antivirus busca automáticamente archivos infectados cada vez que inserte un disco flexible o use su módem para bajar un archivo. Existen algunos programas Antivirus excelentes, algunos incluso son gratuitos. Una nota de precaución: CONSTANTEMENTE ESTAN APARECIENDO NUEVOS VIRUS, por lo cual se requiere ofrecer una protección absoluta contra ellos.

## 1.3. HISTORIA DE LOS VIRUS

Aunque la piratería de los sistemas de *software*, es el delito informático más predominante, uno igual, del preocupante, es la creación de virus computacionales. Un virus es al ámbito de la computación, un programa parásito oculto dentro de otro programa legítimo o almacenado en un área especial del disco llamada *Boot Sector* (sector de arranque). Al ejecutar el programa legítimo o al acceder al disco se activa

el virus, el cual puede estar programado para hacer muchas cosas, incluyendo copiarse a sí mismo en otros programas, mostrar información en la pantalla, destruir archivos de datos o borrar un disco duro completo. Un virus es programado para mantenerse dormido por un tiempo específico o activarse hasta cierto día.


## CRONOLOGIA DE LOS VIRUS Y MACROVIRUS MAS IMPORTANTES

| |
|---|
| La primera aparición fue en ESTADOS UNIDOS en el año de 1974 y en EUROPA en 1987. |
| En 1986 surge el virus BRAIN |
| En 1987 surge el virus CASCADE |
| En 1990 se crea el primer virus polimorfo DARK AVENGER |
| En ese mismo año se crea la E.I.C.A.R. (European Institute of Computer Anti Virus Reseach) |
| En 1991 surge el virus "MIGUEL ANGEL" |
| EN 1993, México sufre el ataque masivo del virus NATAS |
| En 1994 surge el rumor del virus GOODTIMES, resultando una broma |
| En 1995 surge otro virus polimorfo llamado Dir.Byway |
| En el mismo año surgen los primeros MACROVIRUS |
| En 1996 surge el primer virus para la plataforma de Windows, llamado el BOZA |
| En julio de ese mismo año aparece el primer MACROVIRUS para Microsoft Excel llamado XM.LAROUX. |
| También en julio aparecen los virus SPM (Stealth, Polymorfic, Multipartite). |
| El multipartita HARE KRISNA, causó grandes pérdidas de información a empresas de Estados Unidos y Canadá. |
| En México en el mes de julio aparece el virus ROTCEH. Dicho virus jamás se activa debido a un "Bug[2]" de programación. |

(2) Bug = bicho, error de programación

Como primer programa dañino, se comenta del famoso virus **MIGUEL ANGEL,** que causó un susto nacional en 1991, estaba programado para activarse el día del cumpleaños del artista. Cuando los usuarios prendieron sus computadoras infectadas ese día, el programa formateó sus discos duros borrando todos los datos y programas que estaban almacenados ahí. Los científicos del área de cómputo, discutieron por primera vez en 1992, la posibilidad de que un programa es capaz de duplicarse a sí mismo y extenderse entre las computadoras. Pero no fue sino hasta 1993 que un sistema *software* de Antivirus avanzado fue creado, cuando un estudiante en la universidad de California, Fred Cohen, escribió una tesis de doctorado sobre el tema.

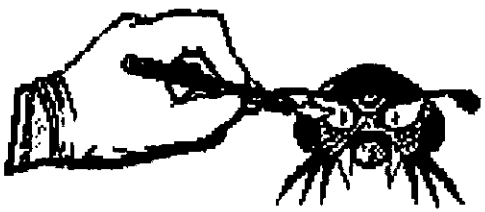
## 1.4. COMO FUNCIONA UN VIRUS COMPUTACIONAL

La función principal de un virus, es filtrase en los equipos cómputo contaminándolos, para después reproducirse y causar alteraciones en el funcionamiento de los mismo y de los programas.

Además, los virus informáticos son tan pequeños e invisibles que no puede ser vistos en algún directorio de la PC como si se tratara de cualquier programa de computación.

La segunda función para la que fue diseñado un virus computacional, es la REPRODUCCION, efecto que le permite infectar a una máquina con rapidez, siempre requerirá de algún medio para introducirse a la PC, ya sea por medio de *diskettes*, módem's (Internet) ó redes.

## 1.5. ANALISIS DE LOS CARACTERISTICAS DE UN VIRUS



Anatomía de un virus

Las principales cualidades de un programa de virus técnicamente son: 1.- La Reproducción, 2.- La Protección, 3.- El Disparador (*Tigger*) y 4.- El Efecto (*Payload*)

### 1.5.1. LA REPRODUCCION

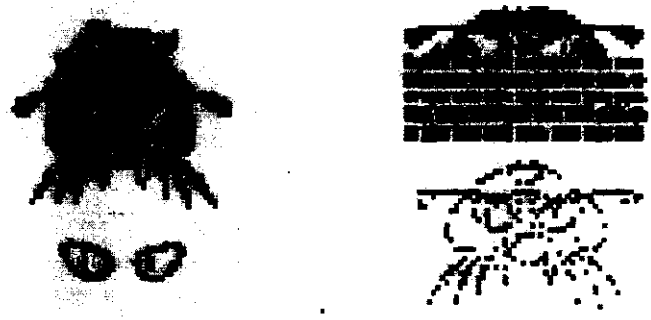
Es la principal actividad de los virus, un virus no puede infectar una máquina por si solo, sino que requiere de algún medio transmisor como un *diskette*, una red o un módem, etc.

Un virus es invisible que no puede ser visto tan fácilmente en una PC como un programa de archivo o sistema. Principalmente la infección se propagará en donde

haya archivos ejecutables o en archivos de texto elaborados en la plantilla de *Microsoft Office*, llamados "Macrovirus".

### 1.5.2. LA PROTECCION

Es la capacidad que tienen los virus, para defenderse de los buscadores de Antivirus mediante técnicas de ocultamiento y/o encriptamiento.



Son raros los Antivirus que buscan archivos comprimidos o particionados, pero al momento de descompactarse o unirse el virus empieza nuevamente a causar efectos. (Mientras esté compactado no podrá causar daño).

### 1.5.3. El DISPARADOR

Es el tercer componente llamado *Tigger*. Siendo éste la condición que debe cumplirse para que un virus se active o se dispare, pudiendo ser una fecha o un contador, etc. Un claro ejemplo lo tenemos en el reportado virus **DIR.BYWAY**, el cual se activa o se dispara cada mes mediante la siguiente operación aritmética:

(El número del mes X 2)+2

Tenemos que el mes de enero el virus se disparará el día 4, y para los demás meses serán los siguientes días:

| | |
|---|---|
| 1 X 2 + 2 = 4 | El virus se activa el día 4 de Enero. |
| 2 X 2 + 2 = 6 | El virus se activa el día 6 de Febrero. |
| 3 X 2 + 2 = 8 | El virus se activa el día 8 de Marzo. |
| 4 X 2 + 2 = 10 | El virus se activa el día 10 de Abril. |

| | |
|---|---|
| 5 X 2 + 2 = 12 | El virus se activa el día 12 de Mayo. |
| 6 X 2 + 2 = 14 | El virus se activa el día 14 de Junio. |
| 7 X 2 + 2 = 16 | El virus se activa el día 16 de Julio. |
| 8 X 2 + 2 = 18 | El virus se activa el día 18 de Agosto. |
| 9 X 2 + 2 = 20 | El virus se activa el día 20 de Septiembre. |
| 10 X 2 + 2 = 22 | El virus se activa el día 22 de Octubre. |
| 11 X 2 + 3 = 24 | El virus se activa el día 24 de Noviembre. |
| 12 X 2 + 2 = 26 | El virus se activa el día 26 de Diciembre. |

Además, despliega el mensaje: *"TRABAJEMOS TODOS POR VENEZUELA"* y toca el himno de este país por la bocina, a las 03:00, 06:00, 09:00; 15:00, 18:00, 21:00 y 24:00 hrs.

### 1.5.4. El EFECTO

Es la reacción del virus que será observada al estar ejecutando un sistema, pueden notarse cosas o acciones raras, también puede transformarse la información en código *ASCII*, borrar datos o producir sonidos raros. También es la forma de manifestación del virus una vez activado, pudiendo ser desde un mensaje musical, o imágenes, hasta el borrado de la información.

Aproximadamente a mediados de 1998, se conocen más de 17,500 tipos de virus diferentes incluyendo sus variantes, la mayoría de los sistemas de Antivirus, cuentan con una biblioteca incluida en su menú de soporte con el nombre de los virus, sus efectos y donde residen, que daños causan, cuando se activan y que tipos de variantes existen.

Los virus poseen otras características principales: *SEALTH* (Ocultamiento), *POLIMORPHISM* (Polimorfismo), *FAST-INFECTOR* (Rapidez) y *SLOW–INFECTOR* (lentitud).

### 1.5.5. OCULTAMIENTO

Es la capacidad de los virus para poder ocultarse e infectar antes de ser descubiertos, cuando el virus termina de ejecutarse enseguida pasa el control al programa *Boot Sector*, etc.

### 1.5.6. POLIMORFISMO

Es la capacidad de los virus para encriptarse de forma distinta cada vez que infectan.

| | | |
|---|---|---|
| ARCHIVO EJECUTABLE | VIRUS |  |
| ARCHIVO EJECUTABLE |  | VIRUS |

### 1.5.7. RAPIDEZ

Es la capacidad de los virus para infectar de forma sumamente rápida de los sistemas

Ejemplo.-

> Existe un fast-infector (**DIR.BYWAY**, por ejemplo) y utilizan un *software* que ejecuta muchos archivos. En ese momento, todos ellos ya están infectados por el virus.

### 1.5.8. LENTITUD

Es la capacidad de los virus para infectar de forma sumamente lenta los sistemas.

Ejemplo.-

Existe un *low-infector* que sólo infectará los archivos que sean copiados del sistema infectado a un *diskette*.

## 1.6. CLASIFICACION DE LOS VIRUS

### 1.6.1. VIRUS DE ARCHIVO

Son aquellos que infectan archivos de programas ejecutables **". EXE"**, los archivos de programas ejecutables son aquellos que llevan como extensión:

| | | | |
|---|---|---|---|
| .EXE | .COM | .DLL | .OVL |
| .APP | BIN | .DOT | .DOC |
| .XTP | .QLB | .DEV | .BAT |
| .INI | .DRV | .CMD | .SYS |

Ejemplo: Virus **TSR**[3] de archivo, como el virus DIR.BY.WAY

Virus **NO TSR** de archivo, como el virus VIENNA

### 1.6.2. VIRUS DE SECTOR DE ARRANQUE

Son aquellos que infectan el sector de arranque (*Boot Sector*) de discos duros y *diskettes*. El Sector de arranque es la parte que contiene el código necesario para poder encender la computadora (donde se carga el *File System* del *DOS*).

**Nota**: Un *diskette* sólo tiene sector de arranque, no de partición. El disco duro tiene los dos sectores.

### 1.6.3. VIRUS DE SECTOR DE PARTICION

Son aquellos que infectan el sector de partición, (también conocido como el *MASTER BOOT RECORD*) de los discos duros. El ***MBR*** es la parte que contiene información referente al número de sectores de cada partición, su localización, etc.

(3) TSR = TERMINATE STAY RESIDENT = PROGRAMA QUE RESIDE EN LA MEMORIA ALTA

**SECTOR MBR**

Es el primer sector del disco duro que se activa cuando el sistema enciende, contiene información del disco, así como el número de sectores de cada partición y su localización.

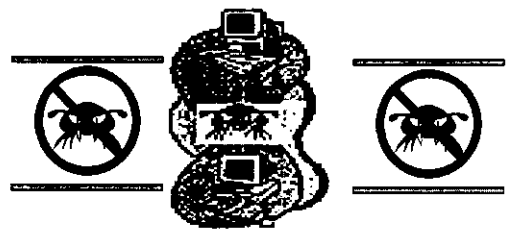
### 1.6.4. VIRUS MULTIPARTITAS

Son aquellos que infectan tanto archivos de programas ejecutables como sectores de arranque de discos duros, *diskettes* y sectores de partición de discos duros. Ejemplo: el virus **NATAS**.

### 1.6.5. MACROVIRUS

Son la nueva generación de virus informáticos y tienen la peculiaridad de infectar archivos de datos creados bajo *Microsoft Word* y *Microsoft Excel*. Son multiplataformas ya que pueden infectar bajo *Windows* 3.x, *Windows 95*, *Windows NT* y *Macintosh*, infectan con tan solo abrir un documento y están desarrollados en *WordBasic*.

## 1.7. PROCESO DE AFECTACION A UNA ORGANIZACION POR VIRUS



Una empresa o cualquier organización que cuente con sistemas de cómputo, módem's o redes, está susceptible de que los usuarios, gente de soporte técnico, familiares de los empleados, *software* original, otro *software* (juegos, *shareware*) y vendedores (corriendo demos), pueden infectar de virus los equipos; tenemos los siguientes casos:

| | |
|---|---|
| Caso 1 | Máquina limpia, *diskette* infectado con un virus de sector de arranque (archivos limpios). |
| Caso 2 | Máquina limpia, *diskette* infectado con un virus de archivo (sector de arranque limpio). |
| Caso 3 | Máquina infectada con un virus de sector de arranque *diskette* limpio. |
| Caso 4 | Máquina infectada con un virus de archivo, *diskette* limpio. |

## 1.8. DAÑOS QUE OCASIONA UN VIRUS

Los daños que puede causar un virus en el *hardware* y *software*, van desde mínimos hasta ilimitados, los tipos de daños son los siguientes:

- DAÑO TRIVIAL
- DAÑO MENOR
- DAÑO MODERADO
- DAÑO MAYOR
- DAÑO SEVERO
- DAÑO ILIMITADO

### 1.8.1. DAÑO TRIVIAL

Este tipo de daño es insignificante, ya que la integridad de la información no corre ningún peligro.

Ejemplo.-

El virus **FORM** hace sonar un **Beep** cada vez que el usuario presiona una tecla; esto sucede los días 18 de cada mes, tiene resultados triviales, tarda 30 minutos en repararse, puede infectar los sectores de arranque y de partición, reside en memoria, tiene poca capacidad de ocultamiento, no tiene propiedades para encriptarse y solo existen dos variantes.

### 1.8.2. DAÑO MENOR

En este caso el usuario se da cuenta inmediatamente de que hay algo raro en la computadora, sospechando de algún tipo de virus.

Ejemplo.-

El virus **JERUSALEM**, una vez cargado en memoria, borra todo programa que intente ser ejecutado los días viernes 13. Lo peor que puede pasar es reinstalar algunos programas, tarda 30 minutos en repararse, infecta a los archivos con extensión: .COM y .EXE, además reside en memoria, tiene poca capacidad para ocultarse, encripta algunos archivos, es conocido también como el **ISRAELI**, tiene 10 variantes con nombres distintos.

### 1.8.3. DAÑO MODERADO

El usuario pierde toda su información pero puede recuperar parte de ella, utilizando el "*Backup*" realizado el día anterior.

Ejemplo.-

El virus más famoso por ocasionar un daño moderado, es el "**MIGUEL ANGEL**". Un daño moderado sucede cuando algún virus formatea el disco duro sobre escribe basura en él, o de plano destruye la ***FAT***[4].

(4) FAT = *FILES ALLOCATION TABLE* (TABLA DE LOCALIZACIÓN DE ARCHIVOS"

### 1.8.4. DAÑO MAYOR

El usuario pierde su información y al intentar recuperarla con sus "*Backup's*", se da cuenta que también estos respaldos están dañados.

Ejemplo.-

El virus **DARK AVENGER**, cada 16 veces que un archivo infectado con este virus es ejecutado, el virus escribe **"EDDIE lives... some where in time"**, en un sector al azar del disco duro. El usuario sabe que su información está corrupta por que ve el mensaje.

### 1.8.5. DAÑO SEVERO

El usuario no se da cuenta de que su información así como sus "***Backup's***", están dañados ya que el virus actúa lenta y progresivamente.

Ejemplo.-

El usuario hace su respaldo sin saber si su información está correcta o dañada, el virus sigue latente, no hay que buscar como en el caso anterior (el mensaje **"EDDIE lives... some where in time"**).

### 1.8.6. DAÑO ILIMITADO

El usuario no se da cuenta de que el virus violó la seguridad y ahora cualquiera puede infiltrarse en los sistemas.

Ejemplo-

El virus **CHEEBA**, obtiene el password del administrador del sistema y crea un nuevo usuario con todos los privilegios, con un nombre de usuario determinado y password. El daño que se puede hacer teniendo este usuario y password es enorme. Este virus afecta archivos con extensión: .COM y .EXE, infecta el sistema de

memoria, tiene poca capacidad de ocultamiento, por completo encripta al virus y tiene alta capacidad de defensa contra sistemas de Antivirus y existen sólo dos variantes.

## 1.9. DAÑOS EN EL HARDWARE

Existen diferentes criterios con respecto al tipo de daños en el hardware:

1. Algunos desarrolladores de sistemas de Antivirus, dicen que no existe virus que dañe físicamente el hardware de un equipo de cómputo.

2. Otros dicen que existen algunos virus que provocan el aumento de velocidad de un disco duro; esto solo lo hará variar en su funcionamiento, pero no se comenta que físicamente lo dañe.

3. Hay quienes afirman que recibieron un mensaje en su sistema, "El disco sufre alto calentamiento"; después no tuvieron acceso a él; y en todos los casos trataron de repararlo y, al no conseguirlo, optaron por abrirlo hallándolo internamente calcinado. No ha sido demostrado técnicamente que la causa haya sido por algún virus.

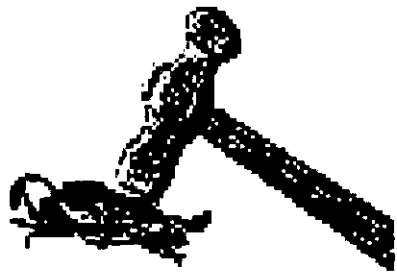
4. Otros criterios explican y afirman; que como un virus es un programa, este programa puede activar en sus instrucciones, la orden para que las cabezas lectoras se aterricen sobre la superficie del disco duro y entonces se dañe físicamente uno o varios sectores.

5. Con respecto a los virus que infectan a los sectores de arranque y partición, tanto como los que contaminan el área de memoria superior, no se conocen comentarios de que hallan sufrido daño físico.

# CAPITULO 2

# EFECTOS Y MEDIDAS DE PREVENCION DE UN ANTIVIRUS

## 2.1. MEDIDAS DE PREVENCION[1]



Los virus informáticos se han convertido en una seria amenaza para los datos y programas de computadoras. Ahora todas las PC's son candidatas a ser infectadas por un virus, lo que puede llegar a costar grandes cantidades de dinero. Ningún virus puede funcionar por sí solo; requiere forzosamente de algún lugar para alojarse y desde ahí comenzar su infección, este lugar puede ser:

- Un sector de arranque
- Un sector de partición
- Un archivo

Hasta el momento algunos fabricantes de Antivirus, no tienen noticia de que algún virus dañe *físicamente* el *Hardware* de una máquina, por lo que únicamente peligra el *Software* y la información que se tenga almacenada en la computadora.

(1) PC Anti-Virus Book
Dr. Alan Solomon & Tim Kay

Un virus no puede infectar una máquina por sí solo, sino que requiere de algún medio transmisor como un *diskette*, una red, un módem, etc. Un virus es tan pequeño e invisible que no puede ser visto en algún directorio de la PC como cualquier otro archivo (nombre, extensión)

Cuatro medidas básicas de prevención contra los virus:

| |
|---|
| Escáner "*ON–DEMAND*" en cada máquina. |
| Escáner "*ON-ACCESS*" en cada máquina. |
| Computadora "*SEEP-DIP*". |
| Protección en Red. |

### 2.1.1. ESCANER "*ON–DEMAND*"

Todos los *diskettes* deben ser escaneados con un escáner "*ON-DEMAND*". Cada usuario tendrá la obligación de hacerlo. Un escáner "*ON–DEMAND*", es aquel que únicamente va a realizar sus funciones cuando el usuario se lo indique por medio de un comando. En otras palabras es la instrucción que tiene que teclear el usuario para verificar la existencia de virus en su equipo.

### 2.1.2. ESCANER "*ON-ACCESS*"

Esta medida hace que el usuario no note la presencia del escáner, salvo en el momento en que se encuentre un virus. Además, evita que una PC se infecte. Un escáner "*ON-ACCESS*", es aquel que realiza sus funciones una vez cargado en memoria. Este tipo de escáner es un *TSR*, el usuario ni siquiera sabe que está presente.

(3) TSR = TERMINATE STAY RESIDENT = PROGRAMA QUE RESIDE EN LA MEMORIA ALTA

**Nota**: ***TSR*** *(TERMINATE AND STAY RESIDENT)* programa que reside y permanece en memoria, se refiere a programas que permanecen en memoria de forma que se pueden extraer en cualquier aplicación, pulsando simplemente una combinación de teclas. El programa se visualiza o bien en una ventana pequeña en la parte superior del texto, o bien en la pantalla completa, cuando sale de este programa, se restauran los contenidos de la pantalla anterior.

Todos los Antivirus tienen un *TSR* que actúa como centinela, el cual vigila en todo momento cuando está encendida la PC, impidiendo la lectura de un archivo contaminado. Por lo que se recomienda a los usuarios, tener siempre actualizada la versión del Antivirus, de no ser así, se corre un gran riesgo de que un nuevo virus pase inadvertido para la versión actualmente instalada, por lo tanto no lo podrá eliminar.

### 2.1.3. COMPUTADORA *"SEEP-DIP"*

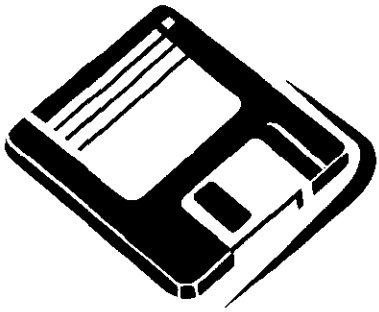
Para la gente de Soporte Técnico resulta muy práctico tener una computadora de sacrificio, ya que las actualizaciones son fáciles de realizar. Esta computadora tendrá las funciones de limpiar cada *diskette* a utilizar en el corporativo. Funciona como una "ADUANA". Esta medida será de gran importancia y ayuda para el área de cómputo, ya que un descuido puede ser fatal. El virus puede entrar, reproducirse e infectar archivos, pero mientras no se active o cause daño, es conveniente calendarizar una revisión para asegurarse de que no exista virus en los equipos de cómputo.

### 2.1.4. PROTECCION EN RED

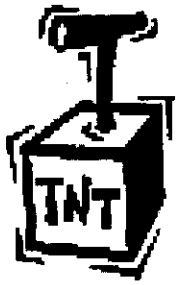
- Crear directorios *"READ-ONLY"*.
- Crear programas *"EXECUTE-ONLY"*.
- Crear archivos individuales *"READ-ONLY"*.
- Instalar un *NLM's*[5]
- Instale servicios.

(5) NLM = NetWare Loadble Module = Módulo cargable
NetWare (Diccionario de Computacion *ALAN FREEDMA)

También es conveniente respaldar periódicamente los archivos más importantes en otro lugar del área de cómputo.



## 2.2. POR QUE SE PIERDE INFORMACION




La información se puede perder por las siguientes causas:

- POR ERROR HUMANO
- POR FALLAS EN EL *SOFTWARE*
- POR FALLAS EN EL EQUIPO
- POR CASOS DE VIRUS

### 2.2.1. POR ERROR HUMANO

- La información se pierde en este caso por errores humanos, cuando se desconoce el manejo de los comandos de los sistemas con los que se trabaja.

- Cuando se hacen prácticas con el movimiento o copia de archivos.

- Cuando se utilizan *diskettes* defectuosos para grabar información, ya sea por el trato o por su mala fabricación.
- Por sobre escribir en un archivo y luego salvarlo sin darse cuenta que está eliminando a la información anterior.
- Por no saber renombrar correctamente el nombre y extensión de un archivo.
- Cuando algo falla en la PC o se produce pérdida de datos, la causa más probable no será un virus o un problema del *software*, sino un error humano. Todos cometemos errores, como introducir la secuencia de teclas equivocada o pulsar DEL *.* en la carpeta incorrecta, lo que puede provocar serias consecuencias. Recuerde que la parte más valiosa de la computadora son los datos introducidos; el *hardware* y programas se pueden sustituir, pero los datos sólo se pueden recuperar si ha realizado una copia de respaldo.

### 2.2.2. POR FALLAS EN EL *SOFTWARE*

- En este caso se puede perder información cuando no se cuenta con el *software* original. La mayoría de los usuarios en especial en este país, practican la

piratería del *software*, algunas veces los sistemas están protegidos contra los piratas del *software* y no son fácilmente copiables, también algunos productores de *software* instalan sistemas llamados "Caballos de Troya", los cuales se activan al instalar el *software* ilegal en el equipo de cómputo.

- Cuando un usuario avanzado altera los archivos para que no puedan ser ejecutados, generando *Bugs* de programación.

### 2.2.3 POR FALLAS EN EL EQUIPO

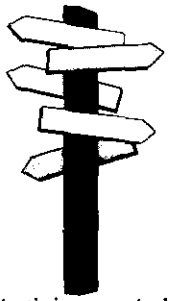
- La pérdida de información cuando falla el equipo, puede deberse a que la fuente de alimentación del ordenador este variando el voltaje y provoque variaciones en el procesamiento de las funciones que realiza el procesador.
- También puede deberse al estado físico del disco duro, cuando tiene sectores dañados. En este caso, si al momento de estar guardando o escribiendo en el disco duro, se llega al lugar donde se encuentra un sector dañado, es posible que la información no sea correctamente grabada, particionándola, y al querer leerla nuevamente ya no es posible abrirla o leerla.
- Por falta de mantenimiento o falla electromecánica en la unidad *drive* de lectura y grabación de discos flexibles.
- Por falta intempestiva de voltaje o apagar el equipo sin haber guardado la información.

### 2.2.4. POR CASOS DE VIRUS

- Cuando un virus llega a manifestar sus efectos, puede convertir la información en caracteres raros, también borrarla, y quizás hasta dañar el disco duro. Hoy en día existen virus tan avanzados que destruyen completamente la FAT[4] de los discos duros, siendo imposible repararlos. Estos virus son adquiridos en su mayoría por los usuarios que manejan y bajan información por Internet.

(4) FAT = *FILES ALLOCATION TABLE* (TABLA DE LOCALIZACIÓN DE ARCHIVOS)

## 2.3. LINEAMIENTOS PARA UNA POLITICA DEL ANTIVIRUS



los lineamientos de una política Antivirus, están basados en 4 aspectos principales:

- REGLAS
- PROCEDIMIENTOS
- EDUCACION
- HERRAMIENTAS

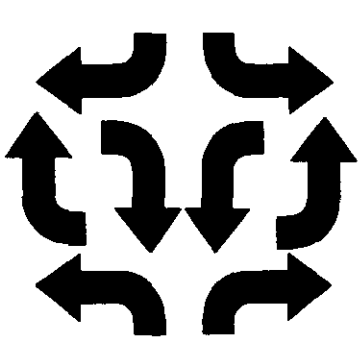
El principal objetivo es: Evitar que los virus informáticos se alojen sin ser descubiertos por los usuarios; entonces es necesario formar una organización.

- Las reglas estipulan "LO QUE HAY QUE HACER"
- Los procedimientos indican "¿CÓMO HAY QUE HACERLO?"
- La educación nos permite "¡ENTENDER EL PORQUÉ!"
- Las herramientas "COMO LO HACEN"

### 2.3.1. REGLAS

- Cualquier persona que introduzca un *diskette* a la Empresa, deberá llevarlo a área de Soporte Técnico, para que sea verificado y autorizado.

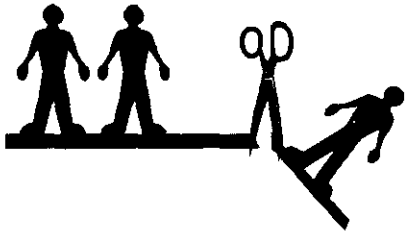
- Cualquier persona que detecte un virus (o sospeche que tiene un virus) deberá notificar a Soporte Técnico de inmediato para su comprobación y eliminación.



### 2.3.2. PROCEDIMIENTOS

- Para escanear un *diskette* en la computadora de sacrificio ("*SHEEP-DIP*") el usuario deberá tener instalado y activo en memoria, un sistema de Antivirus; en este caso hablaremos del funcionamiento del sistema de Dr. Dolomon's:
  1. Introducir el *diskette* en el *drive* de disco flexible
  2. Seleccionar la opción 1 "Buscar por virus"
  3. En caso de encontrar virus, seleccionar la opción 2 "limpiar virus de A:\> "
  4. Para terminar o salir, presionar la tecla ESC

### 2.3.3. EDUCACION



Hay que acostumbrar a los usuarios, a hacer respaldos diarios, semanales o quincenales de su información.

- Hay que explicarles los riesgos que trae consigo un virus computacional.
- Hay que explicarles la diferencia entre *software*, *shareware* y *freeware*.

***Software:*** Son instrucciones para una computadora. También son una serie de instrucciones que realizan una tarea en particular, llamado programa o sistema de *software*. Las dos categorías principales son *software* de sistema y, de aplicaciones.

- El *software* de sistemas se compone de programas de control, incluyendo el sistema operativo, *software* de comunicaciones y administrador de base de datos.
- El *software* de aplicaciones es cualquier programa que procesa datos para el usuario (inventario, nómina, hoja de cálculo, procesador de texto, etc.).

***Shareware***: *(Software compartido). Software* distribuido a través de BBS[6] y servicios de información libres de cargo sobre una base de prueba. Si se utiliza, se paga por él, con el que se recibe una documentación adicional, un soporte o posiblemente la siguiente mejora sin costo alguno. Se requieren licencias de pago para su distribución comercial.

***Freeware***: *Software* distribuido sin cargo. La propiedad la retiene el desarrollador que tiene el control de su redistribución, incluyendo la capacidad de cambiar la siguiente versión del *freeware*.

## 2.3.4. HERRAMIENTAS[1]

No podemos eliminar virus con nuestras manos, por lo que requerimos de un buena herramienta Antivirus que nos asegure una prevención y en su caso una buena reparación.

(1) PC Anti-Virus Book
Dr. Alan Solomon & Tin Kay
Ultimo Capítulo "Enciclopedia de Virus"

(6) BBS = Bulletin Board System

## 2.4. BOLETINES DE VIRUS

En los Estados Unidos la primera aparición de estos fue en 1974 (7 años antes del lanzamiento de la primera IBM PC). Ese mismo año se crea a la *BBS*.

**BBS** (*Bulletin Board System*)

Sistema de tablero de anuncios o boletines. Un sistema de computación que funciona como un sistema de mensaje y como fuente centralizada de información para grupos de interés particular. Los usuarios se comunican vía telefónica con el tablero de boletines, revisan y dejan mensajes para otros usuarios, así como se comunican con otros usuarios del sistema al mismo tiempo. Los tableros de boletines pueden proveer acceso o puertas a otros programas de aplicación.

- Artículos sobre virus algunas veces llamados "*Worms*", aparecieron por primera vez en medios impresos a principios de 1980.
- El éxito de un virus se basa en la capacidad de autoreplicación y este código fue demostrado por primera vez en los laboratorios de *Rank Xerox*.

- En el Reino Unido su primera aparición fue en 1987.

- En 1987 apareció en la Universidad de Delaware un virus en el *Boot Sector* de un *Floppy*.

- También en 1987 nació el virus **CASCADE**.

- En 1990 fue el año en el que se creó al primer virus polimorfo, aparece el temible "**DARK AVENGER**".

- En ese mismo año, los desarrolladores de Antivirus deciden organizarse para combatir a las organizaciones desarrolladoras de virus que se estaban formando; fue así como en el mes de diciembre surge la *EICAR* (*European Institute for Antivirus Research*) en la ciudad de Hamburgo.
- Los años de 1991, 1992 y 1993 fueron años de gran avance tecnológico en aspectos del desarrollo de nuevos virus.

- Aparecen nuevos productos Antivirus:
- NORTON en diciembre de 1990.
- CPAV en abril de 1991.
- Algunos más de origen Israelí.

- Se crea el primer BBS para intercambio de virus en Bulgaria.
- Probablemente el evento más importante de *1992* fue el caso del virus **MIGUEL ANGEL**.
- En el año de 1993 la *EICAR* permitió la distribución del código "*Engines*" de índole polomórfico.
- También era la primera vez que una compañía que desarrollaba Antivirus (XTREE) se retiraba del mercado.
- Apareció un grupo en Holanda llamado *Trident* y el principal autor de ellos, *Masourf Khafir*, escribió "TPE" (*Trident Plymorphic Engine*).
- Para 1993, México toma conciencia de este problema con el ataque masivo del virus **NATAS**. Se calcula que al menos 70% de las computadoras en México se vieron afectadas por este virus.

- Para el año de 1974 se alcanzó la cifra de 6000 virus en el campo y continúa creciendo.
- Surge también en 1994 el rumor del virus "**GOOD TIMES**", que se suponía estaba siendo enviado por correo electrónico (e-mail), resultando ser sólo una falsa alarma, que más bien era un fallo aleatorio.

- La aparición de los MACROVIRUS en 1995, da como resultado que cualquier plataforma de sistema operativo puede ser infectada por el intercambio de archivos de datos.
- En agosto de 1995 aparece un nuevo virus polimorfo **DIR.BYWAY**, que toma el control del *File System* de *DOS*
- En el mismo año aparece el *WinWord* **CONCEPT**, virus relacionado multiplataformas que ataca a todos los usuarios del sistema *Word* en el mundo.
- En enero de 1996 aparece el primer MACROVIRUS que infecta documentos de AMPIPRO y se le conoce como **GREE STRIPE**.
- En febrero de 1996 se crea el primer virus para la plataforma *Windows 95* llamado "**BOZA**".
- En Julio de 1996 aparece el primer MACROVIRUS para Excel llamado **XM.Laourx**, escrito en *Visual Basic for Aplications* (*VBA*).
- En ese mismo mes aparece un virus **SPM** muy peligroso llamado **HARE KRSNA**, causando grandes pérdidas de datos en empresas de Estados Unidos y Canadá.
- En septiembre de 1996 *Microsoft* embarca un Macrovirus llamado **WAZZU** dentro del CD de Solution Provider.
- En noviembre de 1996 aparecen en México los MACROVIRUS **WAZZU**, **NPAD** y **MDMA**.
- A inicios de 1997, surge un nuevo virus llamado **INTCE**, diseñado específicamente para impedir el encendido normal de las computadoras. En febrero de 1997, se descubre un nuevo MACROVIRUS llamado **ShareFUN**, cuya característica principal es que utiliza *Microsoft Mail* como medio de dispersión para infectar documentos.
- La edición de septiembre de 1996 de *Microsoft SPCD* (*Solution Provider CD*) contiene un documento infectado con el virus **WM.Wazzu**. esta edición del *SPCD*, incluye *Microsoft Internet Explorer*, conexiones a *SITES WWW*, demos

de productos, logos de *Solution Provider*, etc., ha sido distribuido a todos los "*Solution Providers*" de *Microsoft*. El archivo infectado se llama: ED3905A.DOC, y se encuentra localizado en el directorio: \SIA\MKTOOLS\CASE. Así mismo, el *web-site* en CD-ROM "*Letz* Fetz on the *Netz*", distribuido por *Microsoft* en el reciente "*Orbit trade-show*" en Basle, Suiza, también contiene un archivo infectado con el **WM.Wazzu**; inclusive un documento que estaba localizado en el web-site suizo de *Microsoft*, contenía también al virus **Misc.** Entonces lo que quitó del Site, al descubrir estos incidentes de virus.

## 2.5 ACTIVIDADES Y EFECTOS DE LOS VIRUS MAS COMERCIALES

### 2.5.1. INTCE

Es un virus de sector de arranque y de partición (infecta sectores de arranque de *diskettes* y sectores de partición de discos duros). Pero esto no es lo que lo hace único, lo particular de este virus es que está diseñado específicamente para evitar que el usuario encienda su máquina desde un *diskette* de arranque libre de virus.

Ejemplo:

> Si tratamos de limpiar una máquina infectada de virus, primero la encendemos y la iniciamos en limpio desde un *diskette*, de esta forma el virus no puede cargarse en memoria y por lo tanto no puede ocultarse, lo que significa una fácil detección y reparación del mismo.

Hasta antes del virus **INTCE,** lo anterior era válido y suficiente para eliminar este tipo de virus. Sin embargo, a partir de este momento ya no lo es (al menos en este caso). Para evitar un encendido de la computadora "en limpio", **INTCE** inserta cierto código en el disco duro, lo que ocasiona que el DOS se bloquee al tratar de encontrarlo, todo esto es por supuesto, antes de que el sistema operativo se cargue por completo. La máquina se vuelve inaccesible. *Peter Morley*, experto investigador

de *Dr. Solomon's Software* dijo: "hasta ahora, si alguien me hubiera dicho que no podía encender en limpio, yo le hubiera dicho que se trataba de un problema de *hardware, a*hora tendré que revisar mis notas". Cuando el virus infecta la computadora y se carga en memoria, es casi imposible detectarlo: ningún *software* Antivirus es capaz de identificarlo, afortunadamente para nuestros usuarios, la marca de Antivirus (*Dr. Solomon's Software*) cuenta con un *diskette* de arranque libre de virus (garantizado) llamado "MAGIC BULLET", incluido en el Antivirus TOOLKIT. De hecho, es el único desarrollador de Antivirus que tiene este tipo de herramienta.

El sistema MAGIC BULLET, utiliza una tecnología propietaria para iniciar la máquina por lo que no utiliza el mecanismo de *DOS*, utilizado por el virus para prevenir un encendido en limpio: esto significa que el MAGIC BULLET es capaz de identificar y reparar al virus **INTCE**.

### 2.5.2. WM.SHAREFUN

Acaba de ser descubierto un nuevo Macrovirus llamado **ShareFun**, cuya característica principal, es que utiliza *Microsoft Mail* como medio de dispersión para infectar documentos. Este Macrovirus ha sido encontrado únicamente en un solo lugar en Estados Unidos, por lo que no podemos afirmar que ya está "en el campo". De hecho, para que un virus pueda ser considerado "en el campo" debe ser visto en más de dos lugares diferentes e independientes entre sí.

### 2.5.3. CARACTERISTICAS DEL MACROVIRUS[7]

Como se mencionó al inicio de este subtema, **ShareFun** utiliza *Microsoft Mail* para esparcirse a todas las computadoras. Cada vez que un archivo infectado es abierto, existe un 25% de probabilidad de que el virus se dispare (1 de cada 4 veces). Si *Microsoft* Mail está activado, el virus obtiene el nombre de tres personas distintas de la dirección de correos establecida en el *Mail* y les manda un correo electrónico en

(7) Tomado de la Enciclopedia del sistema de Antivirus de Dr. Solomon's Vers. 7.86

el título (subjet) siguiente: "*You have GOT to see this*". Dicho correo no contiene nada de texto; en cambio trae adjunto un documento llamado DOC1.DOC, que es una copia del documento que el usuario había abierto cuando el virus se activó. Por supuesto que DOC1.DOC trae consigo el Macrovirus. Si alguien que recibió dicho e-mail abre el documento adjunto, infectará todo el sistema de *Microsoft Word*.

Observaciones:

Es importante enfatizar los siguientes puntos con relación a este nuevo Macrovirus **ShareFun**, sólo ha sido visto en un lugar de Estados Unidos, por lo que no está catalogado como un virus "en el campo". El intento del **ShareFun** por utilizar *Microsoft Mail* no es del todo adecuado, por lo que en la mayoría de las instalaciones con *MS* Mail fallará en su dispersión. **ShareFun** posee las características estándar de cualquier otro Macrovirus, lo que significa que no importa que no se tenga *Ms Mail*, con abrir un documento infectado a través del *MS Word* bastará para que comience su infección.

### 2.5.4. WM WAZZU[7]

Es un Macrovirus que infecta documentos de *Microsoft Word* para *Windows*. El virus es distinto de la mayoría de los Macrovirus, debido a que sólo contiene una macro, **AutoOpen**. La gran mayoría de los Macrovirus requieren de más macros para su correcto funcionamiento, no importando si están ejecutando desde la plantilla global (NORMAL.DOT – que en este caso, el sistema ya está infectado). O si se trata de una nueva infección. El virus **WAZZU** utiliza una técnica más eficiente que la anterior ya que checa el nombre del documento maestro. Debido a que el nombre de la macro que utiliza este virus, es el mismo de todas las versiones de *Word* en sus diferentes idiomas. **WAZZU** es el primer virus que se replica exitosamente en todas las versiones internacionales de *Word*. **WM.Wazzu** tiene un payload más interesante e ingenioso. Cuando un documento es abierto, el virus genera un número aleatorio mayor a 0 y menor a 1. Si este número es menor que 0.2

(1 de 5 veces), el virus mueve una palabra a otro lugar al azar dentro del mismo documento, lo que representa una probabilidad del 48.8% de que al menos una palabra va a ser movida de su posición original. Después de hacer 3 veces lo mismo, el virus vuelve a generar un número aleatorio mayor a 0 y menor que 1. Si este número es menor que 0.25 (uno de 4 veces), el virus inserta la palabra "**wazzu**" (también en un lugar al azar dentro del documento). Finalmente el virus regresa al principio del documento. Es importante que los archivos que hayan sido abiertos en una PC infectada con este virus sean revisados manualmente, para asegurarse que no hayan sido modificados, puede utilizarse la función FIND de *Word* para buscar la palabra "**wazzu**". La palabra "**wazzu**" aparentemente es usada con frecuencia en el noroeste de E. Unidos para referirse a la Universidad estatal de Washington (en Pullman, Washington). Sin embargo, es imposible decir si el virus salió de ahí o no.

### 2.5.5. DIR.BYWAY[7]

Es un virus polimorfo que toma el control del *File System* de *DOS*, e infecta de manera sorprendente rápida a las computadoras y *diskettes* en todo el mundo, apareció por primera vez el 9 de Agosto de 1995.

Orígenes.- "**Dir.Byway**" fue nombrado así debido al segundo de 2 mensajes encriptados que contiene el virus: "*The Hndv* y *<by:WaiChan,Aug94,UCV>*." También se debe su nombre a un viejo virus residente en memoria él: "**DIR II**" que ataca en forma similar, **DIR II** se propagó en todo el mundo pero ya no es encontrado frecuentemente en el campo debido a que no es compatible con *DOS* 6.0, *Dmirty Grayaznov*, miembro del equipo de investigación de S&S, cree que el

(7) Tomado de la Enciclopedia del sistema de Antivirus de Dr. Solomon's Vers. 7.86

mensaje del virus puede ser una broma, debido a que el texto sugiere a Venezuela como el país de origen. Sin embargo el autor firmó como *WaiChan*, lo que podría indicar un origen chino. Las primeras muestras de este virus que recibió S&S International fueron en el mes de Julio, estas muestras fueron provenientes de Inglaterra y Estados Unidos, por lo que el equipo de investigación de S&S advierte que es una seria amenaza para todos los usuarios de computadora. El virus "**Dir.Byway**", como todos los virus polimorfos, (mutación) cambia cada vez que infecta, haciéndose extremadamente difícil su identificación y eliminación. Este virus opera como si fuera un *TSR* (programa residente en memoria). Cuando el directorio raíz de un archivo ejecutable es accedido, el virus infecta a todos los archivos: .COM y .EXE. Pero esta infección no se limita sólo al directorio raíz por *default*, sino que infecta a todos los archivos ejecutables que se encuentren en los directorios indicados en la FAT. Además de esto, no se requiere de mucho para activar el "*trigger*" del virus. Un simple comando DIR es suficiente para que el virus se dispare. Por ejemplo, si el usuario teclea "WIM" en lugar de "WIN" que es el comando utilizado para correr *Microsoft Windows*, *DOS* busca el ARCHIVO WIN.COM, WIN.EXE o WIN.BAT en todos los directorios listados en el *path* definido en el AUTOEXEC.BAT, y de esta manera logra infectar a todos los archivos *.EXE y *.COM, de todos los directorios indicados en el *path*. Esta característica de infectar a los archivos: .EXE y .COM de todos los directorios que están definidos en el *path* de la computadora, hace que el virus "**Dir.Byway**" sea clasificado como "*superfast infector*" o en otras palabras, es un virus con un sistema de infección sorprendentemente rápido. A diferencia de muchos otros virus de computadora, "**Dir.Byway**" no agrega su código a los archivos infectados. En lugar de eso, crea un archivo llamado "CHKLIST.MS" en el directorio raíz y cruza las ligas de todos los archivos ejecutables infectados. El virus sustituye las entradas de directorio normales del *DOS* haciendo del archivo "CHKLIST.MS", el *cluster* de inicio para todos los archivos infectados. Con el comando DIR/ahs, se puede ver el archivo "CHKLIST.MS" y de esta forma confirmar que la computadora está

infectada por el virus "**Dir.Byway**". Si el usuario borra el archivo "CHKLIST.MS", este aparecerá otra vez cuando se ejecute cualquier archivo infectado. Si el usuario enciende la máquina con un *diskette* limpio del *DOS* y corre el comando CHKDSK, este indicará un gran número de ligas cruzadas de archivos (asignaciones o cadenas perdidas). En cambio, si se enciende la máquina desde el disco duro y se hace el mismo procedimiento, CHKDSK no reportará ningún error.

*Trigger* (activación)
El virus se dispara si la fecha del sistema indica el año 1996 o los años siguientes, además el día del mes es igual al número del mes multiplicado por 2 más 2.
Ejemplo: (mm-dd-aa) 01-04-96, 02-06-96 y 12-26-96.

Cuando el virus se dispara despliega un texto cada tres horas en múltiplos de tres. Por ejemplo: 09:00, 12:00 y 15:00, el texto que despliega el virus dice:

"TRABAJAMOS TODOS POR VENEZUELA"

En sistema multimedia, el texto viene acompañado con el himno de Venezuela.

### 2.5.6. WM.NPAD

Este virus consiste realmente en una sola MACRO llamada **AutoOpen**, dicha macro está encriptada y protegida con el método estándar de definir las macros como sólo lectura, lo que evita que los usuarios puedan ver ó modificar el código fuente de la macro. La macro **AutoOpen** contiene 8 subrutinas, 5 de las cuales controlan el "*trigger*" del Macrovirus (disparo o activación del mismo).

¿Cómo infecta?
Cuando un documento infectado es cargado en un *Word* libre de virus (no infectado), el virus recibe el control a través de la macro **AutoOpen** del documento infectado, y entonces la rutina MAIN de la macro es ejecutada, el funcionamiento es el siguiente, primeramente hace una llamada a la función *Disablenput*() para evitar

que el usuario detenga la ejecución de la macro utilizando la tecla ESC y asegurar que las macros estén habilitadas. Enseguida el virus se copia así mismo a la plantilla global (NORMAL.DOT) y curiosamente esto sólo lo va a ser si la macro está encriptada. Cuando los investigadores de Antivirus hallan desencriptada la macro con el propósito de experimentar y tratar de analizar este virus, habrán evitado que el virus siga infectando (la macro estará desencriptada). Si la macro no está encriptada o el proceso de copiarse asimismo falla, "**Npad**" llamará a la rutina para infectar otros archivos que no sean NORMAL.DOT, antes de infectar **Npad** checa si el documento es una plantilla, si es así entonces comienza a copiar la macro, si no "**Npad**" checa que el código de la macro esté encriptado lo copia y guarda el nuevo archivo infectado. De esta forma el virus puede controlar ambos procesos; el infectar la plantilla global o el infectar solo documentos, con tan sólo una macro.

¿Cómo se activa?

Cuando se ejecuta la rutina MAIN de la macro **AutoOpen**, "**Npad**" utiliza la función *GET-ProfileS-tring*$() para leer la palabra "**Npad 328**" en la acción "*compatibility*" dentro del archivo WIN.INI.

1. Si el contador de esta sección es igual a 23:
    - La rutina de "*trigger*" se ejecuta,
    - El contador sé reinicializa a 0
    - Se graban nuevamente dentro del WIN.INI
2. Si no es así, es decir, el contador no es igual a 23:
    - El contador se incrementa en 1 y
    - Se graba nuevamente del WIN:INI.

La rutina de trigger utiliza la barra de "status" (el área de la parte inferior izquierda de cualquier ventana) para enviar el siguiente mensaje: "**DOEUNPAD94, v.2.21, (2)*Maret* 1996, *Ban dung*, Indonesia**". Dicho mensaje aparece inicialmente en la parte izquierda de la barra de "status" y comienza a moverse hacia la derecha, rebotando de un lado a otro para finalmente salir nuevamente por la parte izquierda.

Estilo de programación:

**NPAD** es un virus interesante ya que fue desarrollado en dos secciones; la primera sección (código de replicación) es completamente diferente a la segunda sección (código de activación o *trigger*). En la primer parte los nombres de las variables y subrutinas están en inglés pero en la segunda parte se utilizan nombres en un lenguaje diferente, presumiblemente un lenguaje de Indondesia.

### 2.5.7. WM.MDMA

Está diseñado totalmente para destruir, es un virus que destruye información y elimina archivos de *Windows*. Infecta la plantilla de "*default*" NORMAL.DOT, como lo hacen todos los Macrovirus, esto lo realiza utilizando la macro **AutoClose**. Hasta el momento se sabe que este tiene un "*trigger*", que hace que se dispare el día primero de cada mes y cuando se dispara presenta una caja de dialogo con el siguiente mensaje:

**"You are infected with MDMA_DMV.Brought to you by MDMA (Many Delinquent Modern Anarchists"**

El daño que puede ocasionar depende del sistema operativo como se muestra enseguida:

- *Windows* 3.x — Agrega DELTREE al AUTOEXEC.BAT
- *Windows NT* — Borra información utilizando la opción *.*
- *Windows 95* — Borra C:\WINDOWS*.HLP
  Borra C:\WINDOWS\SYSTEM*.CPL
  Daña el REGISTRY
- OS\2 — Agrega DELTREE al AUTOEXEC.BAT
- Macintosh — Borra el MacID (borra todos los archivos)

Este Macrovirus actualmente ya se ha encontrado en México, el sistema Antivirus de Dr. Sólomon's puede detectar y eliminar este virus utilizando el EXTRADIVER.

### 2.5.8. NATAS

Es un virus múltiple muy peligroso ya que cuando hizo su aparición causo serios problemas en los equipos de cómputo, en algunas de sus variantes llego a borrar completamente la información del disco duro, en otros casos se tuvo que formatear el disco duro de la PC para poder eliminarlo. Tiene alta capacidad para reproducirse, tiene la cualidad de protección, es polomórfico y sé encripta. Además se dispara 1 de cada 512 reencendidas y como efecto, formatea el disco duro. Afecta archivos COM y EXE al ejecutarse o cerrarse (por ejemplo, al copiar un archivo, se infectan tanto el origen como el destino). No infectan los archivos COM de más de 60,692 bytes o menos de 1,000 bytes, ni los archivos EXE de más de 938,040 *bytes*. El virus también infecta el sector de partición y el sector BOOT de los *diskettes*. El sector de partición del disco duro se infecta al ejecutar un programa infectado o al iniciar la PC desde un *diskette* infectado. Los *diskettes* de infectan con el acceso de lectura (por ejemplo, desde los comandos DIR o COPY). Crecimiento de archivos: 4,744 bytes, descripción, al ejecutar un programa infectado o al iniciar la PC desde un *diskette* infectado, **NATAS** se hace residente en memoria e infecta el sector de partición, el virus no cambia la ubicación del sector de partición original. Bloquea el código ejecutable de partición y cambia 41 bytes, pero no modifica la tabla de particiones. El código del virus se almacena en nueve sectores al final de la primera pista, sin incluir el último sector de ella. El virus **NATAS** infecta el sector *Boot* de los *diskettes* a los que se accede desde una PC infectada. El virus no cambia la ubicación del sector *Boot* original. El virus bloquea el sector BOOT y cambia 41 bytes. El código de virus adicional se almacena en 9 sectores al final del disco y se bloquea el bloque de parámetros del *Bios* (*Bios Parameter Blocks*, *BPB*) para asegurar que dichos sectores no se sobrescriban con datos. Los archivos infectados por **NATAS** tienen una encriptación y un polimorfismo variable, **Natas** *stealth* para ocultarse cuando es residente en memoria. Si se examina el sector de partición mientras que un virus está residente en memoria, no se muestra el sector de partición original, el virus no oculta el código adicional de virus al final de la primera pista, al

contrario de la mayoría de los virus *stealth*, **NATAS** puede sobrevivir a los *backup's* (*Backup's* y *PcBackup's*), a la archivación (*ARJ*, *LHARC*, *PKZIP*) y a la transferencia de archivos infectados por módem (*ZMODEM*, *XMODEM*, etc.). Asimismo, no activa los informes de errores del sistema de archivos con CHKDSK. **Natas** también utiliza *stealth* para ocultar el aumento de tamaño de los archivos, al iniciar la PC desde un disco duro infectado. Existe una probabilidad de 1 entre 512 de que se active el virus y formatee todos los discos duros del sistema, con lo que destruye todos los datos. El virus también se puede activar al rastrearlo con un depurador, dispone de las cadenas encriptadas **NATAS**, BACK Y MODEM. El autor de este virus que también escribió **SATANBUG**, es un viejo conocido de las autoridades.

**Nota.**-Ya que el virus se oculta, es de vital importancia que todo el trabajo de los sistemas infectados se realice después de iniciar desde un disco limpio de *DOS* protegido contra escritura y que todo el *software* que se ejecute esté limpio. Si se ejecuta infectado, se infectarán todos los ejecutables a los que acceda posteriormente, esto no lo detectan los escáneres que no puedan detectar el virus en memoria y que escaneen los archivos con el virus activo en memoria. Se recomienda que se ejecuten los programas de Antivirus desde el *diskette* protegido contra escritura original hasta que haya sido eliminado el virus.

### 2.5.9. ROTCEH

Este virus aparece por primera vez en la ciudad de México en el mes de julio de 1996, dicho virus jamás se activa solo que exista un *Bug* de programación.

**Bug** : (Bicho) error

- Es un error persistente en el *software* o en el *hardware*.
- Si existe en el *software* puede corregirse modificando el programa.
- Si existe en el *hardware* deberán diseñarse nuevos circuitos. El término fue acuñado en los años 40's cuando se encontró una polilla aplastada entre los contactos de un relé electromecánico en el *Mark I Glitch*.

***Glitch***(Interferencia, fallo aleatorio)

Cualquier mal funcionamiento temporal o aleatorio en el *hardware*. Nótese la diferencia con ***Bug***[2] (bicho) que es un error permanente, algunas veces "bicho" en un programa puede hacerse parecer que el *hardware* tenga un fallo aleatorio y viceversa. A veces puede ser extremadamente difícil determinar si un problema está ubicado en el *hardware* o en el *software*.

### 2.5.10. NEUROQUILA

Es un virus de características múltiples, afecta al *Boot Sector* de los *diskettes* y al sector de partición de los discos duros, al iniciar la PC desde un *diskette* infectado o al ejecutar un archivo EXE infectado. Es conocido mundialmente como Neuroquila.mp, residente en memoria. Si es posible, se carga en los bloques de memoria superior (*UPPER MEMORY BLOCKS, UMB*) proporcionados por EMM386. El virus utiliza *stealth* para ocultar los cambios que realiza en los sectores de partición y en los sectores de *Boot* de los *diskettes*. En los *diskettes*, el virus formatea una pista adicional y la utiliza para almacenar el cuerpo principal del código del virus. Este virus puede modificar algunos programas Antivirus residentes en memoria (por ejemplo, *TBDRIVER*, *TBDIK*, *VSAFE*). Encirpta el sector de partición, de esta forma no se puede acceder al disco duro si se inicia la PC desde un disco de sistema de *DOS* si se utiliza FDISK/MBR para eliminar este virus, no se podrá acceder al disco duro (no es aconsejable utilizar FDIK/MBR para eliminar los virus). Es en algunos aspectos es similar al virus **Tequila.mp** de ahí su nombre. Lo escribió el autor de virus que sé auto denomina Neuobaster (autor de *Tremor* y *Nighfall*). **Neuroquila.mp** [.a] contiene una cadena que aparece un par de meses después de que se infecte la PC:

**<HAVOC> by Neurobaster'93/Germany**

**-GRIPPED BY FEAR – UNTIL DEATH US DO PART!**

(2) **Bug** = bicho, error de programación

### 2.5.11. MIGUEL ANGEL

Este peligroso causó un susto nacional al aparecer en el año 1991, está programado para activarse el día del cumpleaños del artista. Los efectos que causa a las computadoras infectadas ese día, es formatearle el disco duro, borra además todos los datos y programas que estén almacenados. Es un virus de *Boot Sector*. Afecta al *Boot Sector* (sector de arranque) de los *diskettes* y el sector de los discos duros al iniciar la PC desde un *diskette* infectado. El virus infecta el sector de partición del disco duro al iniciar desde un *diskette* infectado. A continuación, si el virus está residente en memoria, infecta cualquier *diskette* al que se acceda.

En *diskettes* de:

- 360 KB; el *Boot Sector* original se copia en el cilindro 0, cabeza 1, sector 3.
- Otros: el sector del *Boot* original se copia en el cilindro 0, cabeza 1, sector 14, que es el último sector de directorio de *diskettes* de 1.2 MB, y el penúltimo en *diskettes* de 1.44 MB.
- No existen estos sectores en *diskettes* de 720 KB.

En Discos duros:

El sector de partición original se traslada al cilindro 0, cabeza 0, sector 7 y a continuación se escribe el virus.

Siempre se activa cada 6 de marzo (cumpleaños de MICHELANGELO), si la PC es un AT o un PS/2, el troyano se activa y sobrescribe el disco duro con valores nulos. En discos duros, la geometría es 256 cilindros, 4 cabezas y 17 sectores por pista, además se trata de un virus relacionado con el **Stoned**.

### 2.5.12. DARK AVENGER

Es un virus residente en memoria, afecta a los archivos COM y EXE. Sólo funciona en MS-DOS versión 3.0 y superior, sólo se infectan los archivos superiores a 1,800 bytes.

- Crecimiento de archivos:

1,800 bytes, sujetos a un redondeo hasta los siguientes 16 bytes.

- Su descripción:

La infección se puede activar por una serie de acciones realizadas en un archivo:

1. Si se copia, se infectan tanto el origen como el destino
2. Si se lee
3. Si e cambian los atributos
4. Si se ejecuta

Los archivos de sólo lectura se convierten en de lectura-escritura y tras la infección, este atributo, se redefinen. Se utiliza el sector Boot para almacenar datos. El virus escribe un sector que comienza con **"Eddie lives... some where in time"**, a intervalos en un sector aleatorio del disco duro. Este sector puede sobrescribir cualquier sector del disco, incluso sectores en blanco, un sector de código de programa o parte de un archivo de datos. Por lo tanto, el daño producido es sutil, y puede pasar inadvertido durante algún tiempo. Cualquier *backup* realizado incluirá estos daños. El virus incluye otros dos mensajes que no se utilizan:

**This program was written in the city of Sofia © 1988-89 Dark Avenger**

**Diana P.**

- Variantes

**Dark Avenger 2 (Eddie 2)**:

Los archivos aumentan 651 *bytes*, no contienen carga explosiva, pero en el código aparece la cadena **Eddie lives**.

**Dark Avenger 2000 (Eddie 3, V2000, Die young, Traveller):**

Los archivos de más de 1,958 bytes se infectan y crecen 2000 bytes. Si se ejecuta un programa que contenga un mensaje de *Copyright* de *Vasselin Bontechv*, el sistema se bloquea (*Vasselin Bontchev* es un investigador Antivirus de origen búlgaro). Apareció por primera vez en Bulgaria, contiene el texto 666, como el virus 512 y utiliza muchas de las mismas ideas. En una versión del virus, aparece el texto:

**COPY me –I want to travel, en otra aparece Only the good die young...**

**Dark Avenger 2100 (Eddie-4, V2100):**

Los archivos crecen 2,100 bytes (ocultos si el virus está en memoria) y el virus contiene el texto "Eddie Lives". Utiliza la interrupción 13h para dañar el disco mediante la escritura de texto que no sirve en sectores aleatorios. Existen dos versiones: una utiliza el registro SI en varios lugares, la otra utiliza el registro DI, es una versión desarrollada en **Dark Avenger** y **Dark Avenger 3**.

### 2.5.13. BOOZA

Este fue el primer virus que infecto al ambiente operativo de *Windows*. Afecta a los archivos. EXE en formato de archivo ejecutable de *Windows*. Su crecimiento de archivos es = 3 KB. Es sumamente normal y poco sofisticado. Se trata de un virus de apéndice de acción directa (no residente). Procede de Australia e infecta archivos de programa con formato de archivo *Portable Executable* (*PE*) de *Windows* 32 de *Microsoft*, por lo que puede infectar archivos ejecutables de *Windows* 95 y *Windows* 32S. Infecta hasta tres archivos del directorio actual siempre que se ejecute un programa ya infectado. No se hace residente en memoria, con lo que se reduce de forma considerable su capacidad para protegerse y de esta forma ponerse en circulación. No tenía carga explosiva de carácter destructivo, su único objetivo parece ser propagarse, pero no lo consigue y a veces estropea los archivos que intenta infectar. El virus muestra un cuadro de diálogo del día 31 de cada mes.

### 2.5.14. WM.CAP

Este Macrovirus fue reportado por primera vez en febrero de 1997 y ya se ha diseminado ampliamente por nuestro país y por todo el mundo. El virus consiste en una gran macro **CAP** (de ahí el nombre del virus), que es llamada desde las otras macros del virus **AutoExec**, **AutoOpen**, **FileSave**, **FileSaveAs**, **Filetemplates**, **ToolsMacro**, **FileClose**, **FileOpen** y **AutoClose**.

La macro **CAP** contiene el siguiente comentario:

**C.A:P.: Un virus social... y ahora digital...**

**"j4cKy Qw3rTy" (jqw3rty@hotmail.com).**

**Venezuela, Maracay, Dic. 1996**

**P.D. Que haces gochito ? Nunca serás Simón Bolívar ...Bolsa!**

Cuando el virus se replica, lo primero que hace es copiar el conjunto básico de 10 macros, después examina cada uno de los menús del *Word* para *Windows* y almacena sus nombres (porque pueden ser diferentes en otros idiomas o porque el usuario los haya personalizado), para interceptar hasta cinco de estas macros adicionales, insertando un apuntador a la macro principal **CAP**. A continuación borra todas las macros del sistema que hayan sido definidas en la plantilla global antes de ocurrir la infección. El virus también remueve las entradas del menú Herramientas (Tools) ¦ Macro y del menú Herramientas (tools) ¦ Personalizar (Customize). La entrada de menú Archivo (File) ¦ Plantillas (templates) sigue apareciendo después de la infección pero ya no funciona bien.

Síntomas que se presentan cuando *Word* se ha infectado por el virus **WM.CAP** :

1) Al abrir un documento infectado le mandará el mensaje de error mostrado anteriormente.
2) En el momento de cerrar un documento ya no dejará abrir los documentos desde la opción abrir del menú archivo, enviando dicho mensaje:
3) Notará que el virus ha personalizado *Word*, de manera que la opción de "Herramientas" | "Personalizar" habrán desaparecido:

Para mover satisfactoriamente el MACROVIRUS **WM.CAP**:
Es muy importante que elimine (borre) la plantilla global (NORMAL.DOT) para obligar a *Word* a crear una nueva plantilla limpia la próxima vez que sea ejecutado. Si tiene una versión antigua de Antivirus o si no funciona el sistema que tiene a la mano, se recomienda usar el EXTRA DRIVER.

# CAPITULO 3

# PROCEDIMIENTOS PARA APLICAR LOS RECURSOS

## 3.1. GRAFICA DE ACCIONES PROPUESTAS A SEGUIR[8]

Esta gráfica muestra las acciones que debemos seguir y las herramientas que debemos utilizar para poder erradicar un virus y que hacer en casos difíciles o cuando se desconoce el manejo del sistema Antivirus.

| Lugar / Acción | Sector de partición de un disco duro | Sector de arranque de un disco duro | Sector de arranque de *diskettes* |
|---|---|---|---|
| 1. Reconstruir | FDISK / MBR | SYS <DRIVE> | CLEAN*BOOT* SYS <DRIVE> |
| 2. Encontrará el sector y regresará al: Fin del volumen Fin del disco físico Sectores malos u ocultos | CLEANPART *TOOLKIT* /ID | *TOOLKIT* /ID | *TOOLKIT* /ID |
| 3. Encontrar el virus y sobre escribir en él. | *TOOLKIT* /ID | *TOOLKIT* /ID | |

### 3.1.1. SECTOR DE PARTICION DE UN DISCO DURO

En computadoras personales, existe una rutina "*Bootstrap*" en el chip ROM que automáticamente se ejecuta cuando la PC se enciende o se inicia la actividad. Ella busca el sistema operativo, lo instala en memoria y le transfiere el control. En computadoras de mayor tamaño, el procedimiento suele requerir una secuencia más elaborada de ingresos por teclado y precisiones de botones, su posición es:

Cabeza 0, cilindro 0, sector 1.

(8) PC Viruses – Detection, Analysis and Cure
Dr. Alan Solomon & Tin Kay

### 3.1.2. SECTOR DE ARRANQUE DE UN DISCO DURO

(*Boot* Sector) sector de inicialización. Area del disco que contiene instrucciones y/o datos que hacen que la computadora localice y cargue el sistema operativo. Normalmente es el primer sector de partición del disco, su posición es:

Cabeza 0, cilindro 1, sector 1.

### 3.1.3. SECTOR DE ARRANQUE DE DISCO FLEXIBLE

(Manipulador de arranque, de inicio).

Es el sector que contiene los archivos de inicio o de arranque de un sistema operativo y se crea para iniciar una PC que carece de estos archivos, dichos archivos son protegidos mediante atributos.

### 3.1.4. FDISK

Utilidad del *MS-DOS* que hace particiones al disco duro en varias secciones como si fueran discos independientes, también nos permite eliminar las particiones que causan conflicto, ejemplo:

| | |
|---|---|
| **FDISK/?** | Nos muestra como usar el comando |
| **FDISK/STATUS** | Nos muestra tamaño y particiones existentes |

### 3.1.5. MBR

(Master *Boot* Record) Esta es una instrucción no documentada en los manuales de *MS-DOS*, ya que es de alta responsabilidad el manejo de ella. Controla el sector maestro de arranque o inicio de una PC. Ejemplo: Cuando la PC no *inicia* o sea, que no aparece el prompt **C:\>**, se necesita crear un disco de sistema o de arranque y precisamente se usa cuando ya fueron transferidos los archivos de sistema y aún así no aparece el prompt **C:\>**, realice los siguientes pasos:

1. Cree un disco de arranque que este limpio de virus en otra PC, teclee:

**C:\>SYS A:** y oprima <Enter>

2. Copie ahora el archivo FDISK.EXE[9] al diskette flexible.
3. Inserte este disco en el *drive* de disco flexible de la otra PC que no *inicia* y encenderla. Espere a que aparezca el indicador o prompt: **A:\>** y teclee en él:

   **A:\>SYS C:** y oprima <Enter>
4. Se supone que la PC debe iniciar el acceso al disco duro, pero si no, entonces volvemos apagar la PC y dejamos que arranque con el disco que ya le insertamos, después de que aparezca el prompt A:\> Teclee:

   **A:\>FDISK/MBR:** y oprima <Enter>
5. Esto hará que funcionen los archivos de sistema, se apaga la PC, se retira el *diskette* de arranque y se prende la PC, bien, si no funciona se debe a que hubo incompatibilidad de versiones y se tiene que volver a instalar el sistema operativo.

**Nota** : Es muy importante saber lo que se hace, ya que si existe un virus que haya alterado el proceso de inicio de la PC, ya no funcionará. Es mejor cerciorarse de que no haya existido virus. Puede ser que esta instrucción sea una herramienta adversa y no permita el acceso al disco duro. También no debe usarse en versiones de *Windows* 95 si no existe como plataforma inicial el sistema operativo de *MS-DOS*.

### 3.1.6. *CLEANBOOT (Encender en limpio)*

Encienda en limpio una PC; significa crear un disco de arranque flexible de otra PC, que contenga los archivos de la misma versión del Sistema Operativo. Esto es necesario hacerlo cuando se requiere vacunar una PC infectada por algún virus.

## 3.2. DONDE OBTENDRA INFORMACION ACERCA DE UN VIRUS

Si tiene un problema de Soporte Técnico con un virus computacional y no cuenta con la vacuna para erradicarlo, debe consultar con el sistema de Internet, en este sistema podrá encontrar el origen del virus en cuestión, además le mostrará los posibles sistemas de Antivirus que le podrán servir para erradicar el virus. Lo

(9) **FDISK.EXE** - Archivo del sistema Ms-DOS o Windows 95

anterior es correcto pero no quiere decir que sea lo mejor ya que debe forzosamente adquirir un sistema de Antivirus para proteger su sistema de computo. En este caso se recomienda al sistema de Antivirus McAfee, el cual cuenta con servicios de Soporte Técnico, las 24 horas del día. En caso de no contar con el antidoto para eliminar el virus de tu PC, le indicarán los pasos que deberá seguir, para que le envíe el espécimen a su laboratorio, y en menos de 24 horas le harán llegar el antídoto para erradicar el virus de su equipo; no importa que no cuente con algún sistema de Antivirus. Para recibir ayuda sobre la utilización del sistema de Antivirus, le informamos que contacte con Soporte Técnico de McAfee, lo podrá hacer de la siguiente manera:

1. En línea las 24 horas al día, a través de **BBS**[6] de McAfee, CompuServe, Fax, o Internet (vea acceso en línea para actualizaciones y Soporte Técnico en el siguiente tema).
2. Por teléfono, al (408)988-3832 de Lunes a Viernes de 7:30 a 17:30

Para que la ayuda sea más rápida y apropiada, por favor tenga a la vista la siguiente información en el momento de hacer contacto con McAfee:

- Nombre del programa, número de versión y número de serie
- Tipo y marca de la PC, disco duro y de cualquier periférico
- Versión del *MS-DOS* o Sistema Operativo *Windows*, junto con cualquier otro TSR o controladores en uso.
- Una copia impresa de los archivos AUTOEXEC.BAT Y CONFIG.SYS
- Una copia impresa del contenido de su memoria, desde el comando MEM (*MS-DOS* 4.0 y superiores) o de una utilería similar.
- Una descripción exacta del problema que tiene en ese momento. Por favor sea lo más específico posible; de no estar frente a su computadora cuando llame, por lo menos tenga una copia impresa de los mensajes de error que aparecieron en la pantalla.

(6) BBS = Bulletin Board System

- Si está fuera de los Estados Unidos, también puede contactar con gente autorizada de McAfee que están localizados en mas de 50 países alrededor del mundo, ellos le ofrecerán los productos para su venta o también Soporte Técnico para los programas. Por favor consulte el archivo AGENTS.TXT, para obtener una lista completa de los agentes de McAfee.

### 3.2.1. ACCESO EN LINEA PARA ACTUALIZACIONES Y SOPORTE TECNICO CON EL ANTIVIRUS MCAFEE

McAfee actualiza el programa de Antivirus *VirusScan* cada 6 u 8 semanas, en promedio, para añadir nuevos detectores y removedores de virus, nuevas opciones y corregir los errores reportados. Para distribuir estas nuevas versiones, activamos un sistema de boletín multilínea BBS y espacios en CompuServe, Internet y en América Online. El Antivirus McAfee está permanentemente en desarrollo, los expertos nunca detiene sus investigaciones. Se les reconoce por tener el mejor respaldo en servicio y Soporte Técnico en el mundo de los Antivirus. El Soporte Técnico cuenta con un Staf de investigadores, programadores, profesionales de tiempo completo y se proporciona directamente por McAfee o por la red de sus agentes autorizados en más de 50 países en el mundo entero.

### 3.2.2. OTRAS FUENTES DE INFORMACION

Los ***BBS*** de McAfee y el "*CompuServe Virus Help Forum*" son excelentes fuentes de información para la protección Antivirus. Ahí se proporcionan archivos de tipo "batch" y algunas utilerías que le ayudarán a usar el software de McAfee. Existen publicaciones, escuelas y algunos centros de entrenamiento independientes. Los agentes también le pueden informar y capacitar en la protección contra los virus y en lo referente a seguridad de su información en las computadoras. McAfee le recomienda especialmente las siguientes:

(6) BBS = Bulletin Board System

- *Febrache, David. A Pathology of Computer Viruses. London: Springer-Verlag, 1992.*
- *Hoffman, Lance J. Rogue PrograMS: Viruses WorMS and Trojan Horses. Van Nostrand. 1991.*
- *Robert V. Jacobson, Using McAfee Associates Software for Safe Computing. New York : International Security Technology, 1992.*


### 3.2.3. SOPORTE TECNICO PARA DR. SOLOMON'S

A continuación se describen las direcciones electrónicas a la que podrás consultar en Internet y contar con el servicio de soporte técnico cuando así lo requieras.

- **ACCESO A INTERNET**:

| | |
|---|---|
| Dr. Solomon's Group | http:\\www.drsolomon.com |
| Dr. Solomon's Group | http:\\www.drsolomon.com.mx |
| *National Computer Security Association (NCSA)* | *http:\\www.ncsa.com* |
| *Virus Bulletin* | *http:\\virusbtn.com* |

- **COMPUSERVE**:

| | |
|---|---|
| *Dr. Solomon's Group* | *GO drsolomon* |
| *Dr. Solomon's México* | *GO mexhelp* |
| *National Computer Security Association (NCSA)* | *GO ncsa* |

- **BBS**:

| | |
|---|---|
| *Dr. Solomon's Group* | *98 44 0 12906 318810* |
| *Dr. Solomon's México* | *5 250 39 48* |
| *Dr. Solomon's México* | *5 250 39 58* |

(Soporte Técnico)

Si surgen problemas al instalar o ejecutar el sistema *Toolkit*, existen varias posibilidades para obtener ayuda. Compruebe la documentación con cuidado, incluyendo los archivos README de los discos así como este manual y el texto de

ayuda. Asegúrese de que ha instalado el software de forma correcta. Asimismo, podrá obtener ayuda del distribuidor autorizado. Si, de todas formas, no puede resolver el problema, el personal del servicio técnico de Dr. Solomon's se encuentra a su disposición para ayudarle. Se trata de un servicio gratuito. Puede ponerse en contacto con Dr. Solomon's en una de las formas siguientes:

- Oficina del Reino Unido:
  Dr. Solomon's Software Ltd.
  Alton House Business Park
  Gatehouse Way
  Aylesbury
  Bucks HP19 3XU
  Reino Unido
  Tel: +44 (0)1296 318700
  Fax: +44 (0)1296 318777
  Correo electrónico: support@uk.drsolomon.com
  Tel. del servicio técnico: +44 (0)1296 318700
  Fax del servicio técnico: +44 (0)1296 318734
  BBS: +44 (0)1296 318810
- Oficina de EE.UU.:
  Dr. Solomon's Software, Inc.
  1 New England Executive Park
  Burlington MA 01803
  EE.UU.
  Tel: +1 781 273-7400
  Fax: +1 781 273-7474
  Correo electrónico: support@us.drsolomon.com
  Tel. gratuito al servicio técnico: 800-595-9175
- Oficina en Alemania:
  Dr. Solomon's Software GmbH
  Luisenweg 40
  20537 Hamburg
  Alemania
  Tel del servicio técnico: +49 (0)1805 237678
  Correo electrónico: support@de.drsolomon.com
  En todo el mundo:
  ftp anónimo: ftp://ftp.drsolomon.com
  CompuServe: GO DRSOLOMON

  World Wide Web: http://www.drsolomon.com

Al ponerse en contacto con Dr. Solomon's, se recomienda que tenga la siguiente información disponible:

- Nombre y empresa.
- El número de serie que aparece en el disco de instalación 1, del sistema *Toolkit*.
- La versión de *Windows* que utiliza.
- El número de versión de *Toolkit* que utiliza (esta información aparece en la etiqueta de los *diskettes* de instalación).
- Un *diskette* del sistema *DOS* limpio (sin virus) protegido contra escritura.

En caso de tratarse de un error de la aplicación ó cualquier mensaje aparecido. Si es posible, debe estar junto a la computadora cuando nos llame. Es probable que necesitemos información adicional o quizás le pidamos que lleve a cabo alguna prueba de diagnóstico. Si deseas otra empresa de sistemas de Antivirus, en Internet podrás encontrarla, tecleando solo el nombre de la marca. También podrás conocer los antecedentes de los virus en las enciclopedias, además Dr. Solomon's cuenta con un boletín mensual en cual te muestra los últimos secretos y avances de los sistemas de Antivirus, este boletín te lo hace llegar a tu domicilio suscribiéndote sin ningún costo.

### 3.3. CONFIGURE UNA PC DE SACRIFICIO

Los virus informáticos se han convertido en una seria amenaza para los datos y programas de computadoras. Ahora todas las PC's son candidatas a ser infectadas por un virus, lo que puede llegar a costar grandes cantidades de dinero. En sus principios muchos de los virus computacionales no representaban peligro alguno; actualmente existen varios que si ocasionan daño. Ningún virus puede funcionar por sí solo; requieren forzosamente de algún lugar para alojarse y desde ahí comenzar su infección. Este lugar puede ser: un sector de arranque, un sector de partición o un archivo. Es conveniente tener siempre en nuestra área de cómputo una PC de sacrificio, la cual no debe tener información importante, ya que corre el riesgo de

perderse o también de contaminar a los otros equipos, si no se cuenta con una versión de Antivirus actualizada, pueden suceder serios problemas.

Pasos:

1. La PC debe tener instalado un programa de Antivirus.
2. Debe actualizarse mínimo cada mes esta versión de Antivirus.
3. Si al detectar que un virus no es posible eliminarlo con la versión que se trabaja, entonces es conveniente enviar el espécimen a la empresa que elaboró el sistema de Antivirus.
4. No debe olvidar que todo *diskette* que ingrese a nuestra área de cómputo, debe ser verificado en esta PC de sacrificio.

## 3.4. LINEAMIENTOS PARA UNA LIMPIEZA DESPUES DE UN ATAQUE DE VIRUS

Después de haber sufrido un ataque de virus en nuestra PC, es conveniente realizar las siguientes acciones una vez vacunada la PC y eliminado el o los virus:

1. Haga respaldos de la información más importante en *diskettes* o cintas de magnéticas.
2. Verifique nuevamente que no exista infección en el disco duro utilizando otro sistema de Antivirus, para confirmar que verdaderamente ya no existe infección.
3. Verifique y corrija la superficie del disco duro, con cualquier sistema de *diagnostico como* SCANDISK[10] o NDD[11], y verificar que no haya sectores dañados.
4. Defragmente el disco duro después de la verificación y diagnostico de la superficie. Esto es para evitar que posibles residuos o embriones vuelvan a reproducirse y comience de nuevo la infección. Se puede usar el comando DEFRAG[10] del sistema *DOS* o el SPEEDISK[11] de Norton Utilities.
5. Instale un sistema de Antivirus o actualizar la versión con que se protege a nuestra PC.

(10) **SCANDISK** y **DEFRAG** .- Archivos del sistema Ms-DOS o Windows 95
(11) **SPEEDISK** y **NDD** Utileria de Doctor Norton Utilities

6. Si no se conoce el manejo de lo explicado en los puntos anteriores, entonces consulte al supervisor del área o sistema.

Aunque los virus representan un problema, se debe tener presente la escala del problema. La causa más común en la pérdida de datos, es el error humano. La segunda causa más común es error del hardware, la tercera causa son los problemas del software y alteraciones. Los virus llegan en un triste cuarto lugar. Sin embargo; al aplicar una política Antivirus estricta, se protegen los datos de todo tipo de pérdida, incluyendo los virus. En particular, debe tener en cuenta los tres siguientes elementos de protección:

- **Prevención** - Para limitar la propagación de virus.
- **Detección** - Para asegurar que si un virus aparece, se descubra lo antes posible.
- **Recuperación** - Para asegurar que si un archivo se pierde o se daña, se pueda restaurar lo antes posible.

Con el sistema de Antivirus *Toolkit*, se cubre una parte significativa de esta política de detección y de recuperación, pero a continuación se sugieren otros elementos que son aconsejables:

- REALIZE COPIAS DE RESPALDO
- VERIFIQUE LAS FUENTES DE SOFTWARE
- TOME PRECAUCIONES CON LOS *DISKETTES* Y OTROS MEDIOS
- EVITE LA ENCRIPTACIÓN Y PROTECCIÓN CON CONTRASEÑA
- CONSIGA LA COLABORACIÓN DE LOS EMPLEADOS.

Para lograr la máxima seguridad al utilizar el sistema *Toolkit*, también puede **iniciar en limpio**[15] (con un diskette de archivos de sistema) y/o ejecutar las herramientas desde los *diskettes* de instalación.

(15) "Encender en limpio".- Explicación en el Capítulo 3, punto 3.1.6. (pág. 62)

### 3.4.1. CONSTRUYA COPIAS DE RESPALDO

La mayor precaución que puede tomar contra cualquier tipo de pérdida de datos, es realizar una copia de respaldo del sistema de forma regular; si no la realiza, se encuentra en peligro. Recuerde, verifique siempre las copias de respaldo con frecuencia y asegúrese de que puede recuperar datos con ellas. Verifique que dispone de *diskettes* con copias limpias de todos los archivos ejecutables. Todos los *diskettes* de respaldo y los de *Boot* deben estar protegidos contra escritura.

### 3.4.2. VERIFIQUE LAS FUENTES DE SOFTWARE

Asegúrese de que todo el software proviene de fuentes fiables. Averigüe que el software lleve el embalaje original. Nunca utilice software ilegal, incluso si considera que puede utilizar otra copia de forma temporal (debido, por ejemplo, a que dejó la copia con licencia en otro lugar), recuerde que la copia puede exponer a la computadora, a una infección por virus. El *software* puede introducirse en la PC, mediante los puertos de comunicaciones de la misma forma que a través de medios portátiles. Tenga cuidado a la hora de transferir *software* desde las computadoras portátiles y a través de redes, así como al cargar archivos de la **BBS**[6] y de Internet.

### 3.4.3. TOME PRECAUCION CON LOS *DISKETTES* Y OTROS MEDIOS

El riesgo de una infección por virus mediante *diskettes* es especialmente alto, pero puede realizar una serie de simples pasos para aumentar la seguridad:

- Mantenga los *diskettes* protegidos contra escritura siempre que sea posible, para evitar que se copien los virus.
- Cuando apague la PC, no deje los *diskettes* en la unidad de disco flexible, así evita intentar de forma accidental, iniciar desde un *diskette* infectado con un virus de *Boot* sector.
- Si inicia sin querer desde un *diskette* que no es de arranque, apague la computadora y comience de nuevo, retire el diskette e intente iniciar desde:

C:\>

- Si no inicia así, cambie la configuración de CMOS de la PC para que arranque primero desde la unidad **C:\>** en vez de la unidad **A:\>** (Esto no es siempre posible en unidades SCSI).
- Siempre que sea posible, utilice métodos alternativos para transferir archivos.
- No olvide que los archivos en cinta, pueden haberse infectado al realizar la copia de respaldo.

### 3.4.4. EVITE LA ENCRIPTACION Y LA PROTECCION CON CONTRASEÑA

La encriptación y la protección con contraseña suponen formas de proteger los archivos contra accesos no autorizados. Por desgracia, los programas de búsqueda, no pueden acceder a los archivos protegidos de esta forma, lo que puede llevar a que los virus no sean descubiertos. Por ejemplo: los documentos de *Word* pueden contener macros que se pueden encontrar infectadas; si un documento de *Word* no está protegido con contraseña, se puede buscar para encontrar posibles virus. Si por el contrario está protegido con contraseña, no se podrá buscar. Tenga en cuenta que los documentos infectados de *Word,* son en realidad plantillas que los virus han disfrazado como documentos. Los documentos de *Word* no pueden contener macros.

Como solución se considera:

- Que todo documento que esté protegido contra escritura, sea desprotegido para que el rastreador de virus, logre una correcta verificación.
- También se debe verificar, que si se va a trasladar información a un diskette; el documento deberá ser verificado; que no contenga macro virus.

### 3.4.5. CONSIGA LA COLABORACION DE LOS USUARIOS

Necesita la colaboración desinteresada de los usuarios, para llevar a cabo una política Antivirus. Si el personal considera que va a ser sancionado al descubrir un virus, es poco probable que informe de cualquier anomalía; puede resultar útil dar a

un usuario o a un grupo pequeño la responsabilidad de verificar y distribuir el software.

### 3.4.6. INICIE SU PC, EN LIMPIO

Al utilizar una utilería de Dr. Solomon's, el sistema verifica la memoria de la PC antes de ejecutarse la herramienta (puede que el virus se haya cargado en la memoria durante el arranque de la PC, por ejemplo). No obstante, existe la posibilidad de que algún virus pueda eludir esta detección; en este caso, el virus puede interferir en la búsqueda para ocultarse e incluso propagarse mediante el proceso de búsqueda.

Para estar completamente seguro de que esto no suceda, puede **"iniciar en limpio"**[15], antes de realizar la búsqueda. Arranque en limpio significa, iniciar la PC desde un *diskette* con archivos de sistema operativo sin virus, en lugar de desde el disco duro (y si no dispone de un *diskette* de sistema limpio, puede utilizar el sistema Magic Bullet[32], de Dr. Solomon's). Puesto que sólo puede iniciar en *DOS* desde *diskettes*, únicamente podrá ejecutar las utilidades de *DOS* para buscar y eliminar virus. Estas utilerías son las siguientes:

***Findvirus.-*** Esta utilería se proporciona en formato de *DOS* en el *diskette* Magic Bullet[32] *(de Dr. Solomon's)*, además de la versión *Windows* suministrada en los *diskettes* de instalación de *Toolkit,* es necesario utilizar el comando *Findvirus* para *DOS*.

**CleanBoot.-** Duplica la funcionalidad de la opción del menú: 'Reemplazar sector *Boot*' de la interfaz de usuario, es necesario utilizar el comando *CleanBoot*.

**Nota**:

Si desea iniciar en limpio[15] y dispone de una unidad de disco duro que precisa un *driver* especial (como una unidad comprimida o una unidad IDE extendida), asegúrese de que las copias limpias de los *drivers* correspondientes se hallen

(15) "Encender en limpio".- Explicación en el Capítulo 3, punto 3.1.6. (pág. 62)
(32) MAGIC BULLET (ver sección 3.4.7.)

en el *diskette* del sistema. A continuación, la PC se puede iniciar en limpio con los *drivers* correctos. Si estos *drivers* no se utilizan, el verificador Antivirus no podrá acceder a los archivos de la unidad del disco duro.

### 3.4.7. MAGIC BULLET

**(Sistema en diskette de Dr. Solomon's; para reastrear y erradicar virus).**

Una forma cómoda de iniciar en limpio y ejecutar *Findvirus* para *DOS* y *Windows* eficazmente, consiste en utilizar el *diskette* Magic Bullet[32]; este *diskette* contiene el código que permite realizar ambas operaciones. Tras el inicio del Magic Bullet[32], se inicia una interfaz del *Findvirus* para *DOS* de forma automática.

***Findvirus*** para *DOS,* permite encontrar virus en los sectores *Boot* y de partición, además de virus en los archivos de *DOS.*

Magic Bullet[32] funciona en todas las unidades locales.

> **Nota**: Si dispone de una unidad que necesita un driver especial, como por ejemplo, una unidad comprimida o una unidad IDE extendida, Magic Bullet[32] no podrá buscar los archivos del disco. Aún así, al iniciar desde el sistema Magic Bullet[32] se busca la partición *Host* de la unidad.

Para iniciar en limpio y buscar mediante el sistema Magic Bullet[32], realice los pasos siguientes:

2. Apague la computadora e introduzca el *diskette* Magic Bullet[32] y vuelva a encenderla, si dispone de más de una unidad de *diskettes*, asegúrese de introducir el *diskette* Magic Bullet[32] en la unidad A:\> ; la computadora *inicia* desde Magic Bullet[32] y aparece la interfaz de usuario de forma automática.
3. Pulse la tecla de función para la opción que necesite: F2, F3 o F4.

(32) MAGIC BULLET (ver sección 3.4.7.)

4. Al finalizar la búsqueda, observe los resultados mostrados. Si no ha utilizado la tecla F4 originalmente y se indica que hay una infección, debe utilizar dicha tecla. Debe repetir la búsqueda con F4, hasta que aparezca el mensaje de que no hay virus.
5. Para salir del sistema Magic Bullet[32], pulse ESC y siga las indicaciones.

### 3.4.8. LINEA DE COMANDOS DEL FINDVIRU

El comando para ejecutar la versión para *Windows* 95 de *Findvirus* es:

**wfindv32 [path[\file...]] [/switch]...**

El comando para ejecutar la versión para *DOS* de *Findvirus* (que se proporciona en el *diskette* Magic Bullet[32]), y es:

**FV86 [PATH[\FILE...]] [/SWITCH] [/SWITCH]...**

Es posible escribir por ejemplo:

**WFINDV32 C:\WINDOWS /DOALLFILES**

De esta forma, se utiliza el parámetro opcional [path] y un parámetro para buscar todos los archivos en el directorio de *Windows*.

O también se puede escribir:

**WFINDV32 C:*WINDOWS*\NOTEPAD.EXE**

Así, se utiliza el parámetro opcional [path\archivo], para buscar sólo el archivo:

**NOTEPAD.EXE**

No se puede utilizar el mismo parámetro más de una vez y de forma simultánea en la línea de comandos. Por ejemplo, si ha escrito:

**Wfindv32 /D=A /D=C**

la segunda '**D =**' será ignorada

(32) MAGIC BULLET (ver sección 3.4.7.)

### 3.4.9. DESINFECCION DE SECTORES *BOOT*

En *Windows* puede utilizar la opción de menú "Desinfectar Sector *Boot*"

Si utiliza *DOS*, quizás después de iniciar con un disco limpio necesite utilizar la utilidad 'Clean*Boot*', siga los siguientes pasos:

1. Introduzca el *diskette* sospechoso.
2. Introduzca el comando:

   **3. CLEANBOO [drive] [/type] [/NOASM]**

   Por ejemplo: **CLEANBOO B: /4** Escribe en el sector *Boot*, para un *diskette* de 1.44 Mb de 3½", en el *diskette* que se encuentra en la unidad **"B:\>"**.
4. Especifique la unidad de *diskette*, si se le pide (no se le pedirá, sí ya se ha especificado en la línea de comandos).
5. Especifique el tipo de disco si se le pide (no se le pedirá, sí ya se ha especificado en la línea de comandos).
6. Si especifica "Autodetección" confirme la selección automática de disco.

   **Nota**: Cuando se utiliza *CleanBoot*, el sector *Boot* ha de remplazarse por un sector *Boot* para la capacidad de formato ya existente. *CleanBoot* debe detectar la capacidad de formato, por ello normalmente no habrá necesidad de alterar este dato.
7. Responda a la pregunta ¿No coincide.....? (Esta sólo aparecerá si el tipo de formato especificado no coincide con el tipo detectado).

   **Nota**: Si el tipo de disco detectado no es el que usted espera, es posible que el *diskette* tenga formateo cruzado.
8. Una vez concluido el proceso, pulse la letra "S" para desinfectar otro *diskette* o, la "N" para salir.
9. Haga un "DIR" en el disco y verifique los archivos, si hay archivos o parecen haber desaparecido o directorios que tengan problemas, es posible que se haya utilizado un sector *Boot* para la capacidad equivocada. En este caso intente utilizar *CleanBoot* de nuevo, esta vez seleccione un tipo diferente de disco y

anule la detección automática. Los archivos en el *diskette* no se perderán a menos que intente escribir en él mientras tiene el sector *Boot* equivocado.

### 3.4.10. EJECUCION DE LAS HERRAMIENTAS DESDE LOS *DISKETTES* DE INSTALACION

Al emplear una utilería, en primer lugar se ejecuta una "prueba de integridad", con esto se verifica si la herramienta está infectada; no obstante, existe la posibilidad de que un virus infectante pueda eludir esta detección, en cuyo caso, el propio proceso de búsqueda puede propagarlo. Para estar absolutamente seguro de que esto no suceda, puede ejecutar la herramienta desde el *diskette,* como los *diskettes* proporcionados están protegidos contra escritura, no existe la posibilidad de que los archivos que contienen, estén infectados. Para tener la máxima seguridad posible, en primer lugar puede iniciar en limpio y a continuación, ejecutar la versión de *DOS* de *Findvirus*, o la utilidad *'CleanBoot'* desde el *diskette*, puede iniciar en limpio y utilizar *Findvirus* para *DOS,* simplemente mediante desde el *diskette* Magic Bullet[32].

(32) MAGIC BULLET (ver sección 3.4.7.)

# CAPITULO 4

# INSPECCION EN DISCO DURO PARA DIAGNOSTICAR UN VIRUS DIFICIL DE DETECTAR Y ELIMINAR

## 4.1. EXPLORACION DE LA COMPOSICION DE UN DISCO DURO

Un disco duro o disco rígido, es un disco magnético hecho de metal y cubierto con una superficie de grabación magnética. Los discos duros vienen en variedades removibles y fijas que contienen desde 10 megabytes, hasta varios Gigabytes.

### 4.1.1. ESPECIFICACIONES DE UN DISCO DURO[12]

A continuación apreciamos la (tabla 4.1); muestra algunos tipos de discos duros:

Tipo de método de velocidad de transferencia

| | | |
|---|---|---|
| ST506 | MFM | 625K |
| ST506 | RLL[13] | 937 |
| IDE | RLL | 0.625 –2 M |
| ESDI | RLL | 1 – 3M |
| SCSI-1 | RLL | 1 – 5M |
| SCSI-2 | RLL | 1- 40M |
| SMD | RLL | 1-4M |
| IPI | RLL | 10-25M |

(Tabla 4.1)

La mayoría de los discos duros utilizan RLL, pero el método de codificación no va prescrito con interfaces.

(14) **RLL (Run Length Limited)** Longitud limitada de ejecución. Método de codificación de los discos magnéticos
(12) **Diccionario de Computación** de Alan Freedman, Ed. Mc. Graw Hill

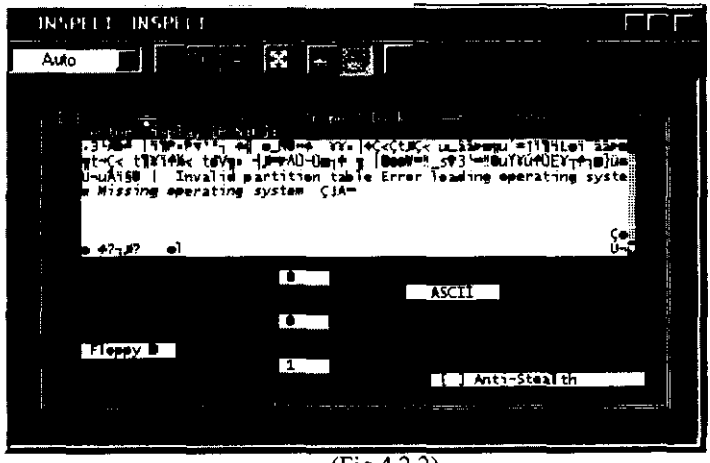
## 4.2. SECTOR DE DISCO DURO[12]

Es la unidad de almacenamiento más pequeña leída o escrita en un disco duro o flexible. Los sectores tienen longitud fija y en cada pista reside generalmente la misma cantidad de sectores. No obstante, el hardware puede variar la velocidad del disco, para acomodar más sectores en las pistas ubicadas en los bordes externos de la superficie del disco. El sector es la unidad física invocable mediante una instrucción. Por ejemplo: READ TRACK 17 SECTOR 23.

### 4.2.1. SECTOR INTERLEAVE[12]

La intercalación de sectores, es la manera en que se enumeran los sectores en un disco duro. La intercalación puede ser secuencial: 0, 1, 2, 3, o alternada: 0, 3, 6, 1, 4, 7, 2, 5, 8. En la numeración secuencial, si se leen datos en el sector 1, para cuando se da el acceso al sector 2, el comienzo del mismo ha pasado ya el cabezal y debe dar una vuelta para quedar nuevamente bajo el mismo. La alternancia de los sectores optimiza las lecturas y escrituras de un disco. Se denomina también *"sector map"*.

### 4.2.2. VISTA DEL SECTOR DE PARTICION IDEAL PARA MS-DOS.




(Fig 4.2.2)

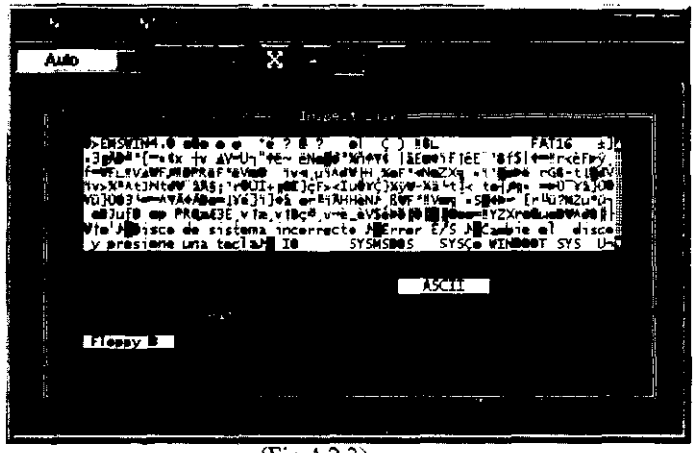
*(12) Diccionario de Computación*
de Alan Freedman
Ed Mc. Graw Hill

La imagen (Fig 4.2.2), muestra al código que se halla en el sector de partición ideal del disco duro, para equipos que cuentan con la versión de Sistema Operativo MS-DOS de la 5.0 en adelante y su posición se observa en el siguiente cuadro:

| | |
|---|---|
| CILINDRO | 0 |
| CABEZA | 0 |
| SECTOR | 1 |

La imagen fue obtenida por una utilería que posee el sistema de Antivirus de Dr. Solomon's, llamada INSPECT DISK, ésta herramienta es de gran utilidad puesto que nos permite conocer físicamente y explorar lo que se ha grabado en todos los sectores del disco duro, no importa que el archivo esté protegido, dicha herramienta nos permite la visualización profunda. Con dicha utilería podemos también eliminar un virus de sector de partición.

### 4.2.3. VISTA DEL SECTOR DE ARRANQUE IDEAL PARA MS-DOS




(Fig 4.2.3)

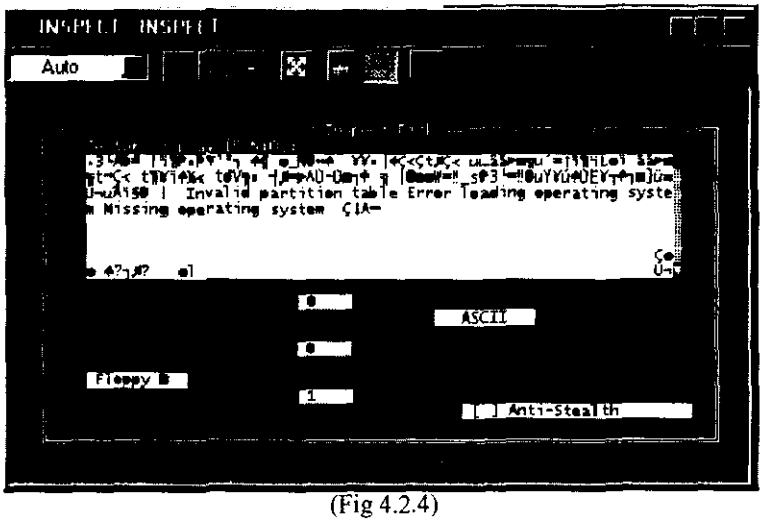
La imagen (Fig 4.2.3), muestra al código que se halla en el sector de arranque ideal del disco duro, para equipos que cuentan con la versión de Sistema Operativo MS-DOS de la 5.0 en adelante y su posición se observa en el cuadro siguiente:

(12) Diccionario de Computación de Alan Freedman

| | |
|---|---|
| CILINDRO | 0 |
| CABEZA | 1 |
| SECTOR | 1 |

Como podemos observar, la ubicación del sector de partición es muy similar a la del sector de arranque solo que el número de posición de la cabeza en vez de 0 es 1, también es posible eliminar virus de sector de arranque en la exploración, si se tienen conocimientos y experiencia para identificarlo, si no aparece esta configuración o código en dicho sector, la PC no podrá iniciar.

### 4.2.4. VISTA DEL SECTOR DE PARTICION IDEAL PARA WINDOWS 95



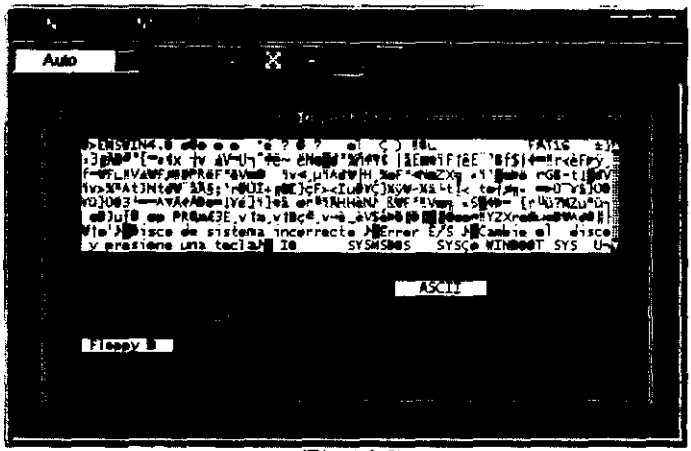

(Fig 4.2.4)

La imagen (Fig 4.2.4), muestra al código que se halla en el sector de partición ideal de un disco duro, para equipos que cuentan con la versión de Sistema Operativo *Windows* 95, y en el cuadro siguiente se muestra su posición:.

| | |
|---|---|
| CILINDRO | 0 |
| CABEZA | 0 |
| SECTOR | 1 |

Si comparamos el contenido del sector de partición de *Windows* 95 con el de MS-DOS, hay gran diferencia, aunque relativamente funcionan igual. Algunas versiones aparecen con código de frases en español, solo la utilería de Dr. Solomon's puede permitirnos esta exploración, si navegamos y no aparece este código en el citado sector, es indispensable buscarlo entre otros sectores para que inicie el disco duro.

### 4.2.5. VISTA DEL SECTOR DE ARRANQUE IDEAL PARA WINDOWS 95



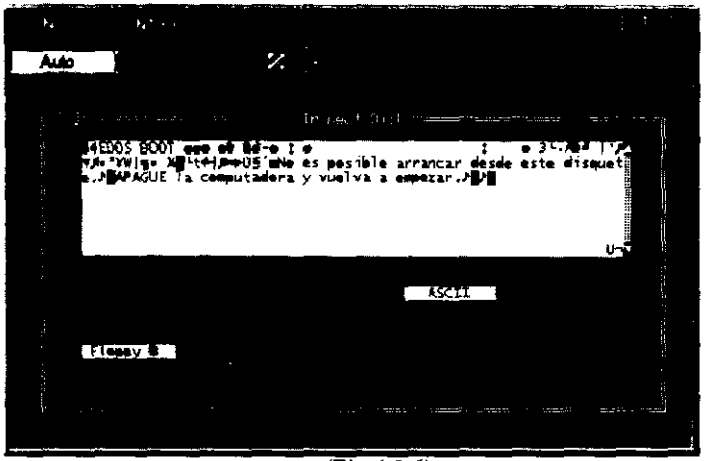

(Fig 4.2.5)

La imagen (Fig 4.2.5), muestra al código que se halla en el sector de arranque ideal del disco duro, para equipos que cuentan con la versión de Sistema Operativo *Windows* 95, y su posición la describe el siguiente cuadro:

| | |
|---|---|
| CILINDRO | 0 |
| CABEZA | 1 |
| SECTOR | 1 |

Se nota que el código existente en el sector de arranque es muy similar al del *MS-DOS* y su ubicación es la misma. Se puede cambiar este sector al igual que los otros mediante una activación secreta de teclas, pero por razones de seguridad se debe consultar a una persona especializada en Soporte Técnico para realizar los cambios siempre y cuando sea necesario y no se tenga la versión de Antivirus actualizada.

### 4.2.6. VISTA DEL SECTOR DE ARRANQUE DE UN DISCO FLEXIBLE




(Fig 4.2.6)

EL disco flexible o *diskette*, NO POSEE SECTOR DE PARTICION, **SOLO TIENE SECTOR DE ARRANQUE**. Este es el sector según la (Fig 4.2.6), .más importante pues en él es donde se guarda al código que activa a los archivos de sistema que arrancan a una PC que no inicia.

| | |
|---|---|
| CILINDRO | 0 |
| CABEZA | 0 |
| SECTOR | 1 |

Si se cuenta con la utileria INSPECT DISK del sistema de Antivirus de Dr. Solomon's, es posible eliminar el virus en el sector de arranque del disco flexible, aunque el sistema Antivirus no esté actualizado. Este procedimiento es delicado si no se cuenta con un técnico especializado, puede ya no servir el *diskette*.

### 4.2.7. DISCO DE ARRANQUE

(Funcionamiento del un disco de arranque)

Después de una verificación de todos los componentes del hardware de una PC, el Boot Program (programa de arranque) contenido en la *Rom Bios* de las

computadoras, ordena a los chips del *drive* 'A', para ver si el *diskette* flexible contiene el formato. El programa buscará las especificaciones y localizaciones de los archivos de sistema que contienen al Sistema Operativo. Ordinariamente no se ven estos archivos de sistema porque cada uno está etiquetado con un atributo especial de archivo, que lo oculta del comando DIR del *MS-DOS*. En algunas PC's los archivos son nombrados como: IO.SYS y MSDOS.SYS. En computadoras IBM, los archivos son nombrados IBMBIO.COM y IBMDOS.COM, si el drive de disco flexible está vacío, el programa de arranque checa al disco duro 'C', para buscar los archivos de sistema, si no hace un *diskette* de arranque correcto con los archivos de sistema, el programa de arranque enviará un mensaje de error.

Después de localizar el disco con los archivos de sistema, el programa de arranque lee los datos almacenados en el primer sector del *diskette* y copia estos datos a ubicación específica de la memoria *RAM*. Esta información constituye el registro de arranque del *MS-DOS*. El registro de arranque es localizado en la misma ubicación de cada disco formateado. El *Boot Record* mide solamente acerca de 512 bytes, código suficiente para iniciar la carga de dos sistema archivos ocultos.

Después del programa de arranque "*BIOS*", *se* cargará el *Boot Record* dentro de la memoria en código hexadecimal 7C00. El *BIOS*, pasa al control del *Boot Record* por la ruta dada a esa dirección.

El registro de arranque toma el control de la PC y carga al IO.SYS dentro de la memoria *RAM; el* archivo IO.SYS, contiene extensiones para la memoria *ROM BIOS* e incluye una rutina llamada SYSINIT, que ordena reiniciar o el arranque del disco duro. Después de cargarse el IO.SYS, el registro de arranque ya no es necesario, y es reemplazado en la *RAM* por otro código.

El SYSINIT:

- Asume el control del proceso de inicio y carga al MSDOS.SYS dentro de la *RAM*. El archivo MS-DOS.SYS, trabaja con el *BIOS* para mantener los archivos, ejecuta programas y responde a señales del hardware.
- Buscará al directorio raiz del disco de arranque para llamar al archivo CONFIG.SYS. Si el CONFIG.SYS existe, el SISINIT dirá al MSDOS.SYS que ejecute el comando en el archivo.

El CONFIG.SYS[12]:

- Es un archivo de configuración que personaliza los DOS y OS/2 de Microsoft para un ambiente de hardware específico.
- Reside en el directorio raíz, y es examinado en el momento de la inicialización.
- Se usa principalmente para activar los controladores de los dispositivos periféricos que hayan sido agregados al sistema.

El SISINIT llamará al archivo MSDOS.SYS para cargar al archivo COMMAND.COM, los archivos del Sistema Operativo consisten en tres partes:

1. Una es la extensión para la entrada o salida de funciones, esta parte está cargada en la memoria y el BIOS viene a formar parte del Sistema Operativo.
2. La segunda parte del archivo COMMAND.COM, contiene los comandos internos del *MS-DOS* como el DIR, COPY y el TYPE, que son cargados en la memoria alta convencional de la *RAM*, donde pueden ser sobrescritos por programas de aplicaciones que por alguna razón necesitan de la memoria.
3. La tercera parte del COMMAND.COM, es usada solamente una vez; esta buscará al directorio raíz para después llamar al archivo AUTOEXEC.BAT, este archivo es creado por un usuario de computadora y contiene series del *MS-DOS*, de archivos por lotes, comandos y otros nombres de programas que los usuarios

(12) Diccionario de Computación
de Alan Freedman, Ed. Mc. Graw Hill

necesitan para correr, cada vez que la computadora es reiniciada. La PC está nuevamente iniciada, y lista para ser usada.

## 4.3. OPCIONES DE ESCANEO DEL ANTIVIRUS DR. SOLOMON'S

Opciones *VIVERIFY*, dialogo para detectar cambios y opciones avanzadas del Antivirus Dr. Solomon's. A continuación se presenta una lista de las opciones de *VIVERIFY,* que se pueden visualizar al abrir el diálogo "Detectar cambios y opciones avanzadas", con sus parámetros correspondientes, todos los parámetros comienzan con: *'/'*

Parámetros más usuales:

- **Boot/NOBOOT**
- ***/BEEP***
- **/FPRINT=ARCHIVO**
- **/REPORT=ARCHIVO**
- **/DESINFECT**
- **/NOFILES**
- **/DOALLFILES**
- **/UNZIP**
- **PACK/NOPACK**
- **/NOPART**
- **VIRUS/BEEP**
- **/ONEONLY**
- **/ANALYZE**

**Boot/NOBOOT**

Verifica sectores *Boot,* el parámetro especifica la opción seleccionada; un ejemplo de una situación en la que se desactivaría esta opción, es en el caso cuando se esté verificando una unidad de red, ya que las unidades de red no tienen sectores *Boot.*

***/BEEP***

Hará sonar al sistema, emite un pitido cada vez que el escaneado encuentra un archivo que haya cambiado.

**/FPRINT=ARCHIVO**

Especifica el archivo de firmas que se vaya a utilizar, si no se especifica un *path* diferente, la carpeta se colocará por defecto en la carpeta de *TOOLKIT.VIVERIFY*, que le permite crear múltiples archivos de firmas con nombres únicos. Sólo los archivos que tienen una entrada en el archivo de firmas, pueden verificarse para ver si se han realizado cambios. Cualquier archivo que el *VIVERIFY* intente verificar pero que no tenga una entrada, se reportará como si se tratase de un archivo nuevo. Esto puede evitarse si, comprobando los cambios de una selección de unidades específicas, elige el archivo de firmas que se creó con la misma combinación de unidades seleccionadas.

**/REPORT=ARCHIVO**

Selecciona un nombre de reporte de archivo alternativo y/o *path*, si reporta a un archivo, se selecciona en el diálogo 'Detectar cambios', si no se especifica un *path* diferente, la carpeta se colocará por defecto en la carpeta de *TOOLKIT*, como ejemplo tenemos a los siguientes algoritmos:

- CCITT CRC/CRC

  Se basa en firmas del algoritmo CCITT CRC.

- TAMAÑOS/SIZES

  Se basan en firmas del algoritmo tamaño de archivo.

- AUTO CHEQUEO/WHOLESUM

  Se basan en las firmas de la suma de todos los bytes en el archivo.

- DES/DES

  Este algoritmo, pide otro *diskette* después del escaneado de cada *diskette*, el parámetro especifica que la opción está desactivada.

- TURBO/NT

  La modalidad, checa solamente los 4 primeros Kbytes de un archivo en vez de todos los bytes, que es la opción por defecto, el parámetro especifica que la opción está desactivada.

- N BYTES/N=N

  Checa solamente "n" número de bytes del ARCHIVO.SIN el parámetro el valor por defecto para "n" es 5.

**/REPORT=ARCHIVO**

Especifica el archivo de reporte, el reporte a un archivo se activa utilizando la opción "Reporte a archivo" en el diálogo "Buscar virus".

**/DESINFECT**

Tenga en cuenta que la mayoría de estas opciones, son aplicables también a búsquedas de desinfección iniciadas desde el menú 'Desinfectar' o de la pantalla principal. Las excepciones no las opciones del análisis heurístico, checan a los archivos ejecutables y escanean todos los archivos. Para escaneos de desinfección que se inician desde la línea de comandos; los parámetros pueden utilizarse en conjunción con el parámetro "/DESINFECT".

**/NOFILES**

Checan los archivos ejecutables, desactivando ésta opción se desactiva la opción "Escanear todos los archivos", el parámetro especifica la opción desactivada. Desactive esta opción si sólo desea verificar los sectores *Boot* y de partición.

**/DOALLFILES**

Verifica todos los tipos de archivos, no sólo los ejecutables, activando esta opción se activa también la opción "Archivos Ejecutables", esta opción aumenta la seguridad, pero prolonga el tiempo de escaneado. Es recomendable utilizar esta opción en

sistemas de verificación o cuando se esté efectuando una limpieza tras una infección.

**/UNZIP**

Escanea archivos empaquetados y comprimidos con extensión: ZIP, ARJ, etc, (use PKLITE), sí sólo quiere escanear los archivos empaquetados. Los archivos comprimidos y empaquetados que escaneará: poseen los siguientes formatos: ARC. PKZip, PKLite, LZExe, ARJ, ICE, LZH, Diet (Versión 1.0) y CryptCom.

**PACK/NOPACK**

Escanea archivos empaquetados y comprimidos con los siguientes formatos: PKLite, LZExe, ICE, Diet (versión 1.0) y CryptCom, el parámetro equivalente a esta opción es: '**/PACK'**, existe otro parámetro '**/NOPACK'**, para especificar este parámetro ha de utilizarse añadido al parámetro '**/UNZIP'** (que equivale a la opción 'ZIP, ARJ'). Si se especifica '/UNZIP /NOPACK' el escaneo comprenderá los archivos escaneados con "**/UNZIP**" además de aquellos que sé escanearán también con "**/PACK**".

**/NOPART**

Escanea sectores de partición, el parámetro especifica la opción desactivada, activando esta opción se activa también la opción "Sectores *Boot*".

Para escanear un subdirectorio [path[\file]] *parameter*, escanea al subdirectorio o el archivo especificado solamente. El parámetro [path\file] se especifica en la línea de comandos, se puede especificar un sólo archivo a escanear en el cuadro "Escanear un subdirectorio", en el diálogo "Opciones avanzadas".

**VIRUS/BEEP**

Hará sonar al sistema, emite un pitido cada vez que el escaneado encuentra un archivo con un virus.

**/ONEONLY**

Para múltiples *diskettes*, pide un nuevo *diskette* una vez escaneado el anterior, el parámetro especifica la opción desactivada.

**/ANALYZE**

Usar el análisis heurístico, que identifica posibles nuevos virus, esta opción aumenta la seguridad, pero prolonga el tiempo de escaneado. Si se descubre un nuevo virus, el reporte de *Findvirus* indicará una infección sin dar nombre al virus.

La alarma de red ante: **virus/tell=usuario/msg="msg",** envía un mensaje informando al supervisor, sobre la infección en la red Novell. Para los parámetros, "usuario" es el nombre con el que se haya conectado a la red, es necesario asi mismo incluir las comillas en "**msg**". La alarma de red ante el virus y su usuario de destino se especifica en el diálogo "Opciones de Red". La opción "Alarma de red ante virus" también aparece en este diálogo el estado "**activado/desactivado",** de esta opción se sincroniza de forma automática los diálogos "Opciones de red" y "Buscar virus - Opciones avanzadas". El mensaje de red de **Findvirus** está activado por defecto, el usuario de destino por defecto es "Supervisor" y el mensaje por defecto es ¡¡¡Virus detectado en estación de trabajo!!!.

Nombre de archivo de reporte/report=archivo, especifica el archivo de reporte. El reporte a archivo se activa en "Reporte a archivo" en el diálogo "Buscar" virus.

### 4.3.1. OPCIONES DE ESCANEO DEL FINDVIRU CON EL BOTON DERECHO DEL RATON

A continuación se presentan los parámetros de esta ficha, con el parámetro equivalente (este parámetro comienza con el carácter '/').

**/DOALLFILES**

Comprueba todos los archivos de datos, no sólo los ejecutables.

**/UNZIP**

Escanea los archivos de empaquetado y compresión, los archivos comprimidos en ellos. (También utilice PKLite, si desea escanear archivos empaquetados). Los formatos que se incluyen son los siguientes: ARC, PKZip, PKLite, LZExe, ARJ, ICE, LZH, Diet (Versión 1.0) y las utilidades CryptCom.

**PKLITE, LZEXE/PACK LZEXE/NOPACK**

Escanean archivos empaquetado y los que se encuentran comprimidos en ellos, los formatos que se incluyen son los siguientes: PKLite, LZExe, ICE, Diet (Versión 1.0) y CryptCom. El parámetro equivalente a esta opción es "PACK". Para utilizar '/NOPACK', especifíquelo además del parámetro "/UNZIP" (que es el equivalente a la opción ZIP, ARJ, etc.). Al especificar "/UNZIP /NOPACK", sé escanean los archivos que '/UNZIP' suele escanear aparte de los que "/PACK" ya ha escaneado.

**/NOBOOT**

- Escanea los sectores *Boot*. El parámetro determina que la opción se encuentra desactivada.

**/NOPART**

- Escanean a los sectores de partición, el parámetro determina que la opción se encuentra desactivada.

# CAPITULO 5

## RECOMENDACIONES A USUARIOS Y MANEJO DE SECTORES DEL DISCO DURO

[8] Los virus informáticos se denominan de esta forma porque se copian a sí mismos. Existen otros tipos de *software* que pueden causar problemas en la computadora. Sin embargo, ningún otro tipo de *software* se puede replicar, y esta característica es la que convierte a un programa en virus (virus de archivo, virus de macro, virus de sectores *Boot* y de partición, virus acompañantes, virus de sobre-escritura y virus múltiples). También existen los cuentagotas y empaquetadores que facilitan la propagación de los virus. Las características principales de los virus son: la ocultación, el polimorfismo, sus nombres, las variantes y la como se propagan.

Normalmente, un virus está diseñado para copiarse a sí mismo sin conocimiento del usuario. Por ejemplo, puede unirse al programa FORMAT y ejecutarse siempre que formatee un *diskette*. Si los virus no hacen otra cosa que copiarse a sí mismos, ¿por qué provocan tantos problemas?

En primer lugar, la mayoría de los virus producen efectos secundarios de forma deliberada o accidental. Algunos de ellos parecen inofensivos, ya que sólo muestran un mensaje, hacen que las letras caigan de la pantalla o emiten un sonido. Otros están específicamente diseñados para resultar destructivos, al sobrescribir datos seleccionados o eliminar archivos del disco duro. Además, muchos *virus no* funcionan tal y como los idearon los creadores debido a las alteraciones en el *software*; por lo que los efectos secundarios de estos virus son imprevisibles. Desde el punto de vista del usuario, no tiene importancia si el daño causado por un virus es el resultado directo de la intención del autor del virus o de un fallo en el programa.

(8) PC Viruses – Detection, Analysis and Cure
Dr. Alan Solomon & Tin Kay

Existen pocos virus ideados para *Windows* 95. En segundo lugar, los virus permanecen en la memoria de la PC, donde puede causar problemas al interferir con otro *software*. Normalmente *Windows* 95 evita esto. En tercer lugar cuando posea un virus, es probable que se lo transmita sin querer a un compañero o usuario, lo que puede poner en peligro la confianza depositada en usted y en la empresa.

La mayoría de los virus actuales, se diseñaron para funcionar en *DOS*. Gran parte de ellos utilizan funciones específicas de *DOS*, para actuar y se aprovechan de sus características que se encuentran sin documentar y que se han eliminado en *Windows* 95.

Los macro virus son cada vez más comunes. Se escriben en el lenguaje de macro de aplicaciones como Microsoft *Word* y pueden infectar cualquier plataforma que ejecute la aplicación. No existe ningún virus que sea totalmente inofensivo; todos fueron programados para realizar un efecto, todos provocan pérdida de tiempo para ser erradicados aunque algunos no hagan gran daño; tiempo de procesamiento, de espacio en memoria y en disco. Dr. Solomon's Antivirus *Toolkit*, puede servir de ayuda para garantizar que la PC se encuentre libre de estos trastornos y de las infecciones de virus.

Si tiene un brote de virus importante en su organización, es imprescindible que busque y limpie todos los medios y sistemas infectados. Si deja un *diskette* o alguna estación de trabajo sin limpiar, pronto tendrá otro brote.

No se trata de un problema trivial cuando hay muchas PC's involucradas. Antes de iniciar la limpieza, debe calcular el alcance del problema, incluso si cree que sólo un pequeño porcentaje de las PC's, estén infectadas. Es imprescindible verificar a todas las PC's, todos los *diskettes*, y todos los medios de almacenamiento de datos de la empresa.

### 5.1.1. SUPERVISION

Debe visitar todas las áreas de usuario, y verificar los medios; reúna todos los *diskettes* en una ubicación de chequeo central. En este último caso, también tiene que asegurarse de que todos los *diskettes* sean devueltos a sus legítimos propietarios.

### 5.1.2. VERIFICACION

En primer lugar, debe calcular cuántas PC's y *diskettes* se deben verificar. A continuación, puede estimar cuántas personas va a necesitar y cuánto tiempo va a durar la operación. Puede calcular una media de 50 *diskettes* por computadora, con un máximo de 100 y un mínimo de 25. Para escanear los *diskettes* son necesarias varias PC's. Asegúrese de que dispone de unidades de 3½" y 5¼", si utiliza ambos tipos de *diskette*. Es obvio que en primer lugar, es necesario asegurarse de que las PC's utilizadas para efectuar el chequeo estén limpias Si hay varios miles de *diskettes* para verificar, puede ser útil alquilar o comprar un autocargador de *diskettes*. Existe una versión especial de *Toolkit* para su ejecución en PC conectadas a un autocargador. Para obtener más información, póngase en contacto con Dr. Solomon's *Software* o con el distribuidor autorizado. Una vez que conozca las dimensiones de la tarea, puede organizar al personal necesario. Como parte de la limpieza, es necesario tratar los *diskettes* infectados. Si los *diskettes* permiten la lectura, en primer lugar ejecute *FindVirus* para buscar virus. A continuación, si fuera necesario, utilice *FindVirus* para eliminar los virus mediante la opción "Desinfectar". Si tiene dudas, debe apartar al *diskette* para efectuarle un chequeo final. Los *diskettes* que pasen el chequeo final deben ser devueltos al controlador de *diskettes* para su devolución al usuario. Se deben proteger contra escritura y marcar todos los *diskettes* verificados para indicar que están limpios. Esto se hace con el principal objetivo de asegurar a los usuarios que se han limpiado los *diskettes*.

Al finalizar la operación, debe quedar un número relativamente pequeño de *diskettes* infectados que son fáciles de tratar. En el caso de virus de sector *Boot*, la solución es

hacer una copia archivo por archivo de un *diskette* a otro o, en el caso de virus de archivo, eliminar el archivo.

### 5.1.3. BUSQUE VIRUS EXISTENTES

Para buscar los virus existentes, utilice la herramienta *FindVirus*. Se recomienda siempre, utilizarla antes de intentar grabar a disco flexible; información que emitirá a otro usuario. También use esta utilería cuando reciba información en discos o de archivos que reciba por correos electrónicos; si no realiza la verificación, puede ocurrir la filtración, y propagación de algún virus.

### 5.1.4. EVITE INFECCIONES FUTURAS

Diríjase al archivo de ayuda independiente de *Winguard* (utilería de Dr. Solomon's). *Winguard,* funciona constantemente en segundo plano para evitar que la PC se infecte. Rastrea la existencia de virus en los archivos, los sectores *Boot* y de partición al accederse a ellos, y da la alerta cuando detecta un virus. Al igual que *FindVirus*, se puede configurar *Winguard* para que desinfecte de forma automática. *Winguard* funciona de forma independiente con respecto a *FindVirus* y dispone de un programa de instalación propio. Para detectar y desinfectar con la máxima seguridad, utilice el *diskette* Magic Bullet[32] desde este se arranca la PC y a continuación ejecuta la versión de *FindVirus* para *DOS*.

## 5.2.VIRUS DE SECTORES *BOOT* Y DE PARTICION

### 5.2.1. SECTOR DE ARRANQUE[12]

- Es el área del disco duro que contiene instrucciones y/o datos que hacen que la computadora localice y cargue el sistema operativo. Normalmente es el primer sector de la parte del disco duro.
- Es la primera parte del disco duro y de un *diskette* que se lee tras iniciar el sistema.

(12) Diccionario de Computación
De Alan Freedman. Ed. Mc. Graw Hill
(32) MAGIC BULLET (ver Capítulo 3.4.7.)

Un diskette se puede preparar con datos que contengan el código preciso para mostrar el mensaje que indica que la PC, no se puede iniciar al disco.

La mayoría de las PC están configuradas para intentar arrancar primero desde la unidad A:\> Si el sector *Boot* de un *diskette* se encuentra infectado, el virus se ejecuta cuando intenta arrancar desde el *diskette* e infecta al disco duro. Por ejemplo, si deja un *diskette* dentro de la unidad de *diskette flexible* durante toda la noche y al día siguiente enciende la PC, aparece el siguiente mensaje o uno similar:

ESTE DISKETTE NO TIENE EL SISTEMA DE ARRANQUE
CÁMBIELO POR OTRO Y PULSE CUALQUIER TECLA

Si el *diskette* se encuentra infectado con un virus de sector *Boot*, dicho virus ya se ha ejecutado y puede que *la* PC ya se haya infectado. Una PC con Intel es vulnerable a los virus de sector *Boot* y del sector de partición. Pueden infectar cualquier PC, independientemente del sistema operativo, ya que el virus se ejecuta antes de que el sistema se inicie.

### 5.2.2. SECTOR DE PARTICION[13]

- Es el sector que contiene información sobre el disco, tales como el número de sectores en cada partición y las ubicaciones de todos ellos.
- Término utilizado en algunos sistemas operativos para referirse a un área estática de la memoria que se emplea para trabajos, y también se aplica, por asociaciones, a los trabajos realizados en dicha área.
- También se denomina ***MBR*** *(Master Boot Record)*.

## 5.3. PROCEDIMIENTOS PARA ELIMINAR UN VIRUS DE SECTOR DE PARTICION DE UN DISCO DURO SIN ANTIVIRUS

- Como podemos observar la imagen según (Figura 4.2.2, del Capítulo 4, pág. 78), al sector de partición ideal para *DOS*, se dice ideal por su contenido en código *ASCII*, ya que cuando un virus de sector de partición es introducido al disco duro, cambia y manda el contenido de este "sector ideal" a otro lugar

(13) Diccionario de informática
OXFORD UNIVERSITY PRESS. Ed. Diaz de Santos

aleatoriamente y el contenido del virus de sector de partición se adueña de este sector: CILINDRO 0, CABEZA 0 SECTOR 1.

- Para eliminarlo manualmente, se requiere contar con la utileria de Dr. Solomon's; "INSPECT DISK", instalada en el disco duro de la PC.; mediante combinaciones de teclas clave, es posible inspeccionar todos los sectores del disco duro. Primeramente notaremos que el sector de partición no es el ideal que conocemos, por lo tanto ya sabemos que el disco duro tiene virus en el sector de partición, entonces exploramos en donde se localiza este sector ideal de partición. Al ir explorando quizás lo hallemos en la siguiente ubicación: SECTOR 0, CABEZA 0 y SECTOR 7, (no siempre es este sector). Entonces procederemos a copiar el contenido del sector ideal de partición ubicado en esta posición, y lo copiamos al lugar que le corresponde, se salvan los cambios y se reinicia la PC. OK ya no existe el virus en el sector de partición.

## 5.4. PROCEDIMIENTOS PARA ELIMINAR UN VIRUS DE SECTOR DE ARRANQUE DE UN DISCO DURO SIN ANTIVIRUS

Como podemos observar la imagen (Figura 4.2.3. del Capítulo 4, pág. 79), al sector de arranque ideal, para *DOS*. Se dice ideal por su contenido en código *ASCII:* ya que cuando un virus de sector de arranque es introducido al disco duro, cambia y manda el contenido de este "sector ideal", a otro lugar aleatoriamente, y el contenido del virus de sector de partición, se adueña de este sector: CILINDRO 0, CABEZA 1 SECTOR 1.

- Para eliminarlo manualmente, se requiere contar con la utilería de Dr. *Solomon's; INSPECT DISK instalada en el* disco duro de la PC. Mediante combinaciones de teclas clave, es posible inspeccionar todos los sectores del disco duro, primeramente notaremos que el sector de arranque no es el ideal que conocemos, por lo tanto ya sabemos que el disco duro tiene virus en el sector de arranque, entonces exploramos en donde se localiza este sector ideal de arranque. Al ir explorando quizás lo hallemos en la siguiente ubicación: SECTOR 0,

CABEZA 0 y SECTOR 12, (no siempre es este sector). Entonces procederemos a copiar el contenido del sector ideal de arranque ubicado en esta posición y lo copiamos al lugar que le corresponde, se salvan los cambios y se reinicia la PC. OK ya no existe el virus en el sector de arranque.

## 5.5. OTROS PROGRAMAS QUE NO SON VIRUS

Existen algunos programas que confunden en ciertas ocasiones a los usuarios tanto principiantes como avanzados, ya que al notar una actitud anormal en el equipo de cómputo, se piensa inmediatamente en virus, pero en algunas ocasiones no es asi, estos programas son:

- BUGS DE PROGRAMACION
- FALSAS ALARMAS
- TROYANOS
- PROGRAMAS CORRUPTOS
- WORMS
- BOMBA LOGICA
- BOMBAS DE RELOJERIA
- ALTERACIONES
- BLOQUEOS
- BROMAS
- ERRORES HUMANOS

### 5.5.1. BUGS DE PROGRAMACION

Un *Bug* es un error NO intencional dentro de un programa, que hace que éste no funcione como debería. Los *software* Antivirus no detectan los *bugs* de programación.

### 5.5.2. FALSAS ALARMAS

Las falsas alarmas no son virus. Una falsa alarma es cuando se piensa erróneamente que se tiene un virus, y en realidad se trata de un problema de *hardware* o *software*.

### 5.5.3. TROYANOS

Un troyano es un programa que está diseñado para hacer lo inesperado. Generalmente ocasionan daños severos en la información (borran archivos, formatean el disco duro, etc.). Los troyanos son programas que realizan algo inesperado y normalmente dañino. No se encuentran tan extendidos como los virus, porque no se replican, pero pueden representar una amenaza cuando se copian. Mucha gente confunde ambas manifestaciones: el disco *Aids Information*, a menudo mencionado por los medios de comunicación como un ejemplo de virus, era en verdad un troyano. Además, los virus contienen a veces troyanos. Es poco probable que se encuentre con troyanos si obtiene siempre el *software* de fuentes con buena reputación, pero la mejor defensa contra los daños que estos programas provocan es realizar una copia de respaldo del sistema. El sistema *Toolkit* detecta e identifica algunos troyanos conocidos y los trata como si de un virus se tratase.

### 5.5.4. PROGRAMAS CORRUPTOS

Son programas alterados por fallas en el *hardware*, no por virus. Los *software* Antivirus, no detectan programas corruptos, entre estos tenemos como ejemplo a los "*worms*" y a las "bombas lógicas".

### 5.5.5. **WORMS** (gusano)

- Es un programa destructivo, que se copia así mismo a todo lo largo del disco, y la memoria; consumiendo los recursos de la computadora y eventualmente abatiendo el sistema.
- También es un programa que se mueve por toda una red y deposita información en cada nodo, con propósitos de diagnóstico, o hace que las computadoras ociosas compartan algo de la carga de procesamiento.

### 5.5.6. BOMBA LOGICA

- Es una rutina de programa, que destruye datos; por ejemplo, puede formatear el disco duro o aleatoriamente insertar basura dentro de los archivos de datos.
- Puede ser llevada a una computadora personal, cargándole un programa de dominio público que ha sido adulterado; una vez ejecutado, hace su daño inmediatamente.

### 5.5.7. BOMBAS DE RELOJERIA

Las bombas de relojería y las bombas lógicas son tipos particulares de troyanos. La bomba de relojería se activa para una fecha concreta, mientras que la bomba lógica se acciona con un conjunto específico de condiciones, tales como el número de archivos en un disco o una secuencia de caracteres que se introducen. Normalmente, ambas bombas causan efectos dañinos. Algunos usuarios muy inteligentes en computación, hacen este tipo de programas, mediante ficheros ".BAT" y luego los cargan entre archivos de otros sistemas, de manera que si ejecutamos un archivo de estos, con un caballo de Troya invisible con atributos, se van activar los efectos y comandos que hayan sido determinados por el programador que diseño el archivo.

En este capitulo se proporciona un "*tip*" para evitar que un programa NO se ejecute correctamente, esto nos sirve en algunas ocasiones para que otro usuario no haga uso

de nuestros sistemas o lo copie para su conveniencia, como ejemplo pondremos al archivo ejecutable del sistema Excel.

Procedimiento para evitar que no se pueda activar:

1. Nos ubicamos en el indicador de sistema: C:\>
2. Nos enrutamos hacia donde se encuentra localizado el archivo ejecutable del sistema Excel.

   **C:\>CD MSOFFICE** más *<Enter>*

   **C:\>MSOFFICE>**

   **C:\>MSOFFICE>CD EXCEL** más *<Enter>*

   **C:\>MSOFFICE\EXCEL>**

3. Desde esta ruta editamos al archivo EXCEL.EXE

   C:\>MSOFFICE\EXCEL>EDIT EXCEL.EXE más *<Enter>*

4. Una vez desplegado el contenido de este archivo, procedemos a alterarlo, es importante recordar cual fue el cambio que le hicimos a este archivo, si non no podrá volver a ejecutarse.
5. Salimos y salvamos el archivo EXCEL.EXE, y posteriormente entramos a *Windows* y llamamos al sistema Excel para que se ejecute y notaremos el efecto.

### 5.5.8. ALTERACIONES

Las alteraciones son los errores no intencionados en un programa que se pueden considerar virus por equivocación.

Virtualmente, todo *software* complejo contiene alteraciones, las alteraciones menores provocan simples inconvenientes, mientras que las alteraciones mayores pueden causar pérdidas catastróficas de datos. No existe ninguna manera de detectar las alteraciones y la única defensa consiste en realizar regularmente una copia de respaldo de los datos importantes.

### 5.5.9. BLOQUEOS

Los programas de bajo nivel son aquellos que funcionan directamente en discos. Se denominan de esta forma debido a que funcionan por debajo del nivel del sistema operativo que normalmente controla el acceso a los discos y obliga a mantener ciertas normas.

Entre los programas de bajo nivel, se incluyen:

- Editores del sector de disco
- Programas de memoria caché en disco
- *Software* de compresión de disco
- Defragmentadores

Por lo general, estas herramientas son bastante seguras si se ejecutan una a una; sin embargo, pueden aparecer problemas si ejecuta dos o más herramientas de bajo nivel a la vez. Si dos o más herramientas intentan acceder al disco, pueden causar bloqueos potencialmente peligrosos. A causa de que estas herramientas son cada vez más comunes, este tipo de problema puede aparecer con más frecuencia.

Para evitar problemas con herramientas de bajo nivel:

- Realice siempre copias de respaldo antes de utilizar cualquier utilidad de disco.
- No ejecute más de una utilidad a la vez.
- No utilice estas herramientas a la vez que utiliza *software* residente en memoria.
- Lea siempre los manuales y todos los archivos README proporcionados con el producto. Si el fabricante ha incluido advertencias especiales, seguro que hay un motivo para ello.

### 5.5.10. BROMAS

Algunos programas causan efectos aparentemente destructivos a la computadora, cuando en realidad se trata sólo de bromas inofensivas. Por ejemplo, puede aparecer

un mensaje que indica que el disco duro se va a formatear. Por desgracia, resulta fácil reaccionar de forma exagerada ante tal broma y causar más daño al intentar solucionar un problema que, en realidad, no es un virus.

**Nota** :

*"El sistema Toolkit, detecta e identifica los programas de bromas conocidas"*

### 5.5.11. ERRORES HUMANOS

Si se notan fallas en la PC y se producen pérdidas de información, la causa más probable no será un virus o un problema del *software*, sino un error humano. Todos cometemos errores, como introducir la secuencia de teclas equivocada o pulsar **DEL** *.* en la carpeta incorrecta, lo que puede provocar serias consecuencias.

> **Nota**: Recuerde que la parte más valiosa de la computadora son los datos introducidos. El *hardware* y los programas se pueden sustituir, pero los datos sólo se pueden recuperar si ha realizado una copia de respaldo.

## 5.6. DESINFECTE SECTORES DE *BOOT* DE *DISKETTE*S

Es posible desinfectar los sectores *Boot* de los *diskette*s con la opción "Desinfectar unidad" o utilizando la pantalla principal. También es posible desinfectar los sectores *Boot* de los *diskette*s, sustituyéndolos por una copia limpia. Para máxima seguridad puede realizar esta operación, utilizando la utilidad de *DOS "CleanBoot"*, una vez que haya vuelto a arrancar desde un disco limpio.

También es posible desinfectar los sectores *Boot* de los *diskette*s desde la interfaz del usuario, para ello realice los siguientes pasos:

1. Introduzca el *diskette* sospechoso

2. En el menú "Desinfectar" de la interfaz del usuario, seleccione "Reemplazar sector *Boot*"
3. Aparecerá el cuadro de diálogo "Reemplazar sector *Boot*"
4. Seleccione la unidad apropiada en la lista "Unidades"
5. Seleccione el tipo de *diskette* de la lista, o seleccione "Detección de disco automática"
6. Haga clic en "Reemplazar"
7. Si el tipo especificado no coincide con el tipo detectado aparecerá el mensaje: 'La capacidad del *diskette* no coincide con la capacidad elegida'. Haga clic en "Aceptar" o "Cancela". Tenga en cuenta: que el sector *Boot* ha de reemplazarse por un sector *Boot*, para la capacidad formateada ya existente; esto debe detectarse correctamente y por ello normalmente no debe ignorarse. Si el tipo de disco detectado no es el que usted especificó, es posible que el *diskette* tenga formateo cruzado.
8. Compruebe si el directorio tiene archivos perdidos o directorios dañados, si los tiene, es posible que se haya utilizado un sector *Boot* con la capacidad incorrecta. En este caso, intente utilizar *CleanBoot* de nuevo, pero seleccionando un tipo de disco diferente e ignorando la detección automática. Los archivos en el *diskette* no se perderán, a menos que intente escribir en el *diskette* mientras el sector *Boot* es incorrecto.
9. Si se muestra un mensaje a 'no se puede escribir en el disco', compruebe que disco no esté protegido contra escritura.

# CAPITULO 6

## SUGERENCIAS Y PROCEDIMIENTOS DE INSTALACION DE UN ANTIVIRUS

Si una máquina está infectada con algún virus, se recomienda "**encender en limpio**"[15]. El proceso involucra un encendido de la computadora con un *diskette* de arranque libre de virus. De esta forma el virus no puede cargarse en memoria y por lo tanto no puede ocultarse, lo que significa una fácil detección y reparación del mismo. Los virus informáticos representan un problema cada vez mayor. Cuando Dr. Solomon's *Software* publicó la primera versión de Antivirus *Toolkit* en 1989, la cantidad de virus en todo el mundo no llegaba a diez. Un año más tarde, existían 50 y al año siguiente aumentaron a 200. En mayo de 1997, había más de 12.000. Cada mes aparecen entre 300 y 350 nuevos virus.

### 6.1. CONSEJOS A USUARIOS[16]

- Mucha gente se alarma cuando oye la palabra virus. Sin embargo, no olvide que los virus se pueden evitar, si se localizan a tiempo, la infección no tiene por qué provocar demasiados trastornos. Es recomendable tomar la mayor cantidad de medidas preventivas como le sea posible, pero además necesita estar capacitado para enfrentarse a un virus, en caso de que aparezca.
- Tenga en cuenta que existe la posibilidad de considerar otro tipo de problemas como brotes de virus. Entre estos problemas, se incluyen: alteraciones, bloqueos en *software* de bajo nivel, troyanos, bombas de relojería y bombas lógicas, bromas, y errores humanos.

(15) "Encender en limpio".- Explicación en el Capítulo 3, punto 3.1.6. (pág. 62)
(16) Manual de Usuario, de Dr. Solomon's

- Dr. Solomon's Antivirus *Toolkit* detecta los virus y resuelve las infecciones que provocan. Localiza y elimina los virus conocidos, es decir, que sean conocidos en la versión actual del archivo del *driver*. Además, existe una opción para que el sistema *Toolkit* encuentre nuevos virus (anteriormente sin descubrir).

### 6.2. SISTEMA DE ANTIVIRUS DE MCAFEE

En este tema se explicará, como verificar su sistema y cómo instalar el *software* de *McAfee* bajo *MS-DOS*, *Windows* y *OS/2*. No utilice ningún otro método para instalar *VirusScan* de *McAfee*, o correrá el riesgo de propagar algún virus.

El disco de distribución contiene opciones para certificar su sistema, instalar el *VirusScan* de *McAfee*, modificar los archivos de configuración (si es necesario) y activar *VShield* de *McAfee*, como parte del proceso de instalación. Estas tareas se describen con detalle más adelante en éste mismo capítulo.

- La versión de *VirusScan* de *McAfee*, instala *Scan* y *Vshield* en el directorio C:\>*SCAN*2 de su disco duro. También modifica automáticamente el archivo AUTOEXEC.BAT, para que el programa *VShield* sea invocado y ejecutado cada vez que encienda su computadora.
- El programa de instalación de *VirusScan* para *Windows* copia los archivos del directorio de: C:\>MCAFEE de su disco duro y modifica el archivo AUTOEXEC.BAT, para que el programa *VShield* sea invocado y ejecutado cada vez que encienda su PC. La instalación en *Windows* debe completarla usted mismo.
- En *OS/2*, por favor copie la versión para *OS/2* de *Scan* y la versión *DOS* para el programa *VShield* en: C:\>MCAFEE\VIRUS*SCAN* de su disco local y modifique el archivo AUTOEXEC.BAT, para que el programa *VShield* sea ejecutado de manera automática cuando inicie su sesión de *DOS* o de *Windows*.

- Si durante el proceso de instalación el programa se encuentra con una versión anterior, del Virus*Scan* (previamente instalada), le preguntará si desea actualizarla. Si en cualquier momento desea abandonar el programa de instalación, presione Ctrl-Pausa y regresará a la línea de comandos de *MS-DOS* u *OS/2* según sea el caso.

## 6.3. RECOMENDACIONES ANTES DE UNA INSTALACION DE ANTIVIRUS

(Trataremos el procedimiento del sistema de Antivirus de ***Mcafee***).

### 6.3.1 RESPALDE SU DISCO DURO

Cuando se limpian algunos virus pueden dejar algunos archivos o discos inservibles. Para tener la oportunidad de recuperarlos:

1. Copie todos los archivos de trabajo de su disco duro a discos flexibles limpios o a cintas de respaldo.
2. Puede usar programas de respaldo comerciales o los que vienen incluidos en los sistemas operativos *DOS* u *OS/2*.
3. Ejecute un rastreo con *Scan* antes de efectuar el respaldo, para estar seguro que el programa de respaldo no esté infectado.
4. No ejecute el respaldo si el programa está infectado. En lugar de ello, reinstale el programa, apagando y arrancando con el disco limpio y partiendo de sus discos originales.
5. Si algunos de los archivos que va a respaldar están infectados, es preferible que obtenga una copia aunque esté infectada, a no tener ninguna.
6. No borre los respaldos anteriores (sobre escribiéndolos), si no estaban infectados.

### 6.3.2. SI DETECTA ALGUN VIRUS[17]

1. Será necesario ejecutar el programa *Scan*, configurando la opción /CLEAN, para erradicar de esta manera los virus que fueron encontrados en los discos.

(17) Manual de Usuario, de *McAfee*

2. Si no está seguro de cómo proceder, una vez que haya encontrado un virus, consulte a Soporte Técnico de *McAfee*[18] o cualquiera de sus agentes autorizados para que sea apoyado.
3. Si no está familiarizado con los programas de Antivirus y sus métodos, le recomendamos ampliamente, que obtenga ayuda experimentada en el tratamiento de los virus. Esto es especialmente cierto cuando se trate de virus críticos que infectan la tabla de partición (MBR), y el sector de arranque (*Boot*); ya que si son removidos de una manera inadecuada, pueden causar la pérdida total de información en los discos infectados.
4. Si los virus no se pueden eliminar, consulte a soporte técnico.
5. Si recibe el siguiente mensaje:

**"Virus cannot be removed from this file."**

6. Asegúrese de anotar el nombre del archivo ya que usted necesitará restaurar este archivo desde su disco de programa original o respaldo. Ejecute nuevamente *SCAN* pero ésta vez utilice las opciones /ADL /CLEAN /DEL para poder borrar los archivos infectados. Si tiene alguna duda, consulte con Soporte Técnico[18].
7. Si los virus son eliminados satisfactoriamente, examine nuevamente sus discos hasta obtener el mensaje de que no se encontraron virus.
8. Si se eliminaron todos los virus, reinicie su computadora. Vuelva a instalar como se describe en la sección "Instalando *VirusScan*", si su sistema ha quedado libre de virus, continúe hasta dejar instalado el programa *VShield.*
9. Una fuente común de virus son los *diskettes* flexibles, por lo que le recomendamos que una vez que se haya concluido la instalación, se realice un rastreo de todos sus *diskettes* flexibles.

### 6.3.3. FALSAS ALARMAS[17]

- Aveces son causa de la naturaleza del *software* Antivirus, existe la posibilidad de que *Scan* le reporte la presencia de un virus y que en realidad la PC no esté infectada.

(17) Manual de Usuario, de *McAfee*
(18) Soporte técnico de *McAfee* - ver Capítulo 14, sección 14.2.2.

- La mayoría de las ocasiones; estas suceden cuando se ha instalado en la memoria más de un programa o protección Antivirus, especialmente si un virus es reportado en la memoria y al reiniciar con un disco flexibles limpio, no se detecta en los archivos o alguna otra área del sistema. En ese caso decimos que se produjo un falso positivo o falsa alarma.

> **Nota**: Si *Scan* le reporta un virus y usted sospecha que se trata de un error, por favor consulte con *McAfee* como se describe en Soporte Técnico[18].

### 6.3.4. GENERANDO UN *DISKETTE* DE ARRANQUE LIMPIO[17]

- En *MS-DOS* o *Windows* es necesario que genere un *diskette* flexible de arranque, limpio, para poder crear su "campo esterilizado" en el caso de que su sistema llegara a infectarse.
- Esto no es necesario en *OS/2*. Sin embargo, también le será útil para copiar programas importantes de *MS-DOS* en un *diskette* limpio.

### 6.3.5. GENERANDO UN DISKETTE PARA MS-DOS

Para generara el diskette, continúe con los siguientes pasos:

1. Dentro de *MS-DOS*, inicie su sistema hasta que tenga el control en la línea de comandos: **C:\>**, mientras que en *Windows*, puede abrir una ventana de *MS-DOS* o seguir los siguientes pasos a través del manejador de archivos (*File Manager*) de *Windows*.
2. Inserte un *diskette* nuevo o uno que ya no tenga información útil para usted, en la unidad: **A:\>**

   > **Nota**: si el *diskette* contiene información, con este procedimiento se eliminará cualquier dato ya existente en dicho disco.
3. Dé formato al *diskette* y al mismo tiempo transfiera el Sistema Operativo al disco de arranque, escribiendo:

(17) Manual de Usuario, de *McAfee*

**C:\>FORMAT A: /S /U**

**Nota**: Si está utilizando alguna versión de *MS-DOS* anterior a 5.0 omita la opción /U. Esta opción, (sólo disponible en las versiones recientes) asegura que todos los sectores del disco serán sobrescritos, es decir, que no será respetada la información presente anteriormente en el disco, en otras palabras: este comando realiza, en un *diskette* flexible un formateo de bajo nivel.

4. Cuando el programa FORMAT le solicite la etiqueta del volumen, escriba: EMERGENCIA o cualquier otro nombre de hasta once caracteres.
5. Copie los programas del sistema operativo que puedan serle útiles. Aquí le presentamos algunos, suponiendo que sus archivos del Sistema Operativo se encuentran en el subdirectorio: C:\>DOS

   **C:\>COPY C:\DOS\FORMAT.* A:**

   **C:\>COPY C:\DOS\XCOPY.* A:**

   **C:\>COPY C:\DOS\DISKCOPY.* A:**

   **C:\>COPY C:\DOS*.SYS A:**

   **C:\>COPY C:\DOS\FDISK.* A:**

   **Nota:** De esta misma manera copie aquellos programas del *MS-DOS* que usted crea que le puedan ser útiles en el futuro, en caso de emergencia.
6. Copie el programa *Scan* y los archivos que este requiere para operar en el *diskette* flexible, aquí le indicamos una manera de hacerlo, suponiendo que los programas estén en el subdirectorio **C:\>SCAN2**:

   **C:\>COPY C:\SCAN2*SCAN*.EXE A:**

   **C:\>COPY C:\SCAN2*SCAN*.DAT A:**

   **C:\>COPY C:\SCAN2\CLEAN.DAT A:**

   **C:\>COPY C:\SCAN2\NAMES.DAT A:**
7. Retire el *diskette* flexible de la unidad y protéjalo contra escritura, para que no pueda ser infectado.
8. Etiquete el *diskette* flexible como "disco de arranque sin virus" y guárdelo en un lugar seguro. Úselo si llega a necesitar establecer nuevamente un ambiente libre

de virus. Es muy útil anotar el número (en Español o en Inglés) de la versión del Sistema Operativo instalado en su equipo. Si la desconoce escriba el comando VER desde C:\> y anote sobre la etiqueta del disco la versión y el lenguaje del Sistema Operativo que tiene instalado.

### 6.3.6. GENERANDO UN DISKETTE PARA *OS/2*

Con *OS/2* realmente no necesita un *diskette* de arranque libre de virus. Sin embargo le puede servir para mantener una copia limpia de algunos archivos importantes. Copie el programa *OSCAN* y sus archivos de datos, así como el AUTOEXEC.BAT y CONFIG.SYS a su *diskette* flexible limpio, protéjalo contra escritura y guárdelo en un lugar seguro.

## 6.4. PROCEDIMIENTO DE INSTALACION DEL ANTIVIRUS MCAFEE EN MS-*DOS*, W*INDOWS Y OS/2*

### 6.4.1. REINICIE DESDE UN AMBIENTE LIMPIO[17]

- El programa *Scan,* debe ejecutarse desde un ambiente libre de virus; con *DOS* o *Windows*, reinicie su equipo desde un disco flexible, si tiene *OS/2* simplemente cierre todas las sesiones de *DOS* y *Windows OS/2*.
- Con *DOS* y *Windows*, la única manera de asegurarse que el ambiente esté limpio, es apagar la computadora para eliminar cualquier virus de la memoria, después reinicie su equipo desde un disco flexible libre de virus, de preferencia del disco original del Sistema Operativo que viene en su equipo (este disco deberá estar protegido contra escritura). Si no lo tiene, pídalo prestado o compre uno nuevo, pero no use cualquier otro *diskette* que pudiera estar infectado. Usted podrá crear un nuevo *diskette* de arranque libre de virus, siguiendo las indicaciones que se dan en la sección "Generando un disco de arranque limpio". Pero este disco sólo deberá ser creado cuando se tenga la seguridad de que el sistema está limpio:

Continúe con los siguientes pasos:

(17) Manual de Usuario, de *McAfee*

1. Apague su computadora por 15 segundos. (No basta con oprimir "Reset" o el conjunto de teclas: CTRL-ALT-DEL, ya que esto puede dejar algún virus activo en la memoria de la computadora).
2. Asegúrese de que su disco de arranque. libre de virus, esté protegido contra escritura.
3. Para los discos de 3.5" corra la presilla para que se pueda observar que el orificio está abierto.
4. Para los discos de 5.25" cubra la ranura de la esquina superior derecha con una etiqueta no transparente.
5. Inserte el disco de arranque en la unidad de disco: A:\>
6. Encienda su computadora y espere hasta comprobar que el sistema haya arrancado desde el *diskette* flexible y que se le ceda el control desde la línea de comandos A:\> no se ejecute ningún programa contenido en su disco duro, ya que podría reactivar el virus.

### 6.4.2 INSTALACION EN MS-DOS

- Es conveniente hacer respaldos, antes de efectuar el procedimiento de instalación de *VirusScan.* De cualquier manera, si desea realizar esta tarea en forma manual o si desea rastrear de nuevo, una vez que haya eliminado un virus. De manera periódica, el proceso se describe más adelante.
- El programa *Scan* examina la memoria de la PC y sus discos, para detectar si tienen virus. La primera vez que active *Scan,* hágalo desde su disco original que está protegido contra escritura, ello evitará ser infectado.
- Si está utilizando *OS/2,* cierre todas las sesiones de *MS-DOS, Windows* y *OS/2* y abra entonces la carpeta de comandos del "*System Folder*" del *OS/2* y haga "*click*" en el icono de "Pantalla Total" de *OS/2* o en el icono de *OS/2 Windows.*

Después de escribir cada línea de instrucciones, presione [Return o *Enter*]:

1. Inserte el programa de *VirusScan* en la unidad de: A:\>

2. Examine el disco: C:\> par buscar virus conocidos tecleando:

| | |
|---|---|
| *DOS* o *WINDOWS* | **A:\>SCAN C:/REPORT C:\VIRUS.LOG** |
| *OS/2* | **A:\>OSCAN C:/REPORT C:\VIRUS.LOG** |

**Nota**: O si usted tiene más de un disco duro explórelos al mismo tiempo. Por ejemplo: si tiene los discos: C y D.

| | |
|---|---|
| *DOS* o *WINDOWS* | **A:\>SCAN D:/REPORT C:\VIRUS.LOG** |
| *OS/2* | **A:\>OSCAN D:/REPORT C:\VIRUS.LOG** |

3. Si lo desea, puede explorar en todas las unidades locales utilizando la opción: /ADL. Por Ejemplo:

| | |
|---|---|
| *DOS* O *WINDOWS* | **A:\>SCAN ADL:/REPORT C:\VIRUS.LOG** |
| *OS/2* | **A: \>OSCAN ADL:/REPORT C:\VIRUS.LOG** |

4. Al programa *Scan,* puede tomarle varios minutos el dictaminar si existen virus en la memoria y posteriormente en él o en los discos del sistema. El programa *Scan* le mantendrá informado del progreso realizado. Lea cuidadosamente la información presentada en la pantalla. A continuación, un ejemplo de lo que le reportará *Scan* después de rastrear un disco:

**Virus data file V9508 created 08/16/95 12:02:37**

**No viruses found in memory,**

**Scanning C:**

**Summary report on C:**

**File(s)**

**Analized:.....1500**

**Scanned:..... 750**

**Possibly infected.....0**

**Master *Boot* Record(s).1**

**Possibly infected.....0**

**Boot Sector(s).....1**

**Possibly infected.....0**

**Time: 20:04 sector de arranque**

5. Si *Scan* le reporta que no halló virus, felicidades existe una gran posibilidad de que su sistema esté libre de virus.
6. Si *Scan* encuentra uno o más virus, le mandará un mensaje como el que sigue:

**Scanning C:**

**Scanning file C:\DOS\ATTRIB.EXE**

Found **The Jerusalem Virus**

No se preocupe, aún si el virus ha infectado ya varios archivos, lo importante en este momento, es que no active ningún otro programa del disco infectado, especialmente si el virus se detectó en la memoria. Vaya directamente a la sección: (**6.3.2. "SI DETECTA ALGUN VIRUS"**, en este mismo capítulo), para aprender, sobre los detalles de cómo debe erradicar al virus.

7. El programa *Scan,* cuenta con varias opciones para controlar y ajustar el rastreo, validación del mismo y su operación de búsqueda.
8. Si está bajo ambiente *Windows* o en cualquier otro programa de aplicación, salga de ellos completamente (no abra una ventana *MS-DOS* en *Windows*) hasta que se encuentre en la línea de comandos de *MS-DOS.*
9. Inicie desde la línea de comandos del sistema. Si se encuentra en ambiente *Windows* o en un programa de aplicación, salga hasta la línea de comandos del Sistema Operativo a: **C:\>**
10. Si están en *OS/2*, cierre todas las sesiones de *MS-DOS* o las ventanas de *OS/2* y abra la carpeta de comandos de la línea de comandos en él "*OS/2 System Folder*" y dé "click" en el icono de "*OS/2 Full Screen*" (pantalla total) o en el icono "*OS/2 Windows*".
11. Después de escribir cada línea de instrucciones, por favor presione la tecla [Return] o [*Enter*].
12. Inserte el programa de *VirusScan* de *McAfee* en la unidad de disco flexible A:\>
13. Si en su computadora, la unidad A:\> no corresponde al formato del disco de distribución de 3.5", cámbiese a la unidad de disco flexible B:\> escribiendo B: [*Enter*].

14. Inicie el programa de instalación tecleando: A:>\INSTALAR , y oprima [*Enter*].
15. Aparecerán algunos mensajes de advertencia y sobre los Derechos Reservados (*CopyRight*). Para avanzar en ellos, oprima [*Enter*] hasta que obtenga la pantalla del menú principal.
16. Es recomendable usar primero la opción 7 (Rastrear unidades locales) del menú, para verificar que los discos duros no se encuentren infectados por algún virus.
17. Si el procedimiento le reporta algún virus, será necesario que apague su PC, espere 15 segundos y reinicie con un disco flexible con Sistema Operativo de la misma versión que la del disco duro, libre de virus y protegido contras escritura. Si no cuenta con él suspenda la operación hasta conseguirlo.
18. Después de arrancar con el disco flexible limpio, saque el disco e inserte el disco de distribución de *VirusScan* de *McAfee* en la unidad A:\> y ejecute los siguientes comandos:

    **A:\>KILLER**[19] **C: /LIMPIA** más la tecla [*Enter*]

19. Y al finalizar la ejecución, escriba:

    **A:\>*SCAN* /ADL/ALL/CLEAN** más la tecla [*Enter*]

20. Al terminar, repita ambos comandos hasta asegurarse que su PC ya no tenga virus. Si no fue posible eliminarlo(s) llame a Soporte Técnico.
21. En caso necesario, vuelva a ejecutar **ARMO**[20] (usando el disco de distribución en: A:\> y cuando obtenga la pantalla del menú principal, escoja la opción número 4 (instalar paquete en disco duro).
22. El proceso de instalación copiará y desempacará algunos archivos.
23. El programa de instalación copiará los archivos y realizará cualquier modificación que sea necesaria en los archivos de arranque que utiliza su sistema, para que así el programa *VShield* sea ejecutado automáticamente cada vez que encienda su computadora.
24. ¡Felicidades! Ha instalado exitosamente su programa de *VirusScan*. Ahora reinicie su computadora y verifique que se haya cargado *VShield*.

(19) **KILLER** = Archivo que elimina un virus, pertenece al sistema de Antivirus de Mcafee
(20) **ARMO** = Archivo que instala el Antivirus de Mcafee en MS-DOS

25. Si no encontró virus durante la instalación, es conveniente que elabore un *diskette* de arranque de Sistema Operativo, que tenga el programa de *Scan* para ser utilizado en caso de emergencia. Lea la sección: (6.3.4. "GENERANDO UN *DISKETTE* DE ARRANQUE LIMPIO", de este mismo capítulo), al terminar, asegúrese de proteger contra escritura su nuevo disco de arranque.

### 6.4.3 INSTALACION EN OS/2[17]

Con *OS/2*, usted puede eliminar cualquier virus de la memoria con sólo cerrar todas las sesiones *DOS*, *Windows*, *OS/2* y las sesiones VDM (*Virtual DOS Machine*). Debido a que en *OS/2*, los programas corren en modo protegido, los virus no pueden infectar ningún otro programa que no esté en su sesión.

### 6.4.4. INSTALACION EN *WINDOWS*[17]

En la segunda parte del proceso de instalación para MS-DOS de virus *Scan;* para *Windows* se instalan dos iconos el *Scan* y *Vshield*, que crean al grupo "*McAfee*".

Para utilizarlos, simplemente:

1. Coloque el cursor con el ratón sobre el icono, presione doble "*click*" y consulte como operar con el *VirusScan* en el ambiente *Windows*
2. Si detecta un virus activo en la memoria, por favor no utilice *Scan* para *Windows* para eliminar virus, debido a que puede estar contaminado el mismo programa de virus u otros archivos y así se corre el grave riesgo de diseminar la infección.
3. Sí ha detectado un virus, salga de *Windows*, apague la máquina y arranque desde el *diskette* flexible. Entonces ejecute *Scan* para *MS-DOS*, como se describe en la sección correspondiente a este proceso: **"SI DETECTA ALGUN VIRUS"**, (punto **6.3.2.**, de este mismo capítulo).

(17) Manual de Usuario, de *McAfee*

## 6.5. METODOLOGIA DEL SISTEMA DE ANTIVIRUS MCAFEE

- CARACTERISTICAS DE LAS VACUNAS
- RASTREO DE FIRMAS
- CHEQUEO DE INTEGRIDAD
- MONITOREO
- ANALISIS HEURISTICO
- OTROS METODOS

### 6.5.1. CARACTERISTICAS DE LAS VACUNAS

Una vacuna es un programa que trata de evitar los virus, se pueden dividir en:

- Preventivas (antes del virus)

  Antes de que un programa sea infectado por un virus

- Correctivos (después del virus)

  Después de que un programa es infectado por un virus

### 6.5.2. RASTREO DE FIRMAS

*La mayoría de los programas Antivirus funcionan* detectando "Firmas"; revisan o escanean los programas para localizar una secuencia de instrucciones que son únicas para ese virus. Es decir: que lo identifican.

### 6.5.3. CHEQUEO DE INTEGRIDAD

Otro método, es el de detección de cambios a programas por medio de algún cálculo como el *CRC* (*cyclic redundancy check*), chequeo de redundancia cíclica. Se toman las instrucciones de un programa como si fuesen datos y se hace un cálculo, se graban en un archivo los resultados y posteriormente se revisa si un programa fue alterado (probablemente por un virus) recalculando y comparando contra el *CRC*.

### 6.5.4. MONITOREO

- Otros lo que hacen es interceptar o bloquear instrucciones sospechosas o riesgosas, tales como cuando un programa pide cargarse en memoria y permanecer residente.
- Grabar en disco directamente (sin intermedio del sistema operativo), es alterar el área de arranque (*Boot*), o modificar un archivo de programa (y no de datos).
- Funciona como un *TSR (*residente en memoria), que supervisa continuamente. Cuando se ejecuta un programa, entonces intercepta los llamados a funciones sospechosas y cuando la instrucción se va a llevar a cabo, avisa para que el usuario decida si detener el programa o dejarlo continuar.
- Verifica a un sólo programa: el que se está ejecutando y avisa cuando está a punto de suceder algo raro.

### 6.5.5. ANALISIS HEURISTICO

- Un método más, es el de un análisis heurístico del código de un programa para detectar instrucciones sospechosas.
- Analiza cada programa sospechoso sin ejecutar las instrucciones, lo que hace es desensamblar o "destraducir" el código de máquina para deducir que haría el programa si se ejecutara, avisando que el programa tiene instrucciones para hacer algo que es raro en un programa normal, pero que es común en un virus.
- Puede revisar varios o todos los programas de un disco y avisa qué puede suceder algo raro cuando se ejecute el programa.

### 6.5.6. OTROS METODOS

- Otros programas controlan la ejecución de sólo programas autorizados; Pueden ser programas residentes en memoria o programas de menú para ejecutar solamente los programas y aplicaciones configurados.
- Otra ventaja es que suelen tener contraseñas (*passwords*) de acceso con lo que sólo el personal autorizado podrá hacer uso de la computadora.

# CAPITULO 7

# APLICACIONES PARA RECUPERAR INFORMACION Y CORREGIR LA SUPERFICIE DE UN DISCO DURO

## 7.1 RECONSTRUCCION DEL ACCESO DE ARRANQUE DE UN ORDENADOR CON SISTEMA OPERATIVO MS-DOS Y WINDOWS 95

La mayor parte de veces cuando una PC no arranca, se debe a que el usuario inexperto, eliminó los archivos de sistema que arrancan a la PC. El mensaje que recibiremos será el siguiente:

**No system boot**

**Boot failure**

**Insert disk of system**

Algunos virus llegan a eliminar también a estos archivos de sistema, como el **MONKEY.b** y el **ISRAELI**, y otros más.

Para corregir este problema seguiremos la siguiente dinámica:

1. Formatea un *diskette* en otra PC, pero antes debemos asegurarnos que ésta, no esté contaminada por virus.

2. Copiamos los archivos de sistema de la máquina limpia al *diskette* y tecleamos lo siguiente desde el indicador de sistema:

   **C:\>SYS A:** mas oprima *Enter*

   Aparecerá: **"C: \>Sistema transferido".**

3. Una vez cargado los archivos de sistema en el *diskette*, entonces lo introducimos en la máquina que no arranca y la encendemos con el *diskette* dentro.

   Aparecerá el prompt: **A:\>**

   Entonces; desde aquí tecleamos lo siguiente, para la transferencia de archivos:

   **A:\>SYS C:** mas oprima *Enter*

   Aparecerá: **"A:\>Sistema transferido".**

4. Esto indica que los archivos del sistema de arranque, se han transferido a la PC. Si sospechamos de la existencia de virus, insertamos el *diskette* Antivirus y rastreamos la máquina para limpiarla.

5. Una vez concluida la operación, retiramos el *diskette* y reiniciamos el equipo.

6. Sin no funciona esto, debemos verificar que exista el archivo COMMAND.COM o buscar en el directorio raíz, el último archivo AUTOEXEC.* o CONFIG.* debemos elegir el de fecha reciente.

7. Después creamos un nuevo directorio para respaldar los archivos **AUTOEXEC.BAT** y **CONFIG.SYS.**

**C:\>MD RESPALDO** más *Enter*

**C:\COPY *.* RESPALDO** más *Enter*

8. Y se copian todos los archivos del directorio raíz a este directorio, ésta acción nos permitirá rescatar también los archivos de sistema en un futuro evento.

### 7.1.1 PROCEDIMIENTOS DE RECONSTRUCCION DEL ARRANQUE DE SISTEMA MS-DOS

Si algunos sistemas no funcionan, y estos trabajan bajo la plataforma de *MS-DOS*, debemos hacer lo siguiente:

1. Como ya están respaldados los archivos principales: AUTOEXEC.BAT y CONFIG.SYS, entonces se proceden a eliminarlos y después del respaldo que tenemos, escogemos los archivos más recientes; los copiamos al directorio raíz, y luego los renombramos. A continuación se describe como se debe hacer el procedimiento:

   **C:\>DEL AUTOEXEC.BAT** más *Enter*

   Desea borrar el archivo (S/N) poner S más *Enter*

   **C:\>DEL CONFIG.SYS** más *Enter*

   Desea borrar el archivo (S/N) poner S más *Enter*

2. Después nos cambiamos al subdirectorio de RESPALDO

   **C:\>CD RESPALDO** más *Enter*

   **C:\>RESPALDO>** más *Enter*

3. Copiamos los archivos **AUTOEXEC.?** y **CONGIG.?** De fecha más reciente, supongamos que se trata de los archivos: AUTOEXEC.123 y CONFIG.123, procedemos a copiar y luego renombrar como sigue:

   **C:\RESPALDO>COPY AUTOEXEC.123 C:** más *Enter*

   **C:\RESPALDO>COPY CONFIG.SYS.123 C:** más *Enter*

4. Como ya están copiados los archivos con extensión (*.123), seguimos con el siguiente paso:

   **C:\RESPALDO>CD..** más *Enter*

   Aparecerá entonces: C:\>

5. Quedamos en el indicador de sistema, desde aquí empezamos a renombrar:

   **C:\>REN AUTOEXEC.123 AUTOEXEC.BAT** más *Enter*

   **C:\>REN CONFIG.123 CONFIG.SYS** más *Enter*

6. Posteriormente tecleamos "DIR", en el símbolo de sistema para verificar que en realidad los citados archivos aparezcan correctamente en este directorio raíz:

   **C:\>DIR** más *Enter*

7. Una vez comprobada su existencia, procedemos a apagar o reiniciar la PC. Por lo tanto suponemos que se han resuelto los problemas, si no, las causas se deben a que el usuario inexperto, eliminó archivos o sistemas, entonces el sistema que no funciona, está incompleto y requiere de su reinstalación.

   **Nota**: Este procedimiento es aplicable para arrancar las PC's con Sistemas Operativos *MS-DOS*, *Windows* 3x, NO *Windows* 95. Si estos procedimientos no funcionan correctamente, entonces se recomienda la reinstalación del Sistema Operativo en último de los casos.

### 7.1.2. PROCEDIMIENTOS DE RECONSTRUCCION DEL ARRANQUE DE SISTEMAS: WINDOWS 3.0, 3.1, 3.11Y WINDOWS 95

Así como el Sistema Operativo *MS-DOS* que posee tres archivos muy importantes para el inicio de las aplicaciones y comandos del sistema; como son el

COMMAND.COM, AUTOEXEC.BAT y el CONFIG.SYS, y que el resguardo de ellos es de vital importancia, para casos de recuperación del funcionamiento del sistema. También *Windows* 3x Windows 95(**), tienen sus propios archivos de sistema; el WIN.COM, WIN.INI y SYSTEM.INI. El manejo de estos es muy delicado, ya que si no se tiene experiencia en lo que se hace, puede ser que el sistema de *Windows* ya no funcione correctamente, y se tenga que volver a la instalación del sistema.

- Si *Windows* no se inicia correctamente, por las siguientes causas como:
    1. Se queda bloqueado en el tapiz
    2. Inicia pero se sale al símbolo del sistema C:\>
    3. No ejecutan algunas aplicaciones
    4. Aparece entrecortada la imagen o los iconos encimados
- Estas causas pueden ser, a que el usuario inexperto, eliminó archivos que están vinculados con la plataforma del ambiente operativo *Windows* 3x o 95.
- Para los puntos anteriores del *1* al *3*, se deberán seguir las siguientes instrucciones, trabajando desde el indicador de sistema: **C:>**:

1. Dentro del directorio de *WINDOWS*, creamos un nuevo subdirectorio:

   **C:\WINDOWS\>MD RESPALDO** más *Enter*

2. Después, copiamos todos los archivos con la extensión (*.INI) del directorio de *Windows* al subdirectorio RESPALDO:

   **C:\WINDOWS>COPY *.INI RESPALDO** más *Enter*

3. Como ya están respaldados los archivos: *.INI de Windows en el subdirectorio de RESPALDO, entonces se procede a eliminar los archivos: WIN.INI y SYSTEM.INI, del siguiente modo:

((**) Tanto Windows 3x como Windows 95, ambos tienen los mismos archivos de arranque (*WIN.INI, SYSTEM.INI* Y WIN.COM

4.

| | |
|---|---|
| **C:\WINDOWS>DEL WIN.INI** | más *Enter* |
| Desea borrar el archivo (S/N) poner: S | más *Enter* |
| **C:\WINDOWS>DEL SYSTEM.INI** | más *Enter* |
| Desea borrar el archivo (S/N) *poner*: S | más *Enter* |

4. Después nos cambiamos al subdirectorio de RESPALDO

| | |
|---|---|
| **C:\WINDOWS>CD RESPALDO** | más *Enter* |
| **C:\WINDOWS\RESPALDO>** | más *Enter* |

5. Y copiamos los archivos WIN.? y SYSTEM.?, (el de fecha más reciente). Supongamos que se trata de los archivos: WIN.XPS y SYSTEM.XPS, procedemos a copiar y luego renombrar como sigue:

**C:*WINDOWS*\RESPALDO>COPY WIN.XPS C:*WINDOWS*** más *Enter*
**C:\ *WINDOWS*\RESPALDO>COPY SYSTEM.XPS C:*WINDOWS*** más *Enter*

6. Como ya están copiados los archivos con extensión (*.XPS) a *Windows*, seguimos con el siguiente paso:

| | |
|---|---|
| **C:\WINDOWS\RESPALDO>CD..** | más *Enter* |
| **C:*WINDOWS*>** | |

7. Y quedamos en el indicador de sistema de *Windows*, y desde aquí empezamos a renombrar:

| | |
|---|---|
| **C:\WINDOWS>REN WIN.XPS WIN.INI** | más *Enter* |
| **C:\WINDOWS>REN SYSTEM.XPS SYSTEM.INI** | más *Enter* |

8. Posteriormente tecleamos "DIR" en el simbolo de sistema para verificar que en *realidad los citados* archivos aparezcan correctamente en este directorio raíz:

**C:\WINDOWS>DIR *WIN.INI** más *Enter*

**C:\WINDOWS>DIR *SYSTEM.INI** más *Enter*

9. Una vez comprobada su existencia, procedemos a apagar o reiniciar la PC. Por lo tanto suponemos que se han resuelto los problemas, si no, las causas se deben a que el usuario inexperto, eliminó archivos o sistemas, entonces el sistema que no funciona está incompleto y requiere de su reinstalación.

> **Nota**: Este procedimiento es aplicable para *Windows* 95. Si estos procedimientos no funcionan correctamente, entonces se recomienda la reinstalación del Sistema Operativo en último de los casos.

Para el punto 4, donde se menciona: "Aparece entrecortado el tapiz del logotipo de *Windows*", o los iconos encimados, se deberá seguir las siguientes instrucciones:

1. Copie el archivo WIN.COM de otra PC, al directorio por medio de *diskette*:

**C:\WINDOWS**

El problema es sencillo de resolver, no se alarme pues no se trata de ningún virus, solo que aveces el sistema de *Windows*, no cierra correctamente y el archivo WIN.COM llega a fragmentarse, también se puede corregir esto utilizando la utilería de *MS-DOS* (SCANDISK) o la utilería (NDD) de Norton Utilities. Ambos verifican la superficie del disco duro y corrigen los problemas de defragmentación de archivos.

### 7.1.3. PROCEDIMIENTO DE RECONSTRUCCION DEL ARRANQUE DEL SISTEMA *WINDOWS* 95, ( PROBLEMA CON "VFAT")

*Windows* 95, es un Sistema Operativo más avanzado con respecto al Sistema Operativo *MS-DOS*, ya que nos permite auto detectar una gran variedad de problemas de Soporte Técnico, en su programa de ayuda.

### 7.1.4. CREE UN DISCO DE INICIO EN WINDOWS 95

Si la PC tiene instalado el sistema de Windows 95, fácilmente la creación de un *disco de inicio*, lo podemos hacer con los procedimientos ya aprendidos en los pasados capítulos, si nos ubicamos en el símbolo de sistema de MS-DOS, así:

**C:\>SYS A:** más *Enter*

**C:\>Sistema transferido**

De igual forma, ya transferidos los archivos del sistema de *Windows* 95 al *diskette*, se procede a introducirlo en la PC que no arranca y transferimos estos archivos, como iniciamos la máquina con el *diskette* flexible, aparecerá el prompt:

**A:\>**

Desde aquí transmitimos los archivos de sistema a otra PC, del siguiente modo:

**A:\>SYS C:** más *Enter*

**A:\>Sistema transferido**

OK, procedemos en apagar la PC y volver a iniciarla, seguramente debe iniciar bien, si no, se debe a que existe otro problema y será necesario copiar el archivo MSDOS.SYS de otra PC, si el problema no se resuelve satisfactoriamente, entonces se procederá a la reinstalación del sistema. Ahora, si logramos entrar en modo: "A PRUEBA DE FALLOS", y accedemos a las propiedades de mi PC, en *Windows* 95, en el icono de AGREGAR O QUITAR PROGRAMAS; tenemos la comodidad de hacer un disco de sistema con sólo introducir un *diskette* y seguir las fáciles instrucciones de la siguiente manera:

1. Haga *clic* en: INICIO + CONFIGURACION + PANEL DE CONTROL, para abrir el cuadro de diálogo "AGREGAR O QUITAR PROGRAMAS".
2. Siga las instrucciones de su pantalla.

   **Nota:** Para crear un disco de inicio, necesitará un disco con al menos 1.2 MB de capacidad.
3. Puede utilizar el disco de inicio para iniciar otra PC, si tiene dificultades al iniciar *Windows 95*, cuando inserte el disco de inicio, la PC se iniciará desde el diskette.

4. Observará todos los archivos y extensiones de nombre de archivo.

## 7.2. RECUPERACION DE ARCHIVOSEN WINDOWS 95

A continuación se describe el procedimiento para la recuperación de archivos eliminados en *Windows 95*:

1. En el icono: "Mi PC" o en el "Explorador de *Windows*", abra la carpeta que desee examinar.
2. En el menú "Ver", haga clic en "Opciones".
3. Haga clic en la ficha "Ver" y a continuación en "Mostrar todos los archivos".
4. Si desea ver todas las extensiones de nombres de archivo, asegúrese de que la casilla de verificación "Ocultar las extensiones de archivo de *MS-DOS*" para los tipos de archivo, no esté activada.
5. Crear de nuevo el nombre de las carpetas, de donde se eliminaron los archivos.
6. Regrese a la pantalla de inicio y haga doble clic en el icono "Papelera de reciclaje".
7. Haga clic en el archivo o en el acceso directo que desee recuperar.
8. Para recuperar varios elementos, mantenga presionada la tecla CTRL mientras hace clic en cada uno de ellos.
9. En el menú "Archivo", haga clic en "Restaurar".

   **Nota.**- Si elimina una carpeta, sólo los archivos incluidos en esa carpeta aparecerán en la "Papelera de Reciclaje". Si restaura un archivo que se encontraba ubicado en una carpeta eliminada, *Windows* volverá a crear la carpeta y después, restaurará el archivo en ella.

10. *Windows* almacena los archivos eliminados en la "Papelera" de reciclaje, situada en el escritorio, podrá utilizarla para recuperar archivos eliminados por error, o vaciarla para crear más espacio en disco. Si no encuentra la "Papelera de reciclaje", haga clic en un área vacía de la barra de tareas con el botón secundario del MOUSE (ratón) y a continuación, haga rpã- ãÿˆMi nimizar todas las ventanas".

- Utilice en Windows 95 "Backup", para hacer copias de seguridad de los archivos.
- Puede utilizar el "Backup" para hacer copias de seguridad de archivos en su disco duro. Puede hacer copias de seguridad en discos, en una unidad de cinta o en otro equipo de su red. Las copias de seguridad pueden utilizarse para restaurar los archivos originales, cuando éstos se dañen o se pierdan.
- Para iniciar Backup, haga clic aquí
- Para obtener más información acerca de cómo utilizar *Backup*, haga clic en el menú "Ayuda de *Backup*".

## 7.3. PROCESO DE RECUPERACIÓN DE ARCHIVOS QUE FUERON VACIADOS DE LA "PAPELERA DE RECICLAJE" EN *WINDOWS 95*:

### 7.3.1. UTILICE EL ARCHIVO UNDELETE.EXE DE MS-DOS

1. Para lograr la recuperación de archivos eliminados en la "Papelera de Reciclaje" de Windows 95, se requiere obtener el archivo: **UNDELETE.EXE** del Sistema Operativo (MS-DOS Vers. 6.22) en *diskette*.
2. Iniciar la PC que tiene *Windows 95* en la modalidad del símbolo de sistema: **C:\>**
3. Copiar ahora del diskette, el archivo UNDELETE.EXE al directorio de donde fueron eliminados los archivos que desea recuperar.
4. Una vez copiado, se procede a recuperar tecleando en el indicador así:

**C:\>UNDELETE** más la tecla Enter

### 7.3.2. UTILICE EL ARCHIVO UNDELETE.EXE DE MS-DOS

Se requiere tener, el archivo **UNERASE.EXE,** del sistema de soporte técnico de NORTON UTILITIES, en un *diskette*; siga los siguientes pasos:

1. Inicie la PC que tiene *Windows 95*, en la modalidad del símbolo de sistema: C:\>

2. Copiar ahora del diskette que contiene la información necesaria, los archivos UNERASE.* al subdirectorio C:\>NORTON, si no existe, entonces hay que crearlo.

3. Una vez copiados, se procede a recuperar tecleando en el indicador así:

   **C:\>NORTON\UNERASE** más la tecla Enter

4. Aparecerá una pantalla, la cual al explorarla, nos dará las aplicaciones para proceder a recuperar los archivos del subdirectorio que fueron eliminados.

> **Nota**: En los equipos de cómputo que tengan instaladas las versiones de Norton Utilities 2.0 y 3.0, en *Windows 95*, no tienen ningún problema para recuperar información que fue eliminada, de la "Papelera de Reciclaje".

## 7.4. VERIFIQUE ERRORES DE DISCO AL INICIAR SU PC CON WINDOWS 95

1. En la pantalla inicial de *Windows* 95, haga clic en: INICIO, elija: "Programas" y luego en "Herramientas del Sistema" seleccione: "Scandisk". Para verificar los errores de la superficie del disco duro, siga los pasos de la pantalla.

Es importante que Verifique todas las unidades de disco duro y particiones de los mismos.

> **Nota**.- Si desea especificar cómo debe reparar Scandisk cualquier error que detecte, asegúrese de que la casilla de verificación "Reparar errores automáticamente" esté activada.

- Para obtener Ayuda acerca de un elemento del cuadro de diálogo "Opciones avanzadas de Scandisk", haga clic en la parte superior del cuadro de diálogo y, a continuación, en el elemento:

1. Haga clic en el botón iniciar Scandisk
2. Haga clic en la unidad que desee verificar

3. Haga clic en "Completa"

- Si desea cambiar la configuración que Scandisk utiliza al verificar la superficie del disco, haga clic en "Opciones".

- Si desea cambiar la configuración que Scandisk utiliza al verificar archivos y carpetas, haga clic en "Opciones avanzadas".

> **Nota**.- Si desea especificar cómo debe reparar Scandisk cualquier error que detecte, asegúrese de que la casilla de verificación "Reparar errores automáticamente" esté activada.

# CAPITULO 8

## SISTEMA AUTOMATICO PARA ELIMINAR VIRUS Y UN MACROVIRUS

El siguiente procedimiento, nos mostrará como crear un pequeño sistema en un *diskette* flexible, que automáticamente podrá limpiar virus de una PC.

### 8.1. GENERE UN SISTEMA DE ERRADICACION DE VIRUS EN UN DISCO FLEXSIBLE

Recopile los archivos de sistema:

1. Primero debe copiar los archivos del sistema de arranque de una PC, a un *diskette* flexible. Es conveniente copiar los archivos de un sistema actualizado, como Windows 95, ya que estos nos permitirán trabajar con sistemas operativos antiguos.
2. El procedimiento para copiar los archivos de sistema a un *diskette* flexible, ya fue comentado en otros capítulos anteriores.

**Nota**: Este procedimiento sólo es valido en las versiones de Sistemas Operativos, que no estén formateados sus discos duros a FAT32.

3. La estructura de este disco, es un poco similar al que compone el disco Magic Bullet[32] de DR. Solomon's. Después de que se han cargado los archivos del sistema de arranque, al diskette, se procede entonces a cargar los archivos que ejecutan el sistema automático, el cual llamaremos: "LIMPIA.BAT". Este sistema servirá para vacunar a la PC, los archivos serán ejecutados por ficheros como: el AUTOEXEC.BAT y CONFIG.SYS.
4. Copie los siguientes archivos del sistema de Antivirus Dr. Solomon's, al *diskette* flexible; los cuales están cargados en el directorio TOOLKIT, del disco duro:

   **C:>TOOLKIT>COPY CLEANBOO.EXE A:** más *Enter*
   **C:>TOOLKIT>COPY CLEANPAR.EXE A:** más *Enter*
   **C:>TOOLKIT>COPY FV86.EXE A:** más *Enter*
   **C:>TOOLKIT>COPY FINDVIRU.EXE A:** más *Enter*
   **C:>TOOLKIT>COPY EXTRA.DRV A:** más *Enter*
   **C:>TOOLKIT>COPY FINDVIRU.DRV A:** más *Enter*
   **C:>TOOLKIT>COPY LICENCE.DRV A:** más *Enter*
   **C:>TOOLKIT>COPY MESSAGES.DRV A:** más *Enter*

5. El procedimiento se debe hacer sobre la *plataforma de MS-DOS* y forzosamente necesita ubicarse, en el indicador de sistema, creando los siguientes archivos:

   **A:\>EDIT AUTOEXEC.BAT** más *Enter*
   **A:\>EDIT CONFIG.SYS** más *Enter*
   **A:\>EDIT LIMPIA.BAT** más *Enter*

6. Dentro de estos tres ficheros se agregarán las instrucciones, que se ejecutarán para la limpieza automática. Por ejemplo dentro del fichero **AUTOEXEC.BAT**, se agregarán las siguientes instrucciones:

   **@ECHO OFF**
   **C:\DOS\SMARTDRV /X /U**

(32) MAGIC BULLET (ver seccion 3.4.7.)

**PROMPT $p$g**
**PATH C:\DOS;C:\WINDOWS;C:\WINDOWS\COMMAND;**
**KEYB SP,,C:\DOS\KEYBOARD.SYS**
**LIMPIA**
**CD..**

7. En el fichero **CONFIG.SYS**, se agregarán las siguientes instrucciones:

**DEVICE=C:\DOS\HIMEM.SYS**
**DEVICE=C:\DOS\EMM386.EXE NOEMS HIGHSCAN**
**DOS=UMB**
**LASTDRIVE=Z**
**FCBS=4,0**
**DOS=HIGH**
**COUNTRY=003,850,C:\DOS\COUNTRY.SYS**

8. Y por *último* en el *fichero* LIMPIA.BAT, se agregarán las siguientes *instrucciones*:

**CD TOOLKIT**
**FINDVIRU C: /DOALLFILES /REPAIR**
**CD..**

## 8.2 MODO DE EMPLEO DEL DISCO ANTIVIRUS "LIMPIA"

- Se debe capacitar a los usuarios, para lograr una erradicación exitosa: pueden existir problemas si no se tienen precauciones con el virus DIR.BYWAY, como se explica en el siguiente punto 3.2.1.
- El *diskette* de sistema Antivirus, llamado: "LIMIPA", es muy práctico para usuarios INEXPERTOS; con solo insertarlo en la PC, y al iniciarla, el sistema que se incluyó en el disco flexible, realizará todos los pasos y automáticamente detectará los virus existentes, eliminándolos.

### 8.2.1. RECOMENDACIONES ANTES DE USAR EL DISCO "LIMPIA"

La recomendación más importante para los usuarios, es que primero deberán verificar que NO exista el virus **DIR.BYWAY**, para ello deberán identificarlo de la siguiente manera:

1. Encienda normalmente la PC y ubíquese en el indicador de sistema: C:\>, teclee lo siguiente:

**C:\DIR *.*/AHS** y oprima *Enter*

2. Si aparece un archivo **CHKLST .MS** y mide 2045 bytes
3. Entonces NO utilice el *diskette* de limpieza automática llamdo: "LIMPIA". Lo que deberá hacer entonces, es limpiar primero este virus con la utilería "**FBW2"** de Dr. Solomon's, así:

**A:\FBW2 C:** y oprima Enter

4. Posteriormente podrá usar dicho *diskette* automático, cuando haya eliminado e este virus.
5. Si no apareció el archivo **CHKLIST .MS**, entonces proceda sin ninguna preocupación.
6. Solo apague su PC e introduzca el *diskette* de limpieza automática, y deje que el sistema instalado realice todo el proceso.
7. Con toda seguridad su PC quedará limpia de virus. Si no es así el sistema le indicara el procedimiento a seguir.

## 8.3. MACROVIRUS

### 8.3.1 ANTECEDENTES DE LOS MACROVIRUS[1]

- Los Macrovirus, son programas de los más recientemente desarrollados, y a los que nos enfrentamos en la ya eterna lucha, en contra de los virus. El primer Macrovirus fue encontrado en el año de 1995, rápidamente llamó la atención de la prensa y de las personas que escriben sobre virus. Su introducción al mundo de los virus, causó una gran conmoción porque rompieron algunas de las <reglas establecidas>.
- Son los primeros virus multi-plataforma; que no solamente infectan sistemas de PC, sino también a sistemas de *Macintosh*.
- La idea de los Macrovirus no es nueva, de hecho, esta posibilidad había sido considerada por la comunidad Antivirus desde finales de los 80's. Durante la Conferencia en Boston de Virus *Bulletin* en 1995. El profesor *Harold Highland,* reveló que él había desarrollado años antes el primer Macrovirus, a nivel

(1) *PC Anti-Virus Book*
Dr. Alan Solomon & Tin Kay

mundial, utilizando una versión antigua de Lotus 1-2-3. *Highland* creó dicho Macrovirus bajo condiciones controladas y seguras, destruyendo todas las copias una vez que probó que era posible.

- Los autores de virus no le dieron importancia, ya que consideraban más interesante, el hecho de desarrollar los tradicionales virus de sector de arranque y archivos bajo *DOS*. Es muy probable que hayan subestimando las ventajas de los Macrovirus sobre los virus tradicionales.

**El Macrovirus Concept**

**"Primer Macrovirus activado y encontrado en el mundo", en 1995.**

- Los Macrovirus, son los primeros virus que infectan documentos, en lugar de archivos ejecutables (Macrovirus que infectan documentos de *Microsoft Word*). En enero de 1996 apareció el primer Macrovirus para *Ami Pro* de *Lotus*, al cual se le conoce como **GREEN STRIPE**. Esto, nos hace pensar que existe un gran riesgo en otros procesadores o inclusive en otras aplicaciones.

- Los archivos de datos se comparten mucho más que los ejecutables, debido a la información que contienen. Los Macrovirus tienen la capacidad de esparcirse más rápido que los virus tradicionales por el simple hecho de que infectan documentos hechos con *Microsoft Word*. El simple hecho de leer un documento infectado, ocasiona que todo el sistema de instalación de *Word* se infecte. Existen algunos sistemas de e-mail (correo electrónico) que automáticamente abren documentos anexados a un correo con *Microsoft Word*, lo que significa una rápida infección de muchos sistemas.
- En el verano de 1995, *Microsoft Word* distribuyó un CD–ROM llamado *Microsoft Windows 95 Software Compatibility Test*, a miles de compañías OEM (*Original Equipment Manufacturer*). El objetivo de este CD–ROM, era ayudar a dichas compañías a probar que su *hardware* y *software* sean compatibles con

*Windows 95*, pronto a liberarse. Desdichadamente el CD contenía en un documento llamado OEMLTR.DOC el Macrovirus **Concept**, "Primer Macrovirus encontrado en el mundo".

"Las compañías comenzaron a reportar comportamientos extraños en las computadoras de su organización "

- El **Concept**, se volvió famoso, aún más cuando otra compañía distribuyó más ejemplares del Macrovirus, al enviar 5,500 copias de un CD-ROM llamado: *Snap-on Tools for Windows NT*. Al mismo tiempo *Microsoft* de Inglaterra, distribuyó el **Concept**, en su CD-ROM *Microsoft Office 95* and *Windows 95 Bussiness Guide*. *Microsoft* de Inglaterra, se dió cuenta del problema y lo corrigió reemplazando el CD infectado por uno limpio.

- Actualmente, no solo los documentos creados con *Microsoft Word* corren el peligro de infectarse, ya que en fechas recientes se desarrolló, un Macrovirus para el software de Excel y otro para Ami Pro.

## 8.4. EXTRA DRIVER

¿Que es un EXTRA DRIVER?

Ocasionalmente, Dr. Solomon's distribuye un "*driver* extra", que contiene información sobre nuevos virus que no fueron incluidos en el archivo driver estándar, a fin de aumentar el número de virus que se pueden detectar. Para habilitarlo hay que especificarlo en el cuadro de diálogo "Configurar Protección". Se ha de especificar el *path* completo para el archivo del "*driver* extra". Es aconsejable utilizar esta opción sólo con la asistencia de Dr. Solomon's. El archivo "driver extra" se denomina EXTRA.DRV y se halla en el directorio *HomeGuard*, no hace falta especificarlo ya que se hará de forma automática.

### 8.4.1. FUNCIONAMIENTO DEL EXTRADRIVER PARA ELIMINAR MACROVIRUS

Cuando usted ejecuta *FindVirus* de Dr. Solomon's, esta utilería busca cargar un archivo llamado: FINDVIRU.DkV; este archivo se le conoce como "*driver*", y es una base de datos que contiene información acerca de los virus por *FindVirus*.

De tiempo en tiempo, aparece algún nuevo virus en el campo y el laboratorio de Antivirus, envía una "actualización de campo" para combatirlo. La información adicional deberá lograr que *FindVirus* sea capaz de detectarlo y si es posible, removerlo. Esto se hace mediante un archivo llamado EXTRA DRIVER; que se proporciona en la forma de un archivo de texto, y que contiene una serie de números que terminan con el nombre asignado al nuevo virus.

Un EXTRA DRIVER[16], puede ser obtenido como archivo por medio de los servicios en línea de soporte técnico de Dr. Solomon's, o puede solicitarlo por teléfono al 254-39-48 y lo recibirá por FAX, pero tendrá que re-capturarlo en un archivo de texto.

### 8.4.2. USO DEL EXTRA DRIVER

1. Renombre el archivo que reciba, para nombrarlo como: EXTRA.DRV. Si lo recibió por Fax, use un editor de texto simple (como EDIT del *MS-DOS*, por ejemplo), para escribir los números y el nombre del virus, sálvelo como:

   **EXTRA.DRV**

2. Si FindVirus, encuentra un archivo llamado EXTRA.DRV, en su mismo directorio (normalmente **C:\>TOOLKIT**), agregará la detección del virus en forma automática a los que ya conocia por su archivo FINDVIRUS.DRV.
3. Si sospecha que el nuevo virus ha infectado su disco duro:

(16) Manual de Usuario. de Dr. Solomon's

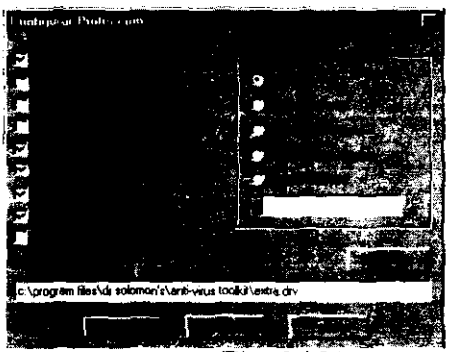
- Apague completamente su máquina (no oprima RESET ni use el método de CTRL-ALT-DEL, porque así el virus puede quedarse presente en la memoria).
- Copie el EXTRA DRIVER al directorio TOOLKIT del disco duro.
- Ejecute *FindVirus* desde su disco flexible original, protegido contra escritura, use el siguiente comando:

**FINDVIRU/LOCALEXTRA=C:\TOOLKIT\EXTRA.DRV**

- Si el *FindVirus* se ejecuta con el parámetro /EXTRA=, el archivo que contenga al EXTRA DRIVER no necesita llamarse EXTRA.DRV, ejemplo: si el EXTRA DRIVER se llama VIRUS.DRV; puede ser usado el comando:

**FINDVIRU/LOCAL/EXTRA=C:\TOOLKIT\VIRUS.DRV**

- Normalmente los nuevos Virus, serán agregados a la ingeniería de detección completa de *FindVirus,* en la siguiente versión de actualización. Al recibir su siguiente actualización de *Toolkit*, por favor elimine el archivo EXTRA.DRV.



(Fig.: 8.4.2.)

Esta imagen, muestra la configuración del Antivirus, y la ubicación del EXTRADRIVER, en Windows 95

Por el momento, *FindVirus* es capaz de manejar solamente un archivo EXTRA.DRV a la vez. Sin embargo, usted puede agregar varios extra *drivers* (para diferentes

virus), al mismo archivo. Agregue los números como se explico anteriormente, dejando un espacio entre cada driver.

### 8.4.3. USO DEL EXTRADRIVER EN WINGUARD

Procedimiento en *WinGuard.* (Vea imagen, Fig.: 8.4.2. "Configurar Protección")

1. Entre al menú de *WinGuard* (haga click sobre el guardia).

2. En la parte inferior izquierda, verá un cajón que dice EXTRADRIVER, escriba ahí el nombre y la trayectoria del archivo que usará como extra driver.

3. Si no recuerda su localización, oprima el botón llamado *Browser* (examinar).

4. Escriba la dirección donde se encuentra el EXTRADRIVER, se recomienda copiar el archivo EXTRADRIVER, en el subdirectorio de Toolkit, ejemplo:

**C:\TOOLKIT\EXTRA.DRV**

5. Habilite la opción de Autorepair de *WinGuard.*

6. Salga de *Windows* y reinicie su PC.

7. Al momento de volver abrir un archivo o documento infectado, WinGuard lo desinfectará automáticamente, pero le enviará antes un aviso.

## 8.5. NAVRHAR ¿UNA NUEVA GENERACION DE VIRUS?[22]

El 12 de diciembre de 1997, los desarrolladores de Antivirus se sorprendieron ante la aparición de un virus nuevo, llamado: **NAVRHAR. 12888;** el cual prácticamente utiliza las macros de documentos del sistema *Word* como transporte para su

(22) Boletín de Antivirus de Dr Solomon's (marzo de 1998)

infección; sin embargo, lo novedoso de este virus es que la infección en sí la realiza un programa llamado **RUNME.EXE**, incluido en el mismo documento.

El concepto es el siguiente: El usuario abre un documento de Word, éste contiene cierto código el cuál es guardado en el disco duro con el nombre **RUNME.EXE** y entonces el Macrovirus lo ejecuta de forma automática infectando así 20 VxDs (Virtual *Drivers* de *Windows* 95), los cuales son abiertos por *Windows*, cada vez que se arranca la computadora. Con esto, el virus se asegura que de ahí en adelante todo documento de Word creado o editado será infectado por **NAVRHAR**.

Este tipo de bicho es novedoso. Hasta la fecha hay dos virus que hacen algo semejante; el primero ya lo mencionamos y el segundo se llama **XF.Paix**, (Macrovirus de Excel), que se caracteriza principalmente por no utilizar: VBA (Visual Basic For Applications), es decir: el tipo de macros que se utilizan comúnmente en la creación de Macrovirus, para macros de Excel 4; este virus, crea el archivo XLSHEET.ELA, el cual es agregado a Excel para que sea leído de forma automática e integrado a todos los documentos utilizados.

El consultor tecnológico, Ing. Israel Juárez, senior de Dr. Solomon's, comenta:

*"Es probable que próximamente veamos con mayor frecuencia, virus que utilizan macros como "medio de transporte", para lograr su infección, además dentro de los documentos de Word, "Caballos de Troya" o programas que generan virus (droppers), sobre todo por que es más fácil crear un programa de esta índole y generar el código de infección en Word, lo cual es muy sencillo".*

Es importante mencionar la diferencia entre un Macrovirus y este nuevo tipo. Los Macrovirus son programa enteramente creados con *Visual Basic For Applications*. Todo su código de infección, activación y manifestación está incluido en el mismo

Macrovirus. El concepto de esta nueva generación de virus es similar: el código de infección, está programado en VBA, pero la diferencia es que el documento infectado contiene un archivo ejecutable o programa, el cual es colocado en el disco duro de la víctima y posteriormente ejecutado. Infecta o activa su manifestación.

Actualmente Dr. Solomon's limpia y protege contra los virus y Macrovirus mencionados, y protegerá a sus usuarios contra estos, y otro tipo de virus nuevos, conforme vayan surgiendo.

Si no cuenta con el diskette EXTRADRIVER, solicítelo a Dr. Solomon's *Software*, si por algún motivo no pudo actualizar su sistema de Antivirus.

**Nota**.- Para la erradicación de Macrovirus, los desarrolladores de Antivirus utilizan:

- Dr. Solomon's; utiliza un archivo llamado: EXTRADRIVER
- PC-CILLIN, utiliza el archivo: MACROTRAP
- Mcaffe, trae el archivo integrado.
- ThunderByte, también trae el archivo incluido.

# CAPITULO 9

# PROCEDIMIENTOS DE MANTENIMIENTO CORRECTIVO, ANTES DE INICIAR UNA INSTALACION DE SOFTWARE

## 9.1 HERRAMIENTAS DE SOFTWARE NECESARIAS PARA PROPORCIONAR MANTENIMIENTO CORRECTIVO A UNA PC

Para obtener buenos resultados en la instalación de un *software*, así como del Antivirus; uno de los dos primeros conceptos, es contar con las siguientes herramientas:

Un sistema verificador de superficie de disco duro, y un sistema desfragmentador de disco duro. Las utilerías que se requieren, se encuentran en el sistema de soporte técnico: **NORTON UTILITIES** y en el sistema operativo de **MS-DOS**, de la siguiente manera:

- Las utilerías de diagnostico, que corrigen y verifican errores de la superficie de un disco duro son: El "**NDD**" (Norton Disk Doctor) de Norton Utilities, o el "**SCANDISK**" de *MS-DOS*. Estas herramientas, son las más comunes e importantes empleadas para este proceso.

- Los sistemas defragmentadores de discos duros, que se recomienda usar; es el "**SPEED DISK**" de Norton Utilities o el "**DEFRAG**" de *MS-DOS*. Estas son las herramientas más comunes empleadas para el proceso de mantenimiento correctivo.

## 9.2. USO DEL "NDD" (Sistema de diagnostico de NORTON DISK DOCTOR)

**NDD**[23] (Comprobador de soporte de datos)

Si al intentar leer alguna vez un *diskette*, ha obtenido como única respuesta una serie de errores de lectura, todo hace indicar que se trata de un *diskette* defectuoso. Lo mismo puede suceder con un disco duro. Con el **NDD** (Disk Doctor de Norton), podrá explorar, corregir y recuperar los datos que contuviese.

### 9.2.1. CONFIGURE EL *TEST* DE SUPERFICIES:

Adapte el Norton Disk Doctor personalmente para ejecución frecuente del Test.

1. Arranque el Disk Doctor, desde el indicador de sistema:

   **C:\NORTON\NDD y oprima Enter**

2. Seleccione el conmutador Options.
3. Seleccione la configuración *SURFACE TEST*.
4. Seleccione el área que ha de comprobar Disk Doctor. En el subcuadro *TEST* se especifica la opción *DISK-TEST*, para comprobar todo el disco, o la opción *FILE-TEST* para comprobar un área determinada.
5. Salte con [Tab] a una de ambas opciones y pulse la [barra espaciadora].
6. Seleccione en la ventana *PASSES*, las veces que tenga que repetir el texto.
7. La opción "*Continuos*", está repitiendo el *TEST*, hasta que se cancele con oprimir la tecla: [Esc].
8. Si selecciona *PASSES*, introduzca en el campo de entrada, el número de veces que ha de ejecutarse el *TEST*. Salte con [Tab] a una de ambas opciones y pulse la [barra espaciadora].
9. En el subcuadro *TEST TYPE*, especifique cuándo y cómo ha de ejecutarse el *TEST* de superficies; si se arranca Disk Doctor, *DAILY* ejecuta un *TEST* rápido de disco. WEEKLY, arranca un proceso cuya duración es el doble que la del anterior.
10. *AUTO-WEEKLY* arranca cada viernes (Si se le da opción a Disk Doctor para hacerlo), un *TEST* básico; en caso contrario, ejecute el *TEST* normal.

(23) Data Becker Norton Utilities 6.0
Istok Kespret - ED. MARCOMBO

11. Salte, oprimiendo la tecla [Tab]. así. se cierra a una de las *tres opciones* y pulse la [barra espaciadora]. Por lo demás, él <<viernes>> se especifica por el calendario interno de la PC. con el comando *DATE* del *DOS* o con *Norton Control Center*. Podrá por lo demás. ratificar o modificar la fecha.
12. Dígale a Disk Doctor en el subcuadro *REPAIR SETTING*. la forma en que ha de proceder cuando surgiese algún error, y salte con oprimir la tecla [Tab], a alguna de las opciones y pulse la [Barra espaciadora].
13. Confirme con la opción: *ACCEPT*, que aparece en la misma pantalla.

## 9.3. SISTEMA DE DIAGNOSTICO, SPEEDISK (NORTON)

**SPEEDISK**[23] (Mas potencia y velocidad mediante organización de archivos):

SPEEDISK, puede acelerar el acceso a sus datos, compactando el área de almacenamiento libre y agrupando los archivos fragmentados en una área única. La lectura de tales datos puede producirse más rápidamente, ya que los archivos pueden leerse <<de un tirón>>. Se evita así la ejecución de complejos y lentos (por mecánicos) saltos del cabezal de lectura.

SPEEDISK, organiza los directorios de acuerdo con determinados criterios, y es capaz de desplazar los archivos y directorios de uso máas frecuente, a las regiones del disco duro más rápidamente accesibles. Los directorios se desplazan hasta el principio físico, es decir, hasta el borde real del disco duro. Así podrán realizarse accesos más rápidos a datos, ya que, por regla general, el acceso a un directorio pasa por encima del directorio raíz, que se encuentra siempre al principio del disco; si no desea especificar ninguna secuencia especial, se tomará la secuencia de la ruta *path* del sistema.

## 9.4. SISTEMA DE DIAGNOSTICO, CALIBRATE (NORTON)

CALIBRATE[23] (Optimización y ajuste de errores del disco duro mediante):

CALIBRATE, puede ayudar a su disco duro a conseguir un incremento insospechado de su velocidad. Este programa está en condiciones de evitar cualquier

(23) Data Becker Norton Utilities 6.0
Istok Kesprei - ED. MARCOMBO

pérdida de datos, mejorar las relaciones poco favorables entre PC y *disco duro:* El denominado factor *Interleave*[12], reformatea para ello al disco duro. Al mismo tiempo, CALIBRATE comprueba todos los *clusters* del disco duro, reconociendo asi de forma anticipada, cualquier problema que pueda aparecer, o las pérdidas de datos.

> **Nota.- Interleave**[12]:Intercalación de sectores, interfoliación de sectores. Manera en que se enumeran los sectores de un disco duro

### 9.4.1. ARRANQUE DE CALIBRATE

En su ejecución, CALIBRATE apenas requerirá de su intervención: como observador, sólo tendrá que acomodarse en su sillón e ir confirmando los sucesivos TEST. Si se arranca CALIBRATE con una opción /BATCH[13], ni eso tendría que hacer.

> **Nota.- BATCH**[13] = Prueba de corrección dentro de los sistemas de proceso de datos y que se aplican a los lotes de datos de entrada particularmente en la etapa de preparación de estos.

## 9.5. USO DEL SISTEMA DE DIAGNOSTICO SCANDISK[24] EN *MS-DOS*

El sistema de diagnostico de SCANDISK, lo podrá llamar desde el indicador de sistema de MS-DOS. Esta operación verificará la superficie del disco duro y diskettes, corregirá todos los errores de asignación que tengan.

- Para verificar discos, teclee para verificar el disco duro **C:\SCANDISK C:**
- Para verificar un diskette, teclee: **C:\SCANDISK A:**
- En los dos casos, siga las instrucciones en pantalla
- El SCANDISK, corregirá errores, NO corrige los daños fisicos que tengan los discos.

## 9.6. USO DEL SISTEMA SCANDISK[25] EN *WINDOWS 95*

Puede utilizar SCANDISK para comprobar si hay errores físicos y lógicos en el disco duro, SCANDISK puede reparar a continuación las áreas dañadas.

(24) SCANDISK, Tomado del Manual del Usuario de MS-DOS, Vers. 6.22
(25) SCANDISK, Tomado del Manual del Usuario de Windows 95

**Nota**.- También puede iniciar SCANDISK en *Windows 95, si hace click en* **Inicio**, selecciona **Programas + Accesorios + Herramientas del Sistema**, *y a continuación, hace click en* SCANDISK. Para obtener información acerca de cómo utilizar SCANDISK, haga click en "**Temas relacionados**".

## 9.7. SISTEMA DE DIAGNOSTICO DEFRAG[24], (DE *MS-DOS)*

Con el tiempo, a medida que los programas lean y escriban información en el disco duro. Esta información almacenada en el disco se podrá fragmentar. La fragmentación ocurre cuando un archivo se divide en fragmentos que se almacenan en posiciones diferentes del disco. La fragmentación no afectará a la información; sus archivos estarán todavía completos cuando se abran; sin embargo, la PC tendrá que invertir mucho más tiempo en leer y escribir archivos fragmentados que los que están sin fragmentar.

### 9.7.1. DEFRAGMENTE LOS ARCHIVOS DEL DISCO DURO

Antes de usar el defragmentador, elimine cualquier archivo innecesario de su disco duro ejecutando los procedimientos siguientes:

**"LIBERE ESPACIO EN EL DISCO".**

1. De preferencia inicie la PC, o salga de todos los programas que se estén ejecutando incluyendo *Microsoft Windows*. No ejecute defragmentar de *MS-DOS*, desde el símbolo de *MS-DOS* dentro de *Windows*.
2. Corrija cualquier unidad de asignación perdida en su disco duro, escribiendo lo siguiente a continuación del símbolo del sistema: **C:\>CHKDSK/F/V**
3. Si *MS-DOS* detecta unidades de asignación perdidas, presentará un mensaje de confirmación similar al siguiente:

**Se encontraron "n" unidades de asignación perdidas en tres cadenas. ¿Convertir las cadenas en archivos?**

(24) DEFRAG. Tomado del Manual del Usuario de MS-DOS. Vers. 6.22

4. *Presione* "S", *para guardar y ver los archivos* FILLE000.CHK que genera esta exploración de las unidades de *asignación perdidas.*
5. Deberá eliminar todos los archivos del disco duro con la siguiente extensión:

   TMP, BAK, MS, UMB, CHK Y _DD
6. Para obtener información sobre el comando CHKDSK, escriba HELP CHKDSK a continuación del símbolo del sistema: **C:\CHKDSK/HELP** y oprima Enter
7. *Inicie defragmentar de MS-DOS* escribiendo lo siguiente a continuación del símbolo del sistema: **C:\>DEFRAG/F** y oprima Enter
8. DEFRAG de *MS-DOS,* presenta una lista de las unidades de disco de su PC.
9. Presione las teclas flecha arriba o flecha a bajo para seleccionar la unidad que desee defragmentar y luego presione Enter. DEFRAG de *MS-DOS,* analizará los datos en esa unidad y recomendará una opción de defragmentación.
10. Para comenzar la *defragmentación,* elija "OPTIMIZAR" presionando entrar. Si desea cambiar las configuraciones de la *defragmentación o desea más* información sobre las configuraciones de la defragmentación actual antes de comenzar, elija "Configurar" presionando la tecla flecha derecha y luego entrar, se presentará el menú "Optimizar".

> **Nota.**- El *defragmentador de disco nos sirve* para aumentar la velocidad de acceso al disco duro. Puede utilizar el defragmentador de disco para volver a organizar los archivos y el espacio no utilizado en el disco duro; de forma que los programas se ejecuten más rápidamente.

## 9.8. SISTEMA DE DIAGNOSTICO DEFRAG[25] (DE *WINDOWS 95*)

Al igual que en el sistema operativo MS-DOS, su funcionamiento es muy similar. Favorece el procesamiento de la PC, acelerando la velocidad de apertura de los *archivos y sistemas.*

1. Para iniciar *DEFRAG, haga click en* **Inicio + Programas + Accesorios + Herramientas del Sistema y "Defragmentador de Disco"**
2. Haga click en la unidad que desee.

(25) SCANDISK. Tomado del Manual del Usuario de Windows 95

3. Haga click en **Aceptar**
4. Para modificar los valores del Defragmentador de disco, haga click en **Configuración**.
5. Mientras se está defragmentando el disco, puede utilizar el equipo para realizar otras tareas. Sin embargo, el equipo funcionará más despacio y tardará más en terminar en defragmentar el disco.
6. Para detener temporalmente el defragmentador de disco, de modo que pueda ejecutar otros programas con más rapidez, haga click en "**Pausa**".

Durante la defragmentación, el defragmentador de disco, debe reiniciarse cada vez que otros programas escriban en el disco; si el defragmentador de disco se reinicia demasiado a menudo, puede que prefiera cerrar otros programas mientras se está defragmentando el disco.

## 9.9. ARCHIVOS DE CONFIGURACION DE DR. SOLOMON'S[16]

Una CONFIGURACION: Es el estado determinado de todos los elementos que pueden modificar la interfaz de usuario y almacenarla en archivos, para que se puedan usar de nuevo rápidamente. Los archivos de configuración se encuentran en texto ASCII, y disponen de la extensión: "**.INI**". La configuración definida para la interfaz de usuario cuando comienza se almacena en el archivo TOOLKIT.INI, así:

1. Puede guardar la configuración actual en un archivo de configuración, y restaurar las configuraciones de un archivo de configuración, desde la misma interfaz de usuario.
2. Puede editar los archivos de configuración con un editor de texto; tenga en cuenta que:

- No debe incluir espacios.
- Cuando se incluyen los nombres de los archivos, se considera que éstos se encuentran en la carpeta estándar de TOOLKIT (C:\TOOLKIT por defecto), a menos que se proporcione un nombre de *PATH* completo.

(16) Manual del usuario de Dr. Solomon's

- Existen opciones que se pueden incluir en todas las secciones del archivo de configuración (Sección *FindVirus*, sección *FileRepair*, sección *ViVerify*).

## 9.10. OTROS DISGNOSTICOS Y FALLAS DE SISTEMA[26]

- Para comprobar la unidad "C" e iniciar y salir de SCANDISK automáticamente dentro de Windows 95 en el menú, teclee:

**C:\WINDOWS\SCANDSKW.EXE D: /N**

- Para comprobar todos los discos duros, pero evitar que SCANDISK corrija los errores que encuentre, escriba en el menú **Inicio + Ejecutar**:

**C:\WINDOWS\SCANDSKW.EXE /A /P**

- Para obtener información acerca de cómo agregar SCANDISK a la carpeta **Inicio** de Windows 95, haga click en: **Inicio + Buscar + Archivos o Carpetas + Ayuda + Temas de Ayuda**, y siga las instrucciones.
- Si desea especificar el modo en que SCANDISK reparará los errores que encuentre; desactive la casilla de verificación: **"Reparar Errores Automáticamente"**.
- Para obtener ayuda de los elementos de SCANDISK, haga click con el botón secundario del *mouse* en el elemento deseado y después click en: **¿Qué es esto?**

### 9.10.1. BLOQUEOS DE SOFTWARE DE BAJO NIVEL[26]

Los programas de bajo nivel son aquellos que funcionan directamente en *diskette*. Se denominan de esta forma debido a que funcionan por debajo del nivel del sistema operativo, que normalmente controla el acceso a los discos y obliga a mantener ciertas normas.

Entre los programas de bajo nivel, se incluyen:

- Editores del sector de disco
- Programas de memoria caché en disco
- Software de compresión de disco

(26) Peter Norton Solución a Problemas de PC
Peter Norotn & Robert Jourdain
ED. PRENTICE HALL

- Defragmentadores

Por lo general, estas aplicaciones son bastante seguras si se ejecutan una a una; sin embargo, pueden aparecer problemas si ejecuta dos o más herramientas de bajo nivel a la vez. Si dos o más herramientas intentan acceder al disco, pueden causar bloqueos potencialmente peligrosos. A causa de que estas herramientas son cada vez más comunes, este tipo de problema puede aparecer con más frecuencia.

SOLUCIÓN: Para evitar problemas con herramientas de bajo nivel:

- Realice siempre una copia de respaldo antes de utilizar cualquier utilidad de disco.
- No ejecute más de una utilidad a la vez.
- No utilice estas herramientas a la vez que utiliza *software* residente en memoria.

Lea siempre los manuales y todos los archivos README proporcionados con los productos. Si los fabricantes han incluido advertencias especiales, seguro que hay un motivo para ello.

### 9.10.2. COMO COMPROBAR LA MEMORIA[26]

Cuando la interfaz de usuario se inicia, se realiza de forma automática una búsqueda de virus en la memoria.

Si desea comprobar la memoria:

1 Seleccione "Comprobar Memoria" en el menú "Escanear" de la interfaz de usuario, en la ventana de *Winguard* de Dr. Solomon's

2 En el diálogo "Detectar virus en memoria", haga click en "Detectar".

### 9.10.3. COPIAS DE RESPALDO[26]

La mayor precaución que puede tomar contra cualquier tipo de pérdida de datos, es realizar una copia de respaldo del sistema de forma regular. Si no la realiza, se encuentra en peligro.

(26) Peter Norton Solución a Problemas de PC
Peter Norotn & Robert Jourdain
ED. PRENTICE HALL

Recuerde verificar las copias de respaldo con frecuencia y asegurarse de que puede recuperar datos con ellas. Verifique que dispone en *diskette* de copias limpias de todos los archivos ejecutables. Todos los *diskettes* de respaldo y los de *Boot* deben estar protegidos contra escritura.

### 9.10.4. DISKETTES Y OTROS MEDIOS[26]

El riesgo de una infección por virus mediante *diskettes* es especialmente alto, pero puede realizar una serie de simples pasos para aumentar la seguridad.

- Mantenga los *diskettes* protegidos contra escritura siempre que sea posible, para evitar que se copien los virus.
- Cuando apague la PC, no deje los *diskettes* en la unidad de *diskette*. Así evita intentar de forma accidental, arrancar desde un *diskette* infectado con un virus de sector *Boot*.
- Si inicia sin querer desde un *diskette* que no es de arranque, apague la PC y comience de nuevo, en vez de intentar arrancar desde la unidad: **C:**
- Cambie la configuración de CMOS de la PC, para que arranque desde la unidad **C:\>** en vez de la unidad **A:\>** (Esto no es siempre posible en unidades SCSI).
- Siempre que sea posible, utilice métodos alternativos para transferir archivos.
- Recuerde que los archivos en cinta pueden haberse infectado al realizar la copia de respaldo.

### 9.10.5. EMPAQUETADORES[26]

Los empaquetadores son programas, que de una forma u otra envuelven al programa original como medida de precaución o para comprimir archivos. Sin embargo, los empaquetadores pueden encubrir la existencia de un virus. Por precaución, cuando se realiza una exploración para identificar la existencia de virus en un disco duro, es conveniente descompactar los archivos compactados, ya que algunos sistemas de virus no los detectan; siendo peligroso si se trata de algún virus que el Antivirus no detecta. También existen algunos divisores de *software*, estos divisores como el

(26) Peter Norton Solución a Problemas de PC
Peter Norotn & Robert Jourdain
ED. PRENTICE HALL

PKZIP, CHOPPER y el BACKUP de *Windows*, que hacen divisiones de los archivos cuando sobrepasan el tamaño del *diskette*. Como el archivo esta dividido, tampoco los escaneadores de Antivirus pueden detectar si un virus se encuentra alojado en un archivo. Por lo que recomendamos se unifique o congregue correctamente el archivo para que sea revisado por un rastreador de Antivirus.

### 9.10.6. DETECCION DE POSIBLES FALLAS DEL HARDWARE[26]

Como utilizar, los solucionadores de problemas de *Windows 95*

Los solucionadores de problemas de *Windows 95*, pueden ayudarle a diagnosticar y resolver problemas técnicos de *Windows* en poco tiempo, para sacar el máximo partido de estos solucionadores de problemas, Siga estas instrucciones básicas:

1. Asegúrese de que puede ver la ventana de "**Ayuda**", que contiene el texto del solucionador de problemas mientras sigue sus instrucciones.
2. Para minimizar todas las ventanas abiertas en la barra de herramientas **Inicio rápido**, haga click en el botón "**Mostrar Escritorio**". "**Error Marcador no Definido**". Haga click en el botón Ayuda de *Windows* de la barra de tareas para restaurar la ventana de "**Ayuda**".
3. Si el *solucionador* de problemas se está ejecutando en Internet Explorer, en la barra de tareas, haga click en el botón de Internet Explorer.
4. Cambie el tamaño de la ventana de "**Ayuda**" y muévala a la mitad derecha de la pantalla, de manera que pueda utilizar la mitad izquierda para seguir las instrucciones.
5. Si está ejecutando el solucionador de problemas desde la ventana de "**Ayuda**", en la barra de herramientas de "**Ayuda**", haga click en "**Ocultar**" para ocultar el panel izquierdo.
6. Siga minuciosamente los pasos del solucionador de problemas, si no lo hace, podrá perder información fundamental y limitar la efectividad del solucionador de problemas.

(26) Peter Norton Solución a Problemas de PC
Peter Norotn & Robert Jourdain
ED. PRENTICE HALL

7. Tras llevar a cabo cada paso del solucionador de problemas, revise la información de la ventana de "Ayuda" y compruebe que ha seguido las instrucciones del solucionador de problemas.

### 9.10.7. CONFLICTOS DEL HARDWARE EN WINDOWS 95[26]

Si al iniciar su PC, tiene conflictos con la configuración del hardware; primero debe buscar y verificar, que no aparezca dos veces un dispositivo, en el "Administrador de dispositivos", siga los siguientes pasos:

1. Para acceder al "**Administrador de Dispositivos**", haga click en **Inicio**, seleccione "**Configuración**", haga click en "**Panel de Control**" y después, haga doble click en "**Sistema**".
2. En la ficha "**Administrador de Dispositivos**", busque dispositivos duplicados.
3. Si un dispositivo aparece dos veces en la ficha "**Administrador de Dispositivos**", *pero sólo tiene un dispositivo de ese tipo instalado en su PC*, vuelva a instalar el dispositivo; para ello, quite todas las apariciones del dispositivo y ejecute el "**Asistente**" para "**Agregar Nuevo Hardware**".

Para quitar todas las apariciones del dispositivo duplicado:

1. Haga click en **Inicio**, seleccione "**Configuración**", haga click en "**Panel de Control**" y después, haga doble *click* en "**Sistema**".
2. En la ficha "**Administrador de Dispositivos**", haga click en una aparición del dispositivo y después, haga click en "**Quitar**".
3. Repita el paso 2 para cada aparición restante del dispositivo. Cuando haya quitado todas las apariciones del dispositivo, cierre el cuadro de diálogo "**Propiedades del sistema**".
4. Vuelva a iniciar su PC, debe mejorar su comportamiento.

(26) Peter Norton Solución a Problemas de PC
Peter Norotn & Robert Jourdain
ED. PRENTICE HALL

### 9.10.8. EJECUTE EL ASISTENTE PARA AGREGAR NUEVO *HARDWARE*[26]

1. Para entrar al asistente de Windows 95, en la ventana principal, haga click en: **Inicio** + **Configuración** + **Panel de Control**, y por último en: "**Agregar Nuevo Hardware**".

2. Siga las instrucciones de la pantalla hasta que el asistente haya finalizado.

3. Vea la ficha "**Administrador de Dispositivos**" para determinar si el dispositivo aparece dos veces después de que el asistente haya finalizado. Si el dispositivo aparece dos veces, quite una aparición del dispositivo y vea la ficha Recursos

### 9.10.9. VERIFIQUE LA FICHA RECURSOS[26]

Haga click en **Inicio**, seleccione "**Configuración**", haga click en "**Panel de Control**" y después, haga doble *click* en "**Sistema**".

1. En la ficha "**Administrador de Dispositivos**", haga doble click en el dispositivo.

2. En la ficha "Recursos", compruebe que ve las propiedades para el dispositivo correcto.

**Nota**:

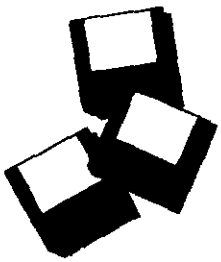
- Si en la ficha Recursos no aparece el dispositivo, o no usa ningún recurso. Cierre este solucionador de problemas y póngase en contacto con el fabricante del dispositivo para resolver un posible conflicto de *hardware*.
- En la ficha de **Recursos**, observe un cuadro con la configuración de recursos o un botón, si aparece, entonces elija: "**Establecer Configuración Manualmente**".

(26) Peter Norton Solución a Problemas de PC
Peter Norton & Robert Jourdain
ED. PRENTICE HALL

# CAPITULO 10

## HERRAMIENTAS BASICAS DEL ANTIVIRUS DR. SOLOMON'S, EJEMPLOS Y DEMOSTRACIONES

En este capítulo tomaremos como ejemplo las herramientas que utiliza el Antivirus de Dr. Sólomon's, y las estudiaremos par comprender aún mejor el funcionamiento de un sistema Antivirus.



### 10.1. TOOLKIT[8]

- Es la interfaz desde donde el usuario puede mandar ejecutar las diferentes herramientas del sistema de Antivirus de Dr. Solomon's.
- Requiere de un archivo con extensión: **.INI**, que contiene los parámetros a seguir durante la ejecución del mismo.
- El archivo clave se llama **TOOLKIT.INI**
- Y las opciones a emplear serán:

  /M Para monitores LCD o monocromáticos

  /G Para diferentes tonos de grises

  /ID Para inspeccionar el disco

  /VE Para consultar en la Enciclopedia de virus

  /# Para confidencialidad y niveles de acceso

(8) PC Viruses – Detection, Analysis and Cure
Dr. Alan Solomon & Tin Kay

## 10.2. FINDVIRU[8]

- Su función principal es la de rastrear los virus, también es llamado Escáner *"ON-DEMAND"*.
- Detecta y repara virus en discos duros físicos, lógicos y *diskettes*.
- Rápido en su desempeño: Aproximadamente rastrea 80 MB de información en 20 segundos.
- Rastrea en archivos comprimidos y compactados.
- Dependiendo de donde se esté ejecutando, "FindViru" utilizará los siguientes archivos:

  **FB86.EXE** (No podrá rastrear dentro de archivos comprimidos o compactados desde *diskette*).

  **FV386.EXE** Todas las capacidades conocidas (desde disco duro).

- Mensajes de error que despliega:

1. No puede ejecutar FINDVIRU.EXE
2. No hay suficiente memoria para cargar FINDVIRU.EXE
3. El programa a sido alterado, por favor reemplace con una buena copia (el archivo está corrupto).

- Mensaje de memoria insuficiente

1. No hay memoria suficiente para ejecutar *FINDVIRUS*:
2. *Bad* MESSAGES.DRV
3. No se encontró el archivo MESSAGES, o está corrupto.
4. Inhabilitado para almacenar el archivo *driver* en XMS.
5. No se cargó el HIMEM.SYS por lo que el programa se está ejecutando desde el disco duro.

- La instrucción más común que se aplica para detectar virus desde MS-DOS, es:

**C:\FINDVIRU C: /DOALLFILES** más *Enter*

(8) PC Viruses - Detection, Analysis and Cure
Dr. Alan Solomon & Tim Kay

- Este comando indicará al disco duro, que ejecute la exploración de todos los virus que puedan alojarse en él.
- Si existe algún virus, entonces se deberá emplear la siguiente instrucción, para reparar o eliminar *cualquier virus:*

  **C:\FINDVIRU C: /DOALLFILES /REPAIR /DELETE /REMOVE /E=N**

Donde la opción:

| | |
|---|---|
| /DOALLFILES | Solo rastrea archivos ejecutables |
| /REPAIR | Repara al archivo infectado por el virus |
| /DELETE | Borra al virus que infecta a los archivos |
| /REMOVE | Remueve al virus y/o embriones que puedan reproducirse |
| /E=N | Significa que rastrea a todos los archivos |

## 10.3. VIRUSGUARD[8]

- Es un programa TSR, y usa únicamente 10 KB de la memoria RAM
- Es conocido como un ESCANER "*ON-ACCESS*"
- No puede ser corrido o ejecutado desde *diskette.*
- Consiste de los archivos GUARD.COM y GUARD.SYS

:

### 10.3.1. GUARD.COM y GUARD.SYS

- **GUARD.SYS** - Base de datos que se ejecuta en el CONFIG.SYS, o el TSR residente en memoria: **DEVICE TOOLKIT/GUARD.SYS**
- **GUARD.DRV** - Base de datos que se ejecuta en el AUTOEXEC.BAT
- **MESSAGES.DRV**

1. Una vez ejecutados los archivos, no pueden ser descargados de la memoria RAM.
2. Por *default* se carga en memoria convencional, pero puede ser movido a la memoria alta.

(8) PC Viruses – *Detection, Analysis and Cure*
Dr. Alan Solomon & Tin Kay

Niveles de seguridad:

**Mínima** (copy=floppy/write=no)

**Estándar** (sin parámetros) es lo más recomendable

**Máxima** (copy=all/write=all)

Es conveniente hacer notar, que estas instrucciones deben existir en el fichero AUTOEXEC.BAT, ya que de ello puede depender la velocidad de procesamiento. En algunas experiencias, se ha tenido que bajar el nivel de seguridad ya que bloquea a la PC, si esta no tiene suficiente memoria RAM. El funcionamiento del Antivirus no afectará el rendimiento de la PC, si cuando mínimo cuenta con 4 Megabytes de memoria RAM. Con los equipos Pentium, ya no existen problemas.

El tiempo que dure la computadora encendida, será el tiempo que *VirusGuard* esté corriendo. Cada disco y cada archivo que sean accedidos, serán verificados en segundos, contra virus. Si se detecta un virus *VirusGuard* prohibirá el acceso evitando así una infección a la máquina.

*VirusGuard,* trabaja de forma completamente transparente para el usuario, y la única vez que se notará su presencia será cuando esté detecte un virus. *VirusGuard* requiere de solo 9 Kilobytes de memoria base, pudiendo ser cargado en memoria alta si lo desea.

## 10.4. AUTHOR[8]

- Permite restringir el uso de *diskettes* en una máquina. Sólo aquellos que estén autorizados podrán ser utilizados en la computadora.
- Trabaja en forma conjunta con *VirusGuard*
- Maneja dos parámetros:

  **Disk.-** Para indicar el *drive* donde se van a autorizar los *diskettes*.

  **Code.-** Para indicar el código de autorización que deberán tener los *diskettes* a utilizar en la computadora.

(8) PC Viruses – Detection, Analysis and Cure
Dr. Alan Solomon & Tin Kay

- Para que trabaje con *VirusGuard*, es necesario que *VirusGuard* sea ejecutado con la opción:

**/CODE= "código".**

- Para evitar el acceso de *diskettes* no autorizados. *VirusGuard* debe ser ejecutado con la opción:

**/STRICT**

## 10.5. GUARDMEM[8]

- Permite rastrear la memoria, en busca de virus sin necesidad de encender en limpio o de cargar *VirusGuard*.
- Consiste de los siguientes archivos:
    1. GUARDMEM.COM
    2. MEM.DRV
- No hay opciones disponibles para este programa.

## 10.6. WINGUARD[8]

- Es un VxD[27] nativo de 32 bits
- Trabaja de forma transparente para el usuario, ya que corre en el "*background*[31]" de *Windows*.
- Consiste de los siguientes archivos:
    1. **WGFE.EXE**
    2. **WINGUARD.386** (es un drive virtual).
- Los mensajes son personalizables (pueden ser traducidos del inglés al español).
- Tiene la capacidad de reparar de forma automática virus de archivo.
- Por *default*, únicamente detiene los virus, no los repara.

Si un archivo está infectado de virus, *WinGuard* detendrá el acceso al mismo pudiendo configurarse, para enviar un mensaje de alerta al administrador del

8) PC Viruses – Detection, Analysis and Cure
Dr. Alan Solomon & Tin Kay
(27) *VxD = Virtual Drivers of Windows 95*
(31) **Background** = Fondo, segundo plano

sistema. *WinGuard* puede incluso interceptar los virus polimorfos más complejos como: El **SMEG**, **MtE**, **One_Half** y el **Trident Ploymorphic Engine**.

## 10.7. CLEANBOOT[8]

- Sólo para *diskettes* (5.25" y 3.5" de doble y alta densidad).
- Reemplaza un sector de arranque infectado, con un sector de arranque limpio.
- Tiene tres opciones:

| | | |
|---|---|---|
| 1. | **/DRIVE** | unidad donde se encuentra el *diskette* |
| 2. | **/NOASM** | inhabilitar ASM |
| 3. | **/TIPO** | donde tipo es igual a: |

  - 5.25 de doble densidad (360 KB)
  - 5.25 de alta densidad (1.2 MB)
  - de doble densidad (720 MB)
  - de alta densidad (1.44MB)
  - formateo especial (2.88MB)
  - Autodetectar

## 10.8. CLEANPART[8]

- Es una utilería sólo para las particiones de los discos duros.
- Reemplaza tanto al sector de arranque como al sector de partición infectados, por unos limpios.
- Puede ser utilizado en 3 formas:

| | | |
|---|---|---|
| 1. | **BACKUP** | para respaldar el MBR, BOOT y CMOS |
| 2. | **RESTORE** | para recuperar el MBR, BOOT y CMOS |
| 3. | **FIX** | para eliminar y reemplazar particiones. |

- Puede hacer referencia al identificador lógico del disco duro o bien al identificador físico.

  Ejemplo: **CLEANPART C:** ó **CLEANPART 128**

(8) *PC Viruses – Detection, Analysis and Cure*
Dr. Alan Solomon & Tin Kay

## 10.9. VIVERIFY[8]

- Es un "CHECKSUMMER" criptográfico.

  **Nota**.- CHECKSUMMER = Suma de verificación. El valor numérico total de un bloque de datos, que se utiliza con propósitos de verificación de errores.

- Genera una "huella digital" de cada uno de los archivos ejecutables de la computadora.
- Recalcula dicha "huella", cuando se requiere verificar cambios en los archivos, debido a algún virus de archivo.
- 3 etapas en la utilización del VIVERIFY:
  1. Crear la lista de archivos a verificar.
  2. Generar las "Huellas Digitales" de esos archivos, cuando se requieran volver a generar dichas "Huellas" y comparar.
  3. Detecta nuevos virus.

Rastrea también el sector de partición y sector de arranque. Permite también detectar virus nuevos o desconocidos vía cambios en los archivos ejecutables. ViVerify utiliza 4 diferentes algoritmos criptográficos, incluyendo el CCITT[28] CRC[29] y DES[30].

## 10.10. TKUTIL[8]

- Programa que proporciona una serie de utilerías a través de sus parámetros
- Unicamente para *DOS./WINDOWS*
- Para *Windows* 95, *WTKUTIL*

## 10.11. FIXBYWAY[8]

- Utilería para remover el virus **Dir.Byway**
- Funciona tanto para *diskettes* como para discos duros.
- Es de distribución gratuita para usuarios de Dr. Solomon's Antivirus *Toolkit*

---

(8) PC Viruses - Detection, Analysis and Cure
Dr. Alan Solomon & Tim Kay
(28) CCITT = Consultative Committee for International Telephony and Telegraphy
(29) CRC = Cyclical Redundancy Cheking
(30) DES = Data Encryptoion Standard

## 10.12. PROGRAMAS DE SACRIFICIO[8]

- Son programas cuya característica principal, es que su tamaño coincide con su nombre.
- Son archivos EXE y COM
- Se utilizan para capturar virus nuevos o desconocidos.

  Ejemplo: H20000.EXE de 2000 bytes.
- Fueron desarrollados por Dr. Solomon's Software.
- Son de distribución gratuita, para usuarios de Dr. Solomon's Antivirus *Toolkit*.

## 10.13. EXTRA DRIVERS[8]

- Son archivos de texto que contienen los métodos de detección y reparación de virus.
- Se utilizan para actualizar el Antivirus, cuando la versión que se tiene no detecta al virus en cuestión.
- FINVIRU y WINGUARD pueden hacer uso de estos EXTRADRIVERS.

## 10.14. DEMOSTRACIONES[22]

Cada año es lo mismo. Al acercarse el mes de Marzo, el departamento de Soporte Técnico de Dr. Solomon's *software*, se satura de llamadas de clientes y periodistas. ¿Cuál es la razón?, Existe un virus llamado **Miguel Angel**, **se activa el 6 de marzo, día del cumpleaños del artista**, han circulado historias terribles sobre la inminente destrucción de la información, para lo cual no hay remedio, cura ni salvación.

Es fascinante descubrir que **Miguel Angel,** no es un virus que se encuentra con frecuencia; en el caso de México, no se ha recibido referencia de incidentes con este virus, y lo que realmente sucede, es que otras empresas Antivirus; intentaron asustar a la gente para que compren su *software* Antivirus.

*Graham Cluley*, consultor tecnológico para Dr. Solomon's comentó al respecto: "La manía de **Miguel Angel,** comenzó en 1992. Un vendedor norteamericano de Antivirus, apareció en el canal de televisión CNN y declaró ante el mundo, que 5 millones de PC's, serían atacadas el 6 de marzo. Esto es algo escandaloso. Se tuvieron quejas de ésta infección (en Inglaterra), de menos de 6 clientes".

El virus **Miguel Angel,** nunca fue la gran amenaza y nunca lo será en el futuro, a pesar de que este virus puede borrar la información de disco duro, aparece muy rara vez.

Dr. Solomon's quiere motivar a los usuarios de computadoras, para que busquen e investiguen más sobre este virus, y puso a su disposición esta información en su página internacional de Internet: **http://www.drsolomon.com**

Esta información habla de los cientos de virus que más comúnmente aparecen, además de explicar por qué los virus no están solamente limitados a aparecer o activarse en fechas determinadas, como son viernes 13 o 6 de marzo, sino que pueden activar cualquier día del año.

## 10.15. RECOMENDACIONES[22]

Algunas veces, se tienen computadoras con dos discos duros. Si usted ha tratado de utilizar el Antivirus de DR. Solomon's con la utilería. CLEANPART, para limpiar el disco duro y <drive> correspondiente, ¿y no ha tenido éxito porque al encender en limpio no se reconoce dicha unidad?.

**CLEANPART,** tiene la capacidad de reconocer la unidad lógica o física correspondiente, por lo que usted puede emplearlo de las siguientes formas:

(8) PC Viruses – Detection, Analysis and Cure
Dr. Alan Solomon & Tin Kay
(22) Boletín de Antivirus de Dr. Solomon's (marzo de 1998)

**CLEANPART C:** (lógica) o **CLEANPART 128** (física).

1. La opción **/OC** (OverRide Checksums) es una opción no documentada, la cuál no es de mucha ayuda cuando ejecutamos por primera vez el FINDVIRU y nos reporta un virus "**Like**"... (que significa virus parecido a...). Es aconsejable volver a ejecutar **FINDVIRU** con la opción **/OC** para comprobar, si el archivo:

- Ha sido mal infectado por un virus.
- Ha sido mal reparado por otro Antivirus.

Uso de la opción **/OC,** para detectar si hubo una mala reparación, teclee:

**FINDVIRU C:\TEST /OC**

Para eliminar:

***FINDVIRU C:\TEST /OC /REPAIR***

### 10.15.1. ENVIO DE MENSAJES DE RED[22]

- Si está en una red Novell, puede enviar mensajes a otros usuarios conectados:
- Seleccione **"Enviar mensaje"** en el menú '**Red**' de la interfaz de usuario.
- Aparece el diálogo **"Enviar mensaje de Red"**
- Escriba el nombre del usuario conectado al que desea enviar el mensaje en el cuadro "**Enviar mensaje a...**".
- Introduzca el mensaje en el cuadro "**Mensaje**".
- Haga clic en **"Enviar"**.

> **Nota**: Para que se reciba el mensaje, "El destinatario debe ejecutar la utilidad adecuada"; por ejemplo: "**WINPOPUP"** en una computadora con *Windows* 95 o **"NWPOPUP",** en una con *Windows* 3.X. Los mensajes que no se puedan enviar, no se almacenan.

(22) Boletín de Antivirus de Dr. Solomon's (marzo de 1998)

Si dispone de una red Novell, *Findvirus* puede enviar mensajes de alerta a los usuarios conectados a la red cuando detecte un virus:

1 Seleccione **"Opciones"** del menú **"Red"** de la interfaz de usuario.
2 Aparece el diálogo **"Opciones de red"**.
3 Compruebe que **"Alarma de red ante virus"** esté activada. Observe que esta opción está activada por defecto. Observe que la misma opción aparece en el diálogo **"Buscar virus - Opciones Avanzadas"**. El estado activada/desactivada de esta opción está sincronizado de forma automática en ambos diálogos.
4 Edite el mensaje del cuadro **"Mensaje de alerta de virus"**.
5 En el cuadro **"Enviar mensaje de alerta de virus a"**, escriba el nombre del usuario conectado que desea que reciba el mensaje.
6 Haga clic en **"Aceptar"**.

## 10.16. ACERCA DE LOS DOMINIOS ANTIVIRUS[16]

Un dominio Antivirus es una colección de máquinas *Windows* NT, *Windows* 95 y *Windows* para trabajo en grupo, que le permiten administrar su estrategia Antivirus, agrupando grandes números de máquinas de una manera lógica.

No existe un límite para el número máximo de máquinas que pueden construir un dominio Antivirus. Antes de instalar los programas de la consola de administración (Management Console), considere como desea dividir su organización en unidades de administración o dominio Antivirus. Puede administrar toda la red como un solo dominio Antivirus, dividirla en varios de ellos o bien seguir la estructura de dominios de redes de Microsoft que ya ha instalado.

La consola de administración le permitirá crear uno o más dominios Antivirus basados en cómo desea agrupar las máquinas su red. Entonces usted podrá instalar,

(16) Manual de Usuario. de Dr. Solomon's

actualizar y configurar su *software* Antivirus, para todos sus dominios, para uno sólo de ellos o para una sola máquina.

Cada dominio Antivirus, deberá tener un servidor de administración (Management Server), para que pueda proporcionar comunicaciones centralizadas, y éste deberá ser una máquina *Windows* NT. Todos, los otros miembros del dominio Antivirus, tendrán un agente de administración (Management Agent) instalado automáticamente con uno o más componentes Antivirus. Puede instalar agentes mensajeros (Messaging Agents) donde quiera que necesite acceso a los recursos de mensajería sobre la red.

## 12.17. SOPORTE TECNICO[16]

En el caso de que sea necesario el soporte técnico en sus instalaciones, el personal de soporte técnico debe asistir al lugar donde se encuentre el equipo.

Soporte técnico en virus nuevos y desconocidos:
Dr. Solomon's Antivirus *Toolkit*, detecta e identifica virus nuevos o desconocidos a través del Análisis Heurístico de *Findviru*, con cero falsas alarmas. Si *Findvirus* llegara a detectar un archivo ejecutable, o de datos, infectado por un virus, mostrando el nombre del virus precedido por la palabra **"Like"**, con toda seguridad se trata de:

- Un virus nuevo o desconocido.
- Un archivo corrupto o dañado por un virus.
- Un archivo que sufrió una mala infección de un virus o una mala reparación de otro Antivirus.

Si se trata de un virus nuevo o desconocido, *Findvirus* renombrará los archivos que no se puedan reparar, insertando en el primer carácter de la extensión del archivo la

(16) Manual de Usuario. de Dr. Solomon's

letra "Virus" de virus, como por ejemplo: **EDIT.VOM,** evitando que estos archivos se puedan ejecutar y por lo tanto seguir infectando la computadora.

El archivo renombrado, es la muestra o ejemplar que deberá ser copiado en un disco flexible, para enviarse al departamento de soporte técnico de Dr. Solomon's.

Una vez que el laboratorio de soporte tenga la muestra, la enviará a Inglaterra a través de correo electrónico, mediante cuentas privadas y con todas las medidas de seguridad pertinentes.

Cuando el laboratorio de Dr. Solomon's en Inglaterra reciba la muestra, lo desembolsará y enviará por el mismo medio, la solución, que en la gran mayoría de los casos no han pasado más de 72 horas hábiles (a partir de que el laboratorio en Inglaterra recibe, el virus).

# CAPITULO 11

# RECOMENDACIONES A LOS USUARIOS FINALES

## 11.1 RECOMENDACIÓN DEL ANTIVIRUS DE MCAFEE[17]

- Es en serio, instalar y hacer funcionar un programa Antivirus; no es como usar otros programas o sistemas de cómputo, aún si usted es un experto en el uso de computadoras personales, es muy importante que lea y utilice los procedimientos de instalación de un Antivirus.
- Lo prioritario es prevenir la propagación de la posible infección, los virus se propagan desde el mismo momento en que se enciende la computadora, con cualquier disco infectado, haciendo funcionar cualquier programa que esté igualmente infectado. Si su computadora ya fue infectada, al instalar y hacer funcionar el Antivirus desde su disco duro, ocasionará que se pueda extender la infección incluyendo a estos programas. Las medidas contempladas en este capítulo son para asegurar que tenga un ambiente limpio para poder así detectar, erradicar y prevenir los virus.
- Es posible establecer una analogía con un equipo de cirujanos, estableciendo un área esterilizada antes de efectuar cualquier cirugía. Una vez establecida, se aseguran que todo lo que traigan a esta área, haya sido previamente esterilizado.

(17) Manual de Usuario, de *McAfee*

- En este procedimiento, se creará un disco de arranque limpio, sin virus, en el cuál se pueda restablecer el área esterilizada, en caso de ser necesario.
- Su *diskette* de Antivirus está protegido contra escritura, para asegurar que ningún virus pueda alterar los programas y la información contenida en él. **Si conoce las formas para violar esta protección, POR FAVOR NO LO USE.**
- Recuerde, que los programas que corren en OS/2 funcionan en modo protegido; los sistemas en OS/2 no son tan vulnerables a los virus como lo son los sistemas en *MS-DOS* y *Windows*. Sin embargo, los usuarios de OS/2 que activan sesiones en *MS-DOS*, son bastante vulnerables. Utilizando los programas de *McAfee*, usted podrá proteger la parte que está en *MS-DOS* de su sistema *OS/2* en caso de quedar infectada.

## 11.2. PROCEDIMIENTOS, QUE HACER EN CASO DE ENCONTRAR UN VIRUS

### 11.2.1. CREE UN DISCO DE SISTEMA[17]

El manual de Mcafee, recomienda primero vacunar la PC infectada por virus y debe proceder a seguir los siguientes pasos:

1. Cree un disco de sistema. Es importante que al hacer este disco de sistema o de arranque, no olvide cargar la instrucción: HIMEM.SYS en el archivo CONFIG.SYS, y aparte de los archivos de arranque, también se recomienda crear un archivo AUTOEXEC.BAT. La creación y contenido de estos ficheros, es igual a la de los archivos originales que aparecen grabados en el directorio raíz del disco duro.
2. Debemos contar con otra PC que no esté infectada y debemos asegurarnos de ello, de preferencia debe tener instalado el mismo sistema operativo de la máquina a la que vamos a descontaminar.

   **Nota.-** Si no se cuenta con el mismo sistema operativo, pueden existir conflictos entre las versiones de sistema operativo, al iniciar la PC y es

(17) Manual de Usuario, de *McAfee*

*posible que algunos sistemas no funcionen correctamente, en especial Windows* ó que no arranque correctamente la PC.

3. Si tiene la PC adecuada, introduzca un *diskette* limpio, de preferencia nuevo y formateado en la unidad de disco flexible (drive), luego ubíquese en el indicador de sistema (*prompt*)de *MS-DOS*.

**C:\>**

4. Los archivos de sistema serán trasmitidos al *diskette*, tecleando en el *prompt*:

**C:\> SYS A:** y oprima la tecla *<Enter>*

5. Después de creado este disco de sistema, retírelo de esta máquina e introdúzcalo en la PC infectada.
6. Introduzca el *diskette* de sistema y encienda la PC, esperamos a que se ejecute el proceso de arranque hasta que aparezca el siguiente *prompt*:

**A:\>**

7. Desde este indicador procedemos a vacunar la PC, retiramos el disco de arranque y metemos el disco rastreador o limpiador de virus, proceda a rastrear el disco duro para localizar y erradicar el o los virus.

**Nota.-** Este disco también le puede servir, cuando un usuario eliminó accidental o intencionalmente los archivos de sistema de una PC, y el procedimiento es similar según se aprecia a continuación:

8. Después de creado el disco de sistema o arranque de la PC limpia, retire el *diskette* e introdúzcalo en la PC que no arranca, encienda la PC y espere a que aparezca el prompt: **A:\>**
9. Teclee en el prompt:

**A:\>SYS C:** más oprimir la tecla *<Enter>*

10. Así, serán trasmitidos los archivos de sistema a esta PC. Después se retira el *diskette* de arranque y se inicia la PC. Debe aparecer normalmente el prompt "**C:\>**", si se trabaja en la versión de *MS-DOS* como plataforma base para *Windows* 3.x

11. Para *Windows* 95, debe copiar después el archivo MSDOS.SYS, por separado, ya que el que se carga en los archivos de sistema es él.

**Nota.-** Si la PC no tiene instalado un sistema de Antivirus, le recomendamos forzosamente la adquisición de uno, ya que es de gran responsabilidad, proteger su sistema para el correcto funcionamiento y protección de la información.

14. Si no logra erradicar al virus o Macrovírus con el sistema de Antivirus que posee, le recomendamos buscar la vacuna actualizada en Internet. Existe gran variedad de desarrolladores de sistemas de Antivirus en el mundo, y que cualquiera de ellos le facilitará apoyo y soporte técnico, para la eliminación. Todos estos sistemas Antivirus, tienen su Shareware.

## 11.3. VALIDANDO MCAFEE[17]

Antes de ejecutar por primera vez el programa *Scan*, por favor verifique que no haya sido dañado o alterado por medio del programa *VALIDATE*, ejecutando las siguiente instrucciones:

- Cámbiese a la unidad **A:\>** de disco flexible, inserte el disco de distribución de *McAfee* y ejecute los siguiente pasos:

**A:\>VALIDATE *.EXE**

**A:\>VALIDATE *.DAT**

- Anote los datos (o mándelos a la impresora usando la tecla "Impr Pant").
- Ahora use los datos de validación en la opción número **11 (DATOS DE VALIDACIÓN PARA LA PRESENTE VERSIÓN)**, del menú principal (ARMO[20]) y compárelas. Escriba ARMO y cuando contenga la pantalla del menú, seleccione la opción 11.

**Nota.-** Si los datos de validación no coinciden, no use el programa ni lo instale. Por favor, consulte con su agente local que le vendió el Antivirus.

(17) Manual de Usuario, de *McAfee*

### 11.3.1. SOLUCIONES[17]

Aunque los virus representan un problema, se debe tener presente la escala del problema. La causa más común en la pérdida de datos es el error humano. La segunda causa más común es error del *hardware*, seguido de problemas del *software* y alteraciones. Los virus llegan en un triste cuarto lugar. Sin embargo, al aplicar una política Antivirus estricta, se protegen los datos de todo tipo de pérdida, incluyendo los virus.

En particular, debe tener en cuenta los tres siguientes elementos de protección:

- Prevención - Para limitar la propagación de virus.
- Detección - Para asegurarse, que si un virus aparece, se descubra lo antes posible.
- Recuperación - Para asegurarse, que si un archivo se pierde o se daña, se pueda restaurar lo antes posible. Con los Antivirus, se cubre una parte significativa de esta política de detección y de recuperación, pero a continuación se sugieren otros elementos que son aconsejables:
- Realice copias de respaldo.
- Verifique las fuentes de *software*.
- Tome precauciones con los *diskettes* y otros medios.
- Evite la encriptación y la protección con contraseña, hasta donde sea posible.
- Consiga la colaboración de los empleados.

Para lograr la máxima seguridad al utilizar un Antivirus, también puede arrancar en limpio y/o ejecutar las herramientas desde los *diskettes* de instalación.

## 11.4. CERTEZA EN LA IDENTIFICACION DE UN VIRUS EN GENERAL[16]

Son múltiples los efectos que se pueden apreciar para identificar la existencia de un virus o Macrovirus, posibles efectos son:

- Que no arranque la PC, puede deberse a que un virus eliminó los archivos de sistema de inicio o alteró los sectores de partición y arranque.
- Que aparezcan archivos raros en el directorio raíz, al abrir el explorador de archivos.
- Que dichos archivos a su vez no se puedan eliminar.
- Que dichos archivos también se eliminen y vuelvan a aparecer cada vez que se inicie la PC.
- Que dichos archivos vuelvan a crearse al abrir el explorador de archivos.
- Que esté desapareciendo misteriosamente la información almacenada en el disco duro.
- Que la PC marque memoria insuficiente.
- Que este realizando instrucciones incorrectas al aplicar los comandos en *Word* y *Excel*, esto se debe a que quizás exista un Macrovirus
- Que estén sucediendo cosas anormales, como distorsión en la imagen o que surjan efectos diversos no generados al operar la PC.
- Para detectar que se trata de un Macrovirus, abra el menú **"Herramientas del Sistema"** *Word* y elija la opción Macro, al abrir esta opción si aparecen listados los nombres de las **"Macros"**; entonces la PC esta infectada por un Macrovirus. Deberá eliminar todas las **"Macros"** de una en una, después borrar el archivo **NORMAL.DOT,** que es la plantilla principal del procesador de textos *Word*. Cierre todos los programas, apague la PC y se vuelva a iniciarla, verificando con el mismo procedimiento que no existan las **"Macros"**, si vuelven a cargarse, entonces requiere de la utilización de un **EXTRADRIVER,** para eliminar al Macrovirus.

(16) Manual de Usuario. de Dr. Solomon's

**Nota.-** *Las falsas alarmas no son virus*, una falsa alarma es cuando se piensa erróneamente que se tiene un virus y en realidad se trata de un problema de *hardware* o *software*. En realidad la mayor parte de veces cuando existe un virus difícil de eliminar, todos los desarrolladores de Antivirus siempre le dirán: **"QUE SE TRATA DE UNA FALSA ALARMA"**. Esto lo comentan para no hacer quedar mal al sistema de Antivirus que representan. ¡**NUNCA DEBE CONFIARSE!**, Ya que esto es muy riesgoso; pues **NO EXISTE ANTIVIRUS PERFECTO**. Se recomienda usar hasta tres sistemas distintos de Antivirus, para estar seguro de que no exista algún virus en la PC.

- Si al ejecutar un programa, no se ejecuta mandando el siguiente mensaje:

**"NO HAY MEMORIA SUFICIENTE PARA EJECUTAR LA APLICACION"**

Esto no quiere decir que se trate de virus o de algún Macrovirus, ni que tampoco falte liberar espacio en disco duro o aumentar la memoria. Este mensaje se debe, a que existe un *Bug* en el archivo ejecutable, que se está abriendo y por esta causa de desborda la memoria convencional. Se recomienda reconstruir este archivo o copiarlo de una fuente fiable.

- Cabe volver a mencionar, que **NO EXISTE ANTIVIRUS PERFECTO,** hoy en día existe aproximadamente en el mundo más de 19,000 diferentes clases de virus, al mes de julio de 1998, y que mensualmente la cifra se incrementa aproximadamente de 1,200 a 1,300 virus. En estos momentos alguien, en algún lugar del mundo está creando virus, por lo que sería imposible para los desarrolladores de sistemas de Antivirus, poder adivinar las causas y efectos de estos programas llamados "virus". La mayoría de estos desarrolladores de Antivirus, actualizan sus sistemas aproximadamente de cada tres semanas a un mes.

## 11.5. RECOMENDACIONES DE DR. SOLOMON'S, SI ENCUENTRA UN VIRUS[16]

¡No se alarme!, ¡ No tenga prisa!

Si tenía seleccionada la opción: **"Utilizar el analizador heurístico"**, puede que se haya detectado un nuevo virus. Para determinar este hecho, compruebe si el informe de infección da un nombre al virus. Si es así, se trata de un virus conocido. De lo contrario, es un nuevo virus. Si descubre un nuevo virus envíe un *diskette* con él mismo, al laboratorio de Dr. Solomon's *Software*.

- Si se trata de un virus conocido, puede utilizar *Findvirus* utilería de Dr. Solomon's, para eliminarlo de forma rápida, desde la pantalla principal o el menú Escanear.
- Para mayor seguridad, se recomienda "Iniciar su PC en limpio" y eliminar el virus mediante el disco con el sistema Magic Bullet[32] de Dr. Solomon's.
- Si existe un departamento de informática en su empresa, debe ponerles en conocimiento de este hecho.

El departamento de informática debe:

- Comprobar las computadoras restantes.
- Comenzar la planificación de una limpieza, si es necesario.
- Decidir si es preciso informar al departamento de delitos informáticos.
- Comprobar todos los *diskettes* que se han podido infectar.
- Revisar la política Antivirus, para intentar evitar otro problema.

### 11.5.1. SI ENCUENTRA UN NUEVO VIRUS[16]

Si sospecha que ha descubierto un nuevo virus, realice los pasos siguientes:

1. Formatee un *diskette* en la computadora infectada (de esta forma se copian los virus de los sectores *Boot* o de partición en el sector *Boot* del *diskette*).
2. Copie los archivos que sospecha que están infectados en el *diskette*.
3. Copie los programas FORMAT.EXE y CHKDSK.EXE en el mismo *diskette*.

(16) Manual de Usuario, de *Dr. Solomon's*
(32) MAGIC BULLET (ver Capítulo 3.4.7)

4. Adjunte una carta y envíela a Dr. Solomon's, en la que explique los síntomas detectados; a menudo. Dr. Solomon's, le dará a conocer de qué problema se trata, incluso si es o no, un nuevo virus. Si le resulta posible, incluya un número de Fax y de teléfono, además de su domicilio.
5. Envíe el *diskette* y la carta a Dr. Solomon's. Consulte en Internet, su domicilio.

No ejecute nada en la PC infectada. Si la PC está conectada a una red, desconéctela, para evitar que otros usuarios accedan a los archivos. Dr. Solomon's le informará las acciones necesarias que se debe tomar.

### 11.5.2. DETECCION MANUAL DEL VIRUS DIR.BYWAY[16]

La mayor parte de usuarios inexpertos, sufren el ataque de este terrible virus y que en el Capítulo 2 ya fue explicado ampliamente, únicamente recordaremos en esta sección, no olvidar la instrucción manual que detecta la existencia de este virus.
Deberá teclear en el indicador de sistema de *MS-DOS*, lo siguiente:

**C:\>DIR *.* /AHS** y oprima la tecla *ENTER*

Si aparece un archivo listado:

**CHKLST .MS** **y mide 2,048 bytes**

Entonces la PC tiene activo al virus **Dir.Byway**

**Nota.-** Este procedimiento será igual para los *diskettes* flexibles. Se introduce el *diskette* en la unidad de disco flexible y teclee lo siguiente, en el indicador de sistema de *MS-DOS*:

**C:\>A:** y oprima *Enter*
**A:\>DIR *.* /AHS** y oprima *Enter*

Por tanto, se tiene que efectuar el proceso para erradicar este virus, ya sea de disco duro o del disco flexible. Para remover el virus **Dir.Byway,** necesita una utilería

llamada **FIXBYWAY**, *que viene adicional en el sistema de Antivirus*, misma que proporciona Dr. Solomon's en su paquete de protección.

### 11.5.3. COMO OPERAN LOS VIRUS BAJO *WINDOWS* 95[16]

*Windows* 95 y virus en sector de arranque. Si una PC con *Windows* 95, es encendida, el sistema evita que se escriba en el *track 0* o sector de arranque, enviando un mensaje en el que se avisa al usuario, que las escrituras a disco han sido inhabilitadas y el sistema se ha bloqueado, requiriendo que se presionen las teclas <Ctrl><Alt><Del> para reiniciar la PC. A primera vista, esto parece impedir que los virus de sector de arranque logren infectar el sistema, dado que estos virus escriben su información en el sector de partición (*MBR – Master Boot Record*), o en el sector de arranque del disco duro.

Sin embargo, las escrituras a disco son inhabilitadas, sólo cuando *Windows* 95 está corriendo y los virus del sector de arranque infectan a nivel BIOS; es decir, antes de que cualquier sistema operativo (*DOS, Windows* 95, *Windows* NT, *OS2/2 y Novell Netware*, etc.), sean cargados. Esto significa, que sólo los programas tradicionales no pueden escribir a disco, pero los virus si pueden y de hecho infectando el sistema. Los virus que infectan directamente el arranque de *Windows* son:

**Form, Empire Monkey, Parity.b, Stealhboot, Jumper, Telefonica, Purcyst y Beijing, Michelangelo.**

"De los cuales en México tan sólo se han reportado **Empire Monkey, Stealhboot, Jumper, Beijing y Exebug"**

Todos ellos fueron capaces de infectar al disco duro. Cuando una PC infectada con un virus de sector de arranque, es reencendida, *Windows* 95 se ejecuta en *<<MS-DOS compatibility mode>>* en lugar de utilizar su sistema de ARCHIVO NATIVO de 32 bits. Lo anterior no se notará, salvo que el usuario utilice los recursos del sistema de forma más exigente que lo usual, o trate de ejecutar una aplicación de 32

(16) Manual de Usuario. de Dr. Solomon's

bits. De otra forma, todo parecerá que trabaja normalmente, después de la primer infección cuando una PC infectada es reencendida en *Windows* 95, el sistema enviará un <<*Performance Dialog*>> con el siguiente mensaje:

**WARNING: Your computer may have a virus. The Master *Boot* Sector on your computer has been modified. Would you like to see more information about this problem?**

En este punto existen varios aspectos importantes a revisar:

**(1)** La referencia al "*Master Boot Record*" (MBR) también es hecha cuando una PC está infectada con el virus **Form**, aunque éste sólo infecte al sector de arranque.

**(2)** El <<*Performance dialog*>> aparecerá sólo en la primer reencendida después de la infección.

**(3)** El <<*Performance dialog*>> no se muestra para cada virus de sector de arranque. Los virus **Michelangelo** y Telefonica no ocasionan este mensaje.

Todos los virus mencionados en este tema, se mantuvieron residentes en memoria bajo *Windows* 95. La mayoría de ellos fueron capaces de infectar *diskettes* y algunos de ellos ocasionaron problemas que fueron detectados por el usuario, y que se listan a continuación:

(a) **Stealthboot:** infectó exitosamente *diskettes*, pero se cicla al intentar acceder a *diskettes* ya infectados.

(b) **Telefonica,** no pudo infectar *diskettes*.

(c) **Michelangelo,** infectó exitosamente *diskettes*, pero al intentar acceder a *diskettes* ya infectados, produjo un mensaje de error: "*General Failure Reading...*". Esto también ocurre bajo *MS-DOS* y *Windows* 3.x, ya que **Michelangelo** fue diseñado para *diskettes* de 360 Kb (5.25 pulgadas, de baja densidad), y además contiene un *Bug* de programación, que evita que el virus pueda manejar *diskettes* de alta densidad.

La mayoría de virus examinados, tienen la capacidad de ocultamiento, es decir; tienen la capacidad *STEALTH,* mientras están residentes en memoria. (**Empire Monkey**, **Parity.b, *Stealthboot*, Telefonica, Purcyst** y **Exebug**), son virus que fueron capaces de ocultarse eficazmente bajo *Windows* 95.

### 11.5.4. *WINDOWS* 95 Y VIRUS DE ARCHIVO[16]

Todos los virus revisados en este ambiente operativo, fueron virus de archivo, diseñados para trabajar bajo *MS-DOS*; como: **Yankee Doodle, Cascade, Jerusalem, Frodo. Tequila** y **Natas**.

- De los cuales, en México sólo se han reportado: **Yankee Doodle, Jerusalem, Frodo. Tequila** y **Natas**.
- De los anteriores, los virus **Tequila** y **Natas,** son virus multipartitas; es decir: infectan sectores de arranque, de partición y archivos.

Los virus: **Yankee Doodle** y **Cascade,** se replicaron como normalmente lo hacen bajo *MS-DOS*; sin embargo; sólo infectaron programas bajo la misma sesión de *MS-DOS, ya que otros programas ejecutados en otra sesión de MS-DOS, se mantuvieron* libres de estos virus. Cualquier intento de ejecutar un programa infectado con el virus **Jerusalem,** ocasionó que dicha sesión se bloqueara, pero no así el sistema completo, ya que se pudo cerrar la sesión con las teclas <Ctrl><Alt><Del>

A diferencia del caso anterior, si se pudieron ejecutar programas infectados con el virus **Frodo;** aunque esto ocasionó que *Windows* 95, fallara al intentar hacer un cambio de aplicación (después de desplegar un error con la siguiente leyenda: **"Fatal exception"**), esto pudiera explicarse debido al comportamiento del virus. **Frodo,** intentó modificar al sector de partición con el objetivo de agregar su rutina de "*Payload*". Cuando la PC fue reencendida, *Windows* 95 no notó ningún cambio en el sector de partición; de igual forma, también se ejecutaron, programas infectados con el virus **Natas,** pero aquí, ocurrió algo curioso: Al tratar de ejecutar

un programa no infectado, el sistema falló y *Windows* 95 se bloqueó (después de desplegar un error con la siguiente leyenda: **"Fatal exception"**). Cuando la PC fue reencendida *Windows* 95 no notó la presencia en el disco duro.

El virus **Tequila** infectó exitosamente el sector de partición y los archivos **KRNL386.EXE** y **COMMAND.COM**, cuando un programa infectado se ejecutó. Este virus se carga en memoria, únicamente cuando sé reenciende una PC infectada en su sector de partición. Aquí hay un problema, al hacer dicho reencendido; el sistema despliega un mensaje de error <*Windows protection error*> y <*Write Fault error writing device* AUX>, en sus sucesivas reencendidas.

### 11.5. *WINDOWS* 95 Y LOS MACROVIRUS[16]

Bajo *Windows* 95, los Macrovirus **Concept** y **Nuclear** se comportan de igual forma que en *Windows* 3.x.

PROTEJA LOS SISTEMAS

Cuando *Windows* 95 está corriendo, la utilería de Dr. Solomon's WinGuard (*programa que trabaja como un* **TSR**[3]), *proporciona una protección completa* contra las infecciones de virus. Cualquier *diskette* insertado en la PC, utilizando el *Explorer* o una sesión de *MS-DOS*, es revisado contra virus de sector de arranque, y los archivos son revisados al momento de ejecutarse o copiarse. Para protección adicional, el WinGuard, realiza un chequeo inicial de memoria cuando se carga. Es importante recordar que el sistema de *MS-DOS*, aún sigue siendo base para *Windows* 95, en algunos equipos. Si se presiona la tecla <Esc>, por ejemplo, durante el encendido de la máquina, el usuario verá como se carga un AUTOEXEC.BAT estándar. Esto se debe a que *MS-DOS*, es el sistema operativo activo hasta antes de cargarse *Windows* 95. De hecho, es posible encender la máquina desde *MS-DOS* ("*MS-DOS compatibility mode*"). Por tal motivo, se requiere de un *TSR*[3] para *MS-DOS*, que proporcione una protección "*ON-ACCES*", para *Windows* 95.

(16) Manual de Usuario. de Dr. Solomon's
(3) TSR = TERMINATE STAY RESIDENTE
Programa que reside en la memoria alta

*VirusGuard* (utilería de Dr. Solomon's), es el *TSR*[3] para *MS-DOS*, y es ejecutado desde el AUTOEXEC.BAT, proporcionando protección mientras está activo el sistema operativo *MS-DOS*, y hasta que *Windows* 95 es cargado, momento en el cual *WinGuard* entra en acción, si la máquina es ejecutada en modo de *MS-DOS*, *VirusGuard* entrará en acción.

En general, los virus del sector de arranque tienen la capacidad para replicarse e infectar bajo *Windows* 95 de forma tan eficiente como lo hacen bajo *MS-DOS* o *Windows* 3.x, lo que significa, que se requiere de una protección Antivirus del mismo tipo para dichas plataformas. Además, este tipo de virus representa aproximadamente el 70% de los virus reportados.

Esto también se aplica para los Macrovirus, cuyos objetivos son las aplicaciones como *Word* para *Windows* y no los sistemas operativos en sí.

### 11.5.6. ELIMINE ALGUNOS MACROVIRUS MANUALMENTE, EN WINDOWS 95[16]

Para ERRADICAR satisfactoriamente algunos MACROVIRUS, siga este procedimiento:

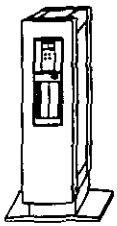
1. Es muy importante que elimine o borre, la plantilla global archivo "**NORMAL.DOT**", para obligar a *Word* a crear una nueva plantilla limpia la próxima vez que sea ejecutado. Sólo así, removerá la personalización de *Word* que le hacen los Macrovirus (Ya que el Macrovirus activo, desaparece del menú "**Herramientas**", la opción "**Macro**").

   **Nota.-** Es conveniente que cargue el **EXTRADRIVER** (utilería de Dr. Solomon's), en el archivo fuente del sistema Antivirus, esto provocará la eliminación automática del Macrovirus.

(16) Manual de Usuario, de Dr. Solomon's
(3) TSR = *TERMINATE STAY RESIDENTE*
Programa que reside en la memoria alta

# CAPITULO 12

# INSTALACIONES DE ANTIVIRUS EN REDES NOVELL, WINDOWS 3.X WINDOWS 95 Y WINDOWS NT



El Antivirus de Dr. Solomon's, está como un conjunto completo de herramientas para detectar y eliminar los virus conocidos y aún los desconocidos, las principales herramientas o utilerías que lo integran son: *Findvirus*, *Virusguard*, *Winguard*, y la Enciclopedia de los Virus y el INSPECT DISK.

## 12.1. REGLAS Y PROCEDIMIENTOS DE INSTALACION DE DR. SOLOMON'S POR MODULOS[16]

Los módulos puede adquirirlos por separado y tienen su propio método de instalación. A continuación se describen los procedimientos de instalación de algunos módulos.

(PRE-INSTALACION)

Antes de realizar la instalación de los módulos del Antivirus *Toolkit* de Dr. Solomon's para cualquier plataforma, es necesario verificar que la computadora "Destino", esté libre de virus. Para la instalación de cualquier módulo es MUY IMPORTANTE QUE VERIFIQUE QUE EXISTA EL ARCHIVO AUTOEXEC.BAT Y QUE NO TENGA ATRIBUTOS.

(16) Manual del Usuario de Dr. Solomon's

### 12.1.1. MODULO VIRUSGUARD PARA AMBIENTE *MS-DOS*[16]

Cuando usted adquiera este módulo, Dr. Solomon's le proporcionará un disco que contiene *Virusguard*, y el número máximo de instalaciones de este programa será el especificado en su licencia. A continuación se explica algunas características como:

1. *Virusguard* es un rastreador *TSR*[3] (programa centinela que residente en memoria para vigilar el acceso de un virus) de Dr. Solomon's. Ocupa únicamente 10KB de memoria y para su instalación basta con insertar en la unidad o *drive* A:\> el *diskette* de instalación de *Virusguard* y escriba el comando:

   **A:\>INSTALL**

2. El procedimiento instalará *Virusguard* en su PC; se modificará el AUTOEXEC.BAT del sistema y se cargará el programa en modo de seguridad ESTANDAR (que es la recomendada).
3. A continuación se le preguntará si desea cancelar la instalación o continuar con ella, presione *Enter* para confirmar la instalación. *Virusguard*, no podrá ser descargado de la memoria mediante comandos. Siempre estará rastreando por virus, ya que es el vigilante permanente de Dr. Solomon's. Si por alguna razón no desea que *Virusguard* se ejecute, elimine la referencia al mismo en el archivo AUTOEXEC.BAT, apague su PC y vuelva a encenderla.

### 12.1.2. MODULO WINGUARD EN WINDOWS 3.X[16]

1. *Winguard* es un rastreador (On-Access) tipo VxD[27] (un archivo VxD en *Windows* es como un *TSR*[3] en *MS-DOS*), de Dr. Solomon's. Funciona únicamente bajo *Windows* y proporciona una protección eficaz contra virus ya que puede autoreparar archivos, o discos infectados, sin necesitar de la intervención del usuario. Técnicamente, es un "*driver*" virtual nativo de 32 bits de *Windows*, que se ejecuta siempre en segundo plano (*background*[31]). Para su instalación basta con insertar en la unidad de discos flexibles, el disco de instalación de *Winguard* y teclear bajo una sesión MS-*DOS*.

(16) Manual del Usuario de Dr. Solomon's
(3) TSR = *TERMINATE STAY RESIDENTE*
Programa que reside en la memoria alta

Este procedimiento instalará *Winguard* en la PC; y se modificarán los archivos WIN.INI y SYSTEM.INI de *Windows* 3.X.

2. A continuación se le preguntará si se desea cancelar la instalación o continuar con ella. Presione *Enter* para confirmar la instalación.

### 12.1.3. MODULO WINGUARD PARA (WINDOWS 95)[16]

- *Winguard* es un rastreador, *ON-ACCESS*, VxD[27] de Dr. Solomon's, que funciona únicamente bajo *Windows* y proporciona una protección eficaz contra virus, y trabaja de forma transparente para el usuario. Además de ser un *driver* virtual *nativo* de 32 bits que se ejecuta siempre en segundo plano. Para su instalación basta con insertar en la unidad de discos flexibles, el disco de instalación de *Winguard* y teclear bajo una sesión *MS-DOS*:

**A:\> INSTALL**

- Este procedimiento, instalará *Winguard* en las PC´s, autorizadas. Se modificarán los archivos **WIN.INI**, **SYSTEM.INI** y los registros del sistema.
- Es importante aclarar que desde la versión 7.68, *Winguard* puede auto-desinfectar archivos, y desde la versión 7.71 también puede limpiar discos infectados en sector de arranque, sin necesitar de la intervención del usuario.

## 12.2. NIVELES DE SEGURIDAD Y PROTECCION DE DR. SOLOMON'S[16]

Al realizar la instalación de *Toolkit*, ya sea de forma completa o modular, el proceso solicitará al usuario que elija el nivel de seguridad, estos son:

MINIMA, ESTANDAR Y MAXIMA

### 12.2.1. NIVEL DE MINIMA SEGURIDAD

Este nivel se recomienda para computadoras de baja capacidad (XT´s o 286, por ejemplo)

Con esta configuración, *Virusguard* rastrea por virus en:

- El sector de arranque de los *diskettes* flexibles.

(16) Manual del Usuario de Dr. Solomon's
(27) *VxD = Virtual Drivers of Windows 95*

- Todos los archivos ejecutables que son copiados desde discos flexibles.
- Todos los archivos que se ejecuten.

Para indicar este nivel de seguridad, *Virusguard* deberá quedar de la siguiente forma en el archivo AUTOEXEC.BAT, como:

**C:\>TOOLKIT\GUARD /COPY=FLOPPY**

### 12.2.2. SEGURIDAD ESTANDAR (*STANDART SECURITY*)[16]

Este es el nivel de seguridad recomendable para la mayoría de los usuarios. En este nivel, *Virusguard* rastrea por virus en:

- El sector de arranque de los disco flexibles
- Los archivos ejecutables cuando sean copiados
- Todos los archivos que sean ejecutables.

Para indicar este nivel de seguridad, *Virusguard* deberá quedar de la siguiente forma en el archivo AUTOEXEC.BAT, como:

**C:\>TOOLKIT\GUARD**

### 12.2.3. SEGURIDAD MAXIMA (*MAXIMUM SECURITY*)[16]

Este nivel de seguridad, Dr. Solomon's lo recomienda, solamente cuando se bajan archivos desde BBS's[6] y de Internet, o cualquier otro servicio en línea.

En este nivel, *Virusguard* rastrea por virus en:

- El sector de arranque de los discos flexibles
- Todos los archivos que sean copiados
- Todos los archivos que sean escritos al disco
- Todos los archivos que se ejecuten

(16) Manual del Usuario de Dr. Solomon's

Esta opción ofrece gran seguridad, sin embargo puede resultar una reducción en el rendimiento del sistema. Para seleccionar este nivel de seguridad, *Virusguard* deberá quedar de la siguiente forma, en el archivo AUTOEXEC.BAT, como:.

**C:\TOOLKIT\GUARD /COPY=ALL /WRITE=ALL**

## 12.3. SI ENCUENTRA UN VIRUS AL EFECTUAR LA INSTALACION[16]

Es muy importante mantener la calma y seguir estos los siguientes pasos, al tratar de eliminar algún virus:

Si el virus que debe eliminar es el **Dir.Byway**

1. Apague completamente la computadora.
2. Inserte un *diskette* de arranque con Sistema Operativo (libre de virus), protegido contra escritura en la unidad de disco flexibles **A:\>** Este *diskette* debe ser de la misma versión de Sistema Operativo que tenga instalada en el disco duro. Si tiene alguna unidad comprimida o algún *hardware* especial, el disco de arranque deberá contener los "*drivers*" necesarios.
3. Arranque la computadora, una vez que aparezca el simbolo **A:\>**, remueva el disco de sistema e inserte el disco de instalación del sistema *Toolkit* de Dr. Solomon's, que contenga el comando **FINDVIRU.EXE** (generalmente localizado en el disco 2 para MS-*DOS*) y escriba desde el indicador de sistema:

   **C:\>FINDVIRU /LOCAL** y oprima *Enter*
4. Esta operación, revisará las unidades locales por virus conocidos. Si *Findvirus* le reporta el virus **Dir.Byway**, consulte como eliminar el virus **Dir.Byway** ya explicado en Capítulo 2. Con cualquier otro virus, por favor revise los siguiente métodos tres métodos de reparación.

- **METODO 1.-** Para virus de archivos ejecutables de sector de arranque y de sector de partición.

1. Con el mismo *diskette* No. 2, de "Instalación", escriba en el indicador de sistema:

   **C:\>FINDVIRU /LOCAL /DOALLFILES /REPAIR**

(16) Manual del Usuario de Dr. Solomon's

2. Este comando revisará las unidades locales por virus conocidos, reparando tanto los archivos infectados como los sectores de arranque y sector de partición.
3. Aquellos archivos que no puedan ser reparados por *Findvirus*, automáticamente serán renombrados. Por ejemplo, supongamos que el archivo infectado y que no pudo ser reparado, sea el COMMAND.COM, entonces será renombrado así: COMMAND.VOM, esto es; *Findvirus* antepone la letra "V" (de virus) a la extensión del archivo.
4. Al llegar a este punto todas las unidades locales ya estarán libres de virus.

- **METODO 2.-** Para archivos ejecutables normales que no se puedan reparar.

1. Use el *diskette* No. 2 de instalación del sistema *Toolkit*, escriba en el indicador:

**C.:\>FINDVIRU /LOCAL /DOALLFILES /OC /REPAIR**

2. Con el parámetro **/OC**, *Findvirus* repara aquellos archivos que hayan sido mal infectados o que hayan sido mal reparados por otros Antivirus.

- **METODO 3.-** Para los virus de sector de arranque y de sector de partición exclusivamente. Para reparar cualquier tipo de virus, siempre se recomienda utilizar el MÉTODO 1, ya descrito; sin embargo, dicha método no siempre funciona frente a los virus de sector de arranque y partición demasiado complejos, por lo que se sugiere este tercer método:

1. Ejecutar la utilería CLEANBOOT, para remover virus del sector de arranque de *diskettes* flexibles infectados. Este programa se encuentra en el disco No. 1, del sistema *Toolkit* para MS-*DOS*. Debe teclear desde el disco flexible lo siguiente:

**A:\>CLEANBOOT**

2. Ejecute CLEANPART, para remover el virus del sector de arranque y sector de partición de discos duros teclee desde el indicador de sistema, así:
   - Para reparar el sector de partición: **A:\>CLEANPART 128 /F**
   - Para reparar el sector de arranque: **A:\>CLEANPART 128 /H**

3. Procure tener preparado un *diskette* flexible limpio y formateado, por que el comando CLEANPART, lo requerirá para hacer una copia de seguridad de los sectores que vaya a reemplazar o reparar.

## 12.4. INSTALACION COMPLETA[16]

A continuación se describe la instalación completa de las plataformas más comunes. Antes de realizar la instalación del Antivirus *Toolkit* de Dr. Solomon's en cualquier plataforma, es necesario verificar que la computadora "Destino" esté libre de virus, realizando los siguientes pasos:

1. Apague la computadora
2. Inserte un disco de arranque o de sistema de MS-*DOS*, libre de virus y protegido contra escritura en la unidad **A:\>** , este *diskette* de sistema, debe ser de la misma versión del MS-*DOS*, que se tiene instalada en el disco duro. Si se tiene alguna unidad comprimida o algún *hardware* especial, el disco de arranque deberá tener los "*drivers*" necesarios.
3. Arranque la PC, una vez que aparezca el prompt **A:\>**, remueva el *diskette* de sistema y reemplácelo por el disco de instalación del *Toolkit* que contenga el archivo **FINDVIR.EXE** (generalmente localizado en el disco No. 2 para MS-*DOS*), y escriba en el indicador de sistema, así:

   **C:\>FINDVIRU /LOCAL** y oprima *Enter*

4. Este comando revisará las unidades locales por virus conocidos. Si *Findvirus* le reporta un virus, intente eliminar el virus para después seguir con la instalación.
5. Cuando esté seguro de que la PC de "Destino" está libre de virus, siga las indicaciones correspondientes en el apartado de la plataforma instalar.

### 12.4.1. INSTALACION DEL ANTIVIRUS DR. SOLOMON'S EN MS-*DOS*[16]

1. Inserte el *diskette* No. 1 de instalación del Antivirus *Toolkit* para MS-*DOS*. Del: C:\>, cambie al prompt A:\> y escriba: **A:\>INSTALL**

(16) Manual del Usuario de Dr. Solomon's

2. A continuación, aparecerá la pantalla donde el *Toolkit* muestra el espacio disponible y el espacio requerido. La instalación para *MS-DOS* requiere de aproximadamente 2.5 MB de espacio en disco duro.
3. El *Toolkit*, se instalará en la unidad C:\> a menos que usted especifique lo contrario. Seleccione la unidad deseada y presione *Enter*.
4. A continuación el sistema le pedirá que seleccione el directorio de destino. La opción predeterminada es el directorio: **C:\>TOOLKIT,** en caso de que desee instalar el *Toolkit* en un directorio distinto al especificado, escriba la ruta completa y presione la tecla *Enter*.
5. Ahora se iniciará la instalación.
6. Una vez terminado el proceso de copiado de los archivos al disco duro, el proceso de instalación le preguntará, si se desea habilitar el *Virusguard*, mostrado en la siguiente pantalla.
7. En la mayoría de las instalaciones, se recomienda contestar *sí* (Y), ya que Virusguard es parte fundamental de la detección de virus. Sin embargo; en las computadoras 286 o anteriores, ésta medida puede afectar el desempeño (volviéndolas lentas).
8. En caso de haber respondido afirmativamente, el sistema le preguntará por el nivel de seguridad deseado *Virusguard* tiene tres niveles de seguridad:

SEGURIDAD MINIMA Con este nivel, *Virusguard* rastreará virus en:

- Los archivos ejecutables que sean copiados desde discos flexibles.
- Todos los archivos que sean ejecutados en todos los casos, cuando se rastrea por virus, Dr. Solomon's considerará como archivos ejecutables, aquellos que tengan las siguientes extensiones:

APP, OVL, BIN, OVR, COM, EXE, SCR, DLL, SYS, DOC, DOT, XTP

- El sector de arranque de los discos flexibles.

SEGURIDAD ESTANDAR.- Con este nivel *Virusguard*, rastreará virus en:

- El sector de arranque de los *diskettes* flexibles.

- Los archivos ejecutables cuando sean copiados.
- Todos los archivos que intenten ejecutarse.

SEGURIDAD MAXIMA.- En este nivel *Virusguard*, rastreará virus en:

- Todos los archivos que sean copiados
- Todos los archivos que se ejecuten
- El sector de arranque de los *diskettes* flexibles
- Todos loa archivos que sean escritos al disco

9. Al final del proceso de instalación se ejecutará *Findvirus* en forma automática buscando por virus.

### 12.4.2. INSTALACION DEL ANTIVIRUS DE DR. SOLOMON'S EN WINDOWS 3.X / MS-DOS[16]

**Nota**: No intente instalar el *Toolkit* dentro de *Windows*. La instalación se debe realizar bajo MS-*DOS*.

1. Salga al indicador del sistema de *MS-DOS*, inserte el disco de instalación del Antivirus *Toolkit* para *Windows* y escriba desde el indicador de sistema:

   **A:\>SETUP** y presione *Enter*

2. Lo que resta, es seguir las indicaciones del proceso de instalación del *Toolkit* (consulte la sección anterior **(12.4.1.)** Para mayor referencia).
3. Al realizar la instalación de AVTK (Antivirus *Toolkit*) para *Windows*, también quedará instalado para *MS-DOS*.

### 12.4.3. INSTALACION DEL ANTIVIRUS DR. SOLOMON'S EN *WINDOWS* 95[16]

1. Verifique que la computadora esté libre de virus siguiendo las instrucciones comentadas para el uso del disco Magic Bullet[32]
2. En *Windows* 95, inserte en la unidad de 3.5" el disco de instalación del Antivirus *Toolkit* para *Windows* 95, etiquetado con "Installation Disk".

*(16) Manual de Usuario, de Dr. Solomon's*
(32) MAGIC BULLET (ver sección 3.4.7.)

3. Haga *click* en el botón "**Inicio**" y seleccione "Configuración", inmediatamente después de un "*click*" en "**Panel de Control**".
4. Cuando esté en la pantalla del "**Panel de Control**", haga doble *click* en el icono "**Agregar o Quitar Programas**", una vez ahí, dé un *click* en el botón de "**Instalar**" y después de otro *click* en "**Siguiente**".
5. Cuando el programa haya detectado el disco flexible correcto en la unidad A:\> de un click en "**Finalizar**".
6. Ahora confirme la instalación del Antivirus *Toolkit* para *Windows* 95. Presione la tecla *Enter* para seguir con la instalación.
7. El *Toolkit* será instalado en la unidad **C:\>** en la carpeta predeterminada, a menos que usted especifique otro destino.
8. Se iniciará el proceso de instalación. Se le pedirá que inserte los discos de instalación subsecuentes. En cualquier momento usted puede cancelar el proceso presionando la tecla ESC. En otro caso, al reinstalar nuevamente el *Toolkit,* asegúrese de borrar todos los archivos que se encuentren en la carpeta de instalación (que se copiaron en el proceso que fue interrumpido). Es muy importante asegurarse de que la opción deseada fue seleccionada correctamente y después presionar la tecla *Enter*. El proceso de instalación copiará los archivos necesarios de los discos flexibles al disco duro, modificando además los archivos de *Windows* 95 y agregando las líneas necesarias para que se cargue adecuadamente el *Toolkit*.
9. A continuación el proceso le pedirá elegir entre instalar *Virusguard* o no. En el caso de que decida instalar *Winguard*, tendrá que elegir entre los dos niveles disponibles para *Windows* 95, Minima Seguridad o Seguridad Estándar.

   **Nota**: No debe usar *Virusguard* sin utilizar *Winguard*.
10. Inmediatamente después, se le preguntará si desea ejecutar Dr. Solomon's Scheduler, cada vez que se inicie *Windows* 95. Esta herramienta es un residente en memoria que le permite programar el rastreo por virus y la ejecución de otros programas o un determinado tiempo. Si contesta afirmativamente se agregará un

icono al menú "**Inicio**" y a partir de este momento, **SCHEDULER** se ejecutará siempre que se inicie *Windows* 95. En caso contrario, cuando desee ejecutar Dr. Solomon's **SCHEDULER**, lo podrá hacer directamente desde el menú de Dr. Solomos Antivirus *Toolkit*.

11. Al terminar la instalación aparecerá un mensaje de confirmación informándole que *Toolkit* ya está instalado. Bastará con dar un "click" en "**Aceptar**" para que automáticamente se ejecute *Findvirus* y revise por virus en los discos duros locales. Si la PC está libre de virus, se le mostrará una pantalla de confirmación similar a la siguiente.

> **Nota**: Si el reporte le indica que algunos archivos no fueron rastreados, esto se debe a que en forma predeterminada, el *Toolkit* únicamente rastrea los archivos ejecutables que pueden llevar un virus como: **(EXE, COM, DOC, DOT, APP, BIN, DLL, OVL, OVT, SCR, SYS y XTP).**

### 12.4.4. INSTALACION DEL ANTIVIRUS DR. SOLOMON'S EN *WINDOWS* NT[16]

La instalación del Antivirus *Toolkit* para *Windows* NT Server, se debe realizar en el mismo servidor, además, deberá realizarla con derechos de administrador.

En el caso de que se vaya a actualizar una versión igual o anterior a la 7.56, es necesario seguir los siguientes pasos antes de continuar con la instalación:

- Borre el elemento SCHEDULER del grupo de programas "Dr. Solomon's **AVTK NT**", si está presente.
- Busque el directorio del *Toolkit* (usualmente **WIN32APP\TOOLIT**) y borre el archivo **TK_SCHED.EXE**

Las instrucciones para la instalación de *Windows* NT *Workstation* son:

1. Conectarse al servidor.
2. Inserte el disco flexible de instalación del Antivirus *Toolkit* para *Windows* NT.

(16) Manual del Usuario de Dr. Solomon's

3. Seleccione en el menú "**Archivo**" del "**Administrador de Programas**" y haga click en la opción "**Ejecutar**".
4. Escriba **A:\>SETUP** y presione la tecla *Enter*. A continuación se le pedirá que confirme el directorio de instalación de *Toolkit*. Si desea seleccionar un directorio diferente al especificado, escríbalo y presione *Enter* para que el sistema verifique la ruta indicada.
5. A continuación el sistema le pedirá los discos flexibles de instalación restante. Puede cancelar la instalación en cualquier momento presionando la tecla ESC. En caso de cancelar el proceso, deberá borrar todos los archivos del directorio en el que se crearon durante la instalación abortada, para que pueda instalar el producto nuevamente.
6. Después se le solicitará la confirmación para instalar Dr. Solomon's SCHEDULER. Esta herramienta, es un programa residente en memoria que le permite programar el rastreo por virus y la ejecución de otros programas, en un tiempo determinado. Por ejemplo, es posible programarlo para que *Findvirus* se ejecute cada semana y busque por virus en los discos duros.
7. La siguiente ventana le pedirá confirmación para la instalación de *Winguard* NT. Se recomienda, por supuesto, que el usuario conteste afirmativamente a esta pregunta, ya que de esta forma estará protegiendo su servidor de una infección masiva de virus.
8. Al término de la instalación, se ejecutará de forma automática Dr. Solomon's *Findvirus*, buscando protección virus en las unidades locales. Si la computadora esta libre de virus, aparecerá una ventana similar a la siguiente.

   **Nota**: el reporte indica que algunos archivos no fueron rastreados esto se debe a que en forma predeterminada. *Toolkit* sólo rastrea los archivos ejecutables **(EXE, COM, DOT, APP, BIN, DLL, OVL, OVR, SCR, SYS y XTP).**

## 12.4.5. INSTALACION DEL ANTIVIRUS DR. SOLOMON'S EN NOVELL[16]

(ANTIVIRUS NOVELL AVTK PARA NETWEARE 3.X)

1. Conéctese a la Red con derechos de supervisor. Se recomienda utilizar el comando ATTACH en lugar de LOGIN, ya que este último activa el "login script" del usuario y se corre el riesgo de ejecutar algún archivo infectado:

   **C:\>ATTACH USER**

2. Inserte el disco de instalación No. 1" del *Toolkit* para NetWare y escriba el comando en el símbolo del sistema, así:

   **A:\>INSTALL [RUTA] 3**

   Por ejemplo: INSTALL :SYSTEM 3

   Los archivos existentes en el directorio de destino, que sean iguales a los dos discos de distribución, serán actualizados y se copiarán los archivos que no existan en el directorio de destino.

3. Después del paso anterior, es necesario copiar el editor de la configuración llamado **NTKEDIT.EXE** al directorio de *Windows* y crear, por supuesto, un nuevo elemento para este programa.
4. Para finalizar el proceso, cargue el Antivirus desde la consola del servidor con el comando:

   **:LOAD N*TOOLKIT***

   **Nota.-** Para NetWare 3.x, será necesario contar con el módulo **CLIB 3.12g** o superior. Esta biblioteca está disponible en el Forum de Novell, en Compuserve o en su página WWW en *http://www.novell.com*

(ANTIVIRUS *TOOLKIT* PARA NETWARE 4.X)

1. Primero deberá crear la cuenta: DRSOLOMON (sin password) con el NetAdmin para ser utilizada con el Conection Monitor del Scheduler. Esta cuenta le será solicitada cuando se cargue el Antivirus.
2. Conéctese a la red e inmediatamente después vaya a la unidad por default de NetWare y configure el texto del Admin. Por ejemplo, en la unidad **O:**, si el

contexto está definido como: **CN=Admin.O=orgname**, donde "**organme**" es el nombre de la organización, entonces se deberá escribir: **CX orgname** y *Enter*.

3. Escriba LOGIN SERVER /ADMIN /NS para conectarse el servidor como Administrador.
4. Inserte el disco de instalación No. 1 del sistema *Toolkit* para NetWare y escriba:

**A:\>INSTALL [RUTA]4**

Por ejemplo: **INSTALL O:SYSTEM4**

Los archivos existentes en el directorio destino que sean iguales a los de los *diskettes* de distribución, serán actualizados y los archivos que no existan en el directorio "**Destino**", serán copiados de los discos.

5. Después del paso anterior, copie el editor de la configuración llamado **NTKEDIT:EXE**, al directorio de *Windows*, creando un nuevo elemento para este programa.
6. Para finalizar el proceso, se tiene que cargar el Antivirus desde la consola del servidor, tecleando:

**:LOAD NTOOLKIT**

**TIP**

Si desea encender un servidor NOVELL sin que éste ejecute el archivo **AUTOEXEC.NCF** o el **STARTUP.NCF**, siga los pasos siguientes:

- SERVER–NS (para que inicie el servidor sin ejecutar STARTUP.NCF)
- SEVER–NA (para que inicie el servidor sin ejecutar AUTOEXEC.NCF)
- Prepárese y tenga a la mano el nombre del servidor y la dirección IP.

## 12.5. CONSEJOS IMPORTANTES PARA NT SERVER EDITION[16]

El sistema *Toolkit* Antivirus desarrollado por Dr. Solomon's para servidores *Windows* NT, incorpora una nueva tecnología denominada "***Managent Edition***". Con esta herramienta, usted podrá instalar, configurar, actualizar y eliminar las aplicaciones del Antivirus en estaciones remotas que estén en red. Usted puede controlar todas estas actividades desde una Consola de Administración, o dentro de una aplicación "*Drag-and-drop*", que se ejecute en ambiente de *Windows* NT o *Windows* 95. El Antivirus *Toolkit* le ayudará a reducir tiempo que usted invierte en la administración de la red cuando realiza instalaciones y mantenimiento al *software* Antivirus, especialmente cuando se trata de redes de gran tamaño. Una ventaja adicional es que todas las tareas se manejan de la misma forma en todas las diferentes plataformas, lo que significa que invertirá menos tiempo en aprender nuevos sistemas. Además le permitirá contar con un centro automatizado de alertas de virus, para notificar al administrador acerca de los problemas que hayan ocurrido en máquinas remotas. Estas alertas pueden ser enviadas por correo electrónico, por la red pueden ser impresas o almacenadas en una bitácora, o silo prefiere, pueden ser alertas SNMP o ser enviadas a un pager (*Beeper*). Usted puede instalar Dr. Solomon's Antivirus *Toolkit* para servidores *Windows* NT, sobre el disco duro local de la estación de trabajo del administrador par tal efecto, usted necesitará tener una cuenta de tipo *Windows* NT *Domain Administrator*.

### 12.5.1. CONSEJOS IMPORTANTES VIRUS BAJO *WINDOWS* NT[16]

No es novedoso saber que *Windows* NT se vuelve cada día uno de los sistemas operativos para servidores más utilizados en la actualidad, evidentemente, NT es un sistema operativo con estructura lógica para almacenar la información en el disco duro, diferente a la de *Windows* 95 y *MS-DOS*, la cual se conoce como **NTFS NT** File System. Este tipo de diferencias puede llegar a provocar que algunos virus funcionen de forma distinta a como deberían de hacerlo en el sistema operativo para el cual fueron programados.

(16) Manual del Usuario de Dr. Solomon's

## 12.5.2. CONSEJOS IMPORTANTES VIRUS DE SECTOR DE ARRANQUE (BOOT VIRUSES)[16]

Bajo un arranque normal, NT impide que se escriba información al track 0 del disco duro, además de proteger de igual forma el sector de arranque. En teoría, esto debería evitar que un virus de sector de arranque infecte el disco duro de NT, dado que este tipo de virus escribe al MBR (*Master Boot Record*) o al sector de arranque del disco duro.

Esta medida debería ser suficiente; sin embargo, hay que recordar que NT, activa esta protección una vez que el sistema está corriendo, y que los virus de sector de arranque infectan desde el BIOS antes de que arranquen el sistema operativo, por lo que si un usuario olvida un disco infectado en la unidad "A:\>" y reinicia, el virus escribirá su código en el sector de partición o de arranque. La protección de NT, sólo sirve para programas que pueden llevar a cabo esta operación después de arrancar el sistema. De cualquier forma, los virus de sector de arranque funcionan como TSR[3], en tiempo real, y NT es un sistema operativo que corre en modo protegido, por lo que este tipo de virus no podrá operar de esta forma.

La consecuencia es obvia: una vez que la PC infectada haya sido reiniciada, el virus no estará activo en memoria y, por lo tanto, no infectará otros discos que sean usados en la PC definitivamente, todo indica que el constante crecimiento del uso de NT hará que el número de virus de sector de arranque disminuya; sin embargo, hay que tomar en cuenta que las PC que corren NT, están expuestas a cualquier manifestación destructiva de algún virus de este tipo. Por ejemplo, el virus "**Telefónica**", el cual arruina el disco después de que se ha iniciado la máquina 400 veces, puede ser ejecutado, ya que el daño será llevado a cabo antes de que el sistema operativo arranque, usando el *BIOS* para escribir al disco duro.

Por todas estas razones, es importante que las PC corriendo a *Windows* 95 estén protegidas contra cualquier virus.

(16) Manual del Usuario de Dr. Solomon's
(3) TSR = TERMINAL STAY RESIDENTE

### 12.5.3. CONSEJOS IMPORTANTES VIRUS DE ARCHIVO EJECUTABLE *(EJECUTABLE FILE VIRUSESS)*[16]

Existen varios virus que infectan archivos ejecutables de *Windows* NT y 95 (PE *Portable Executables*), los cuales evidentemente son de 32 Bits. Dos claros ejemplos de este tipo de virus son "**Boza** y **Semisoft**". De cualquier forma, los virus específicos para infectar *Windows* son de acción directa, es decir, que no permanecen residentes en memoria, sino que infectan otros archivos cuando se ejecuta un programa infectado, lo cual disminuye su capacidad de infección, a diferencia de los que permanecen residentes en memoria, los cuales interceptan las diferentes funciones del sistema operativo. Muchos virus de archivo fueron creados para que actúen como residentes en memoria, es decir, como TSR[3], lo cual limita su actividad para infectar bajo *Windows* NT. Si un programa infectado con uno de estos virus (**Jerusalem**, **Cascade**, **Yankee** y **Doodle**, etc.), es ejecutado bajo una ventana de comando de *Windows* NT, sólo infectará otros archivos de 16 bits que sean ejecutados bajo la misma sesión, es decir; que no contaminará el ambiente NT, invitando así que otros programas (bajo otras sesiones) sean infectados. No sería inconcebible que en el futuro los virus sean creados para monitorear o interceptar de forma activa el disco o la actividad de los archivos en el disco, y definitivamente este tipo de virus sería muy exitoso. Ya vimos el intento (fallido) de un virus que opera como un VxD[27] bajo *Windows* 95. Es probable que los virus de archivos comiencen a desaparecer poco a poco, ya que el mundo empresarial y los usuarios caseros tienden a dejar de utilizar sistemas operativos basados en *MS-DOS*.

### 12.5.4. CONSEJOS IMPORTANTES MACROVIRUS EN WINDOWS NT[16]

Los Macrovirus, representan un gran riesgo para el usuario de *Windows* NT, ya que son virus multiplataformas que atacan sin importar el sistema operativo. Este tipo de virus ha tenido un crecimiento impresionante, desde la aparición del Macrovirus (**WM/CONCEPT**, en Julio de 1995) hasta el momento se han reportado casi 2000 Macrovirus. Los Macrovirus, son el tipo de virus más reportado en la actualidad y

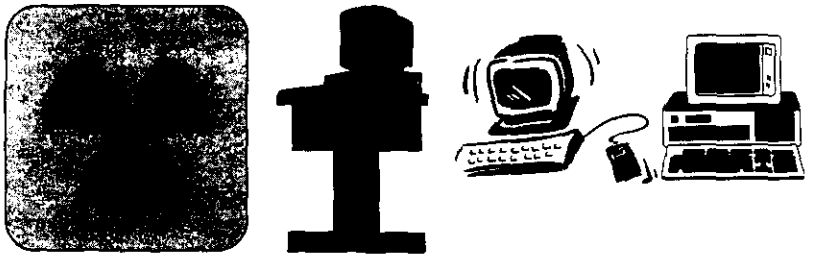
(16) Manual del Usuario de Dr. Solomon's
(27) VxD = Virtual Drivers of Windows 95
*(3) TSR = TERMINATE STAY RESIDENT*
Programa que reside en la memoria alta

representan la mayor parte de los virus registrados en el Departamento de Soporte Técnico de Dr. Solomon's. Pese a que la mayoría de los Macrovirus no dañan información, hay virus que lo hacen como el Macrovirus **WM/MDMA**; sin embargo, existe una limitante para algunos de estos virus, principalmente aquellos que hacen llamadas directamente al sistema operativo, como es el caso de Macro troyano (**WM/FormatC**); este tipo de virus, se verá limitado a afectar únicamente los sistemas operativos para los cuales fueron diseñados. El virus **WM/MDMA,** resuelve esta situación de manera exitosa, ya que tiene manifestaciones diferentes para cada sistema operativo, bajo el cual puede ser ejecutado. Los Macrovirus no son exclusivos de *Microsoft Word for Windows*. En Enero de 1996 se encontró el primer Macrovirus que infecta archivos de *Lotus AmiPro* (*APM/GreenStripe*). A diferencia de *Word* para *Windows*, en el cual los Macros están directamente integrados a los documentos y las plantillas, los Macros de *AmiPro* se almacenan en un archivo por separado, lo cual hace posible intercambiar documentos de *AmiPro* por ejemplo; por correo electrónico sin intercambiar macros infectadas, por esta razón es que los Macrovirus de *AmiPro,* no son tan populares. De cualquier forma hemos visto virus que infectan archivos de *Microsoft Excel for Windows* (el primer espécimen de éstos fue **Xm/Laroux**, el cual apareció en julio de 1996). No se requiere mucha imaginación para pensar, en las posibles consecuencias de los Macrovirus que pueden surgir debido a una hoja de cálculo modificada por un virus. Pensando un poco en el futuro *Microsoft Office* 97 abre la posibilidad de virus que infecten las macros de *Microsoft Power Point*. Los Macrovirus se han vuelto populares y un riesgo potencia debido a varias razones: Los Macrovirus que infectan *Word* o Excel están escritos en *Word Basic*. Crear un Macrovirus es muy sencillo, mucho más sencillo que escribir un virus de archivo, por ejemplo, ya que este lenguaje es fácil de aprender y accesible para cualquier persona que cuente con estas aplicaciones de *Microsoft*. Estos virus infectan documentos, archivos de datos, lo cual les da una mejor forma de replicación, ya que es más común que se intercambien de un documento a un archivo ejecutable. Además, hay que tomar en

cuenta que el desarrollo de Macrovirus ha evolucionado en paralelo al extendido uso del correo electrónico, lo cual abre las puertas a los creadores de virus para distribuir su trabajo de forma prácticamente transparente para los usuarios. Los Macrovirus no afectan una plataforma específica, ya que hay versiones de *Word* For *Windows* para *Windows* 3.x *Windows* 95, *Windows* NT e incluso *Macintosh*, lo cual hace que cualquiera de estos sistemas operativos sean vulnerables a sufrir el ataque de un Macrovirus.

# CAPITULO 13

## ESTRATEGIAS Y REGLAS APLICADAS EN UN CENTRO DE COMPUTO



### 13.1. SUGERENCIA , ANTES DE APLICAR LA ESTRATEGIA

Necesita la colaboración desinteresada de los usuarios para llevar a cabo una política Antivirus. Si el personal considera que va a ser sancionado al descubrir un virus, es poco probable que informe de cualquier anomalía. Puede resultar útil dar a una persona o a un grupo pequeño la responsabilidad de verificar y distribuir el *software*.

### 13.2. DR. SOLOMON'S SUGIERE AFINACION DE LA COMPUTADORA[16]

En máquinas que tengan poca capacidad de memoria no se recomienda instalar VirusGard (*MS-DOS*) y/o *Winguard* (*Windows*), porque pueden bajar el desempeño de la computadora. En la mayoría de los casos, el Antivirus de Dr. Solomon's no causará ningún problema; sin embargo existe dicha posibilidad, por lo que sí llegara a sucederle, tome en consideración lo siguiente:

- No instale *Virusguard* en Máxima Seguridad.

(16) *Manual del usuario* de Dr. Solomon's
(26)Peter Norton Solución a Problemas de PC
Peter Norton & Robert Jourdain
ED. PRENTICE HALL

- No ejecute *Findvirus* cada vez que se encienda la computadora.

- No instale únicamente *Virusguard* cuando se tiene la posibilidad de instalar también *Winguard*. En ocasiones, una vez instalado *Virusguard* y *Winguard*, aparecerá un mensaje de error al intentar cargar *Windows* 3.X, indicándole que no hay suficiente memoria para cargar la base de datos *Virusguard*. (Este archivo es el *driver* de la base de datos sobre virus que utiliza el *Winguard* y que debe cargarse en memoria para que funcione correctamente este último). Esta base de datos se incrementa a razón de 10 Kb por mes aproximadamente y esto se debe a que constantemente aparecen nuevos virus. La solución ideal, es que debería ser incrementar la cantidad de memoria RAM en su computadora, al menos a 6 Mb (aunque 8MB un poco mejor). Una solución alternativa para este problema, es remover las innovaciones al SMARTDRIVE de *MS-DOS* en el AUTOEXEC.BAT, para tratar de liberar memoria, o bien, cargar la base de datos sobre virus en el disco y no en la memoria, esto se logra modificando la línea correspondiente del archivo **AUTOEXEC.BAT**, de la siguiente manera:

**C:*TOOLKIT*\GUARD /MODE=DISK**

- Si decide ya no usar el SMARTDRIVE, esto no debería impactar en el rendimiento de *Windows* 3.11, dado que este tiene su propio caché (llamado "*Vcache*") y mientras más pequeña sea la cantidad de memoria destinada al "Vcache", mayores serán las probabilidades de que no ocurra ningún problema. Si usted está trabajando en *Windows* 3.1, no podrá eliminar el SMARTDRIVE, sólo podrá reducirlo al mínimo usando el comando: **SMARTDRV/X 128**

### 13.2.1. REQUERIMIENTOS DE MEMORIA[16]

- *Virusguard* (Estándar) 10KB
- *Virusguard* (Netware) 13KB
- *Virusguard* (nuevas versiones con XMS) 7.9KB
- *Virusguard* (nuevas versiones sin XMS) 15KB

(16) Manual del usuario de Dr. Solomon's

- *Findvirus* (FV86.exe) 350KB
- *Findvirus* (FV386.exe) 1MB
- *Winguard* 350KB
- *Toolkit* para *MS-DOS* 365KB

- **FB386.EXE**[37] utiliza alrededor de 1MB en memoria.
- *Winguard* utiliza alrededor de 350 KB de la memoria de *Windows* (memoria extendida-XMS).

## 13.3. GUIA GENERAL DE CONFIGURACION DEL ANTIVIRUS MCAFEE, SOPORTE REQUERIDO[17]

Antes de pasar a las guías de optimización de *Windows*, primero de deberá definir una configuración base. Verifique los archivos de configuración del sistema y revise los siguientes componentes para determinar si realmente se están utilizando o no, en caso de que no se estén utilizando, entonces se pueden remover para optimizar la configuración.

Los "*tips*" siguientes suponen un escenario *Windows* 3.11:

1. Computadora "*Stand Alone* " (sin red).
2. Computadora como cliente pero sin compartir ningún archivo.
3. Computadora como cliente y servidor.
4. Computadora como un servidor dedicado.

Adicionalmente a estos escenarios, también se dan algunas guías de configuración que se aplican de manera general a *Windows* 3.11, para permitirle sacar el máximo provecho de ellos.

### 13.3.1. SHARE.EXE[33]

SHARE es un TSR[3] de *MS-DOS*, que permite bloquear y compartir archivos cuando se están corriendo aplicaciones de MS-*DOS*. *Windows* para trabajo en

(17) Manual de Usuario de Mcafee
(33) SHARE.EXE.- Archivo del sistema Ms-DOS
(37) FB386.EXE.- Archivo del sistema de Dr. Solomon's

Grupo. proporciona un VxD[27] (Dispositivo manejador de memoria virtual). llamado **VSHARE.386**[34], que proporciona la misma funcionalidad del **SHARE.EXE**[33], pero *sin utilizar memoria convencional*. Eliminar el **SHARE.EXE** le ahorra aproximadamente 6 KB de memoria convencional.

### 13.3.2. EMM386.EXE[35]

EL EMM386.EXE, viene incluido para *Windows* 3.11 y *MS-DOS, le* permite administrar el acceso a la memoria superior y simula la memoria extendida como expandida. Esto es benéfico para las aplicaciones basadas en *MS-DOS,* pueden utilizar memoria expandida, EMM386, también permite cargar manejadores de dispositivos (*device drivers*) en los bloques de memoria superior. Aunque EMM386 puede liberar más memoria convencional cargando los manejadores de dispositivos en los bloques de memoria superior, esto ayuda realmente sólo cuando se están corriendo aplicaciones basadas en *MS-DOS. Windows for Work Groups,* utiliza la memoria extendida (XMS) para correr el Sistema Operativo y las aplicaciones basadas en *Windows.*

Accesar los manejadores de dispositivos (Device *drivers*) y código de aplicaciones desde los UMB´s (*Upper Memory Blocks*) es más lento que accesar el mismo código directamente de la memoria convencional, para maximizar el rendimiento cuando sé accesan estos dispositivos, se recomienda no utilizar el EMM386; que empleará aproximadamente 150 KB de la memoria extendida, para permitir mapear el rango de memoria de la UMB. y así cargar los manejadores de dispositivos.

**Nota**. Si se están corriendo aplicaciones basadas en *MS-DOS* que requieran utilizar más memoria convencional o que no requieren memoria expandida (EMS), se puede deshabilitar el EMM# del archivo CONFIG.SYS sin que esto tenga ningún efecto.

(33, 34 y 35) Archivos del sistema de MS-DOS
MANUAL Microsoft *Windows & MS-DOS 6.2*
(27) VxD= Dispositivo Manejador de Memoria Virtual

### 13.3.3. SMARTDRV.EXE[36]

Proporciona el soporte de caché de disco cuando *Windows* 3.11 no está corriendo o cuando el acceso a archivos de 32 bit está después habilitado en *Windows* 3.11 o cuando el acceso a 32 bit está también deshabilitado en un volumen de disco dado. Cuando *Windows* 3.11 está corriendo y el acceso a 32 bit está habitado, se tendrá más memoria utilizable al remover el **SMARTDRV.EXE**[36] del archivo **AUTOEXEC.BAT**, o reducir la cantidad de memoria que el **SMARTDRIVE**[36] *utiliza para proporcionar soporte de caché de disco.*

> **Nota**. *Cuando el tamaño del caché de acceso a 32 bit es cambiado, se actualiza la línea del* **SMARTDRV.EXE**[36], *del archivo* **AUTOEXEC.BAT** *para reflejar un valor más pequeño para* WinCacheSize.

Cuando se activa el acceso a 32 bits, puede ser necesario continuar utilizando SMARTDRIVE para proveer funcionalidad de caché de disco, en las siguientes situaciones. *MS-DOS* 6.0 está corriendo con DOUBLESPACE en volúmenes comprimidos. Cuando se decide utilizar el *CACHE* para CD-ROM´s. Cuando se decide utilizar el *CACHE* de disco para discos flexibles.

Identificación de unidades que utilizan SMART*DRIVE*[36]

Cuando el acceso a 32 bits está habitado, el *driver* de acceso a 32 bits, deshabitará el SMARTDRIVE[36] de los volúmenes de disco que el VFAT VxD[27] monta para identificar los volúmenes que continúa utilizando él caché de SMARTDRIVE[36], después de que el VFAT se carga. Escriba SMARTDRV en la línea de comandos de *MS-DOS* dentro de una sesión de *MS-DOS* desde *Windows* 3.11, observe y anote que letras de la unidad están presentes. Las letras de unidad que no aparecen para los *drivers* fisicos en el sistema, estarán siendo "**Cacheados**" por el *driver* a 32 bits.

(36) SMARTDRIVE (38) DOUBLESPACE
Archivos del sistema de MS-DOS
MANUAL Microsoft *Windows* & *MS-DOS* 6.2

### 13.3.4. IDENTIFIQUE LAS UNIDADES QUE EL ACCESO A 32 BITS ESTA CACHEADO[26]

Para identificar que unidades están utilizando el acceso a 32 bits, dé un doble *click* sobre el icono Extendido en el "**Panel de Control**" y presione sobre el botón de "**Memoria Virtual**". Si un *driver* dado se muestra como utilizando un acceso a 32 bits, entonces el *driver* de acceso a 32 bits está "***cacheando***" la unidad y el SMART*DRIVE*[36] no *cachea* al *driver*. Si un *driver* determinado se muestra que está utilizando el acceso a 16 bits, entonces al *driver* de acceso a 32 bits no está *cacheando* al *driver* y SMARTDRIVE[36] está cacheando el *driver*.

### 13.4. PROPAGACION DE UN VIRUS[26]

La forma más común de propagar un virus, es mediante un diskette infectado o un anexo en un correo electrónico. Hoy en dia, los virus de macro son los más frecuentes, con lo que los virus del sector *Boot* han pasado al segundo lugar. Los virus de Macro, se pueden extender al transferir documentos y archivos de datos infectados como anexos de correos electrónicos. Los virus del sector *Boot* sólo se pueden transmitir mediante *diskettes*. Las personas que utilizan *diskettes* en diferentes PC, aumentan el riesgo de emplear un diskette infectado y propagar el virus.

Existen personas que se equivocan al creer que sólo los programas compartidos, los discos gratuitos y los juegos propagan los virus. Aunque los virus se transmiten, algunas veces a través de estos tipos de *software*, ya que se tienden a copiar más. También se han detectado, en *software* precintado distribuido por grandes empresas y en *diskettes* que acompañan al *hardware*. Por este motivo, siempre debe rastrear todos los *diskettes* antes de utilizarlos. Además, los virus de archivo pueden propagarse al cargar programas infectados de la BBS[6] y de Internet, o bien como anexos de correos electrónicos. Debe tomar precauciones y verificar, antes de utilizarlo, cualquier *software* transferido mediante una red o un enlace de

*(36) Archivos del sistema de MS-DOS*
*MANUAL Microsoft Windows & MS-DOS 6.2*
**(26) Peter Norton Solución a Problemas de PC**
*Peter Norton & Robert Jourdain*
ED. PRENTICE HALL
**(6) BBS** = Bulletin Board System

estación de trabajo de una red, se puede infectar de la misma manera que una PC individual y un virus se puede propagar de forma muy rápida a través de una red. Debido a que el efecto de una infección por virus puede resultar muy grave si se infecta un servidor de archivos, debe tener especial cuidado a la hora de proteger las redes de una posible infección.

### 13.4.1. COMO ARRANCAR EN LIMPIO PARA MAYOR SEGURIDAD[16]

Al utilizar una herramienta de Dr. Solomon's, se verifica la memoria de la PC antes de ejecutarse la herramienta (puede que el virus se haya cargado en la memoria durante el arranque de la PC, por ejemplo). No obstante; existe la posibilidad de que algún virus pueda eludir esta detección. En este caso, el virus puede interferir en el rastreo, para ocultarse e incluso propagarse mediante el proceso de rastreo.

Para estar completamente seguro de que esto no sucede, puede "arrancar en limpio" antes de realizar el rastreo. Arrancar en limpio, significa arrancar la PC desde un diskette de sistema limpio en lugar de desde el disco duro (si no dispone de un diskette de sistema limpio, puede utilizar Magic Bullet[32]).

Puesto que sólo puede arrancar en *MS-DOS* desde *diskettes*, únicamente podrá ejecutar las utilidades de *MS-DOS* para buscar y eliminar virus. Estas utilidades son las siguientes:

*Findvirus.-* Esta utilidad se proporciona en formato de *MS-DOS* en el diskette Magic Bullet[832], además de la versión *Windows* suministrada en los *diskettes* de instalación de *Toolkit*, es necesario utilizar el comando *Findvirus* para *MS-DOS*.

*CleanBoot.-* Duplica la funcionalidad de la opción de menú "**Reemplazar sector *Boot***" de la interfaz de usuario. Es necesario utilizar el comando *CleanBoot*.

(16) Manual del usuario de Dr. Solomon's

**Nota**: Si desea arrancar en limpio y dispone de una unidad de disco duro que precisa un *driver* especial (como una unidad comprimida o una unidad IDE extendida), asegúrese de que las copias limpias de los *drivers* correspondientes se hallen en el diskette del sistema. A continuación, la PC se puede arrancar en limpio con los *drivers* correctos. Si estos *drivers* no se utilizan, el escáner Antivirus no podrá acceder a los archivos en la unidad de disco duro.

### 13.4.2. BUSQUE UN VIRUS DESDE LA PANTALLA PRINCIPAL[16]

Para encontrar virus en su PC utilice: "*Findvirus*" de Dr. Solomon's, si desea cambiar la configuración de las opciones, use el menú "**Escanear**", en el "**Explorador**", también puede utilizar el botón derecho del ratón; éste tiene su propia configuración de opciones. Si desea utilizar *Findvirus* con la configuración actual de las opciones, hágalo más rápido utilizando la pantalla principal de la interfaz del usuario:

1. En el cuadro "**Unidades**" seleccione la(s) unidad(es) en las que desee efectuar la búsqueda.
2. Haga clic en el botón **'Buscar'**, verá un diálogo que indica primero el progreso y luego los resultados del rastreo.
3. Puede interrumpir la búsqueda en cualquier momento, haciendo click en el botón "**Salir**", aunque esta acción no es recomendable ya que puede prevenir la detección de virus en su sistema. El reporte proporcionará detalles sobre cualquier virus que se haya encontrado hasta el momento en que se detuvo la búsqueda. Si en este período de tiempo no se encontraron virus, se mostrará el diálogo *Findvirus*.
4. Una vez concluida la búsqueda, compruebe los resultados, luego haga click en Salir para volver al diálogo *Findvirus*. Si se informa de una infección, vaya al **Capítulo 11.2**. (PROCEDIMIENTOS, QUE HACER EN CASO DE ENCONTRAR UN VIRUS).

(16) Manual del usuario de Dr Solomon's

## 13.5. ESTABLEZCA CURSOS DE CAPACITACION A LOS USUARIOS

### 13.5.1. ¿QUIÉNES CREAN LOS VIRUS?[8]

En la actualidad cada compañía desarrolladora de Antivirus, recibe aproximadamente en sus laboratorios alrededor de 400 virus nuevos al mes, lo cual representa una cifra de 13 diarios. Es alarmante pensar en la cantidad de personas que se dedican a crear virus, así como el esfuerzo que el desarrollo de un programa como éste implica.

Es una pena ver cómo cientos, o probablemente miles de aprendices de programadores dedican su tiempo a crear virus, con lo cual no aprenden nada nuevo, en lugar de dedicarse a estudiar o aplicar sus conocimientos de forma productiva. La mayoría de los programadores de virus no tienen conocimientos muy avanzados ya que es prácticamente imposible encontrar un virus "perfecto" que no tenga fallas. Se han dado buenos intentos pero casi ninguno ha logrado dar dolores de cabeza a los desarrolladores de *software* Antivirus. Una anécdota curiosa es la del primer Macrovirus de Excel conocido como **WM/Laroux**; obviamente no se sabe quién lo creó ni cuánto tardó el programador en dicha tarea, pero los investigadores de Antivirus encontraron la forma de detectarlo y erradicar dicho virus en tan sólo diez minutos.

Entonces surge una pregunta:

¿QUIEN CREA LOS VIRUS?.

La respuesta es sencilla: por lo regular son jóvenes masculinos de 14 a 22 años, gente con ganas de demostrar que su capacidad de programación es superior a la de cualquier otra persona. Algunos lo ven como un reto, otros como diversión o juego; sin embargo, todo se resume en lo mismo; tiempo y recursos perdidos.

(8) PC Viruses - Detection, Analysis and Cure
Dr. Alan Solomon & Tin Kay

Hay muchos mitos que indican que son los mismos desarrolladores de Antivirus quienes se dedican a crear estos programas destructivos; sin embargo, compañías como Mcaffe, PC Cillin, Thunderbyte, Norton, F-Prot y Dr. Solomon's jamás contratarían a personas cuyo sueño sea desarrollar virus. Tienen estas empresas un alto grado de ética, aunque no falta quien se les acerque en algún evento o exposición y con un guiño en el ojo preguntarán: "Ya digan la verdad... ustedes son los mismos que hacen los virus para tener trabajo, ¿no?"... no les queda mas que reír y dar la siguiente explicación:

El trabajo de una compañía que se dedica a erradicar virus no consiste únicamente en crear protección contra los mismos; tienen más trabajo que hacer; por ejemplo mejorar sus productos para que sean más rápidos y amigables; por lo tanto aunque llegara el día en que no existiera ningún virus nuevo, tienen mucho trabajo por hacer, por lo tanto no tendrían tiempo ni interés, ni necesidad, de crear nuevos y "mortales" virus.

En consecuencia, gente a la que le gusta perder el tiempo es quien hace los virus; son personas que desean sentirse respetadas y es por eso que inventan absurdos nombres, no únicamente para esconder su verdadera identidad, pero si para inspirar miedo en la persona que sufre un ataque de virus; por favor, imagine lo siguiente: usted está trabajando a altas horas de la noche y se da cuanta que su computadora empieza a actuar en forma extraña; de pronto aparece un mensaje con una calavera y dice algo, como: **"Tu disco duro es historial saludos de el vengador de la santísima muerte".** Es patético.

Definitivamente no queda mas que reír cuando vemos nombres como Deadman, The Black Lord, Nowhere Man, Byte Eater, Cyber Master, entre otros apodos creados con el fin de asustar, sin embargo, si realmente conociéramos a dichas personas nos daríamos cuenta que el nombre no tiene nada que ver con su verdadera apariencia

física y que probablemente sea sólo un chico que al salir de la escuela se encierra en su cuarto a pasar largas horas en la computadora, y esto es hasta que tienen novia, consiguen coche, piden un préstamo y ahí acabó la diversión, ya no tienen más tiempo para perder creando virus.

Pese a ello, en la historia se dieron dos casos relevantes de virus informáticos que han dejado huella y desgraciadamente no han servido como ejemplo de cómo un creador de virus puede terminar. El primero de ellos es el de Robert Morris junior; hijo de un ingeniero de la National Security Association (NSA), en 1988 Robert Morris, que en aquel entonces tenía 23 años, creó un "gusano", el cual se infiltró a través de Internet que en aquél entonces era usada por el departamento de defensa, y cuyo fin era el de replicarse en todas las computadoras posibles, afectando el funcionamiento normal de las mismas al saturar la memoria de la máquina. La creación de Morris afectó a aproximadamente 6,500 computadoras, hasta que el virus fue descubierto y destruido. La Corte Federal de E.U. culpó a Robert Morris junior; a quién se le multó con $250,000 dólares por daños (nada comparable con el estimado de pérdidas que se reportó, que fue de 98 millones de dólares) y una condena de cinco años en la cárcel. Otro gran ejemplo de cómo pude terminar el creador de un virus es Donald Gene Burleson, quien en 1985 implantó una bomba de tiempo en la compañía donde trabajaba para destruir los registros de las comisiones de ventas; sin embargo, fue descubierto y demandado por su empresa. A Donald Burleson se le condenó con 7 años de libertad condicional y una multa de $11,500 dólares. Estos son dos casos de cientos que existen en la actualidad, los dos más importantes y conocidos. Para muchas personas la creación de virus es simplemente curiosidad humana, en otras ocasiones la incansable búsqueda de gloria y en otras más hay motivos más oscuros, como la destrucción especifica por parte de un empleado despedido buscando venganza, o simplemente un desahogo mental (como es el caso del virus "**ROTCEH**", "HECTOR" al revés, virus creado en el Instituto Politécnico Nacional, en México); sin embargo no se dan cuenta del riesgo

que implica, tanto para la sociedad, como para el mismo desarrollador, quien puede terminar en la cárcel. Una persona así jamás mide riesgos; quizá todo empieza como un juego, un simple juego que puede terminar por destruir su vida.

Es conveniente mantener a los usuarios en constante capacitación y hacerle saber a los inexpertos, de la perdida de tiempo que genera la creación de virus, lo cual no es conveniente en ningún centro de cómputo. Debe existir siempre un ambiente de compañerismo y orden sobre todo.

## 13.6. ESTRUCTURE UNA BIBLIOTECA DE MANUALES DE *SOFTWARE* PARA CONOCER Y CONTRA ATACAR UN VIRUS[8]

El sistema de Antivirus de Dr. Solomon's posee una enciclopedia muy completa tanto impresa como "on–line". La enciclopedia proporcionará información vital sobre todos los virus que el *Toolkit* puede detectar. La velocidad de búsqueda tan rápida permite a los usuarios encontrar información de los virus en cuestión de segundos. Le recomendamos obtener todas las publicaciones de los desarrolladores de Antivirus, esto le permitirán siempre tener mas control de la existencia de los virus, los efectos que generan el daño que causan.

## 13.7. SELECCION CRITICA DEL MEJOR SISTEMA DE ANTIVIRUS[8]

Uno de los desarrolladores de Antivirus que trabaja con la mejor tecnología SOS Disk, es Dr. Solomon's, ya que tiene un disco exclusivo para verificar la existencia de virus en cualquier tipo de PC, este disco se llama MAGIC BULLET[32] (Bala Mágica).

El Magic Bullet[32] es un disco de arranque libre de virus desarrollado para facilitar la reparación de una máquina infectada. Los usuarios sólo tienen que encender con Magic Bullet y seleccionar la opción que se adecue a sus necesidades.

(8) PC Viruses – Detection, Analysis and Cure
Dr. Alan Solomon & Tin Kay
(32) MAGIC BULLET (ver Capítulo 3.4.7.)

# CAPITULO 14

# PROPUESTA DE PROTECCION DE VIRUS EN INTERNET

## 14.1. SUGERENCIAS Y PRECAUCIONES PARA LOS RESPONSABLES DE UN CENTRO DE COMPUTO

Dr. Solomon's Antivirus *Toolkit* para *Groupware* es la nueva serie de herramientas que permitirán al administrador de la Red, brindar un nivel más de protección a su equipo de cómputo, ¡Protegiendo las entradas de virus a través del correo electrónico de forma transparente para el usuario!.

Según ICSA[39] (*International Computer Security Association*, antes conocida como NCSA), en su encuesta sobre virus de 1997 (NCSA 1997 *Virus Survey*) descubrió que dos de las fuentes más comunes para infección de virus son tanto el correo electrónico como el acceso de Internet. Lo más común es el uso de *diskettes* entre varias computadoras, la cual queda perfectamente protegida con las herramientas *Winguard* y *Virusguard* de la PC, así como *MacGuard* en el caso de Macintosh.

La infección por correo electrónico es común y principalmente se filtran Macrovirus a través de este medio, ya que es muy sencillo seleccionar el menú "Archivo" en el sistema *Word*, elegir "Enviar a" y posteriormente seleccionar el correo electrónico como medio de distribución y si no se enteran de que están infectados definitivamente se corre el riesgo de generar una epidemia.

La forma favorita de los creadores de virus para hacer de las suyas, es subir sus creaciones a los ***news groups*** o grupos de mensajes en Internet, principalmente los

(39) Boletines de sistema de Antivirus Dr. Solomon's

grupos cuyo tema principal es el sexo, ya que son los de más afluencia en general. Ellos tienden a anunciar sus archivos como "Una excelente gráfica", o bien "programa XXX" y así los curiosos se llevarán la sorpresa de su vida, la cual no es una hermosa mujer o un encantador galán, sino la erradicación de la información del disco duro a través de un Caballo de Troya o, peor aún, un *Drooper*, programa que genera virus de sector de arranque, que crea un virus y el usuario ni siquiera se da cuenta de lo que ocurre, sino que cree que el programa simplemente no funcionó (lo cual es común en Internet).

Otra vía de infección a través de Internet es el *Word Wide Web* (o *World Wide Wait*, según dicen las personas que no cuentan con el enlace dedicado de alta velocidad), ya que ahí se encuentran miles de sitios con programas de dudoso origen, los cuales en ocasiones están infectados por algún virus, ya que las personas que pusieron estos archivos a la disposición del público, no tuvieron la gentileza de revisarlos contra virus, o bien lo hicieron deliberadamente.

En el caso del correo electrónico, Dr. Solomon's ofrece herramientas diseñadas para limpiar toda transacción de correo electrónico y que el usuario este libre de virus si es que usa estos medios. La serie de sistemas Antivirus Toolkit para *Groupware* cuenta con la particularidad de que son transparentes para el usuario final; sin embargo, el administrador siempre estará al tanto de lo que ocurre en la red, permitiéndole mantener un registro de que ocurre en la misma e incluso generar estadísticas de los usuarios que reciben más virus por correo electrónico, por ejemplo:

Actualmente Dr. Solomon's soporta diferentes plataformas de oficinas postales (o *Postoffices*, como se les conoce en inglés): AVTK para *Microsoft Exchange Server*, AVTK para Lotus Domino y por último, *MailGuard*, producto que protege

transacciones de correo electrónico **smtp/pop3**, es decir, el utilizado comúnmente en Internet, el cual es ideal para proveedores de acceso a esta red.

Es importante destacar que estas soluciones fueron diseñadas para instalarse en el servidor de correos limpiando de forma transparente los correos sin que el usuario sepa jamás (a menos que el administrador decida lo contrario) que estuvo apunto de recibir un virus por este medio.

Se antoja una pregunta: ¿Qué pasa con los usuarios de Laptop que además se conectan a otros servidores fuera de su Compañía?, Dr. Solomon's también piensa en ellos y creó una herramienta para usuarios de clientes de correo electrónico de *MS-Exchange* o *MS-MAIL* (como *OUTLOOK* o *INBOX*, por ejemplo) de 32 bits llamado *Microsoft Mailbox Scanner*, la cual puede ser instalada en cualquier equipo de usuario final, sea PC de escritorio o bien una portátil la cual "envuelve" al cliente de correo electrónico y revisa los mensajes que lleguen el mismo, asegurándose de que su correo electrónico esté libre de virus.

Los usuarios protegidos por Dr. Solomon's pueden descansar tranquilos, a sabiendas de que todo lo que pase por la red estará siempre libre de virus.

## 14.2. SISTEMA DE CORREO ELECTRONICO (BBS) DE MCAFEE[17]

El sistema de correo electrónico (BBS)[6] está accesible las 24 horas del día, los 365 días al año, excepto cuando están programados *tiempos fuera o por mantenimiento*. Todas las líneas tienen módem's de alta velocidad operando desde 1,200 bps hasta 128 Kbps con los siguientes parámetros: 32 bits, sin paridad y 1 bit de *stop*. El número telefónico de BBS de McAfee es (408) 988-4004.

### 14.2.1. AREA DE MCAFEE EN COMPUSERV[17]

También tiene un espacio de ayuda de virus en CompuServe. Para hacer uso de este espacio escriba 'GO MCAFEE' cuando esté en línea de comando de CompuServe.

(6) **BBS** = Bulletin Board System
10) Manual del usuario de Mcafee
(17) Manual de Usuario, de *McAfee*

Tenemos disponible una introducción gratuita para socios. (Para mayor información lea el archivo incluido llamado << COMPUSERVE.TXT>>).

### 14.2.2. ACCESO A INTERNET

( Soporte técnico de McAfee )[17]

La última versión del programa de Antivirus de McAfee, está disponible con la cuenta "*anonymous*" en *FTP* (*File* Transfer *Protocol*), en Internet desde mcafee.com. Si su Manejador no acepta nombres use la siguiente dirección IP#192.187.128.1. indique "anonymous" o FTP con su identificación de usuario (*user ID*) y su propia dirección de correo electrónico (*e-mail*) como *password*, los programas están localizados en el directorio pub/Antivirus. si tiene alguna pregunta puede enviar un correo electrónico a la dirección ***support@mcafee.com***

También puede encontrar el *software* Antivirus de McAfee en el archivo SimTel ubicado en Oak.Oakland.EDU en *simtel/msdos*/virus y sus espejos asociados.

( Soporte Técnico de Dr. Solomon's[21] )

A continuación se describen las direcciones electrónicas a la que podrá consultar en Internet y contar con el servicio de soporte técnico cuando así lo requiera.

| | |
|---|---|
| Acceso a Internet: | |
| Dr. Solomon's Group | http:\\www.drsolomon.com |
| Dr. Solomon's Group | http:\\www.drsolomon.com.mx |
| National Computer Security Association (NCSA) | http:\\www.ncsa.com |
| Virus Bulletin | http:\\virusbtn.com |
| COMPUSERVE: | |
| Dr. Solomon's Group | GO drsolomon |
| Dr. Solomon's México | GO mexhelp |
| National Computer Security Association (NCSA) | GO ncsa |

(17) Manual de Usuario. de *McAfee*
(21) Pagina de Internet http://www.drsolomon.com

## 14.3. PROGRAMAS ANTIVIRUS MAS COMERCIALES

### 14.3.1. TBAV: THUNDERBYTE ANTIVIRUS

El ThunderByte Antivirus provee detección por firmas (TbScan), chequeo de integridad por cálculo (TbSetup y TbScan), bloqueo de instrucciones sospechosas (TbMem, TbFile y TbDisk) y detección heuristica de instrucciones sospechosas (TbScan).

### 14.3.2. F-PROT ANTIVIRUS

F-Prot brinda detección de virus por firmas y detección heuristica de instrucciones sospechosas.

### 14.3.3. DR. SOLOMON'S ANTIVIRUS *TOOLKIT*

Dirección para solicitar apoyo de soporte técnico:

BBS[6]:

| | |
|---|---|
| Dr. Solomon's Group | 98 44 0 12906 318810 |
| Dr. Solomon's México | 5 250 39 48 |
| Dr. Solomon's México | 5 250 39 58 |

### 14.3.4. VIRUSCAN DE MCAFEE[17]

El *ViruScan* de McAfee utiliza detección por firmas (Scan2), bloqueo de instrucciones sospechosas (*Vshield*) y chequeo por cálculo de códigos de validación (SCAN2 /AV). El control de acceso lo da un programa llamado CCP, el cual es un producto adicional de McAfee. Se lo venden aparte. *ViruScan* de McAfee

### 14.3.5. NAV: NORTON ANTIVIRUS

El Antivirus de Norton incluye detección por firmas (Nav), bloqueo de instrucciones sospechosas (Virus **Intercept Nav_.Sys**) e "inoculación" y chequeo de cálculo (Nav y Nav_.Sys). Es un programa comercial, por lo que NO está disponible en Internet.

(6) BBS = Bulletin Board System
(17) Manual de Usuario, de *McAfee*

Se debe comprar. Sin embargo, tienen un lugar en Internet para Soporte e información: Antivirus *Reference Center* (*Symantec*) (Norton AV).

### 14.3.6. MSAV: MICROSOFT ANTIVIRUS

El Antivirus que trae el *MS-DOS* versión 6 tiene: detección por firmas (MSav), bloqueo de instrucciones sospechosas (Vsafe) y chequeo por cálculo (MSav y Vsafe).

### 14.3.7. OTROS PROGRAMAS ANTIVIRUS Y VACUNAS EN INTERNET

- Programas Antivirus *Software* Antivirus en *Atlantis utmb Index of* pub ibm-
- Top 10 Antivirus
- Antivirus Programs WAVC Willems Free AV Consultancy
- Antivirus *Software* Update Auto-Notification

### 14.3.8. OTRAS LISTAS DE ANTIVIRUS Y VACUNAS

- *MS-DOS* Antivirus Tools
- Virus Detection Alternatives The Anti-Viral *Software* of *MS-DOS* 6
- Data Fellows World Wide Web Server (F-PROT)
- ftp: complex Iceland (F-Prot home)
- McAfee Associates México Page •
- ICARO: Italian Computer Antivirus Research Organization •Antivirus Reference Center (Symantec) (Norton AV).

## 14.4. PASOS PARA QUITAR UN VIRUS

- Antes que nada SIEMPRE arrancar en frio desde un *diskette* MS-DOS limpio.
- Corra todos los programas (Utilerías, Sistema Operativo y Vacunas) desde *diskettes* limpios, NUNCA desde disco duro (mientras se elimina el virus).
- Identificar el virus con el módulo Antivirus que los detecta.

Por ejemplo: **SCAN C:** **TBSCAN C:**

1. Si se sabe (o se sospecha) que hay un virus en la tabla de particiones:

**C:\ FDISK /MBR**

(¡**CUIDADO**! ¡Puede traer problemas!

Arranque con disco del *MS-DOS* limpio y verifique primero con:

**C:DIR C:**

*Si el disco es accesible y si le da Error NO utilice esta opción.*

2. Para quitar un virus del sector de arranque:

**C:\SYS C:**

3. Usar "Matadores" especiales para los virus (**Natas. Monkey. "Esto te pasa"**). Por ejemplo:

**KILLMONK.**

4. Limpiar de virus los archivos infectados con el modulo u opción Antivirus que los limpia. Por ejemplo:

**C:\>SCAN C: /CLEAN**

**C:\>TBCLEAN C:**

5. Si es Necesario: Borrar completamente los archivos infectados. Por ejemplo:

**C:\>SCAN C: /DEL TBSCAN C: /KILL**

6. - Si es Necesario:

Recupere los archivos desde copias respaldo (*Backup*). Por ejemplo:

**RESTORE A:*.* /S**

7. Si es Necesario:

Reinstalar aplicaciones y programas que se tengan en *diskettes*. Por ejemplo:

**INSTALL C:**

8. Busque o Pida Ayuda:

En Internet: (probablemente a través de otra COMPUTADORA)

(6) BBS = Bulletin Board System

- Preguntas más Frecuentes y sus Respuestas
- Sabe utilizar los grupos de noticias discusión "UseNet", vea: *alt.comp.virus comp.virus* (moderado y más serio, pero más tardado).

Si tiene identificado el virus que "infectó" a su computadora: Puede buscar en los foros de discusión información sobre ese virus en particular en *Dejanews Research Service* en revistas, libros y documentos en su BBS[6] o proveedor de servicios en línea en su escuela o Universidad en el área de soporte de su(s) programas Antivirus.

**Nota**: Sí se Puede, busque una segunda opinión (como con los Médicos).

### 14.4.1. SOLO COMO ULTIMO RECURSO

No es necesario si se tienen las vacunas, utilerías y herramientas adecuadas y se siguieron los pasos con cuidado:

- Dar formato al disco duro: **FORMAT C: /U /S**

Requiere realizar después los pasos 6 y 7...

- También sólo como último recurso y si sabe como hacerlo:

- Particionar el disco duro: FDISK

Requiere Realizar Después los pasos 9, 6 y 7...

## 14.5 CONSEJOS Y RECURSOS DE ANTIVIRUS EN INTERNET[40]

Puede obtener ayuda en Internet, le sugerimos utilizar los siguientes recursos:

- ThunderBYTE World Wide Web Server ThunderByte México
- Dr. Solomon's - Computer Virus Information And More Data Fellows World-Wide Web Server.

(6) BBS — Bulletin Board System
(40) The Computer Virus Crisis
Peter J. Denning & Kone

- Mcafee México
- Virus Encyclopedia Computer Viruses Info Specific Virus Descriptions en Symantec (Norton AV) gopher://csrc.ncsl.nist.gov:71/11/virus/virinfo gopher://index.almaden.ibm.com:1virus/virus.70 Computer virus information

Tipos de virus que se pueden adquirir al accesar a Internet:

- Stealth. PoliMórficos.
- *Boot* Sector. File Infectors.
- Hit Parade

Los Virus más "Populares"... pueden adquirir al accesar a Internet

- Descripciones de Algunos Virus
- **Natas**. **Jerusalem**. **Stoned**.
- Tips Antivirus (Antes del Virus)

### 14.5.1. CONTROLES[40]

(Control de acceso físico a los equipos).

- Control de entrada a los programas de la computadora a través de claves de acceso (*passwords*).
- Registro, verificación y control de los *diskettes* que se introducen a la computadora.
- Se recomienda algún programa de tipo menú que restrinja los programas que se pueden ejecutar a sólo los autorizados a cada usuario.

### 14.5.2. BLOQUEOS[40]

- Se recomienda usar la "Cerradura para floppies" (*driver lock*), uso del candado o llave de encendido, si la computadora lo tiene.

(40) The Computer Virus Crisis
Fritz Johnson & Kratz

- Programas administradores de disco duro, que pueden impedir escrituras al mismo.
- Las activaciones o deshabilitaciones siguientes; son a través del Programa de configuración "SetUp", accesible oprimiendo las teclas Ctrl-Alt-Esc al mismo tiempo en algunas computadoras, o al oprimir la tecla "Del" o "Supr" cuando se está arrancando (*Boot*) la computadora.
- Deshabilitar el arranque (*Boot*) desde la unidad de *diskette*.
- Deshabilitar completamente las unidades de *diskette*.
- Habilitación de la facilidad de palabra clave (*password*).
- Activar la protección Antivirus en BIOS.

### 14.5.3. MANEJO DE DISKETTES Y CONSEJOS IMPORTANTES[40]

Estos son consejos muy importantes, prácticamente todos los virus se introducen a una computadora por medio de *diskettes*. Y en el caso de un desastre, las copias de respaldo en *diskette* serán la salvación de nuestros datos. Verificar contra virus todos los *diskettes* que se introduzcan en la computadora, aunque sólo sean de datos.

- No ejecute programas de origen dudoso.
- No meta *diskettes* extraños. Nunca arranque (*Boot*) desde *diskette* en la operación normal de su computadora.
- Nunca dejar puestos *diskettes* al apagar la computadora.
- Tenga un *diskette* de arranque que esté libre de virus y protegido contra escritura. Si es necesario arrancar desde *diskette*, utilice únicamente este *diskette*.
- Proteja contra escritura sus discos del sistema, así como sus discos de programas de aplicación (originales y copias respaldo).
- Que los usuarios sólo manejen *diskettes* de datos y nunca de programas.
- Los Programas deben estar ya instalados en el disco duro. Instalar nuevos paquetes en una máquina que sirva de "conejillo de Indias" y que esté un tiempo en "observación".

(40) The Computer Virus Crisis
Bates, Johnson & Kratz

- Mantenga copias respaldo, tanto de los programas, como de los datos.
- Haga por separado los respaldos de datos y de programas en *diskettes* diferentes.

### 14.5.4. VACUNAS ANTIVIRUS[40]

Tenga varios programas Antivirus, preferentemente con diferentes enfoques. Utilice o active todas las diversas opciones de protección: Búsqueda de firmas, chequeo de cambios por códigos de verificación CRC, monitoreo residente en memoria, bloqueo de operaciones sospechosas, protección del sector de arranque, etc. Comprar las versiones actualizadas de las vacunas. La Documentación y Manuales de los Antivirus.

### 14.5.5. SERVICIOS EN LINEA

Verificar contra virus todo programa que se transfiera. Verifique contra virus todo archivo auto-descomprimible (aunque sea de datos).

**Nota**:

Capacite a los usuarios en protección contra virus. Desarrolle un plan de emergencia contra virus que prevea procedimientos o máquinas alternas para el proceso de los datos. Y por último: mantenerse informado, leer sobre el tema, leer por ejemplo mi columna en la revista "Personal Computing"; "El Lado Obscuro", pues recuerde:

**En este momento hay al menos un Cracker ideando un Nuevo Virus.**

## 14.6. LOS PELIGROS DE INTERNET[40]

En algún tiempo se conocía a los **Caballos de Troya** como aquellos programas que podrían ser bajados de Internet o BBS (Bulletin Board Service) con la idea de que dicho archivo contenía algún programa útil para el usuario; sin embargo, al ser ejecutado se encontraba con que de pronto su disco duro había sido borrado.

(40) The Computer Virus Crisis
Fites, Johnson & Kratz

Al igual que todo, como en la industria informática, estos *Caballos de Troya* también evolucionaron. Antes, los resultados eran inmediatamente percibidos por el usuario al ver que su disco duro empezaba una frenética actividad mientras era borrado; sin embargo, la acción de estos *Caballos de Troya* ya no es inminente. Pese a esto, ya existe una nueva generación de *Caballos de Troya*.

Un ladrón de *password* es un programa que, de forma secreta, es ejecutado y mientras el usuario se conecta su servicio en línea, este programa "roba" los datos como el *login*, *password* y, en algunos casos hasta la tarjeta de crédito y los envía de forma secreta al creador de este troyano. Los efectos no son inmediatos y el usuario se dará cuenta hasta que su tarjeta de crédito fue desfalcada o que su factura de servicio en linea es por un cargo mucho mayor del que se esperaba.

Otro de los factores por los cuales los ladrones de *password* son sumamente peligrosos, es por que el creador de este programa tiene acceso a la cuenta del usuario y por lo tanto puede hacer uso de la misma, de forma fraudulenta, comprometiendo la integridad del usuario agredido, mientras el agresor sigue suelto.

Dr. Solomon's ha sido capaz de detectar prácticamente cualquier *troyano* desde el inicio de los mismos; sin embargo, la necesidad se volvió aun mayor, ya que se tiene en promedio de uno a tres *troyanos* por día; por lo tanto, la demanda de una herramienta adicional de seguridad se ha vuelto inminente.

Además de la protección con la que ya se contaba, Dr. Solomon's es capaz de detectar nuevos *troyanos* con forme van apareciendo gracias al análisis heuristico. Este tipo de análisis es capaz de detectar cualquier virus (o *troyano*) nuevo e impedir que se propag[illegible]

Además de esta protección, Dr. Solomon's ha liberado una nueva herramienta capaz de buscar, encontrar y erradicar a más de 500 *troyanos*. Además, es importante estar consciente de que con solo borrar el archivo no es suficiente, ya que por lo regular estos programas dañinos alteran los archivos de sistema y del registro de *Windows*.

Este programa esta disponible en Compuserve (GO DRSOLOMN) o en la página de Internet (http://www.drsolomon.cómputo) para que usted lo baje. Cabe destacar que para ejecutarlo requiere *Windows* 3.1x, *Windows* 95 y Dr. Solomon's *Findvirus* 7.77 o superior en ambos casos.

## 14.7. EL RIESGO DE LOS ANTIVIRUS GRATUITOS[39]

Existe una gran batalla en las Empresas para lograr la venta de productos Antivirus. Son muchos los jugadores y todos lucha a capa y espada con el fin de colocar sus productos en las computadoras de los clientes, cobrar la factura y comenzar el ciclo de servicio; sin embargo, nos hemos encontrado con compañías cuyo giro principal no es el Antivirus, sino ofrecer *suite* o conjunto de programas y proporcionar como valor agregado el Antivirus. Esto es totalmente válido, sin embargo, existen varios riesgos para la empresa y, por ende, para el usuario. Al hacer esto, ya que en el caso particular de los Antivirus mantener un producto así suele ser muy caro, a diferencia de otro tipo de aplicaciones ya que se tiene que invertir gran parte del presupuesto en investigación y desarrollo, soporte técnico, mercadotecnia y ventas, etc. Simplemente, el costo del personal encargado de analizar los virus que llegan mes a mes y desarrollar las vacunas para los mismos pude llegar a ser muy elevado. ¿Qué es lo que pasa? Tenemos un producto que cuesta mucho desarrollar y mantener, los costos de operación suelen ser muy elevados (si es que se plantea tener un Antivirus que cumpla y exceda las expectativas del cliente, para que se venda, por supuesto) y, sin embargo, la ganancia es nula o mínima debido a que el producto Antivirus se vuelve un valor agregado o elemento de una *suite* de diversos programas. Debemos recordar que, por lo regular, el resto de los productos que componen la *suite* deben

ser económicos para poder ser competitivos y que en la mayoría de las ocasiones éstos no suelen cubrir por mucho tiempo los cotos de operación de todos esos productos que componen el conjunto, demás del Antivirus. Un claro ejemplo de lo que puede llegar a pasar es lo que ocurrió con IBM. Compañía que también desarrollo su Antivirus (basado en la ingeniería de otro *software* Antivirus) y lo mantenía. Sin embargo, el 19 de mayo de 1998 renunció que dejaría de desarrollar el *IBM Antivirus*, y se olvidaría por completo de él el diciembre de 1998. Esta noticia nos confirma la teoría: cuando el *software no deja ganancias* a la Compañía se vuelve, después de algún tiempo, en un peso para la misma y un costo innecesario. Resumiendo, el punto de este artículo es que un producto gratuito puede perder su valía, ya que los costos de operación de un buen Antivirus suelen ser muy elevados y, al no dejar ganancias terminan por ser una carga para la empresa ¿cuántas Compañías actualmente regalan su producto Antivirus?, ¿Qué valía representa para ellos dicho producto?, ¿Qué interés puede tener una empresa en mantener vivo un producto q lo único q genera son costos?, Y la pregunta final: ¿qué futuro espera a un producto Antivirus que no genera ingresos para la Compañía?. Recordemos, por último que lo importante en una empresa es generar dinero, y que un producto Antivirus no debe ser un juego, sino un aspecto importante de la seguridad informática, con el que deben convivir las empresas día a día. ¿Está usted dispuesto a perder dinero e información en su empresa por utilizar un Antivirus que puede llegar a desaparecer de un momento a otro?.

## 14.8. ANTIVIRUS DE *SOFTWARE*[139]

Son los sistemas o programas más populares, los cuales tienen ventajas y desventajas.

### 14.8.1 VENTAJAS:

- Fáciles de actualizar
- Compatibles con múltiples plataformas

[139] Boletines de sistema de Antivirus Dr. Solomon's

- Fáciles de obtener
- Relativamente baratos y confiables

### 14.8.2. DESVENTAJAS:

- Ocupan recursos de la computadora
- Pueden ser infectados por virus
- Se pueden borrar fácilmente (digamos ¡adiós!. A la protección Antivirus).

## 14.9. ANTIVIRUS DE HARDWARE[39]

Hubo un intento por parte de una compañía Antivirus por hacer esto. Se desarrollaron dos variantes en forma de tarjeta. la cual se coloca dentro de la PC. y otra en la que se instala una especie de candado en el puerto paralelo (de la impresora). en la parte trasera de la PC.

### 14.9.1 VENTAJAS:

- No afecta tanto los recursos de la máquina
- Es una solución elegante

### 14.9.2. DESVENTAJAS:

- Difíciles de actualizar (es más fácil cambiar *software* que tarjetas cada mes)
- Muy caros
- No son multiplataformas
- De cualquier forma interactúan con el sistema operativo
- Requieren *slot*. o ranura de la máquina

[39] Boletines de sistema de Antivirus Dr. Solomon's

### 14.9.3. DIFERENCIAS ENTRE AMBOS

- Los Antivirus de hardware fracasaron, ya que es muy caro y difícil actualizar cientos o miles de equipos con tarjetas en corporativos, además de ser una solución poco práctica.
- Gracias a esta experiencia sabemos que el *software* Antivirus en *software* es mucho más confiable, barato y práctico que cualquier otra solución; sin embargo, existen dos divisiones más en el aspecto de los Antivirus de *software*, y para esto debemos conocer primero el orden del juego.

## 14.10. ANALISIS HEURISTICO[16]

Juego de herramientas estadísticas que pueden ayudar a deducir comportamientos. Se utiliza ampliamente en la industria de los Antivirus para detectar posibles nuevos virus. Como de cualquier forma este método "especula" sobre lo que puede pasar, puede generar las famosas falsas alarmas, es decir, reportar un virus cuando no existe, o bien no detectarlo, aun cuando esté presente. Recordemos que, según el estudio ICSA, 1997 Virus Prevalence Survey, el costo para una empresa por una falsa alarma es, en promedio de 23,000 dólares. Por supuesto, depende mucho de cómo se haya implementado el Análisis Heurístico.

## 14.11. *CHECKSUMMING*[16]

El checksumming es un método en el cual se toman las "huellas digitales" de los archivos y, en cuanto cambian, posiblemente por un virus informático, se le reporta al usuario dicha acción. Evidentemente esto no únicamente detiene cualquier operación que realice el usuario con sus archivos, lo cual puede generar confusión y cientos de falsas alarmas.

[16] Manual de Usuario de Dr. Solomon's

## CONCLUSIONES

Finalmente, la investigación realizada a través de la elaboración de este trabajo, se puede concluir los siguientes aspectos que son de vital importancia a considerar:

- Lo importante de la elaboración de este trabajo, tanto como para usuarios o expertos en computación sea cual sea su situación, es que conozca que hace y como trabaja un Antivirus. Primero que nada es importante recordar que un virus informático es simplemente un programa que se copia a sí mismo en otras computadoras, y que aunque el funcionamiento de un virus informático es semejante al de un biológico, en el sentido de que éste último se replica en otras células que están sanas, la palabra virus es en realidad un acrónimo que significa ***Vital Information Resources Under Siege***, es decir: "Recursos Vitales de Información bajo Acecho".

- *No todos los virus informáticos son de peligro inminente, es decir, que no todos* fueron diseñados para destruir o atacar la información almacenada en la máquina; sin embargo, todo virus es un riesgo, ya que ningún programador de éstos ha sido certificado por las normas de calidad ISO-9000 o el ***Kaizen*** japonés, por lo tanto todo programa está expuesto a sufrir ***bugs*** o errores de programación, *posiblemente causando efectos inexplicables e impredecibles*, para lograr que la computadora actúe de forma extraña.

- En algunos de los casos, los famosos *bugs* han impedido la destrucción de información en las computadoras, como fue el caso del virus **Rotceb** o el más reciente **AccesIV**, los cuales no activan su carga destructiva por errores de programación por parte del creador del programa. Si tomamos dicho concepto (programa que se copia así mismo), la función de un Antivirus es la de evitar que su computadora contraiga un bicho de este tipo, o bien, si ya lo contrajo,

erradicarlo por completo antes de que se siga replicando y mantener su información intacta.

- Un sistema de Antivirus es un conjunto de programas de software que se vinculan dentro de una computadora o un servidor de red y que tienen como finalidad la protección de los sistemas y en último caso del hardware.

- Existen diferentes tecnologías de sistemas de Antivirus, las cuales son conocidas por su área geográfica. Así como existen las redes que abarcan una extensión pequeña conocidas como redes LAN o redes de área local; las redes MAN o redes metropolitanas, que cubren la extensión equivalente a una ciudad; o WAN de área amplia, que abarcan grandes extensiones territoriales o países. Por medio de Internet, ciertos virus viajan de país a país por estos medios de transmisión, dando lugar a que programadores desconocidos expertos en el lenguaje ensamblador erradiquen y creen al mismo tiempo programas llamados: "virus".

- Lamentablemente no existen estándares que rijan a los sistemas de antivirus informáticos, se espera que algún día se desarrolle el sistema estándar para evitar esta problemática.

- El conocimiento de los sistemas de Antivirus y la experiencia del soporte técnico, amplían el horizonte de posibilidades para la solución de problemas y erradicación de virus. Los recursos y servicios de estos desarrolladores, proporcionan al usuario gran apoyo; entre estos servicios destaca el correo electrónico y [illegible]icaciones de comunicación remota de computadoras.

- Los virus dañinos han existido por casi 30 años por diversas etapas, notándose los peligros que han sufrido las computadoras, por lo que es importante estar al pendiente para evitar daños y pérdidas de información.

- Los sistemas de antivirus son económicos, por lo que es de gran responsabilidad tener siempre una protección actualizada.

- Con el fin de mantener una adecuada consistencia en la actualización de los sistemas de antivirus autónomos, los programadores "jackers" utilizan compuertas mediante Internet, para mantener actualizado el sistema de protección de virus en la PC.

- De la misma manera que existe un "Cracker" creador de virus, existe un "Jacker" que estudia los programas llamados virus y que tiene la tarea de encontrar el sistema que elimina y protege a una PC.

- Los servicios y aplicaciones dentro de Internet, implantados para auxiliar desde un usuario novato hasta un experimentado programador.

- La realización de este trabajo pretende apoyar al estudiante y al usuario final, para aumentar sus conocimientos en el campo del soporte técnico, independientemente de su especialidad profesional. Las investigaciones realizadas de muy pocos libros y en su mayoría de la práctica, constituyen una base de interés para esta Estructura de Procedimientos de Soporte Técnico para la Aplicación y Erradicación de Virus Informáticos.

- Es recomendable para los lectores interesados, no perder la continuidad de las aplicaciones y procedimientos mencionados, estos muestran una gran variedad de conceptos del lenguaje técnico. Es conveniente tener apuntes de todas las nomenclaturas de cada sistema de erradicación de virus, debido a que todos poseen sus propias estructuras de ingeniería.

- También es notorio saber que no existe sistema de antivirus perfecto, debido a que los programadores cada dia elaboran programas de virus más elaborados y complicados, por lo que la tarea de erradicación de virus nunca terminará. Es conveniente estar actualizado con los nuevos sistemas que erradican virus informáticos, así como estar al tanto del nombre de los nuevos virus que surgen y del daño que causan, pues para todos es muy importante la seguridad de la información, tanto en casa como en la escuela y el trabajo.

- Los Antivirus de bajo acceso, programas que trabajan de forma transparente en el sistema, y evitan que un virus informático entre a su computadora. Lo que hace en si el Antivirus es revisar todos los archivos que el usuario accesa, asegurándose que éste no tenga virus. La palabra clave aquí es "prevención". Hay muchos virus que resultan difíciles o imposibles de erradicar una vez que están en memoria, por eso es importante detectar y erradicar al virus antes de que entre a la memoria de la máquina y se active. Hay muchos Antivirus que ofrecen este tipo de soluciones; sin embargo, el adecuado para las empresas y usuarios caseros por igual, es uno que sea totalmente transparente, que no utilice recursos de forma excesiva, que no haga más lenta la máquina, y principalmente que sea automático, es decir, que en el momento en que encuentre un virus lo erradique sin dejar la decisión en manos del usuario final sobre qué hacer con el bicho.

- Los Antivirus de bajo demanda.- Desgraciadamente, este tipo de Antivirus no son buenos para prevenir, sino que son correctivos, y en muchos casos totalmente inútiles, ya que, como mencionamos, hay virus que una vez que están en memoria son imposibles de erradicar. Este tipo de virus fueron los únicos que existieron hace tiempo, y lo que hace es sencillo. Se activa por el usuario para hacer la revisión de la memoria, el disco duro y medios de almacenamiento en general (*diskettes*, CD-ROM, etcétera), con el fin de determinar la existencia del algún virus y, en caso de que así sea, erradicarlo. Este tipo de Antivirus se ha

mantenido vigente ya que con ellos es más fácil buscar virus en medios de almacenamiento portátil, sin tener que esperar a que el archivo que abramos los tenga, impidiendo que, en caso de que no lo detectemos con él (Antivirus Bajo-Demanda), ya que no abrimos el archivo infectado, y seguimos regando el virus, sobre todo si los usuarios con los que intercambiamos *diskettes*, cuentan con *software* Antivirus.

- Los virus representan un problema, por lo que debe tener presente la magnitud del problema. La causa más común en la pérdida de datos, son los errores humanos. La segunda razón más común, es error del *hardware*, seguido de problemas del *software* y alteraciones. Los virus y Macrovirus, llegan en un cuarto lugar; sin embargo, al aplicar una política Antivirus estricta, se protegen los datos de todo tipo de pérdida, incluyendo los virus.

- Se sugiere, a las autoridades escolares de este Plantel Universitario, para que sea implementada una nueva materia optativa o especialidad, dentro de la carrera de INGENIERO EN COMPUTACION, debido a experiencias personales, casi el 90% de los estudiantes que egresan de esta carrera profesional, por lo regular carecen de conocimientos de soporte técnico, siendo esto una base y un fundamento muy indispensable para incorporarse como profesionista en las empresas que solicitan de sus servicios.

- Por último, se espera que la información presentada en este trabajo, sea de utilidad para futuras generaciones, que continúan con evolución del desarrollo informático.

# BIBLIOGRAFIA :


- **PC Anti-Virus Book**
  Dr. Alan Solomon & Tin Kay

- **PC Viruses – Detection, Analysis and Cure**
  Dr. Alan Solomon & Tin Kay

- **The Computer Virus Crisis**
  Frites, Johnson & Kratz

- **Diccionario de Computación**
  Alan Freedman
  5ta. Edición
  Ed. Mc. Graw Hill

- **Diccionario de Informática**
  Ingles – Español
  OXFORD UNIVERSITY PRESS
  ED. Diaz de Santos S.A.
  Segunda Edición

- **Data Becker Norton Utilities 6.0**
  Istok Kespret
  ED. MARCOMBO

- **Peter Norton Solución a Problemas de PC**
  Peter Norotn & Robert Jourdain
  ED. PRENTICE HALL

- **Manual del Usuario**
- **Manual Microsoft Windows & MS-DOS 6.2**
- ***Manual del Usuario de Dr. Solomon's***
- **Manual de Usuario de Mcafee**
- **Manual de Usuario de Compucilina**
- **Revistas y Voletines del Sistema de Dr. Solomon's**
- **Páginas de Internet**

**(*)** Revista de Computación "Los Ordenadores Modernos"

# NUMERACION USADA EN LOS CAPITULOS :

**(1) PC Anti-Virus Book**
Dr. Alan Solomon & Tin Kay

**(2) Bug** = bicho, error de programación

**(3) TSR** = TERMINATE STAY RESIDENTE
Programa que reside en la memoria alta

**(4) FAT** = FILES ALLOCATION TABLE
Tabla de Localizacion de Archivos

**(5) NLM** = NetWare Loadble Module
Módulo Cargable NetWare
(Diccionario de Computación *Alan Freedman)

**(6) BBS** = Bulletin Board System

**(7)** Enciclopedia del sistema de Antivirus
de Dr. Solomon's Vers. 7.86

**(8) PC Viruses – Detection, Analysis and Cure**
Dr. Alan Solomon & Tin Kay

**(9) FDISK.EXE**
Archivo del sistema Ms-DOS o Windows 95

**(10) SCANDISK** y **DEFRAG**
Archivos del sistema Ms-DOS o Windows 95

**(11) SPEEDISK** y **NDD**
Utileria de Doctor Norton Utilities

**(12) Diccionario de Computación**
Alan Freedman, Ed. Mc. Graw Hill

**(13) Diccionario de Informática**
OXFORD UNIVERSITY PRESS
Ed. Diaz de Santos

**(14) RLL (Run Length Limited)**
Longitud limitada de ejecución.
Metodo de codificación de los discos magneticos

**(15) "Encender en limpio"**
Explicación en el Capítulo 3, punto 3.1.6. (pag. 62)

**(16)** Manual de Usuario, de Dr. Solomon's

**(17)** Manual de Usuario, de *McAfee*

**(18)** Soporte técnico de *McAfee*.
ver Capitulo 14, sección 14.2.2.

**(19) KILLER**
Archivo que elimina un virus, pertenece
al sistema de Antivirus de Mcafee

**(20) ARMO**
Archivo que instala el Antivirus
de Mcafee para MS-DOS

**(21)** Página de Internet (http://www.drsolomon.com)

**(22) Boletín de Antivirus** de Dr. Solomon's (marzo de 1998)

**(23) Data Becker - Utilities 6.0**
Istok kespret – ED. MARCOMBO

**(24) DEFRAG** - Archivo del sistema de MS-DOS 6.22

**(25) SCANDISK**
Archivo de MS-DOS
Manual Microsoft *Windows & MS-DOS 6.22*

**(26) Peter Norton Solución a Problemas de PC**
Peter Norotn & Robert Jourdain
ED. PRENTICE HALL

**(27) VxD** = Virtual Drivers of Windows 95

**(28) CCITT** = Consultative Committe for International Telephony and Telegraphy

**(29) CRC** = Cyclical Redundancy Cheking

**(30) DES** = Data Encryptoion Standard

**(31) Background** = Fondo, segundo plano

**(32) MAGIC BULLET** (ver Capitulo 3.4.7.)

**(33) SHARE.EXE**
Archivo de MS-DOS
MANUAL Microsoft *Windows & MS-DOS 6.22*

**(34) VSHARE.386**
Archivo de MS-DOS
MANUAL Microsoft *Windows & MS-DOS 6.22*

**(35) EMM386.EXE**
Archivo de MS-DOS
MANUAL Microsoft *Windows & MS-DOS 6.22*

**(36) SMARTDRIVE**
Archivo de MS-DOS
MANUAL Microsoft *Windows & MS-DOS 6.22*

**(37) SMARTDRIVE.**
Utileria de MS-DOS
MANUAL Microsoft *Windows & MS-DOS 6.22*

**(38) DOUBLESPACE**
Utileria de MS-DOS 6.22
MANUAL Microsoft *Windows & MS-DOS 6.2*

**(39)** Boletines de sistema de Antivirus Dr. Solomon's

**(40) The Computer Virus Crisis**
Frites, Johnson & Kratz